



HAL
open science

Blown-up toric surfaces with non-polyhedral effective cone

Ana Maria Castravet, Antonio Laface, Jenia Tevelev, Luca Ugaglia

► **To cite this version:**

Ana Maria Castravet, Antonio Laface, Jenia Tevelev, Luca Ugaglia. Blown-up toric surfaces with non-polyhedral effective cone. *Journal für die reine und angewandte Mathematik*, 2023, 2023 (800), pp.1-44. 10.1515/crelle-2023-0022 . hal-04191697

HAL Id: hal-04191697

<https://hal.science/hal-04191697v1>

Submitted on 21 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

BLOWN-UP TORIC SURFACES WITH NON-POLYHEDRAL EFFECTIVE CONE

ANA-MARIA CASTRAVET, ANTONIO LAFACE, JENIA TEVELEV, AND LUCA UGAGLIA

ABSTRACT. We construct examples of projective toric surfaces whose blow-up at a general point has a non-polyhedral pseudo-effective cone, both in characteristic 0 and in every prime characteristic p . As a consequence, we prove that the pseudo-effective cone of the Grothendieck–Knudsen moduli space $\overline{M}_{0,n}$ of stable rational curves is not polyhedral for $n \geq 10$ in characteristic 0 and in characteristic p , for all primes p . Many of these toric surfaces are related to a very interesting class of arithmetic threefolds that we call arithmetic elliptic pairs of infinite order. Their analysis in characteristic p relies on tools of arithmetic geometry and Galois representations in the spirit of the Lang–Trotter conjecture, producing toric surfaces whose blow-up at a general point has a non-polyhedral pseudo-effective cone in characteristic 0 and in characteristic p , for an infinite set of primes p of positive density.

1. INTRODUCTION

An effective cone of a projective variety X and its closure, the pseudo-effective cone $\overline{\text{Eff}}(X)$, contain an impressive amount of information about the birational geometry of X . An even finer invariant is the Cox ring $\text{Cox}(X)$, at least when the class group $\text{Cl}(X)$ is finitely generated. If X is a Mori Dream Space (MDS) then $\text{Cox}(X)$ is finitely generated, which in turn implies that $\overline{\text{Eff}}(X)$ is polyhedral. A basic example of a MDS is a projective toric variety [Cox95]. Its effective cone is generated by classes of toric boundary divisors. For a toric variety \mathbb{P} , we denote by $\text{Bl}_e \mathbb{P}$ its blow-up at the identity element of the torus. Our main result contributes to the growing body of evidence that this is a very intriguing class of varieties.

Theorem 1.1. *In every characteristic, there exist projective toric surfaces \mathbb{P} such that the pseudo-effective cone $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P})$ is not polyhedral.*

In order to prove Theorem 1.1, we introduce two types of lattice polygons, Lang–Trotter polygons and Halphen polygons. The blow-ups $X = \text{Bl}_e \mathbb{P}$ of toric surfaces associated to these polygons are examples of elliptic pairs studied in §3. An *elliptic pair* (C, X) is a projective rational surface X , with log terminal singularities, and a curve C contained in the smooth locus of X , such that $p_a(C) = 1$ and $C^2 = 0$. Much of the geometry is encoded in the restriction map $\text{res} : C^\perp \rightarrow \text{Pic}^0(C)$, where $C^\perp \subseteq \text{Cl}(X)$ is the orthogonal complement. The order of an elliptic pair is the order of $\text{res}(C)$. A familiar example of an elliptic pair of infinite order in any characteristic is the blow-up of \mathbb{P}^2 in 9 general points. By contrast, elliptic pairs $X = \text{Bl}_e \mathbb{P}$ associated with a toric surface are defined over the base field. In particular, their order is automatically finite in characteristic p .

2010 *Mathematics Subject Classification.* 14C20, 14M25, 14E30, 14H10, 14H52, 14G17.
Key words and phrases. Toric varieties, elliptic curves, moduli of curves.

If the order of an elliptic pair (C, X) is infinite and $\rho(X) \geq 3$, then $\overline{\text{Eff}}(X)$ is not polyhedral (Lemma 3.3). By contrast, polyhedrality of $\overline{\text{Eff}}(X)$ is harder to control for elliptic pairs of finite order (e.g. for our blow-ups of toric surfaces in characteristic p) unless the pair is *minimal*. We use the logarithmic minimal model program to construct a $(K+C)$ -minimal model (C, Y) of any elliptic pair (C, X) and focus on the study of polyhedrality of $\overline{\text{Eff}}(Y)$. Of course if $\overline{\text{Eff}}(Y)$ is not polyhedral then $\overline{\text{Eff}}(X)$ is also not polyhedral. Remarkably, Y has Du Val singularities if the order is *infinite* (Corollary 3.12). On the other hand, if the order is *finite* and Y has Du Val singularities, there is a simple criterion for polyhedrality (Corollary 3.18) in terms of the restriction map and the root sublattice $T \subset \mathbb{E}_8$. The synthesis of these disjoint scenarios is the notion of an *arithmetic elliptic pair of infinite order*, a flat pair of schemes $(\mathcal{C}, \mathcal{X})$ over an open subset in the spectrum of a ring of algebraic integers with elliptic pairs as geometric fibers, of infinite (resp., finite) order over an infinite (resp., finite) place. In §5 we study distribution of polyhedral primes for arithmetic toric elliptic pairs $(\mathcal{C}, \mathcal{X})$ of infinite order. Here we call a prime p polyhedral if $\overline{\text{Eff}}(Y)$ is polyhedral, where (C, Y) is the minimal model of the geometric fiber (C, X) in characteristic p . This distribution is an intriguing question of arithmetic geometry, which we reduce to the question about reductions of points on the elliptic curve in the spirit of the Lang and Trotter analysis [LT77].

We found many examples of *Lang–Trotter polygons* that give rise to arithmetic elliptic pairs of infinite order, see the list of 135 polygons displayed in Database 10.1. For some of these polygons, $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P})$ is not polyhedral in characteristic p for an infinite set of primes p of positive density. We also checked that for every prime $p < 2000$, there exists a Lang–Trotter polygon such that $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P})$ is not polyhedral in characteristic p (see Database 10.2). It seems likely that one can find such a Lang–Trotter polygon \mathbb{P} for every p , but this seems out of reach with our methods. We also found infinite series of Lang–Trotter polygons such that $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P})$ is polyhedral in every positive characteristic p (Theorem 6.2).

We observe a different behaviour in *Halphen polygons*, which give rise to elliptic pairs of finite order with Du Val singularities both in characteristic 0 and in prime characteristic. Here the condition on singularities of the minimal model is not guaranteed by a general theory and needs to be checked by hand. We exhibit an example in Theorem 8.5 of a Halphen polygon such that $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P})$ is not polyhedral in characteristic 0 and in characteristic p for all but a finite set of primes p . Empirically, Halphen polygons seem to be harder to find than Lang–Trotter polygons.

In §10, we describe the Magma package and databases that can be used for computer-aided calculations, for example to check that a given polygon is a Lang–Trotter polygon. However, this analysis involves the step of computing a member Γ of a linear system on the toric surface \mathbb{P} that has a point of large multiplicity at the identity of the torus (the elliptic curve C is the normalization of Γ). While it is relatively straightforward to implement our algorithms on the computer, this *implicit method* has obvious disadvantages, for example it is not clear how to apply it to construct an infinite sequence of examples. To remedy the situation, in §6 we develop a *parametric method*. We start with an elliptic curve C and construct its map to \mathbb{P} that folds many points of C onto a point of high multiplicity. We do this for an infinite sequence of elliptic curves. We hope that this new method may help with other problems loosely related to the Nagata approximation conjecture, where it is desirable to geometrically construct curves with points of high multiplicity.

While most of the Lang–Trotter polygons that we found are not smooth, in §7 we describe a smooth toric elliptic pair (C, X) . It has a large Picard number $\rho = 18$ and the Mordell–Weil rank of C is equal to 9. We don’t know if there is an upper bound on the Picard number (or the Mordell–Weil rank) of a toric elliptic pair.

Our main application of Theorem 1.1 is to the birational geometry of the Grothendieck–Knudsen moduli space $\overline{M}_{0,n}$ of stable rational curves with n marked points. The study of effective cones of moduli spaces has a long history, starting with the pioneering work of Harris and Mumford [HM82], who used computations of effective divisors to show that \overline{M}_g is not unirational for $g \gg 0$.

While the moduli space $\overline{M}_{0,n}$ is a rational variety, its birational geometry is far from understood, in spite of numerous efforts, see for example [AS12, BG21, CT13, CT15, DGJ17, Fed20, FS11, Gib09, GG12, GJM13, GKM02, GM12, KM96]. The Picard number of $\overline{M}_{0,n}$ grows exponentially and it is not a Fano variety for $n \geq 6$, in fact its anticanonical class is not pseudo-effective if $n \geq 8$. In this regard, $\overline{M}_{0,n}$ looks similar to the blow-up of \mathbb{P}^2 in n points (a connection was indeed found in [CT12]) but there is an important difference: $\overline{M}_{0,n}$ is rigid, i.e., it has no moduli.

A question attributed to Fulton, which received a lot of attention, is whether, similarly to the case of toric varieties, any subvariety of $\overline{M}_{0,n}$ is numerically equivalent to a sum of strata. For the case of curves, the statement is known as the F-conjecture. A result of Gibney, Keel and Morrison [GKM02] proves that the F-conjecture, if known for all n , implies the similar statement for $\overline{M}_{g,n}$, for all genera g and number of marked points n , thus giving an explicit combinatorial description to the ample cone of $\overline{M}_{g,n}$. The conjecture holds for $n \leq 7$ and is open for $n \geq 8$.

For the case of divisors, Fulton’s question is whether the class of every effective divisor on $\overline{M}_{0,n}$ is a sum of boundary divisors. Every boundary divisor is an extremal ray of $\overline{\text{Eff}}(\overline{M}_{0,n})$; in fact, these divisors are exceptional, i.e., they can be contracted by birational contractions. For example, $\overline{M}_{0,5}$ is a degree 4 del Pezzo surface, and its boundary divisors form the Petersen graph of ten (-1) -curves, which generate $\text{Eff}(\overline{M}_{0,5})$. Extremal rays of a different type for $\overline{M}_{0,6}$ were found by Keel and Vermeire [Ver02], thus giving a negative answer to Fulton’s question for divisors when $n \geq 6$ ¹. However, Hassett and Tschinkel proved in [HT02] that $\overline{\text{Eff}}(\overline{M}_{0,6})$ is still fairly simple, namely it is a polyhedral cone, generated by the boundary and the Keel–Vermeire divisors (only one up to S_6 symmetry).

A large class of exceptional divisors on $\overline{M}_{0,n}$ was discovered by Castravet and Tevelev [CT13]. They are parametrized by irreducible hypertrees, which can be obtained, for example, from bi-colored triangulations of the 2-sphere. Up to the action of the symmetric group S_n , this gives 1, 2, 11, 93, 1027, \dots new types of exceptional divisors on $\overline{M}_{0,n}$ for $n = 7, 8, 9, 10, 11, \dots$. Equations of these divisors appear as numerators of leading singularities scattering amplitude forms for n particles in $N = 4$ super-symmetric Yang–Mills theory [ABC⁺15, Tev20].

New extremal rays of $\overline{\text{Eff}}(\overline{M}_{0,n})$ were found by Opie [Opi16] disproving an over-optimistic conjecture from [CT13]. Further extremal rays were found by Doran, Giansiracusa, and Jensen [DGJ17]. Our second result explains this complexity.

Theorem 1.2. *The cone $\overline{\text{Eff}}(\overline{M}_{0,n})$ is not polyhedral for $n \geq 10$, both in characteristic 0 and in characteristic p , for all primes p .*

¹Using forgetful maps, one has a negative answer for all cycles of dimension ≥ 2 when $n \geq 6$.

The moduli space $\overline{M}_{0,n}$ is related to blown-up toric varieties via the notion of a *rational contraction*, a dominant rational map $X \dashrightarrow Y$ of projective varieties that can be decomposed into a sequence of small \mathbb{Q} -factorial modifications [HK00] and surjective morphisms. Given a rational contraction, if $\overline{\text{Eff}}(X)$ is a (rational) polyhedral cone then $\overline{\text{Eff}}(Y)$ is also (rational) polyhedral (Lemma 2.2). By [CT15], there exist rational contractions $\text{Bl}_e \overline{LM}_{n+1} \dashrightarrow \overline{M}_{0,n} \dashrightarrow \text{Bl}_e \overline{LM}_n$, where \overline{LM}_n is the Losev–Manin moduli space of chains of rational curves, see [LM00, CT20]. This is a toric variety associated with the permutohedron. Thus $\overline{M}_{0,n}$ has essentially the same birational geometry as the blow-up of a toric variety in the identity element of the torus. Moreover, a feature of \overline{LM}_n , noticed in [CT15] and proved in Theorem 9.1, is its “universality” among all projective toric varieties \mathbb{P} . Specifically, for any projective toric variety \mathbb{P} there exist rational contractions $\overline{LM}_n \dashrightarrow \mathbb{P}$ and $\text{Bl}_e \overline{LM}_n \dashrightarrow \text{Bl}_e \mathbb{P}$ for n sufficiently large. In particular, if the cone $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P})$ is not polyhedral for some toric variety \mathbb{P} then $\overline{\text{Eff}}(\text{Bl}_e \overline{LM}_n)$, and therefore $\overline{\text{Eff}}(\overline{M}_{0,n})$, are not polyhedral either, for n sufficiently large.

A similar strategy was used in [CT15] to show that $\overline{M}_{0,n}$ is not a MDS in characteristic 0 for $n \geq 134$, answering a question of Hu and Keel [HK00]. The bound was lowered to 13 by Gonzalez and Karu [GK16] and then to 10 by Hausen, Keicher, and Laface [HKL18]. Theorem 1.2 gives the same bound $n \geq 10$, but it exhibits an even wilder behaviour than previously expected, as effective cones are a much rougher invariant than Cox rings (the Cox ring is graded and the effective cone is the semigroup of possible weights of the grading). For instance, the toric surfaces used in [CT15] were the weighted projective planes $\mathbb{P}(a, b, c)$. Of course, $\text{Bl}_e \mathbb{P}(a, b, c)$ has Picard number 2 and its effective cone is polyhedral. Nevertheless, Goto, Nishida and Watanabe [GNW94] proved (motivated by a question of Cowsik in commutative algebra) that $\text{Bl}_e \mathbb{P}(a, b, c)$ is not a MDS in characteristic 0 for certain values of a, b, c , by exhibiting a nef but not semi-ample line bundle. However, in characteristic $p > 0$, this line bundle is semi-ample, and therefore this space is a MDS, by Artin’s criterion [Art62], hence, this technique cannot be used. The following corollary of Thm. 1.2 is new:

Corollary 1.3. *If $n \geq 10$, the moduli space $\overline{M}_{0,n}$ is not a MDS in characteristic p , for all primes p .*

By contrast, $\overline{M}_{0,n}$ is a MDS in all characteristics if $n \leq 6$ [HK00, Cas09]. This leaves open the cases $n = 7, 8, 9$.

Acknowledgements. A.-M. C. has been partially supported by the ANR-20-CE40-0023 grant. A.L. has been partially supported by Proyecto FONDECYT Regular n. 1190777. J.T. was partially supported by the NSF grant DMS-1701704, Simons Fellowship, and by the HSE University Basic Research Program and Russian Academic Excellence Project ‘5-100’.

We thank Igor Dolgachev, Gavril Farkas and Brian Lehmann for useful discussions and for answering our questions. We are especially grateful to Tom Weston for sharing and explaining his paper [Wes03]. In the REU directed by J.T. in 2017, Stephen Obinna [Obi17] has started to collect evidence for existence of blown-up toric surfaces with non-polyhedral effective cone. The software Magma [BCP97] was used extensively. Some of the graphics are by the Plain Form Studio.

CONTENTS

1.	Introduction	1
2.	Polyhedrality of effective cones	5
3.	Elliptic pairs: general theory	8
4.	Lang–Trotter polygons and toric elliptic pairs	14
5.	Arithmetic toric elliptic pairs of infinite order	17
6.	Infinite sequences of Lang–Trotter polygons	25
7.	A smooth Lang–Trotter polygon	34
8.	Halphen polygons	35
9.	On the effective cone of $\overline{M}_{0,n}$	38
10.	Databases and Magma Computations	44
	References	52

2. POLYHEDRALITY OF EFFECTIVE CONES

Let k be an algebraically closed field of arbitrary characteristic. We recall some definitions (see for example [Laz04a, Laz04b]). If X is a normal projective irreducible variety over k , let $\text{Cl}(X)$ be the divisor class group and let $\text{Pic}(X)$ be the Picard group of X . As usual, we denote by \sim the linear equivalence of divisors and by \equiv the numerical equivalence. Recall that for Cartier divisors D_1, D_2 , we have $D_1 \equiv D_2$ if and only if $D_1 \cdot C = D_2 \cdot C$, for any curve $C \subseteq X$. We let

$$\text{Num}^1(X) := \text{Pic}(X) / \equiv$$

be the group of numerical equivalence classes of Cartier divisors on X . We denote $\text{Num}^1(X)_{\mathbb{R}} = \text{Num}^1(X) \otimes_{\mathbb{Z}} \mathbb{R}$, $\text{Num}^1(X)_{\mathbb{Q}} = \text{Num}^1(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Sometimes we extend \sim to the linear equivalence of \mathbb{Q} -divisors in a usual way (for \mathbb{Q} -divisors, $A \sim B$ if $kA \sim kB$ as Cartier divisors for some $k > 0$) but mostly we use numerical equivalence of \mathbb{Q} -divisors to avoid confusion.

Similarly, we define $Z_1(X)_{\mathbb{R}}$ to be the group of \mathbb{R} -linear combinations of irreducible curves in X , i.e., formal sums

$$\gamma = \sum a_i C_i, \quad a_i \in \mathbb{R}$$

with all $C_i \subseteq X$ irreducible curves. As in [Laz04a, Def. 1.4.25], we let

$$\text{Num}_1(X)_{\mathbb{R}} = Z_1(X)_{\mathbb{R}} / \equiv,$$

where for two one-cycle classes $\gamma_1, \gamma_2 \in Z_1(X)_{\mathbb{R}}$ we have numerical equivalence $\gamma_1 \equiv \gamma_2$ if and only if $D \cdot \gamma_1 = D \cdot \gamma_2$ for all Cartier divisors D on X . It follows from the definitions that

$$\text{Num}^1(X)_{\mathbb{R}} \otimes \text{Num}_1(X) \rightarrow \mathbb{R}, \quad (\delta, \gamma) \mapsto \delta \cdot \gamma \in \mathbb{R}$$

is a perfect pairing, so $\text{Num}^1(X)_{\mathbb{R}}$ and $\text{Num}_1(X)_{\mathbb{R}}$ are dual vector spaces. In particular, both $\text{Num}^1(X)_{\mathbb{R}}$ and $\text{Num}_1(X)_{\mathbb{R}}$ are finite dimensional real vector spaces. We define the pseudo-effective cone

$$\overline{\text{Eff}}(X) \subseteq \text{Num}^1(X)_{\mathbb{R}},$$

as the closure of the effective cone $\text{Eff}(X)$, i.e., the convex cone generated by numerical classes of effective Cartier divisors ([Laz04b, Def. 2.2.25]). We let $\text{Nef}(X) \subseteq$

$\text{Num}^1(X)_{\mathbb{R}}$ be the cone generated by the classes of *nef divisors*. We define

$$\overline{\text{Mov}}_1(X) \subseteq \text{Num}_1(X)_{\mathbb{R}}$$

the closure of the cone generated by numerical classes of *movable* 1-cycles, see [Laz04b, Def. 11.4.16]. The cones $\overline{\text{Eff}}(X)$ and $\overline{\text{Mov}}_1(X)$ are dual to each other. This was proved first in [BDPP13] for the case when X is a smooth projective variety in characteristic 0, but it holds in general. For X irreducible projective variety over a field k of characteristic 0 this is proved in [Laz04a, Thm. 11.4.19]. For the case of arbitrary characteristic, the same proof holds, see for example [Ful17, Rmk. 2.1].

Definition 2.1. A convex cone $\mathcal{C} \subseteq \mathbb{R}^s$ is called *polyhedral* if there are finitely many vectors $v_1, \dots, v_s \in \mathbb{R}^s$ such that $\mathcal{C} = \mathbb{R}_{\geq 0}v_1 + \dots + \mathbb{R}_{\geq 0}v_s$. The cone is said to be *rational polyhedral* if one can choose the v_i 's in \mathbb{Q}^s .

Lemma 2.2. *Let $f : X \rightarrow Y$ be a surjective morphism of normal projective irreducible varieties. If $\overline{\text{Eff}}(X)$ is (rational) polyhedral then the same is true for $\overline{\text{Eff}}(Y)$.*

Proof. Suppose $\overline{\text{Eff}}(X)$ is a (rational) polyhedral cone. By the duality between the cones $\overline{\text{Eff}}(X)$ and $\overline{\text{Mov}}_1(X)$, it follows that $\overline{\text{Mov}}_1(X)$ is also a (rational) polyhedral cone. The proper push-forward of 1-cycles induces a map of \mathbb{R} -vector spaces

$$f_* : \text{Num}_1(X)_{\mathbb{R}} \rightarrow \text{Num}_1(Y)_{\mathbb{R}}.$$

By [FL17, Cor. 3.12], $f_*(\overline{\text{Mov}}_1(X)) = \overline{\text{Mov}}_1(Y)$. The definitions of $\text{Num}_1(X)$ and $\overline{\text{Mov}}_1(X)$ given in [FL17] coincide with the ones given above, see [FL17, Section 2.1, Ex. 3.3]. It follows that $\overline{\text{Mov}}_1(Y)$ is a (rational) polyhedral cone. Again by the duality between the cones $\overline{\text{Eff}}(Y)$ and $\overline{\text{Mov}}_1(Y)$, it follows that $\overline{\text{Eff}}(Y)$ is a (rational) polyhedral cone. \square

We concentrate on the case of surfaces. The cone and contraction theorems hold in any characteristic with very mild assumptions, see [KM98, Tan14, FT12, Fuj20].

Proposition 2.3. *Let X be a normal projective \mathbb{Q} -factorial surface with Picard number at least 3 and such that the cone $\overline{\text{Eff}}(X)$ is polyhedral. Then:*

- (1) *Every class $C \in \text{Num}^1(X)$ of self intersection 0 (or its opposite $-C$) is in the relative interior of either the cone $\overline{\text{Eff}}(X)$ or its codimension one facet.*
- (2) *The effective cone $\text{Eff}(X)$ is generated by finitely many negative curves². In particular, $\overline{\text{Eff}}(X) = \text{Eff}(X)$ is a rational polyhedral cone.*

Part (2) of Proposition 2.3 appears also in [Nik00].

Proof. (1) Fix h an ample divisor. Let

$$Q := \{ \omega \mid \omega^2 \geq 0, \omega \cdot h \geq 0 \} \subseteq \text{Num}^1(X)_{\mathbb{R}} \tag{2.1}$$

be the non-negative part of the light cone. Then either C or its opposite $-C$ lies on the boundary ∂Q . By Riemann-Roch, the cone Q is contained in $\text{Eff}(X)$. Since the Picard number of X is at least 3, the cone Q is round. In particular, ∂Q can intersect only a facet of $\overline{\text{Eff}}(X)$ of codimension 1 and only in its relative interior.

(2) By (1), any $\omega \in \text{Num}^1(X)$ generating an extremal ray of $\overline{\text{Eff}}(X)$ has $\omega^2 < 0$. By [Deb01, Lemma 6.2(e)]³, for any such ω there exists an irreducible curve E such that ω is a positive multiple of the class of E . \square

²A negative curve is an irreducible curve B with $B^2 < 0$.

³The proof in [Deb01] is for smooth surfaces but the argument works verbatim in our case.

Remark 2.4. In the settings of Proposition 2.3, if the class C admits a positive integer multiple nC such that $|nC|$ is a base point free pencil, then C is not big. Thus it lies in the relative interior of a maximal facet τ of $\overline{\text{Eff}}(X)$, and by the Hodge Index Theorem, the supporting hyperplane of τ is C^\perp . In particular, any class of an irreducible curve R which generates an extremal ray of τ satisfies $R \cdot C = 0$, so that R is an irreducible component of a fiber of the fibration $\pi: X \rightarrow \mathbb{P}^1$ induced by $|nC|$. Since the contribution of the components of a fiber to the “vertical” rank of the Picard group is the number of components minus one, it follows that in order for $\overline{\text{Eff}}(X)$ to be polyhedral it must be

$$1 + \sum_{b \in \mathbb{P}^1} (|\text{Comp. of } f^{-1}(b)| - 1) = \text{rk}(\text{Pic}(X)) - 1. \quad (2.2)$$

Proposition 2.5. *Let X be a normal projective \mathbb{Q} -factorial surface with Picard number at least 3. Assume that $C \subseteq X$ is an irreducible curve with $C^2 = 0$ and $C \equiv -\alpha K_X$ with $\alpha \in \mathbb{Q}_{>0}$. Then the following are equivalent:*

- (1) *There exist irreducible negative curves B_1, \dots, B_s , that generate $C^\perp \subseteq \text{Num}^1(X)_\mathbb{Q}$, and such that*

$$C \equiv a_1 B_1 + \dots + a_s B_s \quad \text{with} \quad a_1, \dots, a_s \in \mathbb{Q}_{>0}. \quad (2.3)$$

- (2) *$\overline{\text{Eff}}(X)$ is a rational polyhedral cone generated by negative curves.*

Proof. Proposition 2.3 gives (2) \Rightarrow (1). We prove (1) \Rightarrow (2) under our additional assumptions. Note that C (hence, $-K$) is nef. Recall that any $\omega \in \text{Num}^1(X)_\mathbb{R}$ generating an extremal ray must have $\omega^2 \leq 0$ and if $\omega^2 < 0$ then ω is the class of a multiple of a curve [Deb01, Lemma 6.2]. The same is true when $\omega^2 = 0$, as if $\omega \cdot C = 0$, by the Hodge Index theorem, ω and C generate the same ray, while if $\omega \cdot C > 0$, then $\omega \cdot K < 0$ and ω is generated by the class of a curve by the Cone theorem. Hence, it suffices to prove that X contains finitely many irreducible curves E with $E^2 \leq 0$ such that E is not numerically equivalent to a rational multiple of C . We can also assume that $E \neq B_i$ for all i .

We consider two cases. If $E \cdot C = 0$ then $E \cdot B_i = 0$ for all i by (2.3) and by our assumption that $E \neq B_i$ for all i . Since B_1, \dots, B_s generate C^\perp over \mathbb{Q} , E must be numerically equivalent to a rational multiple of C , which we have also ruled out.

Suppose $E \cdot C > 0$. Since B_1, \dots, B_s generate C^\perp over \mathbb{Q} , the classes which have fixed intersections with the B_i 's form an affine subspace of dimension one in $\text{Num}^1(X)_\mathbb{Q}$, differing one from another by a multiple of the class of C . Since $E \cdot C > 0$ and $C \cdot C = 0$, there is at most one such class with E^2 also fixed. Hence, it suffices to prove that $E \cdot B_i$ and E^2 belong to a finite set. By assumption (1) and adjunction, we have

$$\frac{1}{\alpha} \sum a_i (E \cdot B_i) = E \cdot (-K) \leq E^2 + 2 \leq 2.$$

Hence, $0 \leq E \cdot B_i \leq 2\alpha/a_i$. As there exists $l \in \mathbb{Z}_{>0}$ (the index of $\text{Pic}(X)$ in $\text{Cl}(X)$) such that the lD is Cartier for any curve D (hence, $l(D \cdot E)$ is an integer), it follows that $E \cdot B_i$ belongs to a finite set. We have $-2 \leq E^2$ by adjunction and nefness of $-K$. As $E^2 \leq 0$, it follows similarly that E^2 must belong to a finite set. \square

3. ELLIPTIC PAIRS: GENERAL THEORY

As in § 2, we work over an algebraically closed field k of arbitrary characteristic. While Propositions 2.3 and 2.5 address polyhedrality of $\overline{\text{Eff}}(X)$ for a general surface X , in this section we study polyhedrality further for a rational surface in the presence of a curve C with self-intersection 0 under some additional assumptions.

Definition 3.1. An *elliptic pair* (C, X) consists of a projective rational surface X with log terminal singularities and an irreducible curve $C \subseteq X$, of arithmetic genus one, disjoint from the singular locus of X and such that $C^2 = 0$. Let $C^\perp \subseteq \text{Cl}(X)$ be the orthogonal complement to C . We define the *restriction map*

$$\text{res} : C^\perp \rightarrow \text{Pic}^0(C), \quad D \mapsto \mathcal{O}(D)|_C.$$

Since $K \cdot C = 0$ by adjunction, we can also define the *reduced restriction map*

$$\overline{\text{res}} : \text{Cl}_0(X) := C^\perp / \langle K \rangle \rightarrow \text{Pic}^0(C) / \langle \text{res}(K) \rangle.$$

We will often study a birational morphism $X \rightarrow Y$, which is an isomorphism in a neighborhood of C . We will then use notation C_X, C_Y , etc, to avoid confusion.

The most familiar elliptic pairs are rational elliptic fibrations $X \rightarrow \mathbb{P}^1$ with a fiber C (which can be a multiple fiber). However, we do not make this assumption. Note that as X is rational, $h^1(X, \mathcal{O}_X) = 0$, and hence $\text{Pic}(X)_\mathbb{Q} = \text{Num}^1(X)_\mathbb{Q}$.

Lemma–Definition 3.2. *We define the order $e = e(C, X)$ of the elliptic pair (C, X) to be the positive integer satisfying any of the following equivalent conditions (or ∞ if none of them are met):*

- (1) $\text{res}(C) \in \text{Pic}^0(C)$ is a torsion line bundle of order e .
- (2) e is the smallest positive integer such that $h^0(C, \text{res}(eC)) = 1$.
- (3) e is the smallest positive integer such that $h^0(X, eC) = 2$.
- (4) e is the smallest positive integer such that $h^0(X, eC) > 1$.

The order $e(C, X)$ only depends on a Zariski neighborhood of C in X .

Proof. The equivalence of (1) and (2) is clear. We use this as a definition of e . In particular, $e(C, X)$ only depends on a Zariski neighborhood of C in X . Since log terminal singularities are rational and C is disjoint from the singular locus of X , if \tilde{X} is a resolution of singularities of X , then $h^0(\tilde{X}, nC_{\tilde{X}}) = h^0(X, nC_X)$ for any integer n . Hence, to prove the remaining equivalences we may assume that X is smooth. For any $n \geq 0$, we have $h^2(X, nC) = h^0(X, K_X - nC) = 0$, since otherwise K_X would be effective. Moreover, by Riemann-Roch $\chi(\mathcal{O}_X(nC)) = 1$ for all n . Thus either $h^0(X, nC) = 1$ and $h^0(C, \text{res}(nC)) = 0$ for every $n > 0$, or for some $n > 0$ we have $h^0(X, nC) = 2$, $h^0(C, \text{res}(nC)) = 1$ and $h^0(X, lC) = 1$, $h^0(C, \text{res}(lC)) = 0$ for $1 \leq l < n$. \square

Lemma 3.3. *Suppose (C, X) is an elliptic pair. Let $e = e(C, X)$. Then*

- (1) $e < \infty$ if and only if C is a (multiple) fiber of a (quasi)-elliptic fibration⁴.
- (2) If $e = \infty$, then C is rigid, which means that $h^0(nC) = 1$ for all $n > 0$.
In this case $\overline{\text{Eff}}(X)$ is not polyhedral if the Picard number $\rho(X) \geq 3$.

⁴If C is smooth or if $\text{char } k \neq 2, 3$ then the fibration is automatically elliptic [BM76]. If not, it can be quasi-elliptic, i.e. have cuspidal generic fibers.

Proof. Suppose $e < \infty$. Then $eC \sim \sum D_i$, for some irreducible curves $D_i \neq C$ by Lemma 3.2 (3). As $C^2 = 0$, it follows that the D_i 's are disjoint from C and $|eC|$ is a base-point-free pencil. Since $C^2 = K \cdot C = 0$ by adjunction, $\varphi_{|eC|} : X \rightarrow \mathbb{P}^1$ is a (quasi)-elliptic fibration. Suppose $e = \infty$. Then C is rigid by Lemma 3.2 (4). By Prop. 2.3, if $\overline{\text{Eff}}(X)$ is polyhedral and the Picard number of X is at least 3, then $\overline{\text{Eff}}(X)$ is generated by negative curves and C is contained in the interior of a facet. Thus $h^0(X, kC) > 1$ for some k and therefore $e(C, X) < \infty$ by Lemma 3.2 (4). \square

Lemma 3.4. *If (C, X) is an elliptic pair, then $K_X + C$ is an effective divisor.*

Proof. As C is contained in the smooth locus of X , we can pass to a resolution of singularities and prove for a smooth surface X that $h^2(-C) = h^0(K + C) > 0$. By adjunction $\mathcal{O}_X(K + C)|_C \simeq \omega_C \simeq \mathcal{O}_C$, so there is an exact sequence⁵

$$0 \rightarrow \mathcal{O}_X(K) \rightarrow \mathcal{O}_X(K + C) \rightarrow \mathcal{O}_C \rightarrow 0.$$

The statement follows from the vanishing $h^0(X, K) = h^1(X, K) = 0$. \square

Definition 3.5. We say that (C, X) is a *minimal* elliptic pair if it does not contain irreducible curves E such that $K \cdot E < 0$ and $C \cdot E = 0$.

Remark 3.6. A curve E as in the definition must have $E^2 < 0$. Indeed, $E^2 \leq 0$ by the Hodge Index theorem, with equality if and only if the classes of C and E are multiples of each other. But since $E \cdot K < 0$ and $C \cdot K = 0$, the latter is not possible. Moreover, E is a rational curve [Fuj20, Thm 5.6]. By the contraction theorem, there exists a morphism $\phi : X \rightarrow Y$ contracting only E . As ϕ is an isomorphism in a Zariski neighborhood of C and Y is log terminal, (C, Y) is an elliptic pair. Moreover, $K_X \equiv \phi^*K_Y + aE$, for some $a \in \mathbb{Q}$. Since $E \cdot K_X < 0$ and $E^2 < 0$, it follows that $a > 0$. Furthermore, $K_X^2 < K_Y^2$.

Lemma 3.7. *Let (C, X) be an elliptic pair. The following conditions are equivalent:*

- (1) (C, X) is minimal;
- (2) $K + C$ is nef;
- (3) $C \sim \alpha(-K)$, for some $\alpha \in \mathbb{Q}_{>0}$, a linear equivalence of \mathbb{Q} -divisors;
- (4) $K^2 = 0$.

Proof. To prove (1) \Rightarrow (2), assume that $K + C$ is not nef. By the cone theorem⁶ for a log surface (X, C) [Tan14, Fuj20], there is an irreducible curve E such that $(K + C) \cdot E < 0$ and $E^2 < 0$. Since $K + C$ is effective, E must be one of its components. Since $C \cdot (K + C) = 0$ and C is nef, we must have $C \cdot E = 0$, hence, $K \cdot E < 0$. This contradicts the minimality of (C, X) .

Next we prove (2) \Rightarrow (3). Since $(K + C) \cdot C = 0$, by the Hodge Index theorem we must have $(K + C)^2 \leq 0$. But since $K + C$ is nef, $(K + C)^2 \geq 0$. Thus $(K + C)^2 = 0$ and it must be that $K + C \equiv \lambda C$, for some $\lambda \in \mathbb{Q}$. As no multiple of K is effective, it follows that $C \equiv \alpha(-K)$, for some $\alpha \in \mathbb{Q}_{>0}$. Since X is rational, in fact $C \sim \alpha(-K)$, a linear equivalence of \mathbb{Q} -divisors;

The implication (3) \Rightarrow (4) is clear. To see (4) \Rightarrow (1), suppose (X, C) is not minimal. By Remark 3.6, there is a contraction $\phi : X \rightarrow Y$ of a curve E such that $K \cdot E < 0$, $E^2 < 0$ and $C \cdot E = 0$. Moreover, $K_Y^2 > K_X^2 = 0$. But (C, Y) is an elliptic pair and so $K_Y^2 \leq 0$ by the Hodge Index theorem, which gives a contradiction. \square

⁵This trick is from the proof of the canonical bundle formula for elliptic fibrations in [BM77]

⁶Note that there are no singularity assumptions on $K + C$ in the cone theorem for surfaces.

Theorem 3.8. *Let (C, Z) be an elliptic pair with smooth Z . Then (C, Z) is minimal if and only if $\rho(Z) = 10$, or equivalently, $K^2 = 0$. If (C, Z) is minimal then*

- (i) $C \sim n(-K)$ for some positive integer n ;
- (ii) Z is a blow-up of \mathbb{P}^2 at 9 points (possibly infinitely near) and the intersection pairing on Z makes $\text{Cl}_0(Z)$ isomorphic to the negative definite lattice \mathbb{E}_8 .

Suppose that (C, Z) is minimal and $e(C, Z) < \infty$. The following are equivalent:

- (1) $\overline{\text{Eff}}(Z)$ is polyhedral and generated by (-2) and (-1) curves.
- (2) $\overline{\text{Eff}}(Z)$ is polyhedral.
- (3) $\text{Ker}(\overline{\text{res}}) \subseteq \mathbb{E}_8$ contains 8 linearly independent roots of \mathbb{E}_8 .

Remark 3.9. Smooth projective rational surfaces Z for which there is an integer $m > 0$ such that the linear system $| -mK_Z |$ is base-point free and of dimension 1, are called Halphen surfaces of index m and have been studied from many different points of view, see for example [ADHL15, CD12, Gri16]. If (C, Z) is an elliptic pair as in Thm. 3.8, then Z is a Halphen surface with index $n \cdot e$, where $e := e(C, Z)$. Let N be the sub-lattice of \mathbb{E}_8 that is generated by roots contained in $\text{Ker}(\overline{\text{res}})$, i.e., N is generated by the classes of all the (-2) curves on Z (see the proof of Thm. 3.8). By the Hodge Index Theorem, the (-2) curves on Z are precisely the irreducible components of reducible fibers of the fibration induced by the linear system $|eC|$, call them S_1, \dots, S_λ . If μ_j denotes the number of irreducible components of S_j , the rank of N (i.e., the maximum number of linearly independent roots of \mathbb{E}_8 contained in $\text{Ker}(\overline{\text{res}})$, or equivalently, the maximum number of (-2) curves that are linearly independent modulo K_Z) equals $\sum_{i=1}^\lambda (\mu_i - 1)$. By a result of Gizatullin, $\sum_{i=1}^\lambda (\mu_i - 1) < 8$ if and only if the automorphism group $\text{Aut}(Z)$ is infinite; in this case there exists a free abelian group G of rank $8 - \sum_{i=1}^\lambda (\mu_i - 1)$, of finite index in $\text{Aut}(Z)$, such that any non-zero element in G is an automorphism that acts by translation on each fiber of the elliptic fibration [Gri16][Thm. 7.11, Cor. 7.12], i.e., $\overline{\text{Eff}}(Z)$ is not polyhedral if and only if $\text{Aut}(Z)$ is infinite.

Proof of Thm. 3.8. By Lemma 3.7, the elliptic pair (C, Z) is minimal if and only if $K^2 = 0$. Since Z is a smooth rational surface, it is an iterated blow-up of \mathbb{P}^2 or a Hirzebruch surface \mathbb{F}_e . As K^2 goes down by one and the Picard number goes up by one when blowing-up a smooth point, $K^2 = 0$ if and only if $\rho(Z) = 10$. We claim that Z is the blow-up of \mathbb{P}^2 at 9 points. Assume not. Then Z is the iterated blow-up of a Hirzebruch surface \mathbb{F}_e ($e = 0$ or $e \geq 2$) at 8 points. A negative curve B on \mathbb{F}_e has $B^2 = -e$ and B^2 goes down by blow-up. By adjunction, and since $-K_Z$ is nef, the only negative curves on Z are (-1) and (-2) -curves, so we must have $e = 0$, or $e = 2$ and none of the blown up (possibly infinitely near) points on \mathbb{F}_2 lie on the negative section. If $e = 0$, we are done, as $\text{Bl}_p \mathbb{P}^1 \times \mathbb{P}^1$ is isomorphic to the blow-up of \mathbb{P}^2 at 2 points. If $e = 2$, we are also done, as a blow-up of \mathbb{F}_2 at a point not lying on the negative section, is isomorphic, via an elementary transformation, to a blow-up of \mathbb{F}_1 at one point. This proves the claim. It follows that $\text{Cl}_0(Z) \cong \mathbb{E}_8$. Since $-K$ is a primitive vector of $\text{Pic}(Z)$, it follows by Lemma 3.7(3) that $C \sim n(-K)$ for some integer $n > 0$.

Suppose that (C, Z) is minimal and $e = e(C, Z) < \infty$. By Lemma 3.3, $|eC|$ gives a (quasi)-elliptic fibration $Z \rightarrow \mathbb{P}^1$. Clearly (1) \Rightarrow (2) and Prop. 2.3 (2) implies (2) \Rightarrow (1), as the only negative curves are (-1) and (-2) curves. Assume (1). By Proposition 2.5, $C \equiv \sum a_i B_i$ for $a_i \in \mathbb{Q}_{>0}$, with irreducible negative curves B_i generating C^\perp over \mathbb{Q} . Since B_i is irreducible, $\text{res}(B_i) = 0$. Since $B_i \cdot K = 0$, each

B_i is a (-2) curve. Since the curves B_i generate C^\perp over \mathbb{Q} , eight of them are linearly independent modulo K . This proves (3).

Assume (3). Let β_1, \dots, β_8 be (-2) -classes in C^\perp , linearly independent modulo K , and such that $\overline{\text{res}}(\beta_i) = 0$. Adding to each β_i a multiple of K , we may assume that each β_i restricts trivially to C . We claim that, for each i , either β_i or $(K + C) - \beta_i$ is effective. Indeed, for each $\beta := \beta_i$ we have a short exact sequence

$$0 \rightarrow \mathcal{O}(\beta - C) \rightarrow \mathcal{O}(\beta) \rightarrow \mathcal{O}_C \rightarrow 0.$$

If β is not effective, $\beta - C$ is not effective either. Hence, $h^1(Z, \mathcal{O}(\beta - C)) > 0$. But $\chi(\mathcal{O}(\beta - C)) = 0$ by Riemann–Roch. Thus $h^2(Z, \mathcal{O}(\beta - C)) > 0$ and so $(K + C) - \beta$ is effective. We have found 8 effective divisors D_1, \dots, D_8 with $\text{res}(D_i) = 0$, $D_i^2 = -2$ and linearly independent modulo K . Each of the divisors D_i belongs to a union of the fibers of the (quasi)-elliptic fibration (and no D_i is a rational multiple of C). Since (-2) -curves are precisely the irreducible components of reducible fibers, it follows that (-2) -curves generate C^\perp over \mathbb{Q} . Clearly, for some integer $l \gg 0$, lC is an effective combination of (-2) curves. Then Prop. 2.5 (1) implies (2). \square

Theorem 3.10. *For any elliptic pair (C, X) , there exists a minimal elliptic pair (C, Y) and a morphism $\pi : X \rightarrow Y$, which is an isomorphism over a neighborhood of C . Consider the Zariski decomposition on X of $K + C$,*

$$K + C \sim N + P, \quad N = a_1 C_1 + \dots + a_s C_s, \quad a_i \in \mathbb{Q}_{>0},$$

the linear equivalence of \mathbb{Q} -divisors⁷. Then:

- (1) Y is obtained by contracting curves C_1, \dots, C_s on X .
- (2) $P \equiv 0$ if and only if $-K_Y \sim C_Y$, in which case N is an integral combination of C_1, \dots, C_s and Y has Du Val singularities.

Definition 3.11. We call an elliptic pair (C, Y) a *minimal model* of (C, X) .

Corollary 3.12. *Let (C, Y) be a minimal model of an elliptic pair (C, X) such that $e(C, X) = \infty$. Then Y has Du Val singularities. Consider the Zariski decomposition*

$$K + C \sim N + P$$

on X . Then $P \sim 0$ and $K + C \sim N$ is an integral effective combination of irreducible curves C_1, \dots, C_s with a negative-definite intersection matrix. The minimal model Y is obtained by contracting curves C_1, \dots, C_s and $C_Y \sim -K_Y$.

Proof. We first prove the theorem and then its corollary. We obtain a minimal model $\pi : X \rightarrow Y$ by running a $(K + C)$ -MMP [Tan14, Fuj20]. Equivalently (by Lemma 3.7), π is a composition of contractions of the form $\phi : X \rightarrow Y$, where each ϕ is the contraction of a K -negative curve E such that $E \cdot C = 0$. On each step, $K_X + C_X \sim \phi^*(K_Y + C_Y) + aE$, with $a \in \mathbb{Q}_{>0}$, a linear equivalence of \mathbb{Q} -divisors. At the end we obtain that $K_Y + C_Y$ is nef, i.e., (C, Y) is minimal. If the curves contracted by π are $C_1, \dots, C_s \subseteq X$, then $K_X + C_X \sim N + P$, with

$$P = \pi^*(K_Y + C_Y), \quad N = \sum_{i=1}^s a_i C_i \quad a_i \in \mathbb{Q}_{>0},$$

⁷Recall that the C_i 's are irreducible curves with a negative-definite intersection matrix and P is a nef effective \mathbb{Q} -divisor such that $P \cdot C_i = 0$ for all i . The \mathbb{Q} -divisor N is determined uniquely.

a linear equivalence of \mathbb{Q} -divisors. The divisor P is nef and effective (Lemma 3.4) and $P \cdot C_i = 0$ for all i . Hence, this is the Zariski decomposition of $K + C$. Moreover, $P \equiv 0$ if and only if $K_Y + C_Y \sim 0$.

Assume now that $P \equiv 0$. Recall an algorithm for computing the Zariski decomposition [Bau09]. Write $K + C \sim b_1 B_1 + \dots + b_t B_t$ as an integral, effective sum of irreducible curves B_i . Let $N' := \sum x_i B_i$, where $0 \leq x_i \leq b_i$ are maximal such that $P' := \sum (b_i - x_i) B_i$ intersects all C_i non-negatively. Then N' and P' give a Zariski decomposition of $K + C$. Since $N = N'$ is unique and $P' \equiv P \equiv 0$, the Zariski decomposition is $K + C \sim b_1 B_1 + \dots + b_t B_t$. To prove the singularity statement, note that $-K_Y \sim C_Y$ implies that K_Y is Cartier. Thus Y has Du Val singularities.

Finally, we prove the corollary. Suppose that $e(C, X) = e(C_Y, Y) = \infty$. If $P \neq 0$, we have $C_Y \sim \alpha(-K_Y)$, for some $\alpha \in \mathbb{Q}, \alpha \neq 1$. Then $C_Y \sim \frac{\alpha}{\alpha-1}(K_Y + C_Y)$, a linear equivalence of \mathbb{Q} -divisors. But $K_Y + C_Y$ restricts trivially to C_Y by adjunction, and therefore $\text{res}(C)$ is torsion, which is a contradiction. So we must have $P \equiv 0$ and this finishes the proof of the corollary by (1)–(2) of the theorem. \square

Remark 3.13. We give an example of a minimal rational elliptic fibration that does not satisfy $C \sim -K$. Let W be a minimal smooth rational elliptic fibration with a nodal fiber I_0 . Blow-up the node of the fiber and contract the proper transform of the fiber (which has self-intersection -4). This produces a minimal rational elliptic fibration Y with a $\frac{1}{4}(1, 1)$ singularity, which is log terminal. The fiber C_0 through the singularity is a nodal multiple fiber of multiplicity 2. We have $C \sim 2C_0 \sim -2K$.

Lemma 3.14. *Let (C, Y) be an elliptic pair such that Y has Du Val singularities. Let $\pi : Z \rightarrow Y$ be its minimal resolution.*

- (1) *(C, Y) is minimal if and only if (C, Z) is minimal. Equivalently,*

$$\rho(Y) = 10 - R,$$

where R is the rank of the root system associated with singularities of Y .

- (2) *Assume (C, Y) is a minimal elliptic pair. Then the following are equivalent:*

- $\overline{\text{Eff}}(Y)$ is a polyhedral cone;
- $\overline{\text{Eff}}(Y)$ is a rational polyhedral cone;
- $\overline{\text{Eff}}(Z)$ is a polyhedral cone.

When $\rho(Y) = 2$, all the above statements hold.

Proof. As $K_Z = \pi^* K_Y$, the pair (C, Z) is minimal if and only if (C, Y) is minimal by Lemma 3.7. As $\rho(Y) = \rho(Z) - R$, the first statement follows. If $\overline{\text{Eff}}(Z)$ is (rational) polyhedral then $\overline{\text{Eff}}(Y)$ is (rational) polyhedral by Lemma 2.2. Assume now $\overline{\text{Eff}}(Y)$ is polyhedral. If $\rho(Y) \geq 3$, then $e(C, Y) < \infty$, by Lemma 3.3 and by Proposition 2.3(1), $\overline{\text{Eff}}(Y)$ is a rational polyhedral cone with C_Y contained in the interior of a maximal facet. If $\rho(Y) = 2$ (the smallest possible), then $\text{Eff}(Y)$ is a rational polyhedral cone by the Cone theorem (it is spanned by the class of C and by the class of the unique negative curve). Note that this doesn't provide any information about $e(C, Y)$. In both cases, it follows that C_Y^\perp contains $\rho(Y) - 2$ effective divisors which are linearly independent modulo K_Y and restrict trivially to C . As $\text{Cl}(Z)_\mathbb{Q}$ decomposes as $\pi^* \text{Cl}(Y)_\mathbb{Q} \oplus T_\mathbb{Q}$, where T is a sublattice spanned by classes of (-2) -curves over singularities of Y , we have $(C_Z^\perp)_\mathbb{Q} = (\pi^* C_Y^\perp)_\mathbb{Q} \oplus T_\mathbb{Q}$. It follows that C_Z^\perp contains $\rho(Y) - 2 + R = 8$ effective divisors which are linearly independent modulo K_Z and restrict trivially to C . As in the proof of Theorem 3.8, it follows that $\text{Eff}(Z)$ is a polyhedral cone. \square

Remark 3.15. In the set-up of Lemma 3.14, if (C, Y) has Du Val singularities and $C_Y \sim -K_Y$, with $\pi : Z \rightarrow Y$ is its minimal resolution, then Z is a Halphen surface of index $e(C, Z)$, as $C_Z \sim -K_Z$. Indeed, this follows from $\pi^*K_Y = K_Z$, $\pi^*C_Y = C_Z$.

Definition 3.16. Let (C, X) be an elliptic pair such that the minimal model (C, Y) has Du Val singularities. Let $\pi : Z \rightarrow Y$ be the minimal resolution of Y . Let

$$T \subseteq \mathbb{E}_8 = \text{Cl}_0(Z)$$

be a root sublattice spanned by classes of (-2) -curves over singularities of Y . We call T *the root lattice of (C, X)* and we denote by \hat{T} its saturation $\mathbb{E}_8 \cap (T \otimes \mathbb{Q})$.

The push forward $\pi_* : \text{Cl}(Z) \rightarrow \text{Cl}(Y)$ induces a map $\text{Cl}_0(Z) \rightarrow \text{Cl}_0(Y)$ with kernel T , i.e., $\text{Cl}_0(Y) \simeq \mathbb{E}_8/T$ and the map $\overline{\text{res}}_Z$ factors through $\overline{\text{res}}_Y$. Moreover,

$$\text{Cl}_0(Y)/\text{torsion} \simeq \mathbb{E}_8/\hat{T}.$$

The intersection pairing on Y and pull back of \mathbb{Q} -divisors realizes \mathbb{E}_8/\hat{T} as a sublattice of the vector space $(T \otimes \mathbb{Q})^\perp \subseteq \mathbb{E}_8 \otimes \mathbb{Q}$ with the intersection pairing on Z .

Remark 3.17. Root lattices $T \subset \mathbb{E}_8$ were classified by Dynkin [Dyn57, Table 11]. The quotient group $\text{Cl}_0(Y) \simeq \mathbb{E}_8/T$ was computed, e.g., in [OS91].

Corollary 3.18. *Let (C, Y) be a minimal elliptic pair with Du Val singularities and $\rho(Y) \geq 3$. Let R be the rank of the root lattice of (C, Y) and suppose $e(C, Y) < \infty$. Then $\overline{\text{Eff}}(Y)$ is polyhedral if and only if there are roots $\beta_1, \dots, \beta_{8-R} \in \mathbb{E}_8 \setminus \hat{T}$, linearly independent modulo \hat{T} and such that $\overline{\text{res}}(\beta_i) = 0$. In particular, if $R = 7$ then $\overline{\text{Eff}}(Y)$ is polyhedral if and only if $\overline{\text{res}}(\beta) = 0$ for some root $\beta \in \mathbb{E}_8 \setminus \hat{T}$.*

The reader will notice a discrepancy between Corollary 3.18, which provides an effective criterion of polyhedrality for minimal elliptic pairs (C, Y) with Du Val singularities and $e(C, Y) < \infty$ and Corollary 3.12, which shows that a minimal model (C, Y) of an elliptic pair (C, X) with $e(C, X) = \infty$ has Du Val singularities. These disjoint scenarios are reconciled in the following definition:

Definition 3.19. Let (C, X) be an elliptic pair with $e(C, X) = \infty$ defined over K , a finite extension of \mathbb{Q} . Let $R \subset K$ be the corresponding ring of algebraic integers. There exists an open subset $U \subset \text{Spec } R$ and a pair of schemes $(\mathcal{C}, \mathcal{X})$ flat over U , which we call an *arithmetic elliptic pair of infinite order*, such that

- Each geometric fiber (C, X) of $(\mathcal{C}, \mathcal{X})$ is an elliptic pair of order e_b which depends only on the corresponding point $b \in U$. We have $e_b < \infty$ for $b \neq 0$.
- The contraction morphism $X \rightarrow Y$ to the minimal model extends to the contraction of schemes $\mathcal{X} \rightarrow \mathcal{Y}$ flat over U .
- All geometric fibers (C, Y) of $(\mathcal{C}, \mathcal{Y})$ over U are minimal elliptic pairs with Du Val singularities and the same root lattice $T \subset \mathbb{E}_8$.

Let X, Y be geometric fibers over a place $b \in U$, $b \neq 0$. We call b a *polyhedral prime* if $\overline{\text{Eff}}(Y)$ is polyhedral. If b is not polyhedral then $\overline{\text{Eff}}(X)$ is also not polyhedral.

Distribution of polyhedral primes is an intriguing question in arithmetic geometry that we will start to address for arithmetic toric elliptic pairs.

4. LANG–TROTTER POLYGONS AND TORIC ELLIPTIC PAIRS

At the beginning we work over an algebraically closed field k of any characteristic. We recall that a polygon $\Delta \subseteq \mathbb{R}^2$ is called a lattice polygon if its vertices are in \mathbb{Z}^2 . If Δ is a lattice polygon, we will denote by $\text{Vol}(\Delta)$ its *normalized volume*, i.e. twice its euclidean area (so that $\text{Vol}(\Delta)$ is always a non-negative integer). We recall that given any Laurent polynomial

$$f = \sum_{u \in \mathbb{Z}^2} \alpha_u x^u \in k[x_1^{\pm 1}, x_2^{\pm 2}], \quad (4.1)$$

where $x^u := x_1^{u_1} x_2^{u_2}$, we can construct a lattice polygon $\text{NP}(f)$, called the *Newton polygon* of f , by taking the convex hull of the points $u \in \mathbb{Z}^2$ such that $\alpha_u \neq 0$.

A lattice polygon Δ defines a morphism

$$g_\Delta: \mathbb{G}_m^2 \rightarrow \mathbb{P}^{|\Delta \cap \mathbb{Z}^2| - 1}, \quad x \mapsto [x^u : u \in \Delta \cap \mathbb{Z}^2],$$

where $x = (x_1, x_2) \in (k^*)^2$. We will denote by \mathbb{P}_Δ the projective toric surface defined by Δ , i.e. the closure of the image of g_Δ , and by $e \in \mathbb{P}_\Delta$ the image $g_\Delta(1, 1)$. A hyperplane section is denoted by H_Δ . The linear system $|H_\Delta|$ is denoted by \mathcal{L}_Δ , and, given a positive integer m , we let $\mathcal{L}_\Delta(m)$ to be the subsystem of \mathcal{L}_Δ consisting of the curves having multiplicity at least m at e . We will denote by $\pi_\Delta: X_\Delta \rightarrow \mathbb{P}_\Delta$ the blowing up at $e \in \mathbb{P}_\Delta$ and by E the exceptional divisor of π_Δ .

Notation 4.1. Given a triple (Δ, m, Γ) where Δ is a lattice polygon, m a positive integer and $\Gamma \in \mathcal{L}_\Delta(m)$, the curve Γ is given by a Laurent polynomial (4.1) and the curve $V(f) = \Gamma \cap \mathbb{G}_m^2$ will also be denoted by Γ . We denote by C the proper transform of Γ in X_Δ . In this section we will investigate properties of pairs (C, X_Δ) . We drop the subscript Δ from notation $\mathbb{P}_\Delta, X_\Delta$ if no confusion arises.

Proposition 4.2. *Consider a triple (Δ, m, Γ) as in Notation 4.1. Suppose Γ is irreducible and its Newton polygon is Δ . The following hold:*

(i) *the arithmetic genus of C is*

$$p_a(C) = \frac{1}{2} (\text{Vol}(\Delta) - m^2 + m - |\partial\Delta \cap \mathbb{Z}^2|) + 1;$$

(ii) *any edge F of Δ of lattice length 1 gives a smooth point $p_F \in C$ defined as the intersection of C with the toric boundary divisor corresponding to F . This point is defined over the field of definition of Γ .*

Proof. Since Δ is the Newton polygon of Γ , $\Gamma \subseteq \mathbb{P}$ does not contain any torus-invariant point of \mathbb{P} . In particular, Γ is contained in the smooth locus of \mathbb{P} , and hence C is contained in the smooth locus of X . By adjunction formula,

$$p_a(C) = \frac{1}{2}(C^2 + C \cdot K_X) + 1 = \frac{1}{2}(\text{Vol}(\Delta) - m^2 + C \cdot K_X) + 1,$$

where the second equality follows from [CLS11, Prop. 10.5.6]. But $C \cdot K_X = \Gamma \cdot K_\mathbb{P} + m$, so that in order to prove (i) we only need to show that

$$\Gamma \cdot K_\mathbb{P} = -|\partial\Delta \cap \mathbb{Z}^2|. \quad (4.2)$$

Observe that $-K_\mathbb{P}$ is the sum of all the prime invariant divisors of \mathbb{P} and each prime invariant divisor $D \subseteq \mathbb{P}$ corresponds to an edge F of Δ , see [CLS11, Prop. 10.5.6]. Let us fix such an edge F . By a monomial change of variables, we can assume that F lies on the x_2 axis. The inclusion of algebras $k[x_1, x_2^{\pm 1}] \rightarrow k[x_1^{\pm 1}, x_2^{\pm 1}]$ gives the

inclusion $\mathbb{G}_m^2 \rightarrow \mathbb{G}_m \times \mathbb{A}^1$, and $V(x_1) \subseteq \mathbb{G}_m \times \mathbb{A}^1$ is an affine open subset of D . Since Γ does not contain any torus-invariant points of \mathbb{P} , $\Gamma \cap D = \Gamma \cap V(x_1)$, and the latter intersection has equation

$$f|_F := \sum_{u \in F \cap \mathbb{Z}^2} \alpha_u x^u = f(0, x_2) = 0. \quad (4.3)$$

The degree of this Laurent polynomial is the lattice length of F , so that (4.2) holds.

Moreover, if F has length 1, the equation (4.3) has degree 1, which means that Γ intersects the prime divisor D transversally at a smooth point $p_F \in \Gamma$. Since D is defined over the base field, if Γ is defined over a subfield $k_0 \subset k$ then so is p_F . \square

Definition 4.3. Let $\Delta \subseteq \mathbb{R}^2$ be a lattice polygon with at least 4 vertices. We say that Δ is *good*, if, for some integer m , the following hold:

- (i) $\text{Vol}(\Delta) = m^2$;
- (ii) $|\partial\Delta \cap \mathbb{Z}^2| = m$;
- (iii) $\dim \mathcal{L}_\Delta(m) = 0$, and the only curve $\Gamma \in \mathcal{L}_\Delta(m)$ is irreducible;
- (iv) the Newton polygon of Γ coincides with Δ ;

A good polygon is said to be:

- a *Halphen polygon* if $\text{res}(C) = \mathcal{O}_X(C)|_C$ is torsion;
- a *Lang–Trotter polygon* if $\text{res}(C) = \mathcal{O}_X(C)|_C$ is not torsion.

Theorem 4.4. *If Δ is a good polygon then (C, X_Δ) is an elliptic pair (we call it a toric elliptic pair), $e(C, X_\Delta) > 1$, and C is defined over the base field. If Δ is Lang–Trotter then $\text{char } k = 0$, $e(C, X_\Delta) = \infty$, and $\overline{\text{Eff}}(X_\Delta)$ is not polyhedral.*

Proof. Let Δ be a good lattice polygon. The curve Γ is irreducible by (iii) and does not pass through the torus-invariant points of \mathbb{P}_Δ by (iv). It follows that C is contained in the smooth locus of X_Δ . Toric surface singularities, i.e. cyclic quotient singularities, are log terminal. By (iv) and [CLS11, Prop. 10.5.6], $\Gamma^2 = \text{Vol}(\Delta)$, so that (i) is equivalent to $C^2 = 0$. Finally, conditions (i) and (ii), together with Prop. 4.2, imply that $p_a(C) = 1$. Thus (C, X_Δ) is an elliptic pair. Observe that $\mathcal{O}_X(C)|_C = \text{res}(C) \in \text{Pic}^0(C)$ (see Definition 3.1), so that being Lang–trotter is equivalent to $e(C, X_\Delta) = \infty$. Suppose this is the case. Since $\dim \mathcal{L}_\Delta(m) = 0$, the curve Γ , and thus also the curve C , and thus also the line bundle $\mathcal{O}_X(C)|_C$, are all defined over the base field. In characteristic p , the group $(\text{Pic}^0 C)(\mathbb{F}_p)$ is torsion, which contradicts $e(C, X_\Delta) = \infty$. Thus $\text{char } k = 0$. Since Δ has at least 4 vertices, $\rho(X_\Delta) \geq 3$ and $\overline{\text{Eff}}(X)$ is not polyhedral by Lemma 3.3. \square

Remark 4.5. We don’t know examples of Lang–Trotter quadrilaterals. Indeed, in the following proposition we are going to prove that they don’t exist, under the additional hypothesis that the multiplicity m coincides with the lattice width of the polygon.

Proposition 4.6. *There are no Lang–Trotter quadrilaterals Δ such that $m = \text{width}(\Delta)$.*

Proof. Assume Δ is a good quadrilateral and let (C, X_Δ) be the corresponding elliptic pair. The divisor $K + C$ is linearly equivalent to an effective one whose components in the support are in C^\perp . In particular, if C^\perp contains the classes of two negative curves R_1, R_2 then, being this space two-dimensional, there are integers a_i , with $a_0 \neq 0$, such that $a_0 C + a_1 R_1 + a_2 R_2 \sim 0$. Taking restriction to C

one deduces that Δ is not Lang–Trotter. If $K + C \sim \alpha R + \beta C$, with $\alpha, \beta \in \mathbb{Q}_{>0}$, then, after cleaning denominators and restricting to C one again concludes that Δ is not Lang–Trotter. If $K + C \sim 0$, then by considering multiplicities at e , we must have $m = 1$, which is impossible since $m = |\partial\Delta \cap \mathbb{Z}^2| \geq 4$. It remains to analyze the case $K + C \sim nR$, with $n > 0$ and R is an irreducible curve in C^\perp . Since we are assuming that $m = \text{width}(\Delta)$, the class of the one-parameter subgroup defined by one width direction lies in C^\perp , so that R must be this class, and in particular its Newton polygon is a segment of lattice length 1. Moreover, by considering multiplicities at e , it must be that $n = m - 1$, so that Δ has m interior lattice points, lying on a line. If Δ were Lang–Trotter, Pick’s formula would give $m^2 = 3m - 2$, which has integer solutions $m = 1, 2$, but this is again impossible. \square

Example 4.7. The polygon Δ with vertices

$$\begin{bmatrix} 0 & 12 & 14 & 9 \\ 0 & 4 & 5 & 15 \end{bmatrix}$$

satisfies the conditions $\text{Vol}(\Delta) = 169$, $|\partial\Delta \cap \mathbb{Z}^2| = 13$ and $\mathcal{L}_\Delta(13)$ contains only one curve Γ , irreducible. Moreover, $\text{width}(\Delta) = 14$, so that this is an example of good polygon with $m < \text{width}(\Delta)$. In particular, the proof of the above proposition does not apply. Nevertheless it is possible to show that Δ is not Lang–Trotter since $e(C, X_\Delta) = 6$.

We remark that even if in all the examples of Lang–Trotter polygons appearing in Database 10 the condition $m = \text{width}(\Delta)$ is satisfied, it is possible to find examples in which m is smaller. For instance, one can check by a computation similar to Computation 10.8 that the polygon with vertices $[0, 0], [12, 4], [11, 7], [9, 12], [8, 12]$ is Lang–Trotter and it has $m = 11$ and $\text{width}(\Delta) = 12$.

Example 4.8. Polygon 111 is the polygon Δ with vertices:

$$\begin{bmatrix} 6 & 5 & 1 & 8 & 0 & 0 & 3 \\ 1 & 4 & 3 & 2 & 6 & 7 & 0 \end{bmatrix}$$

which appears in Table 4 for $m = 7$ (where it corresponds to the blue matrix) and we will use it later in the proof of Theorem 1.2. We claim that Δ is Lang–Trotter.

First of all, $\text{Vol}(\Delta) = 49$ and $|\partial\Delta \cap \mathbb{Z}| = 7$ (see Computation 10.3). By Computation 10.4, $\mathcal{L}_\Delta(7)$ has dimension 0 and the unique curve $\Gamma \in \mathcal{L}_\Delta(7)$ has equation

$$\begin{aligned} & -u^8v^2 + 4u^7v^2 + 8u^6v^3 - 5u^6v^2 - 3u^6v - 5u^5v^4 - 50u^5v^3 + 21u^5v^2 + \\ & 6u^5v + 40u^4v^4 + 85u^4v^3 - 55u^4v^2 - 6u^3v^5 - 85u^3v^4 - 40u^3v^3 + 56u^3v^2 - \\ & 10u^3v + u^3 + 15u^2v^5 + 80u^2v^4 - 40u^2v^3 + u^2v^2 + 3uv^6 - 30uv^5 + \\ & 5uv^4 + 2uv^3 - v^7 + 4v^6 = 0. \end{aligned}$$

The exponents of the red monomials are the vertices of Δ , so that the Newton polygon of Γ is Δ . By Computation 10.5 the curve Γ is irreducible and its strict transform $C \subseteq X_\Delta$ is a smooth elliptic curve. It has the minimal equation

$$y^2 + xy = x^3 - x^2 - 4x + 4$$

by Computation 10.8. This is the curve labelled 446.a1 in the LMFDB database [LMF20]. Since $e(C, X) > 1$, $\text{res}(C) \in \text{Pic}^0(C)$ is not trivial. Since the Mordell–Weil group is \mathbb{Z}^2 , $\text{res}(C)$ is not torsion and therefore Δ is Lang–Trotter.

Remark 4.9. If in Definition 4.3 we substitute condition (ii) with $|\partial\Delta \cap \mathbb{Z}^2| < m$, the curve C will have arithmetic genus $p_a(C) > 1$, so that (C, X_Δ) is no longer an elliptic pair. However, if $\text{res}(C)$ is not torsion, we can still conclude that $\overline{\text{Eff}}(X_\Delta)$ is not polyhedral by Proposition 2.3. In the database [Bal20], there are only two polygons satisfying $|\partial\Delta \cap \mathbb{Z}^2| < m$ together with (i), (iii) and (iv). Both polygons have volume 49 and 5 boundary points, so that by Proposition 4.2 the corresponding curve C has genus 2. In the first case we verified that $2C$ moves (Computation 10.4), so $\text{res}(C)$ is torsion. The second polygon has the following vertices

$$\begin{bmatrix} 0 & 5 & 7 & 3 & 1 \\ 0 & 2 & 3 & 8 & 3 \end{bmatrix}$$

and we claim that in this case $\text{res}(C)$ is not torsion. Indeed the curve C is isomorphic to a hyperelliptic curve with equation

$$y^2 + (x^2 + x + 1)y = x^5 - 3x^4 + x^3 - x.$$

This is the curve labelled 1415.a.1415.1 in the LMFDB database [LMF20] and the Mordell-Weil group of the corresponding jacobian surface is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By Computation 10.4, $\dim |2C| = 0$ and we conclude that $\text{res}(C)$ is non-torsion.

5. ARITHMETIC TORIC ELLIPTIC PAIRS OF INFINITE ORDER

Notation 5.1. Given a lattice polygon $\Delta \subseteq \mathbb{Z}^2$, let \mathcal{P} be the projective toric scheme over $\text{Spec } \mathbb{Z}$ given by the normal fan of Δ , with a relatively ample invertible sheaf \mathcal{L} given by the polygon Δ . Let \mathcal{X} be the blow-up of \mathcal{P} along the identity section of the torus group scheme. Let $\mathcal{E} \simeq \mathbb{P}_{\mathbb{Z}}^1$ be the exceptional divisor. For any field k , we denote by $\mathbb{P}_k, L_k, X_k, E_k$ the corresponding base change (or simply by \mathbb{P}, L, X, E if k is clear from the context). We will assume that Δ is a Lang-Trotter polygon, i.e., $(C_{\mathbb{C}}, X_{\mathbb{C}})$ is an elliptic pair of order $e(C_{\mathbb{C}}, X_{\mathbb{C}}) = \infty$. Then $(C_{\mathbb{C}}, X_{\mathbb{C}})$ is a geometric fiber of an arithmetic elliptic pair $(\mathcal{C}, \mathcal{X})$ of infinite order flat over an open subset $U \subset \text{Spec } \mathbb{Z}$, see Definition 3.19. We assume that $C_{\mathbb{C}}$ is a *smooth elliptic curve*. A geometric fiber (C, X) of $(\mathcal{C}, \mathcal{X})$ over a prime $p \in U$ is an elliptic pair of finite order e_p . There is a morphism of schemes $\mathcal{X} \rightarrow \mathcal{Y}$ flat over U , inducing a morphism $X \rightarrow Y$ to the minimal model for any geometric fiber. Geometric fibers (C, Y) of $(\mathcal{C}, \mathcal{Y})$ over U are minimal elliptic pairs with Du Val singularities and the same root lattice T , which we call *the root lattice of Δ* . Recall that we call p a polyhedral prime of Δ if $\overline{\text{Eff}}(Y)$ is a polyhedral cone in characteristic p . We are interested in the distribution of polyhedral and non-polyhedral primes. Recall that polyhedrality is governed by Corollary 3.18: p is polyhedral if and only if there are roots $\beta_1, \dots, \beta_{8-R} \in \mathbb{E}_8 \setminus \hat{T}$, linearly independent modulo \hat{T} and such that $\overline{\text{res}}(\beta_i) = 0$ in $C(\mathbb{F}_p)/\text{res}(C)$. Here R is the rank of T .

We will need a lemma on arithmetic geometry of elliptic curves.

Lemma 5.2. *Let C be an elliptic curve defined over \mathbb{Q} without complex multiplication over $\overline{\mathbb{Q}}$. Fix points $x_0, \dots, x_r \in C(\mathbb{Q})$ of infinite order. Suppose the subgroup $\langle x_1, \dots, x_r \rangle \subset C(\mathbb{Q})$ generated by x_1, \dots, x_r is free abelian and does not contain a multiple of x_0 . Then the reductions $\bar{x}_1, \dots, \bar{x}_r$ modulo p are not contained in the cyclic subgroup generated by the reduction \bar{x}_0 for a set of primes of positive density.*

Remark 5.3. Note that $x_1, \dots, x_r \in C(\mathbb{Q})$ are not assumed linearly independent.

Proof. For a fixed integer q , let $C[q] \subset C(\bar{\mathbb{Q}})$ be the set of q -torsion points, so that $C[q] \simeq (\mathbb{Z}/q\mathbb{Z})^2$ as a group. Let K be the field $\mathbb{Q}(C[q])$. Since C does not have complex multiplication,

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \quad (5.1)$$

for almost all primes q by Serre's theorem [Ser71]. Choose a basis y_1, \dots, y_s of $\langle x_1, \dots, x_r \rangle$. Since x_0 has infinite order, $y_0 = x_0, y_1, \dots, y_s$ is a basis of the free abelian group $\langle x_0, \dots, x_r \rangle$. Choose points $y_0/q, \dots, y_s/q \in C(\bar{\mathbb{Q}})$. Let K_{y_0, \dots, y_s} be a field extension of K generated by $y_0/q, \dots, y_s/q$ (any choice of quotients gives the same field). By Bashmakov's theorem [Bas72], for almost all primes q we have

$$\mathrm{Gal}(K_{y_0, \dots, y_s}/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \times ((\mathbb{Z}/q\mathbb{Z})^2)^{s+1}.$$

For any $x \in C(\mathbb{Q})$, let $i(\bar{x})$ denote the index of the subgroup $\langle \bar{x} \rangle \subset C(\mathbb{F}_p)$. It suffices to prove that $i(\bar{x}_1), \dots, i(\bar{x}_r)$ are not divisible by q but $i(\bar{x}_0)$ is divisible by q for a set of primes p of positive density. By [LT77], $i(\bar{x})$ is divisible by q if and only if the Frobenius element

$$\sigma_p = (\gamma_p, \tau_p) \in \mathrm{Gal}(K_x/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})^2$$

belongs to one of the following conjugacy classes: either $\gamma_p = 1$ or γ_p has eigenvalue 1 and $\tau_p \in \mathrm{Im}(\gamma_p - 1)$. We can express $x_i = \sum_{j=1}^s a_{ij} y_j$ for $i = 1, \dots, r$, $a_{ij} \in \mathbb{Z}$. To apply the Chebotarev density theorem [Tsc26], it remains to note that the subset of tuples $(\gamma, \tau_0, \dots, \tau_s) \in \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z}) \times ((\mathbb{Z}/q\mathbb{Z})^2)^{s+1}$ such that γ has eigenvalue 1, $\tau_0 \in \mathrm{Im}(\gamma - 1)$ and $\sum_{j=1}^s a_{ij} \tau_j \notin \mathrm{Im}(\gamma - 1)$ for $i = 1, \dots, r$, is non-empty for $q \gg 0$. \square

Remark 5.4. We were inspired by the following theorem of Tom Weston [Wes03]. Suppose we are given an abelian variety A over a number field F such that $\mathrm{End}_F A$ is commutative, an element $x \in A(F)$ and a subgroup $\Sigma \subset A(F)$. If $\mathrm{red}_v x \in \mathrm{red}_v \Sigma$ for almost all places v of F then $x \in \Sigma + A(F)_{\mathrm{tors}}$.

Here is another variation on the same theme:

Lemma 5.5. *Let C be an elliptic curve defined over \mathbb{Q} with points $x, y \in C(\mathbb{Q})$ of infinite order such that $y = dx$ for a square-free integer d . Suppose there exists a prime p of good reduction and coprime to d such that the index of $\langle \bar{x} \rangle$ is coprime to d but the index of $\langle \bar{y} \rangle$ is divisible by d . Then $\bar{x}, 2\bar{x}, \dots, (d-1)\bar{x} \notin \langle \bar{y} \rangle$ for a set of primes of positive density.*

Proof. We need to prove positive density of primes such that the index of the subgroup $\langle \bar{y} \rangle$ in $\langle \bar{x} \rangle$ is equal to d . It is enough to prove positive density for the set of primes such that the index of $\langle \bar{x} \rangle$ in $C(\mathbb{F}_p)$ is coprime to d but the index of $\langle \bar{y} \rangle$ is divisible by d . Arguing as in the proof of Lemma 5.2, we can express this condition as a condition that the Frobenius element σ_p is contained in the union of certain conjugacy classes in the Galois group $\mathrm{Gal} L/\mathbb{Q}$, where L is obtained by adjoining the d -torsion $C[d]$ and the point x/d . To apply Chebotarev density theorem, we need to know that this conjugacy class is non-empty. Arguing in reverse, it suffices to find a specific p such that the condition holds. \square

Theorem 5.6. *Consider Lang–Trotter polygons from Table 1 (numbered as in Table 4). We list the root lattice T , the minimal equation of the elliptic curve C , its*

N	T	C	MW	$\text{res}(C)$
19	A_7	$y^2 + y = x^3 - x^2 - 24x + 54$	\mathbb{Z}^2	$-(1, 5)$
24	$A_6 \oplus A_1$	$y^2 + y = x^3 + x^2$	\mathbb{Z}	$6(0, 0)$
111	$A_6 \oplus A_1$	$y^2 + xy = x^3 - x^2 - 4x + 4$	\mathbb{Z}^2	$(-1, -2)$
128	$A_3 \oplus A_3$	$y^2 + y = x^3 + x^2 - 240x + 1190$	\mathbb{Z}^3	$(15, 34)$

TABLE 1.

Mordell-Weil group $C(\mathbb{Q})$ and $\text{res}(C)$. The set of non-polyhedral primes is infinite of positive density and includes primes under 2000 from Table 2.

N	primes
19	11,41,67,173,307,317,347,467,503,523,571,593,631,677,733,797,809,811,827,907,937,1019,1021,1087,1097,1109,1213,1231,1237,1259,1409,1433,1439,1471,1483,1493,1567,1601,1619,1669,1709,1801,1811,1823,1867,1877,1933,1951,1993
24	29,59,73,137,157,163,223,257,389,421,449,461,607,641,647,673,691,743,797,929,937,983,991,1049,1087,1097,1103,1151,1171,1217,1223,1259,1279,1319,1367,1399,1427,1487,1549,1567,1609,1667,1697,1747,1861,1867,1871,1913
111	47,71,103,197,233,239,277,313,367,379,409,503,563,599,647,677,683,691,719,727,761,829,911,997,1103,1123,1151,1171,1187,1231,1283,1327,1481,1493,1709,1723,1861,1907,1997
128	13,17,23,71,101,103,109,191,233,277,281,283,311,349,379,397,419,433,439,443,449,457,479,509,547,557,571,631,647,653,691,701,727,743,811,829,877,929,953,1021,1031,1033,1097,1123,1129,1151,1187,1213,1237,1277,1297,1423,1459,1471,1483,1499,1531,1549,1559,1583,1621,1637,1699,1753,1783,1879,1889,1907,1979

TABLE 2.

Proof. We first explain an outline of the argument and then proceed case-by-case. We compute the normal fan of Δ and the fan of the minimal resolution \mathbb{P}_Δ of \mathbb{P}_Δ using Computation 10.3. We use Computation 10.6 to compute the Zariski decomposition of $K_X + C$, which by Theorem 3.10 gives curves C_1, \dots, C_s contracted by the morphism to the minimal model Y , and the classes of proper transforms of these curves in \mathbb{P}_Δ . Whenever Δ has lattice width m in horizontal and vertical directions, these curves include 1-parameter subgroups $C_1 = (v = 1)$ and $C_2 = (u = 1)$. We use Computation 10.7 to compute the root lattice T , $\text{Cl}_0(Y)$, and the push-forward map to $\text{Cl}_0(Y)$. Computation 10.4 gives the equation of the unique member Γ of the linear system $\mathcal{L}_\Delta(m)$ and its Newton polygon and Computation 10.5 shows that the proper transform C of this curve in X is an elliptic curve. We use Computation 10.8 to compute the minimal equation of C , intersection points of C with the toric boundary divisors, $\text{res}(C)$ and the images of roots in \mathbb{E}_8 . Reading off the Mordell-Weil group of C from the LMFDB database [LMF20], we can deduce that Δ is Lang–Trotter. In the same Computation 10.8, we apply Corollary 3.18 to test polyhedrality of specific primes from Table 2. Finally, we apply Lemma 5.2 or Lemma 5.5 to prove positive density of non-polyhedral primes. \square

Example 5.7. **Polygon 19** has vertices

$$\begin{bmatrix} 4 & 3 & 1 & 0 & 6 & 5 \\ 6 & 5 & 2 & 0 & 1 & 4 \end{bmatrix} \quad (5.2)$$

The minimal resolution $\tilde{\mathbb{P}}_\Delta$ has the fan from Figure 1, where bold arrows indicate the fan of \mathbb{P}_Δ . Note that $\tilde{\mathbb{P}}_\Delta$ has a toric map to $\mathbb{P}^1 \times \mathbb{P}^1$ and proper transforms of 1-parameter subgroups C_1, C_2 are preimages of rulings. Thus they have self-intersection -1 after blowing up e . The minimal resolution of X contains the configuration of curves from the right of Figure 1 (toric boundary divisors and curves C_1, C_2). Only curves C_1 and C_2 contribute to the Zariski decomposition of

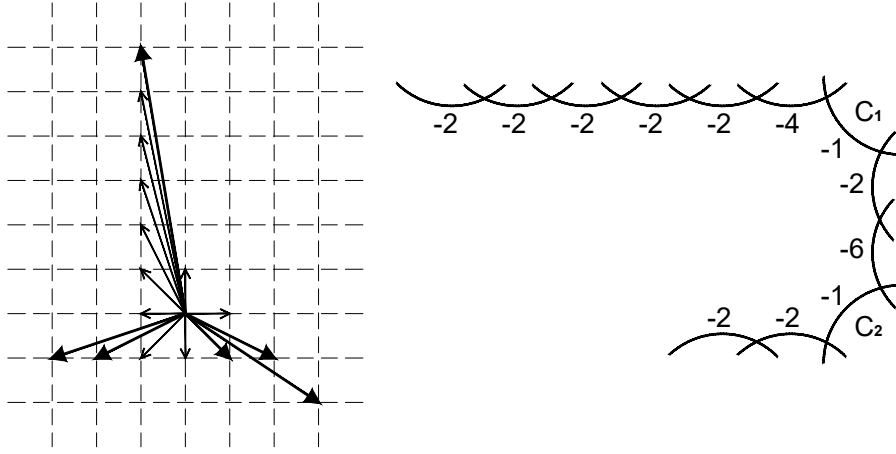


FIGURE 1. Polygon 19

$K + C$ and are contracted by the morphism $X \rightarrow Y$. Equivalently, the surface Y is obtained by contracting the chain of rational curves above. After blowing down (-1) -curves, this is equivalent to contracting a chain of seven (-2) -curves. Thus Y has an A_7 singularity and Picard number 3. There are two conjugate classes of root sublattices of type A_7 in \mathbb{E}_8 ([OS91][p. 85]). In our case $\text{Cl}_0(Y) \simeq \mathbb{Z}$ is torsion-free, thus the embedding is primitive. More precisely, we have $\text{Cl}_0(Y) = \mathbb{E}_8/\mathbb{A}_7$, which corresponds to the \mathbb{Z} -grading of the Lie algebra $\mathfrak{e}_8 = \bigoplus_{\beta \in \text{Cl}_0(Y)} (\mathfrak{e}_8)_\beta$ of the form

$$\begin{array}{ccccccc} \mathbb{C}^8 & \Lambda^2 \mathbb{C}^8 & \Lambda^3 \mathbb{C}^8 & \mathfrak{gl}_8 & \Lambda^3 \mathbb{C}^8 & \Lambda^2 \mathbb{C}^8 & \mathbb{C}^8 \\ 8 & 28 & 56 & 64 & 56 & 28 & 8 \end{array}$$

Let α be a generator of $\text{Cl}_0(Y)$. The images of the roots of \mathbb{E}_8 are $\pm k\alpha$ for $k \leq 3$. Thus polyhedrality condition is that $k \text{res}(\alpha) \notin \langle \text{res}(C) \rangle$ in char p for $k = 1, 2, 3$.

Next we compute $\text{res}(\alpha)$ and $\text{res}(C)$. The curve Γ has equation

$$\begin{aligned} f = & u^4 v^6 + 6u^5 v^4 - 2u^4 v^5 - 14u^5 v^3 - 17u^4 v^4 - 4u^3 v^5 + u^6 v + 11u^5 v^2 \\ & + 38u^4 v^3 + 26u^3 v^4 - 9u^5 v - 27u^4 v^2 - 34u^3 v^3 + 22u^4 v + 16u^3 v^2 - 10u^2 v^3 \\ & - 24u^3 v + 10u^2 v^2 + 15u^2 v + 5uv^2 - 11uv + 1 = 0, \end{aligned}$$

and passes through e with multiplicity $m = 6$. When $p \neq 2, 3, 5$, C has Newton polygon (5.2) and is isomorphic to an elliptic curve with the minimal equation

$$y^2 + y = x^3 - x^2 - 24x + 54.$$

The curve C is labelled 997.a1 in the LMFDB database [LMF20] and its Mordell-Weil group $C(\mathbb{Q}) \simeq \mathbb{Z}^2$ is generated by $Q = (1, 5)$ and $P = (6, -10)$. We have $\text{res}(C) = -Q$, $\text{res}(\alpha) = P - Q$, in particular $\text{res}(C)$ is not torsion in characteristic 0 and thus Δ is Lang-Trotter. Thus $\overline{\text{Eff}}(X)$ and $\overline{\text{Eff}}(Y)$ are not polyhedral in characteristic 0.

In characteristic p , $k\bar{P}$ is not contained in the cyclic subgroup of $C(\mathbb{F}_p)$ generated by \bar{Q} for $k = 1, 2, 3$ for all primes in Table 2. According to the LMFDB database [LMF20], C has no complex multiplication. To prove positive density of non-polyhedral primes, we apply Lemma 5.2 to $x_0 = Q$ and $x_k = kP$ for $k = 1, 2, 3$.

Remark 5.8. Empirically, about 18% of primes are not polyhedral for this polygon. It would be interesting to obtain heuristics for density of non-polyhedral primes.

Remark 5.9. Since C contains an irrational 2-torsion point, the Lang-Trotter conjecture [LT77] predicts that \bar{Q} generates $C(\mathbb{F}_p)$ for a set of primes p of positive density. If true, the Lang-Trotter conjecture implies that $\overline{\text{Eff}}(Y)$ is polyhedral in characteristic p for a set of primes of positive density. However, the Lang-Trotter conjecture is only known for curves with complex multiplication [GM86].

Example 5.10. **Polygon 24** has vertices

$$\begin{bmatrix} 0 & 2 & 5 & 6 & 1 & 0 \\ 0 & 1 & 3 & 4 & 6 & 1 \end{bmatrix}$$

The minimal resolution $\tilde{\mathbb{P}}_\Delta$ of \mathbb{P}_Δ has the fan from the left side of Figure 2, where bold arrows indicate the fan of \mathbb{P}_Δ . As for the Polygon 19, the proper transforms of 1-parameter subgroups C_1, C_2 in X have self-intersection -1 and are the only curves contracted by the map to Y , which therefore can be obtained by contracting the configuration of rational curves from the right of Figure 2. It follows that Y

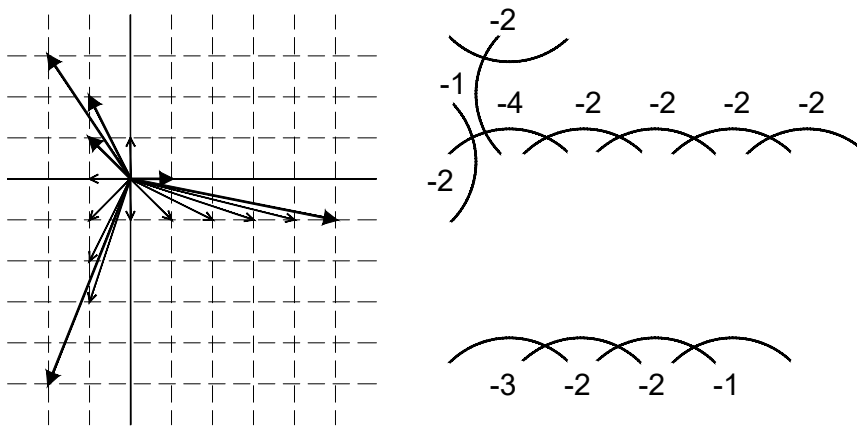


FIGURE 2. Polygon 24

has Picard number 3 and singularities A_1 and A_6 . The curve Γ has a point of multiplicity 6 at e and equation

$$\begin{aligned} f = & -1 + 2v + 7uv - 3u^2v - 23uv^2 + 6u^2v^2 + 2u^3v^2 + 18uv^3 + 20u^2v^3 \\ & - 26u^3v^3 + 10u^4v^3 - 2u^5v^3 - 12uv^4 - 11u^2v^4 \\ & + 6u^3v^4 + 5u^4v^4 - 4u^5v^4 + u^6v^4 + 5uv^5 + 3u^2v^5 - 2u^3v^5 - uv^6, \end{aligned}$$

which has a required Newton polygon when $p \neq 2, 3$. From the Dynkin classification it follows that $\text{Cl}_0(Y) \simeq \mathbb{Z}$. Let α be a generator. The images of roots of \mathbb{E}_8 are equal to $\pm k\alpha$ for $0 \leq k \leq 4$. Thus the polyhedrality condition is that $k \text{res}(\alpha) \notin \langle \text{res}(C) \rangle$ in char p for $k = 1, 2, 3, 4$. The minimal equation of the elliptic curve C is

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

It is the curve 43.a1 from the LMFDB database [LMF20] of elliptic curves. Its Mordell-Weil group is \mathbb{Z} generated by $(0, 0)$. We have $\text{res}(C) = Q = 6(0, 0)$ and $\text{res}(\alpha) = P = -(0, 0)$. It follows that $\text{res}(C)$ is not torsion and thus Δ is Lang-Trotter and $\overline{\text{Eff}}(X)$, $\overline{\text{Eff}}(Y)$ are not polyhedral in characteristic 0. In characteristic p , $k\bar{P}$ is not contained in the cyclic subgroup of $C(\mathbb{F}_p)$ generated by \bar{Q} for $k = 1, 2, 3, 4$ for all prime numbers in the table. Thus these primes are not polyhedral. The positive density follows from Lemma 5.5 with $p = 223$, when the index of \bar{P} is 1 and the index of \bar{Q} is 6.

Example 5.11. Polygon 111 (discussed in Example 4.8 and followed through in computations 10.3–10.8). The corresponding curve has the required Newton polygon in all characteristics $p \neq 2, 3, 5$. The minimal resolution $\tilde{\mathbb{P}}_\Delta$ has the fan from Figure 3, where bold arrows indicate the fan of \mathbb{P}_Δ . Note that $\tilde{\mathbb{P}}_\Delta$ has a toric map to $\mathbb{P}^1 \times \mathbb{P}^1$ and proper transforms of 1-parameter subgroups C_1, C_2 are preimages of rulings⁸; hence, they have self-intersection -1 after blowing up e . The Zariski decomposition of $K + C$ is $2C_1 + C_2 + C_3$, where C_3 is a curve whose image in \mathbb{P}_Δ has multiplicity 3 at e . The Newton polygon of C_3 has vertices

$$\begin{bmatrix} 3 & 0 & 0 & 1 \\ 1 & 3 & 2 & 0 \end{bmatrix}$$

and equation

$$u^3v - 3u^2v - uv^2 + 5uv - u + u^3 - 2u^2 = 0.$$

On X the curve C_3 is disjoint from C_1 and C_2 . The minimal resolution of X contains the configuration of curves from the right of Figure 3 (toric boundary divisors and curves C_1, C_2, C_3). The curves C_1, C_2, C_3 are contracted by the morphism $X \rightarrow Y$. Equivalently, the surface Y is obtained by contracting the chain of rational curves above. It follows that the root lattice is $\mathbb{A}_6 \oplus \mathbb{A}_1$ and the Picard number of Y is 3. From the Dynkin classification, we have that

$$\text{Cl}_0(Y) = \mathbb{E}_8/\mathbb{A}_6 \oplus \mathbb{A}_1 \simeq \mathbb{Z}.$$

Let α be a generator. The images of the roots of \mathbb{E}_8 are equal to $\pm k\alpha$, for $0 \leq k \leq 4$. Thus in characteristic p the non-polyhedrality condition is that $k \text{res}(\alpha) \notin \langle \text{res}(C) \rangle$, for $k = 1, 2, 3, 4$. To prove that this holds for a set of primes of positive density, we apply Lemma 5.2 to $x_i = \text{res}(i\alpha)$, $x_0 = \text{res}(C)$, for $i = 1, 2, 3, 4$. Let us check that the conditions in the lemma are satisfied. Using the minimal equation of the curve C (see Example 4.8) and Computation 10.8, we find that $\text{res}(\alpha) = P =$

⁸The 1-parameter subgroups are in this case $\{u = 1\}$ and $\{u = v\}$.

$(0, 2)$ and $\text{res}(C) = Q = (-1, -2)$. The curve C (labeled 446.a1 in the LMFDB database [LMF20]) has no complex multiplication and has Mordell–Weil group $\mathbb{Z} \times \mathbb{Z}$ generated by P and $-Q = (-1, 3)$. Hence, the points P and Q have infinite order and no multiple of Q is contained in the subgroup generated by P .

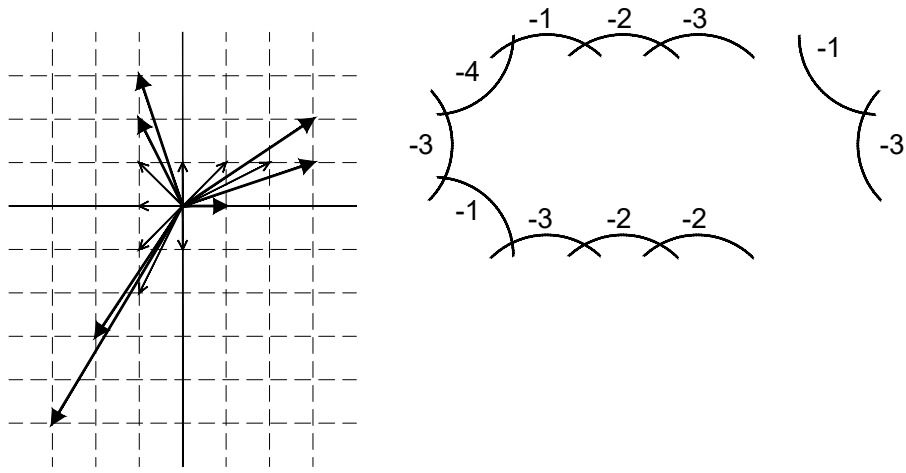


FIGURE 3. Polygon 111

Example 5.12. Polygon 128. This is a polygon with vertices

$$\begin{bmatrix} 0 & 1 & 6 & 7 & 6 & 3 & 1 \\ 5 & 6 & 7 & 7 & 5 & 0 & 3 \end{bmatrix}$$

The minimal resolution $\tilde{\mathbb{P}}$ of \mathbb{P} has the fan from the left side of Figure 4, where bold arrows indicate the fan of \mathbb{P} . The proper transforms of 1-parameter subgroups C_1, C_2 are the only curves contracted by the map $X \rightarrow Y$. Here Y can be obtained from $\text{Bl}_e \tilde{\mathbb{P}}$ by contracting a configuration of rational curves from the right of Figure 4, where we also indicate three boundary divisors, D_2, D_6 and D_7 (the only ones in Figure 4 that do not get contracted by the map to Y). The root lattice is $\mathbb{A}_3 \oplus \mathbb{A}_3$, the Picard number of Y is 4. One of the \mathbb{A}_3 's is indicated with the chain A_1, A_2, A_3 of (-2) -curves (after contracting all (-1) -curves). By the Dynkin classification, \mathbb{E}_8 contains two lattices $\mathbb{A}_3 \oplus \mathbb{A}_3$, one primitive and one non-primitive. In our case $\text{Cl}_0(Y) \simeq \mathbb{Z}^2$ is torsion-free, and therefore we have the primitive one. Next we describe the images in $\text{Cl}_0(Y)$ of roots in \mathbb{E}_8 . In other words, we have a grading of the Lie algebra \mathfrak{e}_8 by the abelian group $\text{Cl}_0(Y)$

$$\mathfrak{e}_8 = \sum_{\tilde{\beta} \in \text{Cl}_0(Y)} (\mathfrak{e}_8)_{\tilde{\beta}}$$

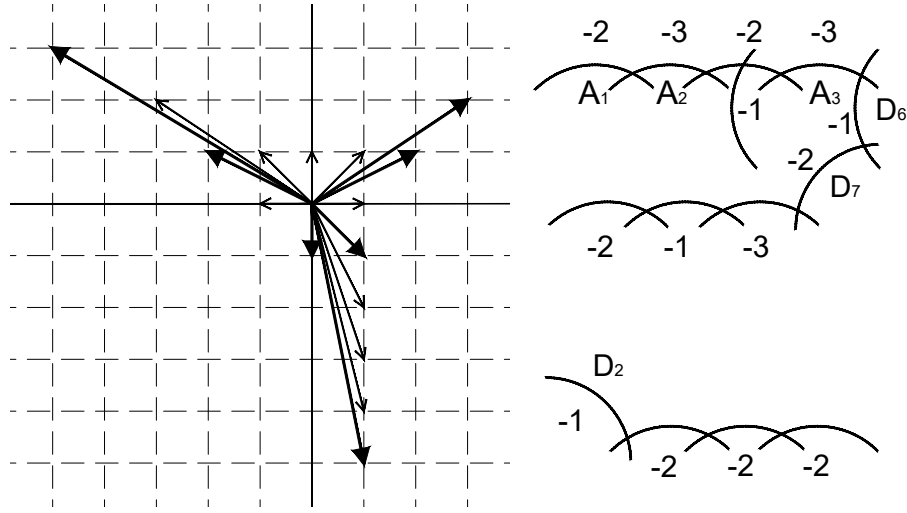


FIGURE 4. Polygon 128

and we need to describe the subset of non-empty weight spaces $\mathcal{B} \subset \text{Cl}_0(Y)$. A convenient interpretation of the lattice \mathbb{E}_8 is the lattice $K^\perp \subset \text{Pic}(\text{Bl}_8 \mathbb{P}^2)$ with the standard basis h, e_1, \dots, e_8 . The positive roots are $e_i - e_j$ for $i < j$, $h - e_i - e_j - e_k$, $2h - e_1 - \dots - \hat{e}_i - \dots - \hat{e}_j - \dots - e_8$ and $3h - e_1 - \dots - 2e_i - \dots - e_8$. The primitive sublattice $\mathbb{A}_3 \oplus \mathbb{A}_3$ is generated by simple roots marked black on Figure 5. It follows

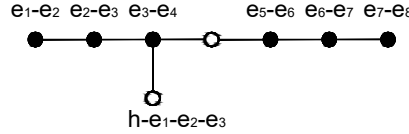


FIGURE 5. $\mathbb{A}_3 \oplus \mathbb{A}_3 \subset \mathbb{E}_8$

that the \mathbb{Z}^2 grading on \mathbb{E}_8 is obtained by pairing with fundamental weights h and $e_5 + e_6 + e_7 + e_8$ that correspond to white vertices of the Dynkin diagram. The \mathbb{Z}^2 grading of \mathfrak{e}_8 has the following non-empty weight spaces (in coordinates given by pairing with h and $e_5 + e_6 + e_7 + e_8$, respectively), where we also indicate dimensions.

4	6	4	16	4	16	4	6	4
4	6	24	32	24	24	6	4	4
4	4	4	16	4	4	4	4	4

It follows that the subset $\mathcal{B} \subset \text{Cl}_0(Y)$ is given by the \pm columns of the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 \\ 0 & 1 & 1 & 2 & 3 & 2 & 3 & 4 & 4 & 5 \end{pmatrix} \quad (5.3)$$

in the basis u, v , where u (resp., v) is the image of the simple root $h - e_1 - e_2 - e_3$ (resp., $e_4 - e_5$). Next we compute vectors u and v in $\text{Cl}_0(Y)$. By inspecting Figure 4,

one can prove that, in the minimal resolution Z of Y , $h - e_1 - e_2 - e_3$ corresponds to the (-2) -class $D_2 - D_7$ and $e_4 - e_5$ to $D_2 - D_6 - A_1 - A_2 - A_3$, which has pushforward $D_2 - D_6$ on X . Next we compute $\text{res}(C)$, $\text{res}(u)$ and $\text{res}(v)$.

The curve Γ has a point of multiplicity 7 at e and its Newton polygon is Δ for $p \neq 2, 3, 7, 11$. The minimal equation of the elliptic curve C is

$$y^2 + y = x^3 + x^2 - 240x + 1190,$$

which is the curve 29157b1 from the LMFDB database of elliptic curves. It has Mordell–Weil group \mathbb{Z}^3 generated by $P = (12, 13)$, $R = (-6, 49)$ and $Q = (-15, 40)$. We have

$$\text{res}(C) = (15, -35) = P - Q - R,$$

$$\text{res}(u) = (120, 1309) = Q - R, \quad \text{res}(v) = (-6, 49) = R.$$

We see that $\text{res}(C)$ is not torsion in characteristic 0 and thus $\overline{\text{Eff}}(Y)$ is not polyhedral. In characteristic p , the condition of polyhedrality is that there exist two linearly independent column-vectors of the matrix (5.3) which, when dotted with the row vector $(\text{res}(u), \text{res}(v))$ are contained in the cyclic subgroup of $C(\mathbb{F}_p)$ generated by $\text{res}(C)$. This gives the list of non-polyhedral primes in the table. To prove the positive density, we apply Lemma 5.2 (with $r = 10$).

Remark 5.13. In Example 5.12, by Lemma 5.2, we get positive density not only for the set of non-polyhedral primes but also for the set of primes p such that the Halphen pencil $|e_p C|$ on Y has only irreducible fibers. For example, $\text{res}(C)$ has order 2 in characteristic 23 and none of the elements of \mathcal{B} , when restricted to C , are contained in the cyclic subgroup of $C(\mathbb{F}_{23})$ generated by $\text{res}(C)$. It follows that $|2C|$ on Y is a Halphen pencil with only irreducible fibers. This property is stronger than non-polyhedrality: in characteristic 13, $\text{res}(C)$ has torsion 5 and $\text{res}(u + v)$ is contained in the cyclic subgroup generated by $\text{res}(C)$ but no other linearly independent vector in \mathcal{B} is. It follows that $\overline{\text{Eff}}(Y)$ is not polyhedral, but the Halphen pencil $|5C|$ on Y contains a reducible fiber with two components and no other reducible fibers.

6. INFINITE SEQUENCES OF LANG–TROTTER POLYGONS

An infinite sequence of pentagons.

Notation 6.1. Let $k \geq 1$ be an integer and let $m = 2k + 4$. Let Δ be the pentagon with vertices $(0, 0)$, $(m - 4, 0)$, $(m, 1)$, $(m - 2, m)$, $(m - 3, m - 1)$.

Theorem 6.2. *The polygon Δ is Lang–Trotter for every $k \geq 1$. Furthermore, every prime is a polyhedral prime of Δ .*

Notation 6.3. Consider an elliptic curve $C \subseteq \mathbb{P}^2$ with the Weierstrass equation

$$y^2 = x(x^2 + ax + b), \quad \text{where}$$

$$a = -(12k^2 + 24k + 11), \quad b = 4(k + 1)^2(3k + 2)(3k + 4).$$

Let

$$x_0 = 2(k + 1)(3k + 2), \quad x_1 = 2(k + 1)(3k + 4).$$

Consider the following points on C in homogeneous coordinates:

$$d_1 = [0 : 1 : 0], \quad d_2 = [x_0 : -x_0 : 1], \quad \tilde{d}_2 = [x_0 : x_0 : 1],$$

$$d_4 = [0 : 0 : 1], \quad d_5 = [x_1 : x_1 : 1].$$

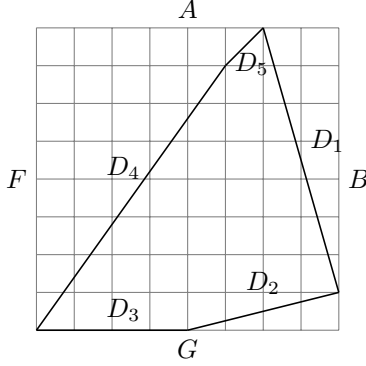


FIGURE 6. Polygon Δ for $k = 2$, $m = 8$

Define rational functions on C as follows:

$$f(x, y) = \frac{x^{k+1}(x-y)}{x-x_0}, \quad g(x, y) = \frac{(x-x_0)(x^{k+1} - x^k y - 2x_0^{k+1})}{x^k(x-y)}.$$

Lemma 6.4. *The curve C is a smooth elliptic curve defined over \mathbb{Q} . The points $d_1, d_2, \tilde{d}_2, d_4, d_5$ are mutually distinct and have the following properties:*

- (i) *The given lines intersect C at the following points, with multiplicities:*

$$\begin{aligned} z = 0 : & \quad 3d_1, & x = 0 : & \quad d_1 + 2d_4, \\ y = x : & \quad d_4 + d_5 + \tilde{d}_2, & x = x_0 : & \quad d_1 + d_2 + \tilde{d}_2. \end{aligned}$$

In particular, we have equivalences of divisors on C as follows:

$$2d_1 \sim 2d_4, \quad d_1 + d_2 \sim d_4 + d_5.$$

- (ii) *The divisors of zeros and poles of the rational functions f and g are*

$$(f) = ((m-1)d_4 + d_5) - ((m-1)d_1 + d_2),$$

$$(g) = (4d_2 + \gamma) - (2d_1 + (m-3)d_4 + d_5),$$

where γ is an effective divisor of degree $m-4$ disjoint from d_1, d_4, d_5 .

- (iii) *The line bundle $\mathcal{O}(d_2 - d_1)$ is not a torsion element of $\text{Pic}^0(C)$.*

Proof. The discriminant equals $16a^2(b^2 - 4a)$ and it is non-zero for all integers k , hence, the curve C is smooth. Part (i) is immediate noticing that $x = x^2 + ax + b$ has solutions $x = x_0$ and $x = x_1$. It follows from (i) that away from the point at infinity d_1 , the rational function f has zeros at $(m-1)d_4 + d_5$ and a single pole at d_2 , while at d_1 , there is a pole of order $(m-1)$. Similarly, g has poles at d_1, d_4, d_5 (of orders 2, $(m-3)$ and 1 respectively) and a zero of order at least 2 at d_2 . After a change of variables $u = x - x_0, v = y + x_0$, we see that C has $v - (2k+1)u = 0$ tangent line at $(0,0)$. After a further change of variables $w = v - (2k+1)u$, one can see that $x^{k+1} - x^k y - 2x_0^{k+1}$ has multiplicity at least 3 at d_2 . Hence, g has multiplicity at least 4 at d_2 . This proves (ii). To prove (iii), choose d_1 as the identity element of the Mordell-Weil group $C(\mathbb{Q})$. By Mazur's theorem [Maz77], it suffices to prove that $nd_2 \neq 0$ for $1 \leq n \leq 12$. We check this in Computation 10.9. \square

Notation 6.5. We label the sides of Δ as D_1, D_2, D_3, D_4, D_5 (see Figure 6). Note that Δ is inscribed in the square of side m in the first quadrant, with one vertex at $(0,0)$ and sides labeled, starting from the x -axis and going counterclockwise, G, B, A, F . The normal fans of Δ and the square give rise to toric surfaces \mathbb{P}_Δ and $\mathbb{P}^1 \times \mathbb{P}^1$. Let S be the toric surface corresponding to the common refinement of the two fans and let

$$\pi : S \rightarrow \mathbb{P}^1 \times \mathbb{P}^1, \quad \rho : S \rightarrow \mathbb{P}_\Delta$$

be the corresponding toric morphisms. For each of $\mathbb{P}_\Delta, \mathbb{P}^1 \times \mathbb{P}^1, S$, we denote the torus invariant divisor corresponding to a ray of the fan by the same letter, so

$$\begin{aligned} B &= (1, 0), & A &= (0, 1), & F &= (-1, 0), & G &= (0, -1), \\ D_1 &= (m-1, 2), & D_2 &= (1, -4), & D_3 &= (0, -1), \\ D_4 &= (-(m-1), m-3), & D_5 &= (-1, 1). \end{aligned}$$

On S we have $G = D_3$ and ρ contracts divisors A, B, F , while π contracts D_1, D_2, D_4, D_5 .

Lemma 6.6. *The following equalities of divisors hold on S :*

$$\begin{aligned} \pi^{-1}B &= B + (m-1)D_1 + D_2, & \pi^{-1}F &= F + (m-1)D_4 + D_5, \\ \pi^{-1}A &= A + 2D_1 + (m-3)D_4 + D_5, & \pi^{-1}G &= D_3 + 4D_2. \end{aligned}$$

Proof. If $\pi : Y \rightarrow X$ is the weighted blow-up of a toric surface obtained by adding a ray generated by a primitive vector $f := \alpha e_1 + \beta e_2$ to a smooth cone of the fan of X generated by primitive vectors e_1, e_2 , then the multiplicity of $V(f)$ in $\pi^{-1}V(e_1)$ is α . (Here $V(r)$ is the torus invariant divisor corresponding to the ray r). \square

As is customary, we view a rational function f on a curve C as the map $C \rightarrow \mathbb{P}^1$.

Proposition 6.7. *Let $\phi = (f, g) : C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ be the morphism given by the rational functions f, g . Let U be the open torus in $\mathbb{P}^1 \times \mathbb{P}^1$, with coordinates $(u, v) = ([1, u], [1, v])$ and let $\Gamma := \phi(C) \cap U$. There are unique morphisms*

$$\chi : C \rightarrow \mathbb{P}_\Delta, \quad \psi : C \rightarrow S,$$

that commute with ϕ and π, ρ as defined in Notation 6.5. Then:

- (1) *The map ϕ is birational onto its image and the equation of Γ in U is*

$$\begin{aligned} (uv + 2x_0^{k+2})(u - 2x_0^{k+1})^{m-1} - 2u^{k+1}(v + x_0)^{k+2}(u - 2x_0^{k+1})^{k+2} - \\ - u^{m-3}(v + x_0)^{m-1}(uv + u(x_0 - x_1) + 2x_1x_0^{k+1}) = 0. \end{aligned}$$

The Newton polygon of Γ is Δ and the multiplicity of Γ at the point q with $u = 2x_0^{k+1}, v = -x_0$ is m .

- (2) *For D_i ($i = 1, 2, 4, 5$) in \mathbb{P}_Δ , we have $\chi^{-1}(D_i) = d_i$ (see Notation 6.3).*
(3) *The induced map $\chi : C \rightarrow \text{Bl}_q \mathbb{P}_\Delta$ is an embedding and the linear system $\mathcal{L}_\Delta(m)$ has C as an irreducible member. Via this identification, we have*

$$\mathcal{O}(C)|_C \cong \mathcal{O}_C(2d_1 - 2d_2).$$

Furthermore, if E is the exceptional divisor in $\text{Bl}_q \mathbb{P}_\Delta$, then $\chi^{-1}(E)$ is a common fiber of the maps $C \rightarrow \mathbb{P}^1$ induced by f and g . In particular,

$$\chi^{-1}(E) \sim (m-1)d_4 + d_5 \sim (m-1)d_1 + d_2 \sim 4d_2 + \gamma \sim 2d_1 + (m-3)d_4 + d_5.$$

Proof. We first prove (1). Set $f(x, y) = u$, $g(x, y) = v$ and solve for x, y . Noticing that $uv = x(x^{k+1} - x^k y - 2x_0^{k+1})$, we obtain after some calculations that

$$x = \frac{u(v + x_0)}{u - 2x_0^{k+1}}, \quad y = \frac{x^{k+2} - u(x - x_0)}{x^{k+1}}. \quad (6.1)$$

In particular, the map ϕ is birational onto its image. It follows that $(u, v) \in \Gamma$ must satisfy the equation obtained by plugging in the above formulas for x, y in the Weierstrass equation of C . After clearing denominators, this equation is

$$(x^{k+2} - u(x - x_0))^2 = x^{2k+2}(x^3 + ax^2 + bx).$$

This equation has a solution $x = x_0$, since the point $y = x = x_0$ lies on C . More precisely, one can factor out $(x - x_0)$, by noticing that

$$(x^{k+2})^2 - x^{2k+3}(x^2 + ax + b) = x^{2k+3}(x - x_0)(x - x_1).$$

As Γ is irreducible and x is not always equal to x_0 along C , it follows that $(u, v) \in \Gamma$ must satisfy the equation

$$u^2(x - x_0) - 2ux^{k+2} = x^{2k+3}(x - x_1),$$

where x is as in (6.1). Substituting x with the formula in (6.1) and simplifying u^2 (u is not constant equal to 0 along Γ , otherwise $x = 0$) it follows $(u, v) \in \Gamma$ must satisfy the given equation. Note, the equation is of type (m, m) in $\mathbb{P}^1 \times \mathbb{P}^1$. Since each of the maps given by the rational functions f and g has degree m and ϕ is birational onto its image, it follows that the closure of Γ in $\mathbb{P}^1 \times \mathbb{P}^1$ is a curve of type (m, m) . In particular, the equation we obtained is irreducible and defines Γ on U . As already noted, the Newton polygon is inscribed in the square with vertices $(0, 0)$, $(0, m)$, $(m, 0)$, (m, m) , the terms

$$u^{m-3}v^{m-1}, \quad u^{m-2}v^m, \quad u^m v, \quad 1$$

appear with non-zero coefficients, and there are no terms $u^m v^i$ except when $i = 1$, or terms $u^{m-1} v^i$ when $i \geq k + 3$. It follows that the Newton polygon has as an edge the segment joining the points $(m - 2, m)$, $(m, 1)$. Similarly, to check that the edges joining $(0, 0)$, $(m - 3, m - 1)$ and $(m - 3, m - 1)$, $(m - 2, m)$ respectively, it suffices to check that there are no terms $u^i v^j$ with $j/i > (m - 1)/(m - 3)$ and no term $u^{m-3} v^m$ respectively. This is straightforward. It remains to prove that

$$u^{m-3}, \quad u^{m-2}, \quad u^{m-1}, \quad u^m$$

appear with zero coefficients, but u^{m-4} has a non-zero coefficient. Setting $v = 0$, the equation becomes (after simplifying x_0^{k+2})

$$2(u - 2x_0^{k+1})^{m-1} - 2u^{k+1}(u - 2x_0^{k+1})^{k+2} - x_0^{k+1}u^{m-3}(u(x_0 - x_1) + 2x_1x_0^{k+1}) = 0.$$

Recall that $m = 2k + 4$. Clearly, u^{m-1} and u^m appear with 0 coefficient. It is straightforward to check that the coefficients of u^{m-2} and u^{m-3} are

$$\begin{aligned} & -4x_0^{k+1} \binom{m-1}{1} + 4x_0^{k+1} \binom{k+2}{1} - x_0^{k+1}(x_0 - x_1) = 0, \quad \text{and} \\ & 2(2x_0^{k+1})^2 \binom{m-1}{2} - 2(2x_0^{k+1})^2 \binom{k+2}{2} - 2x_0^{2k+2}x_1 = 0, \quad \text{respectively.} \end{aligned}$$

The coefficient of u^{m-4} is

$$-2(2x_0^{k+1})^3 \binom{m-1}{3} + 2(2x_0^{k+1})^3 \binom{k+2}{3},$$

which is non-zero for all $k \geq 0$. Making the change of variables $s := u - 2x_0^{k+1}$, $t = v + x_0$, the equation of Γ becomes

$$s^{m-1}(st + 2x_0^{k+1}t - x_0s) - 2(st)^{k+2}(s + 2x_0^{k+1})^{k+1} - t^{m-1}(st + 2x_0^{k+1}t - x_1s) = 0,$$

which has a point of multiplicity m at $s = t = 0$. This finishes the proof of (1).

We now prove (2) and (3). Denote $d'_i = \chi^{-1}(D_i)$. Clearly, $\text{Vol}(\Delta) = m^2$ and $|\partial\Delta \cap \mathbb{Z}^2| = m$. Let C' be the proper transform in $\text{Bl}_q \mathbb{P}_\Delta$ of the closure of Γ in \mathbb{P}_Δ . Note that the map ϕ factors through C' , and C is the desingularization of C' . Up to a change of coordinates on U , we are in the situation of Proposition 4.2. In particular, C' has arithmetic genus one and hence it must be isomorphic to C . We identify C with its image in $\text{Bl}_q \mathbb{P}_\Delta$. As the edges D_i for $i \neq 3$ of Δ have lattice length 1, it follows that each of d'_i , for $i = 1, 2, 4, 5$, is a point. Since C does not pass through the torus invariant points of \mathbb{P}_Δ , the cycle d'_3 is disjoint from d'_i for $i = 1, 2, 4, 5$ and C embeds into $\text{Bl}_e S$ and is disjoint from the torus invariant divisors A, B, F . Hence, $d'_i = \psi^{-1}(D_i)$ for all i . By Lemma 6.6

$$\begin{aligned} \phi^{-1}B &= (m-1)d'_1 + d'_2, & \phi^{-1}F &= (m-1)d'_4 + d'_5, \\ \phi^{-1}A &= 2d'_1 + (m-3)d'_4 + d'_5, & \phi^{-1}G &= d'_3 + 4d'_2. \end{aligned}$$

By the definition of the map ϕ , the preimages of the torus invariant divisors in $\mathbb{P}^1 \times \mathbb{P}^1$ are given by the zeros and poles of the rational functions f and g , so by Lemma 6.4, these are

$$\begin{aligned} \phi^{-1}(u = \infty) &= (m-1)d_1 + d_2, & \phi^{-1}(u = 0) &= (m-1)d_4 + d_5, \\ \phi^{-1}(v = \infty) &= 2d_1 + (m-3)d_4 + d_5, & \phi^{-1}(v = 0) &= 2d_2 + \gamma. \end{aligned}$$

where γ is an effective divisor disjoint from d_i for $i = 1, 2, 4, 5$. By considering multiplicities, the only possibility that these divisors match is when $d_i = d'_i$ for all i . For example, the divisor $\phi^{-1}(v = \infty)$ must equal $\phi^{-1}A$, hence, $d_i = d'_i$ for $i = 1, 4, 5$. Similarly, $\phi^{-1}(u = \infty)$ must equal one of $\phi^{-1}B$ or $\phi^{-1}F$ and as $d_1 = d'_1$, it must be that $d_2 = d'_2$. The exceptional divisor E of $\text{Bl}_q(\mathbb{P}_\Delta)$ restricts to C as an effective degree m divisor which is contracted by both maps $C \rightarrow \mathbb{P}^1$. Hence, it is a common fiber of the two maps and $E|_C \sim (m-1)d_1 + d_2$.

Up to a change of coordinates on U , the linear system $\mathcal{L}_\Delta(m)$ has C as an irreducible member. To prove that Δ is a Lang–Trotter polygon, it suffices to prove that $\text{res}(C) \in \text{Pic}^0(C)$ is non-torsion (this also implies that $\dim \mathcal{L}_\Delta(m) = 0$). Let $X = \text{Bl}_q(\mathbb{P}_\Delta)$ and let E be the exceptional divisor. We have the following relations between the torus invariant divisors on \mathbb{P}_Δ , and hence, on X :

$$(m-1)D_1 + D_2 \sim (m-1)D_4 + D_5, \quad D_3 \sim 2D_1 - 4D_2 + (m-3)D_4 + D_5.$$

From the fan of \mathbb{P}_Δ , we can compute the intersection numbers $D_i \cdot D_j$. Using that $C \cdot D_i = 1$ ($i \neq 3$), $C \cdot E = m$, we obtain

$$C \sim m(m+1)D_1 + (m-2)D_2 - 2(m-1)D_4 - mE.$$

It follows that $\text{res}(C) = 2d_1 - 2d_2$. \square

Proof of Theorem 6.2. By Prop. 6.7(3), up to a change of coordinates on U , the linear system $\mathcal{L}_\Delta(m)$ has C as an irreducible member. It follows from Prop. 6.7(3) and Lemma 6.4(iii) that $\text{res}(C) \in \text{Pic}^0(C)$ is non-torsion. This also implies that $\dim \mathcal{L}_\Delta(m) = 0$ and hence, Δ is a Lang–Trotter polygon. The proper transforms in $\text{Bl}_q S$ of the two one-parameter subgroups C_1 and C_2 of $\mathbb{P}^1 \times \mathbb{P}^1$ have classes $\pi^{-1}B - E$ and $\pi^{-1}A - E$, respectively. It follows by Lemma 6.6 that their proper

transforms C_1, C_2 in $X = \text{Bl}_q \mathbb{P}_\Delta$ have classes $(m-1)D_1 + D_2 - E$ and $2D_1 + (m-3)D_4 + D_5 - E$, respectively. It follows that on X , we have $C \cdot C_1 = C \cdot C_2 = 0$ and C_1, C_2 are (-1) -curves. Since $\rho(X) = 4$, it follows that the minimal model (C, Y) of the elliptic pair (C, X) is obtained by contracting C_1 and C_2 and $\rho(Y) = 2$ and every prime is polyhedral. \square

Remark 6.8. The classes of the two one-parameter subgroups C_1, C_2 can be found from Lemma 6.6. Using the relations between torus invariant divisors, one obtains

$$C_1 \sim (m+1)D_1 + D_2 - 2D_4 - E, \quad C_2 \sim (m-1)D_1 + D_2 - E.$$

It follows that $K + C = (k+1)C_1 + (k+2)C_2$. For $1 \leq k \leq 5$ we checked using Computation 10.7 that the root lattice is $\mathbb{D}_6 \oplus \mathbb{A}_1 \oplus \mathbb{A}_1$ and the Mordell-Weil group of C is $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remark 6.9. The reader may wonder how did we divinate the Weierstrass equation of C in Notation 6.3. We explain how to arrive at the equation of C starting from the polygon Δ , assuming it can be inscribed in a square with sides of length m . In this case, we may add the normal rays of the square to the rays of the normal fan of Δ to obtain a toric surface S with maps $S \rightarrow \mathbb{P}_\Delta, S \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$. If the hypothetical curve C defined by the polygon Δ is smooth, then the canonical map $\chi : C \rightarrow \text{Bl}_e \mathbb{P}_\Delta$ lifts to a map $C \rightarrow \text{Bl}_e S$. The divisor $E|_C$ has degree m and is contracted by the maps $C \rightarrow S$, and hence also by $\phi : C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$. As the width of Δ in horizontal and vertical directions is m , the two maps $C \rightarrow \mathbb{P}^1$ are of degree m . As $E|_C$ has degree m and is contracted by both maps, it follows that $E|_C$ is a common fiber of both maps. If ϕ is given by (f, g) , where f and g are rational functions on C , it follows that the divisors of zeros and poles of both f and g (that is, the preimages of the torus invariant divisors in $\mathbb{P}^1 \times \mathbb{P}^1$) are linearly equivalent to $E|_C$. The preimages of the torus invariant divisors of $\mathbb{P}^1 \times \mathbb{P}^1$ in S can be computed directly from the fan of S (as in Lemma 6.6). Letting $d_i = \chi^{-1}(D_i)$, where D_i are the torus invariant divisors on \mathbb{P}_Δ , we obtain linear relations satisfied by the cycles d_i (points if the corresponding edge has lattice length 1) that eventually determine a Weierstrass model of C . For example, for the pentagons in Notation 6.5, one obtains from Lemma 6.6 and the above argument that

$$E|_C \sim (m-1)d_4 + d_5 \sim (m-1)d_1 + d_2 \sim 4d_2 + \gamma \sim 2d_1 + (m-3)d_4 + d_5.$$

It follows that $2d_4 \sim 2d_1, d_4 + d_5 \sim d_1 + d_2$. Choosing d_1 as the point at infinity and $d_4 = (0, 0)$ for an elliptic curve with Weierstrass equation $y^2 = x^3 + ax^2 + bx$, we obtain a formula for the rational functions f, g whose zeros and poles are as in Lemma 6.4. Along the way, one has to impose the condition that in the linear system given by $(m-1)d_4 + d_5 \sim (m-1)d_1 + d_2 \sim 2d_1 + (m-3)d_4 + d_5$ there exists an element vanishing with multiplicity ≥ 4 at d_2 .

Remark 6.10. Pentagonal curves are fibers C_k of an elliptic fibration $\mathcal{C} \rightarrow \mathbb{P}^1$ with the Weierstrass normal form of Notation 6.3 (the field of rational functions on \mathbb{P}^1 is the field of rational functions in variable k). By Computation 10.9, \mathcal{C} is a rational elliptic fibration of Kodaira type $I_4 I_2^{\oplus 3} I_1^{\oplus 2}$. One can compute the Neron-Tate height of the section of this fibration corresponding to d_2 to conclude that it is not torsion in the Mordell-Weil group of the elliptic fibration. This shows that d_2 is not torsion in a fiber C_k for almost all k by Silverman's specialization theorem [Sil83]. Mazur's theorem gives a more precise statement for every k as above.

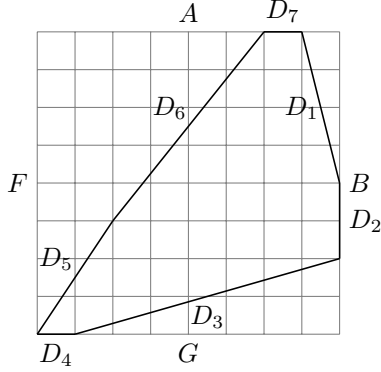


FIGURE 7. Polygon Δ for $k = 2$

An infinite sequence of heptagons. Let $k \geq 2$ be an integer and $m = 2k + 4$. Let Δ be the heptagon with vertices

$$(0, 0), \quad (1, 0), \quad (m, 2), \quad (m, m - 4), \quad (m - 1, m), \quad (m - 2, m), \quad (k, k + 1).$$

Theorem 6.11. *The polygon Δ is Lang–Trotter for every $k \geq 2$. In particular, $\overline{\text{Eff}}(\text{Bl}_e \mathbb{P}_\Delta)$ is not polyhedral in characteristic 0. Furthermore, for all but finitely many k , the set of non-polyhedral primes of Δ has positive density.*

Proof. The strategy is the one in Remark 6.9. The corresponding curve C is a smooth elliptic curve defined over \mathbb{Q} with equation

$$y^2 + exy + by = x^3 + ax^2, \quad \text{where}$$

$$e = -(4k + 2), \quad a = -\frac{k(2k + 1)}{k + 2}, \quad b = \frac{4k(k + 1)^4(2k + 1)}{(k + 2)^2(k - 1)^2}.$$

Labeling the edges and the corresponding torus invariant divisors in \mathbb{P}_Δ as in Figure 7, we let $d_i = \chi^{-1}(D_i)$. Then d_2 is an effective divisor of degree $m - 6$ and all d_i for $i \neq 2$ are points on C . Let \tilde{d}_4 be defined by $d_4 + \tilde{d}_4 \sim 2d_3$. The points d_i have the following properties:

$$d_1 + d_7 \sim 2d_3, \quad d_5 + d_6 \sim 2d_3, \quad 2d_6 + \tilde{d}_4 \sim 3d_3.$$

We choose d_3 to be the point at infinity $[0, 1, 0]$. In our Weierstrass model, the following lines intersect C at the following points with multiplicities:

$$x = 0 : d_5 + d_6 + d_3, \quad y = 0 : 2d_6 + \tilde{d}_4,$$

$$x = x_0 : d_1 + d_7 + d_3, \quad x = -a : d_4 + \tilde{d}_4.$$

The points are $d_6 = (0, 0)$, $d_5 = (0, -b)$, $\tilde{d}_4 = (-a, 0)$, $d_4 = (-a, ae - b)$, $d_1 = (x_0, y_0)$, $d_7 = (x_0, y_1)$, where $y_1 = -y_0 - ex_0 - b$ and

$$x_0 = \frac{2k(k + 1)^2}{(k - 1)(k + 2)}, \quad y_0 = -\frac{2k(k + 1)^2(5k + 3)}{(k - 1)^2(k + 2)}.$$

The torus invariant divisors D_1, \dots, D_7 satisfy

$$D_1 + kD_5 + (k + 2)D_6 + D_7 \sim (m - 1)D_3 + D_4, \quad 4D_1 + D_2 + 2D_3 \sim (k + 1)D_5 + (k + 3)D_6.$$

Using that $C \cdot D_i = 1$ ($i \neq 2$), $C \cdot E = m$, we obtain that in $\text{Cl}(\text{Bl}_e \mathbb{P}_\Delta)$ we have

$$C \sim -4D_1 + (m-2)(m-1)D_3 + mD_4 + mD_5 + (m+2)D_6 - mE.$$

There are three one-parameter subgroups C_1, C_2, C_3 corresponding to lattice directions $\lambda_1 = (1, 0)$, $\lambda_2 = (0, 1)$, $\lambda_3 = (1, -1)$, and with respect to which the width of Δ is m (hence, $C \cdot C_i = 0$ for $i = 1, 2, 3$). It follows that the following hold on C

$$\begin{aligned} d_1 + d_7 &\sim d_5 + d_6 \sim d_4 + \tilde{d}_4 \sim 2d_3, & 2d_6 + \tilde{d}_4 &\sim 3d_3, \\ \mathcal{O}(C)|_C &= \mathcal{O}(2d_3 + 2d_6 - 4d_1). \end{aligned}$$

There is a map $\phi : C \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$, corresponding to rays λ_1, λ_2 , and given by rational functions

$$\begin{aligned} f(x, y) &= \frac{x^{k+1}y}{\alpha(x-x_0-1) + \beta(x+a)}, & g(x, y) &= \frac{x+a}{x^k(x-x_0)y}, \\ \text{where } \alpha &= x_0 + a = \frac{k(5k+3)}{(k-1)(k+2)}, & \beta &= x_0^{k+1}y_0. \end{aligned}$$

The pullbacks of the torus invariant divisors of $\mathbb{P}^1 \times \mathbb{P}^1$ corresponding to the edges A, B, F, G correspond to the zeros and poles of f, g by $f = F/B$, $g = G/A$. The map ϕ is birational onto its image. Letting u, v be coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$ and solving for x, y in $f(x, y) = u$, $g(x, y) = v$, we obtain that $\phi(C)$ has equation

$$\begin{aligned} &((\alpha\beta)uv + (\alpha x_0)u - a)h_2(u, v)^{m-1} - h_1(u, v)^{m-2}h_3(u, v)^2v^2 + \\ &+ (\beta(b + ex_0)uv + (ex_0\alpha)u - b)h_1(u, v)^k h_2(u, v)^{k+2}h_3(u, v)v = 0, \quad \text{where} \\ h_1(u, v) &= (x_0\beta)uv + (x_0\alpha)u, \quad h_2(u, v) = (\beta)uv - 1, \quad h_3(u, v) = (x_0\alpha)u + x_0. \end{aligned}$$

It is straightforward to check that this equation has Δ as its Newton polygon.

One computes the classes of the one-parameter subgroups C_1, C_2, C_3 as

$$\begin{aligned} C_1 &\sim (k+1)D_5 + (k+3)D_6 - E, & C_2 &\sim (m-1)D_3 + D_4 - E, \\ C_3 &\sim (m-3)D_3 + D_4 + D_5 + D_6 - E. \end{aligned}$$

It follows that $K + C \sim C_1 + (k+1)C_2 + (k+1)C_3$.

Computation 10.9 (based on Mazur's theorem as in § 6) shows that $\mathcal{O}(C)|_C$ is not torsion for $k \geq 2$ by showing that $\mathcal{O}(2d_1 - d_6 - d_3)$ is not torsion. In particular, Δ is a Lang–Trotter polygon in this range. The point $p \in C$ such that $\mathcal{O}(2d_1 - d_6 - d_3) = \mathcal{O}(p - d_3)$ is given by

$$x = \frac{4k(k+1)^2(2k+1)}{(k-1)^2(k+2)}, \quad y = \frac{4k^2(k+1)^2(2k+1)(3k+1)}{(k-1)^2(k-2)}.$$

Denote $X = \text{Bl}_e \mathbb{P}_\Delta$ and let $\pi : X \rightarrow Y$ be the map that contracts the one parameter subgroups C_1, C_2 and C_3 . We now compute directly generators $\text{Cl}(Y)$ and $\text{Cl}_0(Y)$. The group $\text{Cl}(X)$ is generated over \mathbb{Z} by D_1, D_3, D_4, D_5, D_6 and E . It follows that C^\perp is generated over \mathbb{Z} by

$$D_3 - D_1, \quad D_4 - D_1, \quad D_5 - D_1, \quad D_6 - D_1, \quad E - mD_1.$$

Denote by \bar{D}_i, \bar{E} the classes of D_i, E in $\text{Cl}(Y)$. Setting the classes of C_1, C_2, C_3 to zero, we obtain the following relations in $\text{Cl}(Y)$:

$$\bar{D}_4 = 3\bar{D}_3 - 2\bar{D}_5, \quad \bar{D}_6 = 2\bar{D}_3 - \bar{D}_5, \quad \bar{E} = (m+2)\bar{D}_3 - 2\bar{D}_5.$$

Then $\text{Cl}(Y)$ is generated by $\bar{D}_1, \bar{D}_3, \bar{D}_5$ and $C_Y^\perp \subseteq \text{Cl}(Y)$ is generated by

$$\alpha := \bar{D}_3 - \bar{D}_1, \quad \beta := \bar{D}_5 - \bar{D}_1,$$

with $\overline{D}_4 - \overline{D}_1 = 3\alpha - 2\beta$, $\overline{D}_6 - \overline{D}_1 = 2\alpha - \beta$, $\overline{E} - m\overline{D}_1 = (m+2)\alpha - 2\beta$. Since the class of C_Y can be expressed as $6\alpha - 2\beta$, it follows that

$$\mathbb{E}_8/T = \text{Cl}_0(Y) = \mathbb{Z}\{\alpha, \beta\}/\mathbb{Z}\{6\alpha - 2\beta\} \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The class of C is divisible by 2. In $\text{Cl}_0(Y)$ the class $\frac{1}{2}C_Y = 3\alpha - \beta$ is the unique non-zero torsion element. It follows that there is a commutative diagram

$$\begin{array}{ccc} \mathbb{E}_8/T = \text{Cl}_0(Y) & \xrightarrow{\overline{\text{res}}} & \text{Pic}^0(C)/\langle \text{res}(C) \rangle \\ \downarrow & & \downarrow \\ \mathbb{E}_8/\hat{T} = \text{Cl}_0(Y)/\text{torsion} & \longrightarrow & \text{Pic}^0(C)/\langle \text{res}(\frac{1}{2}C) \rangle \end{array} \quad (6.2)$$

One can compute directly using a resolution of X that the root lattice is

$$T = \mathbb{A}_3 \oplus \mathbb{A}_2 \oplus \mathbb{A}_1^2.$$

There is a unique embedding of T in \mathbb{E}_8 and it follows that the group \mathbb{E}_8/T is isomorphic to $\mathbb{Z}\{a, b\}/\mathbb{Z}\{6a + 2b\}$, with the roots in $\mathbb{E}_8 \setminus \hat{T}$ having image in \mathbb{E}_8/T belonging to the set $\{\pm a, \pm b, \pm(a+b), \pm(2a+b)\}$. It follows that in $\mathbb{E}_8/\hat{T} \cong \mathbb{Z}$, we have $a = \pm\alpha$ and in $\mathbb{E}_8/\hat{T} \cong \mathbb{Z}$ the images of these roots are the classes of $\{\pm\alpha, \pm 2\alpha, \pm 3\alpha\}$. In order to prove that $\overline{\text{res}}(\gamma) \neq 0$ for any root $\gamma \in \mathbb{E}_8 \setminus \hat{T}$ (for some characteristic p), by (6.2) it suffices to prove that $\text{res}(\alpha)$ is not in the subgroup generated by $\text{res}(\frac{1}{2}C)$. To prove that this holds for a set of primes of positive density, we apply Lemma 5.2 to

$$x_i = \text{res}(i\alpha) = \mathcal{O}_C(id_3 - id_1), \quad x_0 = \text{res}(\frac{1}{2}C) = \mathcal{O}(d_3 + d_6 - 2d_1)$$

for $i = 1, 2, 3$. We check that the conditions in the lemma are satisfied. The curve C does not have complex multiplication because its j -invariant

$$\frac{-4096(k^{12}+1)-24576(k^{11}+k)-58368(k^{10}+k^2)-66560(k^9+k^3)-9216(k^8+k^4)+92160(k^7+k^5)+141312k^6}{27(k^8+4k^7+6k^6+4k^5+k^4)}$$

is not an integer (see [Sil94, Thm. II.6.1]). We already proved that x_0 is not torsion in $\text{Pic}^0(C)$. To prove that x_1 also has infinite order, it suffices to prove that $\mathcal{O}(d_6 - d_1)$ is not torsion, which follows again by Computation 10.9 (based on Mazur's theorem as in §6). It remains to prove that $\text{res}(\alpha)$ and $\text{res}(\frac{1}{2}C)$ (equivalently, $\mathcal{O}_C(d_1 - d_3)$ and $\mathcal{O}_C(d_6 - d_3)$) are linearly independent for almost all k . Using Silverman's specialization theorem [Sil09, App. C, Thm. 20.3] for the elliptic fibration defined by all the heptagonal curves C for $k \geq 2$ (see Remark 6.13), it suffices to prove the statement for a specific k , which we do by a computer calculation. \square

Remark 6.12. The Mordell-Weil group of C is \mathbb{Z} for $k = 2$ and $\mathbb{Z} \times \mathbb{Z}$ for $3 \leq k \leq 6$.

Remark 6.13. "Heptagonal" curves C for $k \geq 2$ can be viewed as fibers C_k of an elliptic fibration $\mathcal{C} \rightarrow \mathbb{P}^1$ with the Weierstrass normal form of Notation 6.3 (here the field of rational functions on \mathbb{P}^1 is the field of rational functions in parameter k). By Computation 10.9, \mathcal{C} is a K3 elliptic fibration of Kodaira type $I_4^{\oplus 3}IV^{\oplus 3}$.

7. A SMOOTH LANG–TROTTER POLYGON

In this section we discuss an example of a minimal elliptic pair (C, Y) with Y smooth and such that $\text{Pic}^0(C)(\mathbb{Q})$ has rank 9. Let $\Delta \subseteq \mathbb{Q}^2$ be the lattice polytope whose vertices are the 19 columns of the following matrix:

$$\begin{bmatrix} 3 & 6 & 8 & 23 & 27 & 30 & 30 & 29 & 21 & 18 & 16 & 13 & 12 & 11 & 9 & 7 & 1 & 0 & 0 \\ 0 & 1 & 2 & 12 & 15 & 18 & 19 & 20 & 26 & 28 & 29 & 30 & 30 & 29 & 25 & 20 & 4 & 1 & 0 \end{bmatrix}$$

The polygon Δ has width $m := 30$, which is obtained along the directions $[1, 0]$, $[0, 1]$, $[1, -1]$. Its volume is m^2 and it has m boundary points. It follows that any curve in the linear system $\mathcal{L}_\Delta(m)$ has arithmetic genus one. A computer calculation shows that $\mathcal{L}_\Delta(m)$ is zero-dimensional and that its unique element is an irreducible curve of geometric genus one, whose defining polynomial has Newton polygon Δ . Thus we get an elliptic pair (C, X) , where X is the blowing-up of the toric surface defined by Δ and C is the strict transform of the unique curve linearly equivalent to the following Weil divisor:

$$[19 \ 30 \ 12 \ 7 \ 7 \ 1 \ 0 \ 0 \ 1 \ 3 \ 6 \ 16 \ 11 \ 29 \ 48 \ 117 \ 187 \ 72 \ 30 \ -30]$$

where the first 19 entries are the coordinates of the pullbacks D_1, \dots, D_{19} of the prime invariant divisors of the toric variety, while the last coordinate is the coefficient of the exceptional divisor E . Observe that X is smooth of Picard rank 18. The linear system $|K_X + C|$ contains eight disjoint (-1) -curves, three of which come from the one-parameter subgroups defined by the width directions of Δ , while the remaining ones come from curves of multiplicity 2, 3, 5, 5, 11 at $(1, 1)$. A list of eight Weil divisors, each of which is linearly equivalent to one of the above eight curves, is given by the rows of the following matrix, where we have kept the same notation used for the curve C above:

$$\begin{bmatrix} 1 & 3 & 2 & 3 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 5 & 8 & 3 & -1 \\ 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 5 & 2 & 1 & -1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 2 & 3 & 8 & 13 & 5 & -2 \\ 2 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 3 & 5 & 12 & 19 & 7 & -3 \\ 3 & 5 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 2 & 5 & 8 & 20 & 32 & 12 & -5 \\ 3 & 5 & 2 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 3 & 2 & 5 & 8 & 19 & 31 & 12 & -5 \\ 7 & 11 & 4 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 2 & 6 & 4 & 11 & 18 & 44 & 70 & 27 & -11 \end{bmatrix}$$

Each of the divisors D_2, D_5 and D_{12} is a (-1) -curve of X , having intersection number 1 with C , so that it is disjoint from the curves in $|K_X + C|$. This claim can be easily proved looking at the primitive generators $\varrho_1, \dots, \varrho_{19}$ of the normal fan of Δ . For example $\varrho_1 = [0, 1]$, $\varrho_2 = [-1, 3]$, $\varrho_3 = [-1, 2]$ show that D_2 is a (-1) -curve, so that the equality $D_2 \cdot C = D_2 \cdot (19D_1 + 30D_2 + 12D_3)$ gives $D_2 \cdot C = 1$. A similar analysis can be performed for the divisors D_5 and D_{12} . As a consequence each of the three divisors remains a (-1) -curve in Y , after contracting the curves in $|K_X + C|$. In particular the linear system $|C + D_2 + D_5 + D_{12}|$ defines a rational map which factorizes through Y , and there it is defined by $|-K_Y + D_2 + D_5 + D_{12}|$. The image of Y via this linear system is a smooth cubic surface of \mathbb{P}^3 whose equation can be calculated by determining the unique cubic relation between the elements of a basis of $H^0(X, C + D_2 + D_5 + D_{12})$. A distinguished basis of the latter vector space is given by a defining polynomial f_0 for C together with three polynomials f_2, f_5, f_{12} , such that $\{f_0, f_i\}$ is a basis of $H^0(X, C + D_i)$. If we denote by $\varphi_i: X \rightarrow X_i$ the contraction of D_i then $C + D_i$ is the pullback of $\varphi_i(C)$ and thus we have an

isomorphism $H^0(X, C + D_i) \simeq H^0(X_i, \varphi_i(C))$. The curve $\varphi_i(C)$ is defined by a modification Δ_i of the polygon Δ obtained in the following way: the $(i-1)$ -th and $(i+1)$ -th edges are extended up to their intersection point. The latter is an integer point if and only if the equation $\varrho_{i-1} + \varrho_{i+1} = \varrho_i$ holds, equivalently if D_i is a (-1) -curve on X . We display the construction of the polygon Δ_i in the following picture.



The normal fan to Δ_i coincides with that of Δ at all rays but ϱ_i . The dimension of the linear system increases by one because a new monomial, corresponding to the new point, has been added. A minimal model for the curve C has equation $y^2 = x^3 + x^2 - 7860946299156x + 8357826814810214400$. Ordering counterclockwise the facets of Δ , starting from the facet $(0, 0) - (3, 0)$, the indices of facets of integer length one are $\{2, 3, 5, 7, 8, 10, 11, 12, 13, 14, 16, 18, 19\}$. For each such index one can compute the point $d_i \in C(\mathbb{Q})$ cut out by the corresponding toric invariant divisor D_i . This information is then used to compute the images of the 240 roots and to determine the non-polyhedral primes of X . Using Computation 10.10 we found 85 non-polyhedral primes in the interval $[1, 2000]$, or 28%.

8. HALPHEN POLYGONS

We consider a variant of the notion of arithmetic elliptic pairs as follows:

Definition 8.1. Let (C, X) be an elliptic pair with $e := e(C, X) < \infty$, defined over a finite extension K of \mathbb{Q} . Let $R \subset K$ be its ring of algebraic integers. There exists a dense open subset $U \subset \text{Spec } R$ and a pair of schemes $(\mathcal{C}, \mathcal{X})$ flat over U , which we call an *arithmetic elliptic pair of finite order* $e < \infty$, such that

- Each geometric fiber (C, X) of $(\mathcal{C}, \mathcal{X})$ is an elliptic pair of order e .
- The contraction morphism $X \rightarrow Y$ to the minimal elliptic pair extends to the contraction of schemes $\mathcal{X} \rightarrow \mathcal{Y}$ flat over U .

We call $(\mathcal{C}, \mathcal{Y})$ the *associated minimal arithmetic elliptic pair*. Let X, Y be geometric fibers over a place $b \in U$, $b \neq 0$. As before, we call b a *polyhedral prime* if $\overline{\text{Eff}}(Y)$ is polyhedral. If b is not polyhedral, then $\overline{\text{Eff}}(X)$ is also not polyhedral.

Since over \mathbb{C} the subgroup $\langle \text{res}(C) \rangle \subset \text{Pic}^0(C)$ is finite of order $e < \infty$, the order of the elliptic pair given by each geometric fiber of $(\mathcal{C}, \mathcal{X})$ stays constant on an open set in $\text{Spec } R$, as it is defined by the condition that $i \text{res}(C) \neq 0$, for $i = 1, \dots, e-1$.

Proposition 8.2. *Let $(\mathcal{C}, \mathcal{X})$ be an arithmetic elliptic pair of finite order $e < \infty$ over some open set $U \subset \text{Spec } R$. Let $(\mathcal{C}, \mathcal{Y})$ be the associated minimal arithmetic elliptic pair. Assume that*

- *The geometric fiber $Y_{\mathbb{C}}$ of \mathcal{Y} has Du Val singularities,*
- *The cone $\overline{\text{Eff}}(Y_{\mathbb{C}})$ is not polyhedral.*

Then all but finitely many primes $b \in U$ are non-polyhedral.

Proof. If the minimal elliptic pair $(C_{\mathbb{C}}, Y_{\mathbb{C}})$ has du Val singularities, by replacing U with a smaller open set, we may assume that all geometric fibers (C, Y) of $(\mathcal{C}, \mathcal{Y})$ over U are minimal elliptic pairs of order e , with Du Val singularities and the same root lattice $T \subseteq \mathbb{E}_8$. Indeed, there exists a scheme \mathcal{Z} , smooth over (a possibly

smaller) U , and a morphism $\pi : \mathcal{Z} \rightarrow \mathcal{Y}$, flat over U , such that on geometric generic fibers Z and Y , of \mathcal{Z} and \mathcal{Y} , this gives the minimal resolution $Z \rightarrow Y$. We may assume that the exceptional locus of π has geometric irreducible components $\mathcal{E}_1, \dots, \mathcal{E}_r \subset \mathcal{Z}$, smooth over U , such that the geometric generic fibers E_1, \dots, E_r are the exceptional (-2) -curves of the resolution $Z \rightarrow Y$. As each \mathcal{E}_i is flat over U , intersection numbers $E_i \cdot E_j$ of the geometric generic fibers do not depend on $b \in U$. In particular, the root lattice is the same for all $b \in U$, and all geometric fibers of $\mathcal{Y} \rightarrow U$ have Du Val singularities.

Consider now any geometric fiber (C, Y) of $(\mathcal{C}, \mathcal{Y})$ and let $Z \rightarrow Y$ be its minimal resolution. Recall that by Lemma 3.14 and Cor. 3.18, the cone $\overline{\text{Eff}}(Y)$ is polyhedral if and only if $\overline{\text{Eff}}(Z)$ is polyhedral, or equivalently, the kernel of the map

$$\overline{\text{res}} : \text{Cl}_0(X) := C^\perp / \langle K \rangle \rightarrow \text{Pic}^0(C) / \langle \text{res}(K) \rangle$$

contains 8 linearly independent roots of $\mathbb{E}_8 = \text{Cl}_0(Z)$. By assumption, the subgroup $\langle \text{res}(C) \rangle$ of $\text{Pic}^0(C)$ is finite of fixed order $e < \infty$, for all geometric fibers. By Theorem 3.8, $C \sim n(-K)$ for some integer n . It follows that the subgroup $\langle \text{res}(K) \rangle$ of $\text{Pic}^0(C)$ is finite of order $\leq e$ for every geometric fiber. Since there are finitely many roots in \mathbb{E}_8 , it follows that by eventually discarding a finite set of places $b \in U$, $b \neq 0$, the maximum number of linearly independent roots of $\mathbb{E}_8 = \text{Cl}_0(Z)$ contained in $\ker(\overline{\text{res}})$ is constant. This finishes the proof. \square

As in Notation 5.1, we may consider arithmetic *toric* elliptic pairs of finite order. Consider a lattice polygon $\Delta \subseteq \mathbb{Z}^2$ and let \mathcal{P} be the projective toric scheme over $\text{Spec } \mathbb{Z}$ given by the normal fan of Δ . Let \mathcal{X} be the blow-up of \mathcal{P} along the identity section of the torus group scheme. We will assume that Δ is a good, but not Lang–Trotter polygon, a so-called Halphen polygon (Def. 4.3). Then $(C_{\mathbb{C}}, X_{\mathbb{C}})$ is an elliptic pair of finite order $e := e(C_{\mathbb{C}}, X_{\mathbb{C}}) < \infty$ and $(\mathcal{C}, \mathcal{X})$ an arithmetic elliptic pair of finite order, flat over an open subset $U \subset \text{Spec } \mathbb{Z}$ (Def. 8.1). Let $\mathcal{X} \rightarrow \mathcal{Y}$ be the morphism inducing the map to the minimal model on each geometric fiber.

Definition 8.3. A polygon $\Delta \subseteq \mathbb{Z}^2$ such that the associated toric arithmetic elliptic pair $(\mathcal{C}, \mathcal{X})$ satisfies the conditions in Proposition 8.2 will be called a *Halphen⁺* polygon.

Theorem 8.4. *Let Δ be a Halphen⁺ polygon. Then $\overline{\text{Eff}}(X_{\Delta})$ is not polyhedral in characteristic 0 and characteristic p , for all but finitely many primes p .*

Proof. This is an immediate consequence of Proposition 8.2. \square

Theorem 8.5. *Consider the polygon Δ with vertices:*

$$\begin{bmatrix} 0 & 1 & 6 & 8 & 7 & 5 & 1 \\ 0 & 0 & 1 & 2 & 5 & 8 & 2 \end{bmatrix}$$

Then Δ is a Halphen⁺ polygon and $\overline{\text{Eff}}(X_{\Delta})$ is not polyhedral in characteristic 0, and in characteristic p for all primes $p \neq 2, 3, 5, 7, 11, 19, 71$.

We will use this polygon later in the proof of Theorem 1.2.

Proof. We have $\text{Vol}(\Delta) = 64$ and $|\partial\Delta \cap \mathbb{Z}| = 8$ (see Computation 10.3). By Computation 10.4, in characteristic 0 the linear system $\mathcal{L}_{\Delta}(8)$ has dimension 0 and the

unique curve $\Gamma \in \mathcal{L}_\Delta(8)$ has equation

$$\begin{aligned} & 4u^8v^2 + 24u^7v^5 - 61u^7v^4 + 58u^7v^3 - 53u^7v^2 + 10u^6v^6 - 126u^6v^5 + \\ & + 244u^6v^4 - 186u^6v^3 + 150u^6v^2 + 20u^6v - u^5v^8 + 8u^5v^7 - 48u^5v^6 + \\ & + 230u^5v^5 - 286u^5v^4 + 120u^5v^3 - 159u^5v^2 - 88u^5v + 10u^4v^6 - 66u^4v^5 - \\ & - 56u^4v^4 + 144u^4v^3 + 94u^4v^2 + 154u^4v - 6u^3v^5 + 89u^3v^4 - 26u^3v^3 - \\ & - 135u^3v^2 - 146u^3v - 54u^2v^3 + 52u^2v^2 + 114u^2v + 19uv^2 - 46uv - 5u + 4 = 0. \end{aligned}$$

The exponents of the red monomials are the vertices of Δ , so that the Newton polygon of Γ is Δ in characteristic 0 and characteristic $p \neq 2, 3, 5, 19$. By Computations 10.5 and 10.8, the curve Γ is irreducible and its strict transform $C \subseteq X_\Delta$ is a smooth elliptic curve in characteristic 0, with minimal equation

$$y^2 + xy + y = x^3 + x^2 - 520x + 4745. \quad (8.1)$$

This is the curve labelled 2130.j4 in the LMFDB database [LMF20]. The Mordell–Weil group is $\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. By Computation 10.4, in characteristic 0 the linear system $\mathcal{L}_{k\Delta}(8k)$ has dimension 0 if $k = 2, 3$ and dimension 1 if $k = 4$. It follows that $\text{res}(C) \in \text{Pic}^0(C)(\mathbb{Q})$ is torsion, of order $e = 4$. Hence, Δ is a Halphen polygon.

The theorem now follows from Computation 10.11. We give the details. By Computation 10.11, the curve C is irreducible and smooth in characteristic 0 or characteristic $p \neq 2, 3, 5, 7, 11, 19, 71$. Unless otherwise specified, we will from now on assume we are in one of these situations.

The normal fan of Δ has rays $v_1 = (0, 1)$, $v_2 = (-1, 5)$, $v_3 = (-1, 2)$, $v_4 = (-3, -1)$, $v_5 = (-3, -2)$, $v_6 = (3, -2)$, $v_7 = (2, -1)$. We denote D_1, \dots, D_7 the corresponding torus invariant divisors in \mathbb{P}_Δ , and abusing notations, also their pullbacks to X_Δ . The divisors D_1, \dots, D_5, E form a basis for $\text{Cl}(X)$ and we have:

$$D_6 \sim 2D_1 + 9D_2 + 3D_3 - 5D_4 - 7D_5, \quad D_7 \sim -3D_1 - 13D_2 - 4D_3 + 9D_4 + 12D_5,$$

$$K_X \sim 3D_2 - 5D_4 - 6D_5 + E, \quad C \sim 2D_1 + 10D_2 + 7D_3 + 21D_4 + 24D_5 - 8E.$$

Note, the class of C is independent of the characteristic if the Newton polygon stays the same. Since Δ has lattice width 8 in the horizontal and vertical direction, the proper transforms C_1 and C_2 on X_Δ of the 1-parameter subgroups ($u = 1$) and ($v = 1$), are among the curves that must be contracted by the morphism $X \rightarrow Y$ to the associated minimal elliptic pair. Using Computation 10.6 we find that $K_X + C = 2C_1 + 2C_2 + C_3$, with curves C_i with classes

$$C_1 \sim D_2 + D_3 + 3D_4 + 3D_5 - E \quad C_2 \sim D_1 + 5D_2 + 2D_3 - E,$$

$$C_3 \sim D_2 + D_3 + 10D_4 + 12D_5 - 3E.$$

Computation 10.6 gives that the curve C_3 has equation

$$u^3v - u^2v^3 + 3u^2v^2 - 5u^2v + uv + 2u - 1 = 0,$$

and so its Newton polygon has vertices $(0, 0)$, $(1, 0)$, $(3, 1)$, $(2, 3)$ in all characteristics other than 2. This polygon has no non-trivial Minkowski decompositions, so the curve C_3 is irreducible in the situations we consider. The curves C_1 , C_2 are irreducible in all characteristics, as they are proper transforms of 1-parameter subgroups.

From the intersection numbers $D_i \cdot D_j$ on \mathbb{P}_Δ (or using Computation 10.7) we find that $C_1^2 = -\frac{1}{4}$, $C_2^2 = -\frac{3}{14}$, $C_3^2 = -\frac{8}{3}$ and $C_i \cdot C_j = 0$ for all $i \neq j$. Since the intersection matrix $(C_i \cdot C_j)_{i,j}$ is negative definite, it follows that the Zariski

decomposition of $K_X + C = N + P$ has the positive part $P \sim 0$. By Theorem 3.10, the minimal model Y has Du Val singularities. Denote \bar{D} the class of a divisor D in $\text{Cl}(Y)$. Setting the classes of C_1, C_2, C_3 to zero, we obtain that $\text{Cl}(Y)$ is freely generated by \bar{D}_2, \bar{D}_3 and \bar{D}_5 and

$$\bar{D}_1 \sim 2\bar{D}_2 + 5\bar{D}_3 - 6\bar{D}_5, \quad \bar{D}_4 \sim 2\bar{D}_2 + 2\bar{D}_3 - 3\bar{D}_5,$$

$$\bar{E} \sim 7\bar{D}_2 + 7\bar{D}_3 - 6\bar{D}_5, \quad C_Y = \bar{C} \sim 3\bar{D}_3 - 3\bar{D}_5.$$

We consider $\alpha := \bar{D}_2 - \bar{D}_5, \beta := \bar{D}_3 - \bar{D}_5$ in $\text{Cl}(Y)$. Then $C_Y^\perp = \mathbb{Z}\{\alpha, \beta\}$ and

$$\text{Cl}_0(Y) = \mathbb{Z}\{\alpha, \beta\} / \mathbb{Z}\{3\beta\} = \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

By Computation 10.7, or using a minimal resolution of \mathbb{P}_Δ , the root lattice is $T = \mathbb{A}_2^3 \oplus \mathbb{A}_1$ and $\rho(Y) = 3$. By Cor. 3.18, the cone $\overline{\text{Eff}}(Y)$ is non-polyhedral if and only if $\overline{\text{res}}(\gamma) \neq 0$, for all roots $\gamma \in \mathbb{E}_8 \setminus \hat{T}$. There is a unique way to embed $\mathbb{A}_2^3 \oplus \mathbb{A}_1$ in \mathbb{E}_8 ([OS91][p.86]). There are generators a, b of \mathbb{E}_8/T with $\text{ord}(a) = \infty, \text{ord}(b) = 3$ such that the images of the roots of \mathbb{E}_8 in $\text{Cl}_0(Y) = \mathbb{E}_8/T$ are

$$\pm ka \ (k = 0, 1, 2, 3, 12), \quad \pm(ka - b) \ (k = 2, 3, 4, 5, 6), \quad \pm(ka - 2b) \ (k = 6, 7, 8, 9, 10).$$

The sets of generators $\{a, b\}, \{\alpha, \beta\}$ of $\text{Cl}_0(Y)$ are related by $b \in \{\pm\beta\}, a \in \{\pm\alpha, \pm\alpha \pm \beta\}$. The images of the roots of \mathbb{E}_8 in $\text{Cl}_0(Y)$, in terms of α, β , are

$$\pm k\alpha \ (k = 0, 1, 2, 3, 4, 5, 7, 8, 10, 12), \quad \pm k\alpha \pm \beta \ (k = 1, \dots, 10).$$

We denote d_i the effective divisor on C such that $\mathcal{O}(d_i) = \mathcal{O}(D_i)|_C$. For every $i \neq 6$, we have that $d_i \in C(\mathbb{Q})$. It follows that in $\text{Pic}^0(C)$ we have

$$\text{res}(\alpha) = \mathcal{O}_C(d_2 - d_5), \quad \text{res}(\beta) = \mathcal{O}_C(d_3 - d_5).$$

Using Computation 10.8, the points $d_2, d_3, d_5 \in \text{Pic}^0(C)(\mathbb{Q})$, using (8.1), are $d_2 = (9, 25), d_3 = (23, 63), d_5 = (53, -387)$. Using Magma, we compute

$$\text{res}(\alpha) = (-7, 93), \quad \text{res}(\beta) = (13, 13), \quad \text{res}(2\beta) = (-27, 13), \quad \text{res}(3\beta) = (13, -27),$$

and the order of $\text{res}(\beta)$ in $\text{Pic}^0(C)(\mathbb{Q})$ is 4. As C has class 3β in $\text{Cl}_0(Y)$, it follows that $\overline{\text{Eff}}(Y)$ is non-polyhedral (in some characteristic) if and only if none of

$$\text{res}(k\alpha) \ (k = 1, 2, 3, 4, 5, 7, 8, 10, 12), \quad \text{res}(k\alpha \pm \beta) \ (k = 1, \dots, 10)$$

belong to $\{0, \text{res}(\beta), \text{res}(2\beta), \text{res}(3\beta)\}$ of $\text{Pic}^0(C)$, which is the subgroup generated by $\text{res}(\beta)$ (from the above formulas, one can see that the order of $\text{res}(\beta)$ is 4 in characteristic 0 or $p \neq 2, 5$). Clearly, this is equivalent to $\text{res}(k\beta)$, for all $k = 7, 8, 9, 10, 12$, not belonging to this subgroup. This is done within Computation 10.11, which gives that this is the case for all primes $p \neq 2, 3, 5, 7, 11, 19, 71$. \square

9. ON THE EFFECTIVE CONE OF $\overline{M}_{0,n}$

For any toric variety X , we denote by $\text{Bl}_e X$ the blow-up of X at the identity element of the torus. Let \overline{LM}_n be the Losev–Manin moduli space [LM00], which is also a toric variety. Its curious feature, noticed in [CT15], is that \overline{LM}_n is “universal” among all projective toric varieties. Moreover, $\text{Bl}_e \overline{LM}_n$ is universal among $\text{Bl}_e X$. Here we make this philosophical statement very precise:

Theorem 9.1. *Let X be a projective toric variety. For any n large enough (see the proof for an effective estimate), there exists a sequence of projective toric varieties $\overline{LM}_n = X_1, \dots, X_s = X$ and rational maps induced by toric rational maps*

$$\mathrm{Bl}_e \overline{LM}_n = \mathrm{Bl}_e X_1 \dashrightarrow \mathrm{Bl}_e X_2 \dashrightarrow \dots \dashrightarrow \mathrm{Bl}_e X_s = \mathrm{Bl}_e X.$$

Every map $\mathrm{Bl}_e X_k \dashrightarrow \mathrm{Bl}_e X_{k+1}$ decomposes as a small \mathbb{Q} -factorial modification (SQM) $\mathrm{Bl}_e X_k \dashrightarrow Z_k$ and a surjective morphism $Z_k \rightarrow \mathrm{Bl}_e X_{k+1}$. If the cone $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \overline{LM}_n)$ is (rational) polyhedral then $\overline{\mathrm{Eff}}(\mathrm{Bl}_e X)$ is also (rational) polyhedral.

Remark 9.2. In [CT15] we used an analogous implication that if $\overline{\mathrm{Eff}}(\mathrm{Bl}_e \overline{LM}_n)$ is a Mori Dream Space then $\overline{\mathrm{Eff}}(\mathrm{Bl}_e X)$ is a Mori Dream Space.

The second statement in Thm. 9.1 follows from the first, using Lemma 2.2 and the fact that if $Z \dashrightarrow Z'$ is an SQM, then we can identify $\mathrm{Num}^1(Z)_{\mathbb{R}} = \mathrm{Num}^1(Z')_{\mathbb{R}}$ and $\overline{\mathrm{Eff}}(Z) = \overline{\mathrm{Eff}}(Z')$. The proof of the first statement in Thm. 9.1 is based on the main technical result of [CT15], which we give here in a slightly reformulated form:

Lemma 9.3 ([CT15, Prop. 3.1]). *Let $\pi : N \rightarrow N'$ be a surjective map of lattices with kernel of rank 1 spanned by a vector $v_0 \in N$. Let Γ be a finite set of rays in $N_{\mathbb{R}}$ spanned by elements of N , which includes both rays $\pm R_0$ spanned by $\pm v_0$. Let $\mathcal{F}' \subset N'_{\mathbb{R}}$ be a complete simplicial fan with rays given by $\pi(\Gamma)$ (ignore two zero vectors in the image). Suppose that the corresponding toric variety X' is projective (notice that it is also \mathbb{Q} -factorial because \mathcal{F}' is simplicial). Then there exists a complete simplicial fan $\mathcal{F} \subset N_{\mathbb{R}}$ with rays given by Γ and such that the corresponding toric variety X is projective. Moreover, there exists a rational map $\mathrm{Bl}_e X \dashrightarrow \mathrm{Bl}_e X'$ which decomposes into an SQM $\mathrm{Bl}_e X \dashrightarrow Z$ and a surjective morphism $Z \rightarrow \mathrm{Bl}_e X'$ (of relative dimension 1).*

Corollary 9.4. *Let $\pi : N \rightarrow N'$ be a surjective map of lattices with kernel spanned by vectors $v_1, \dots, v_s \in N$. Let Γ be a finite set of rays in $N_{\mathbb{R}}$ spanned by elements of N , which includes the rays $\pm R_i$ spanned by $\pm v_i$ for $i = 1, \dots, s$. Let $\mathcal{F}' \subset N'_{\mathbb{R}}$ be a complete simplicial fan with rays given by $\pi(\Gamma)$ (ignore zero vectors in the image). Suppose that the corresponding toric variety X' is projective (notice that it is also \mathbb{Q} -factorial because \mathcal{F}' is simplicial). Then there exists a complete simplicial fan $\mathcal{F} \subset N_{\mathbb{R}}$ with rays $\Gamma \cup \{\pm R_1\} \cup \dots \cup \{\pm R_s\}$ and such that the corresponding toric variety X is projective. Moreover, there exists a sequence of toric varieties $X = X_1, \dots, X_s = X'$ and rational maps induced by toric rational maps*

$$\mathrm{Bl}_e X = \mathrm{Bl}_e X_1 \dashrightarrow \mathrm{Bl}_e X_2 \dashrightarrow \dots \dashrightarrow \mathrm{Bl}_e X_s = \mathrm{Bl}_e X'$$

such that every map $\mathrm{Bl}_e X_k \dashrightarrow \mathrm{Bl}_e X_{k+1}$ decomposes as an SQM $\mathrm{Bl}_e X_k \dashrightarrow Z_k$ and a surjective morphism $Z_k \rightarrow \mathrm{Bl}_e X_{k+1}$.

Proof. We argue by induction on s , the case $s = 1$ is Lemma 9.3. We can assume v_1 is a primitive vector. Let $N'' = N/\langle v_1 \rangle$. We have a factorization of π into $\pi_0 : N \rightarrow N''$ and $\pi' : N'' \rightarrow N'$. Let Γ'' be the image under π_0 of Γ (ignore zero vectors in the image). Then we are in the situation of Lemma 9.3. For the map π' , we use the step of the induction. \square

Proof of Theorem 9.1. We follow the same strategy as [CT15].

Applying \mathbb{Q} -factorialization, we can assume that X is a \mathbb{Q} -factorial toric projective variety of dimension r . The toric data of \overline{LM}_n is as follows. Fix general

vectors $e_1, \dots, e_{n-2} \in \mathbb{R}^{n-3}$ such that $e_1 + \dots + e_{n-2} = 0$. The lattice N is generated by e_1, \dots, e_{n-2} . The rays of the fan of \overline{LM}_n are spanned by the primitive lattice vectors $\sum_{i \in I} e_i$, for each subset I of $S := \{1, \dots, n-2\}$ with $1 \leq |I| \leq n-3$. Notice that rays of this fan come in opposite pairs. We are not going to need cones of higher dimension of this fan. We partition

$$S = S_1 \coprod \dots \coprod S_{r+1}$$

into subsets of equal size $m \geq 3$ (so that $n = m(r+1) + 2$). We also fix some indices $n_i \in S_i$, for $i = 1, \dots, r+1$. Let $N'' \subset N$ be a sublattice spanned by the following vectors:

$$e_{n_i} + e_j \quad \text{for } j \in S_i \setminus \{n_i\}, \quad i = 1, \dots, r+1. \quad (9.1)$$

Let $N' = N/N''$ be the quotient group and let π be the projection map. Then we have the following:

- (1) N' is a lattice;
- (2) N' is spanned by the vectors $\pi(e_{n_i})$, for $i = 1, \dots, r+1$;
- (3) $\pi(e_{n_1}) + \dots + \pi(e_{n_{r+1}}) = 0$ is the only linear relation between these vectors.

It follows at once that the toric surface with lattice N' and rays spanned by $\pi(e_{n_i})$ for $i = 1, \dots, r+1$, is a projective space \mathbb{P}^r . Choose a basis f_1, \dots, f_r for the lattice N' so that $\pi(e_{n_1}) = -f_1, \dots, \pi(e_{n_r}) = -f_r$. Fix one of the indices $1, \dots, r+1$, we start with $r+1$. Choose $e = \sum_{i \in I} e_i$ such that $n_1, \dots, n_r \notin I$, $|I \cap S_1| = k_1, \dots, |I \cap S_r| = k_r$ and $|I| = k_1 + \dots + k_r$. Then $\pi(e) = k_1 f_1 + \dots + k_r f_r$ and

$$\pi(e + e_{n_{r+1}}) = (k_1 + 1)f_1 + \dots + (k_r + 1)f_r.$$

It follows that images of the rays of \overline{LM}_n contain all points with non-zero coordinates bounded by m . Repeating this for all $r+1$ octants shows that the images of the rays of \overline{LM}_n span all lattice points within the region illustrated in Figure 8 for $r = 2$, which contains all rays of X if m is large enough. To be precise, for each $i \in \{1, \dots, r\}$, in the octant spanned by

$$f_1 \dots, f_{i-1}, f_{i+1}, \dots, f_{r+1} \quad (f_{r+1} := \pi(-e_{n_{r+1}}) = -f_1 - \dots - f_r),$$

the region containing all the images of rays of \overline{LM}_n is determined by

$$mf_1, \quad \dots, \quad mf_{i-1}, \quad mf_{i+1} \quad \dots \quad mf_{r+1} = -mf_1 - \dots - mf_r.$$

It remains to notice (see [OP91], [CT15, Prop. 3.1]) that there exists a \mathbb{Q} -factorial projective toric variety W with rays given by the images of the rays of \overline{LM}_n and that the toric birational rational map $W \dashrightarrow X$ is a composition of birational toric morphisms and toric SQMs. Thus we are done by Corollary 9.4. \square

Corollary 9.5. *Let Y be a projective toric surface with lattice \mathbb{Z}^2 and with fan spanned by rays contained in the polygon with vertices*

$$(\pm m, \pm m), \quad (0, \pm m), \quad (\pm m, 0),$$

for some $m \geq 3$ (see Figure 8 for $m = 4$). If $\overline{\text{Eff}}(\text{Bl}_e Y)$ is not (rational) polyhedral then $\overline{\text{Eff}}(\overline{M}_{0,3m+2})$ is not (rational) polyhedral.

Proof. We argue by contradiction. If $\overline{\text{Eff}}(\overline{M}_{0,n})$ is (rational) polyhedral then the pseudo-effective cone $\overline{\text{Eff}}(\text{Bl}_e \overline{LM}_n)$ is also (rational) polyhedral by Lemma 2.2 and [CT15, Theorem 1.1]. In this case $\overline{\text{Eff}}(\text{Bl}_e Y)$ is (rational) polyhedral by Theorem 9.1 (and effective estimates in its proof). \square

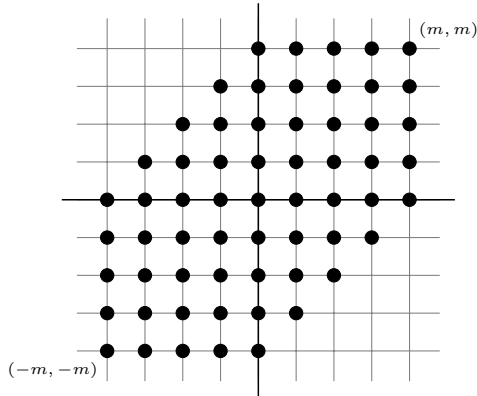


FIGURE 8.

Variations in the choice of projections used in the proof of Thm. 9.1 can lead to further variations and improvements, such as the following:

Corollary 9.6. *Let Y be a projective toric surface with lattice \mathbb{Z}^2 and with fan spanned by rays contained in the polygon with vertices*

$$(\pm l, \pm l), \quad (\pm 1, \mp l), \quad (\pm 1, \mp 1), \quad (\pm l, \mp 1) \quad (9.2)$$

for some $l \geq 2$ (see Figure 9 for $l = 4$). If $\overline{\text{Eff}}(\text{Bl}_e Y)$ is not (rational) polyhedral then $\overline{\text{Eff}}(\overline{M}_{0,2l+5})$ is not (rational) polyhedral.

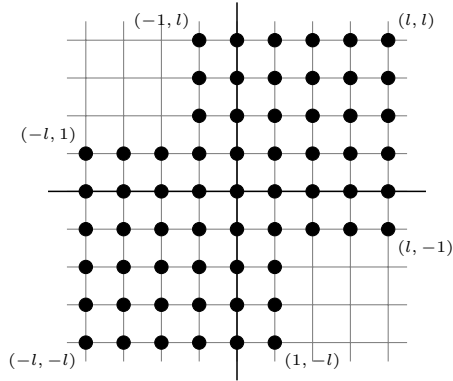


FIGURE 9.

Proof. Similarly, we argue by contradiction. If $\overline{\text{Eff}}(\overline{M}_{0,n})$ is (rational) polyhedral then the pseudo-effective cone $\overline{\text{Eff}}(\text{Bl}_e \overline{LM}_n)$ is also (rational) polyhedral by Lemma 2.2 and [CT15, Theorem 1.1]. In this case $\overline{\text{Eff}}(\text{Bl}_e Y)$ is (rational) polyhedral using the same idea as in the proof of Theorem 9.1. It suffices to prove that one can project in such a way that the images of the rays of the fan of \overline{LM}_n are contained in the polygon given by (9.2).

The rays of the fan of \overline{LM}_n are spanned by the primitive lattice vectors $\sum_{i \in I} e_i$, for each subset I of $S := \{1, \dots, n-2\}$ with $1 \leq |I| \leq n-3$. We partition

$$S = S_1 \coprod S_2 \coprod S_3, \quad |S_1| = |S_2| = l+1, \quad |S_3| = 1.$$

We fix some indices $n_i \in S_i$, for $i = 1, 2$ and let $S_3 = \{n_3\}$. Let $N'' \subset N$ be a sublattice spanned by the following vectors:

$$e_{n_i} + e_j \quad \text{for } j \in S_i \setminus \{n_i\}, \quad i = 1, 2.$$

Let $N' = N/N''$ be the quotient group and let π be the projection map. Then we have the following:

- (1) N' is a lattice;
- (2) N' is spanned by the vectors $\pi(e_{n_i})$, for $i = 1, 2, 3$;
- (3) $-(l-1)\pi(e_{n_1}) + -(l-1)\pi(e_{n_2}) + \pi(e_{n_3}) = 0$ is the only linear relation between these vectors.

Choose a basis f_1, f_2 for the lattice N' given by $\pi(e_{n_1}) = f_1$, $\pi(e_{n_2}) = f_2$. Then

$$\pi(e_{n_3}) = (l-1)f_1 + (l-1)f_2.$$

We calculate the images $\pi(\sum_{i \in I} e_i)$ of the rays of the fan of \overline{LM}_n . Consider the case when $n_1, n_2, n_3 \notin I$. If $|I \cap S_1| = i$, $|I \cap S_2| = j$, then clearly the images of such rays are given by $-if_1 - jf_2$ and all values $0 \leq i, j \leq l$ are possible. This gives a square P which in the given basis, has coordinates

$$(-l, -l), \quad (-l, 0), \quad (0, -l), \quad (0, 0).$$

If $n_1 \in I$, $n_2, n_3 \notin I$, the images $\pi(\sum_{i \in I} e_i)$ will be contained in the translation of P by $f_1 = (1, 0)$. Similarly, if $n_3 \notin I$, then $\pi(\sum_{i \in I} e_i)$ is contained in the union of P with its translates by $f_1 = (1, 0)$, $f_2 = (0, 1)$ and $f_1 + f_2 = (1, 1)$, i.e., the square Q with sides

$$(-l, -l), \quad (-l, 1), \quad (1, -l), \quad (1, 1).$$

Finally, if $n_3 \in I$, then $\pi(\sum_{i \in I} e_i)$ will be contained in the translate Q' of Q by $f_3 = (l-1, l-1)$. Hence, all images of rays are contained in the sum of Q and Q' , i.e., the polygon given in (9.2). \square

Corollary 9.7. *Let Y be a projective toric surface with lattice \mathbb{Z}^2 and with fan spanned by rays contained in the polygon with vertices*

$$(\pm 3, \pm 1), \quad (\pm 3, \pm 5), \quad (\pm 2, \pm 6), \quad (\pm 1, \pm 6), \quad (\pm 1, \mp 3),$$

(see Figure 10). *If $\overline{\text{Eff}}(\text{Bl}_e Y)$ is not (rational) polyhedral then $\overline{\text{Eff}}(\overline{M}_{0,10})$ is not (rational) polyhedral.*

Proof. It suffices to prove that $\overline{\text{Eff}}(\text{Bl}_e \overline{LM}_{10})$ is not (rational) polyhedral. We do a variation of the method in the proof of Thm. 9.1, projecting the lattice \mathbb{Z}^7 of the Losev-Manin space \overline{LM}_{10} (spanned by $\{e_1, \dots, e_8\}$ and subject to the relation $\sum_{i=1}^8 e_i = 0$) from the following rays of the fan of \overline{LM}_{10} : $e_1 + e_2 + e_4 + e_6$, $e_1 + e_2 + e_5 + e_7$, $e_1 + e_4 + e_6 + e_7$, $e_5 + e_6$ and $e_1 + e_5 + e_8$. These vectors generate the kernel of the map $\pi : \mathbb{Z}^7 \rightarrow \mathbb{Z}^2$ given by

$$\begin{pmatrix} 1 & 0 & 1 & -2 & -1 & 1 & 0 \\ 0 & 1 & -1 & -3 & -2 & 2 & 1 \end{pmatrix}$$

We conclude observing that the images of the rays of \overline{LM}_{10} via f are the points of Figure 10. \square

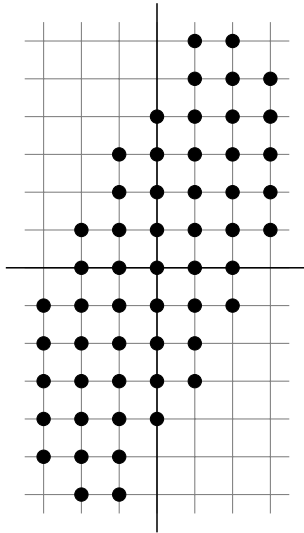


FIGURE 10.

Proof of Theorem 1.2. If the characteristic is 0 or any prime $p \neq 2, 3, 5, 7, 11, 19, 71$, one can use the Halphen⁺ polygon Δ from Theorem 8.5. Indeed, after the shear transformation $(x, y) \mapsto (x, x - y)$, the rays of the normal fan of Δ are

$$(0, -1), \quad (-1, -6), \quad (-1, -3), \quad (-3, -2), \quad (-3, -1), \quad (3, 5), \quad (2, 3),$$

which are among the points of Figure 10, so that we can apply Corollary 9.7.

In order to conclude we are going to produce, for any $p \in \{2, 3, 5, 7, 11, 19, 71\}$, a suitable good lattice polygon Δ , whose normal fan has rays among the points of Figure 10. In particular, since the characteristic is positive, Δ is Halphen, with $e := e(C, X_\Delta) < \infty$. The pencil $|eC|$ defines a fibration $\pi: X \rightarrow \mathbb{P}^1$. Let us denote by $S_i := \pi^{-1}(q_i)$, for $i = 1, \dots, \lambda$, the reducible fibers and by μ_i the number of irreducible components of S_i . It is not hard to see that any such irreducible component is defined over the field \mathbb{F}_p , so we only have to check a finite family. We then conclude showing that

$$\sum_{i=1}^{\lambda} (\mu_i - 1) < \text{Rank}(\text{Pic}(X)) - 2 = \#\text{Vertices}(\Delta) - 3,$$

which, by Remark 2.4, implies that the effective cone is not polyhedral.

In Computation 10.12 we analyze in detail the case $p = 2$, while in the following table we list, for any $p \in \{2, 3, 5, 7, 11, 19, 71\}$, the polygon Δ , the corresponding $e(C, X_\Delta)$, and the cardinality of the reducible fibers.

p	vertices	$e(C, X_\Delta)$	$[\mu_1, \dots, \mu_\lambda]$
2	$\begin{bmatrix} 0 & 6 & 9 & 10 & 9 & 3 & 1 \\ 0 & 2 & 4 & 5 & 6 & 10 & 4 \end{bmatrix}$	1	[2, 3]
3	$\begin{bmatrix} 0 & 5 & 7 & 12 & 13 & 14 & 12 & 6 & 2 \\ 0 & 2 & 3 & 6 & 8 & 11 & 12 & 14 & 6 \end{bmatrix}$	2	[2, 5]

5	$\begin{bmatrix} 0 & 2 & 12 & 13 & 13 & 12 & 11 & 9 & 4 \\ 0 & 1 & 7 & 8 & 9 & 11 & 12 & 13 & 12 \end{bmatrix}$	2	[3, 4]
7	$\begin{bmatrix} 0 & 1 & 4 & 8 & 10 & 4 & 3 & 1 \\ 0 & 0 & 1 & 4 & 7 & 10 & 8 & 3 \end{bmatrix}$	2	[2, 4]
11	$\begin{bmatrix} 0 & 12 & 13 & 13 & 12 & 11 & 9 & 7 & 1 \\ 0 & 4 & 8 & 9 & 11 & 12 & 13 & 12 & 2 \end{bmatrix}$	2	[3, 3]
19	$\begin{bmatrix} 0 & 2 & 8 & 9 & 3 & 2 \\ 0 & 1 & 5 & 6 & 10 & 8 \end{bmatrix}$	2	[2, 2]
71	$\begin{bmatrix} 0 & 3 & 8 & 12 & 13 & 12 & 11 & 5 & 4 \\ 0 & 1 & 4 & 7 & 8 & 10 & 11 & 13 & 12 \end{bmatrix}$	3	[2, 2, 4]

□

Remark 9.8. By Computation 10.3, the rays of the normal fan of Polygon 111 are among the points in Figure 10. By Example 4.8, Δ is a Lang–Trotter polygon, so that by Theorem 4.4, we have another proof that $\overline{\text{Eff}}(X_\Delta)$ is not polyhedral in characteristic 0. Moreover, in Database 10.2, we collect many more Lang–Trotter polygons such that their normal fans (sometimes after a shear transformation) fit into Figure 10. This shows that $\overline{\text{Eff}}(\overline{M}_{0,10})$ is not polyhedral in characteristic p for $p < 2000$. We find that this is a strong indication that one could also use Lang–Trotter polygons to prove that $\overline{\text{Eff}}(\overline{M}_{0,10})$ is not polyhedral in characteristic p , for all primes p .

10. DATABASES AND MAGMA COMPUTATIONS

Database 10.1. We give in Table 4 the list of all Lang–Trotter polygons with $m \leq 7$. It is obtained as follows. We consider all lattice polygons of volume up to 49 (modulo equivalence) appearing in the database [Bal20]. We impose the conditions of Definition 4.3 using our Magma package. Computation 10.3 gives (i) and (ii). Computations 10.4 and 10.5 give (iii), (iv) and the equation of Γ . This leaves 184 lattice polygons and in all the cases the curve C turns out to be smooth by Computation 10.5. Furthermore, for all but one polygon in this list, we also have that the point e is an ordinary multiple point of Γ . The exceptional case is **Polygon 23**, in which case the tangent cone to the curve Γ at e contains a double line. The curve C turns out to be tangent to the exceptional divisor at the corresponding point, so that also in this case C is smooth. Therefore, for any polygon in the list, C is a smooth genus 1 curve and moreover, since Δ has at least 4 vertices and $|\partial\Delta \cap \mathbb{Z}^2| = m \leq 7$, we also have that at least one edge F of Δ has lattice length 1. By Proposition 4.2 we conclude that the curve C has a rational point p_F that we can choose as the origin, so that in what follows we can treat C as an elliptic curve. This fact allows to check the last condition of the definition of a Lang–Trotter polygon, i.e., that $\mathcal{O}_X(C)|_C = \text{res}(C)$ is non-torsion. Indeed, we can compute the minimal equation of the elliptic curve C using Computation 10.8. We are then able to compute the order d of the torsion subgroup of the Mordell–Weil group of the elliptic curve, and we have that $\text{res}(C)$ is not torsion if and only if $\text{res}(dC)$ is non-trivial. By Definition–Lemma 3.2 this is equivalent to $h^0(X, dC) = 1$, and the latter condition can be checked by Computation 10.4.

Another approach is to find a multiple of d using Nagell–Lutz Theorem [ST15]: if p is a prime of good reduction for C , then the specialization map induces an injective homomorphism of abelian groups $C(\mathbb{Q})_{\text{tors}} \rightarrow C(\mathbb{F}_p)$. Therefore, the torsion order d of $C(\mathbb{Q})$ divides the order of $C(\mathbb{F}_p)$ for any prime p of good reduction, which is easy to compute from the defining equation of Γ . We then find a multiple of d by taking the greatest common divisor of the orders of $C(\mathbb{F}_p)$ as p varies.

5	$\begin{bmatrix} 0 & 4 & 2 & 1 & 5 \\ 0 & 4 & 5 & 5 & 3 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 & 2 & 5 & 3 \\ 2 & 4 & 1 & 5 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 & 5 & 1 & 2 \\ 2 & 1 & 0 & 4 & 5 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 & 0 & 5 & 1 \\ 2 & 4 & 5 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 & 0 & 5 & 0 \\ 1 & 5 & 1 & 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 & 0 & 5 & 1 \\ 1 & 4 & 5 & 2 & 0 \end{bmatrix}$
6	$\begin{bmatrix} 1 & 0 & 6 & 5 & 6 \\ 3 & 4 & 2 & 6 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 & 0 & 5 & 6 \\ 0 & 0 & 6 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 6 & 0 & 2 & 1 & 0 \\ 4 & 2 & 1 & 6 & 0 \end{bmatrix}$	$\begin{bmatrix} 5 & 1 & 6 & 6 & 0 \\ 6 & 5 & 1 & 0 & 4 \end{bmatrix}$	$\begin{bmatrix} 2 & 5 & 0 & 7 & 5 \\ 5 & 1 & 4 & 0 & 6 \end{bmatrix}$	$\begin{bmatrix} 0 & 6 & 3 & 6 & 4 \\ 6 & 4 & 1 & 5 & 0 \end{bmatrix}$
	$\begin{bmatrix} 6 & 3 & 1 & 0 & 2 \\ 1 & 5 & 0 & 0 & 6 \end{bmatrix}$	$\begin{bmatrix} 4 & 2 & 6 & 6 & 5 \\ 5 & 1 & 5 & 6 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 5 & 1 & 4 & 0 \\ 5 & 2 & 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 & 1 & 6 & 0 \\ 5 & 0 & 1 & 2 & 5 \end{bmatrix}$	$\begin{bmatrix} 3 & 4 & 1 & 0 & 6 \\ 6 & 1 & 0 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 & 5 & 0 & 0 \\ 5 & 0 & 2 & 5 & 6 \end{bmatrix}$
	$\begin{bmatrix} 1 & 6 & 5 & 0 & 3 \\ 2 & 1 & 4 & 0 & 5 \end{bmatrix}$	$\begin{bmatrix} 4 & 1 & 0 & 2 & 6 \\ 1 & 6 & 6 & 1 & 4 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 5 & 6 & 2 \\ 5 & 6 & 0 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 5 & 0 & 5 & 3 & 6 \\ 3 & 4 & 6 & 0 & 5 \end{bmatrix}$	$\begin{bmatrix} 5 & 0 & 2 & 5 & 6 \\ 3 & 2 & 5 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 5 & 0 & 6 \\ 6 & 1 & 3 & 1 & 4 \end{bmatrix}$
	$\begin{bmatrix} 3 & 1 & 2 & 5 & 0 \\ 0 & 1 & 5 & 3 & 6 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 & 5 & 2 & 6 \\ 1 & 0 & 6 & 5 & 5 \end{bmatrix}$	$\begin{bmatrix} 4 & 0 & 0 & 5 & 1 \\ 1 & 5 & 6 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 6 & 5 & 6 & 0 \\ 2 & 5 & 6 & 6 & 3 \end{bmatrix}$		
7	$\begin{bmatrix} 4 & 6 & 2 & 7 & 0 \\ 7 & 4 & 8 & 5 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 7 & 0 & 3 \\ 3 & 0 & 1 & 0 & 7 \end{bmatrix}$	$\begin{bmatrix} 4 & 1 & 7 & 0 & 5 \\ 2 & 6 & 0 & 5 & 8 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 1 & 2 & 0 \\ 4 & 3 & 6 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 6 & 5 & 1 & 0 & 7 \\ 6 & 7 & 3 & 4 & 0 \end{bmatrix}$	$\begin{bmatrix} 5 & 6 & 7 & 2 & 0 \\ 1 & 7 & 0 & 3 & 5 \end{bmatrix}$
	$\begin{bmatrix} 1 & 0 & 3 & 7 & 5 \\ 0 & 0 & 5 & 1 & 7 \end{bmatrix}$	$\begin{bmatrix} 6 & 7 & 0 & 2 & 0 \\ 7 & 7 & 4 & 0 & 6 \end{bmatrix}$	$\begin{bmatrix} 1 & 4 & 2 & 7 & 0 \\ 2 & 7 & 0 & 7 & 6 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 5 & 1 & 7 \\ 2 & 0 & 2 & 7 & 3 \end{bmatrix}$	$\begin{bmatrix} 7 & 2 & 6 & 0 & 4 \\ 0 & 6 & 5 & 4 & 7 \end{bmatrix}$	$\begin{bmatrix} 0 & 7 & 6 & 4 & 7 \\ 3 & 5 & 2 & 0 & 7 \end{bmatrix}$
	$\begin{bmatrix} 4 & 7 & 2 & 6 & 7 \\ 5 & 6 & 0 & 1 & 7 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 & 0 & 5 & 6 \\ 7 & 7 & 0 & 6 & 4 \end{bmatrix}$	$\begin{bmatrix} 6 & 7 & 5 & 2 & 0 \\ 3 & 1 & 4 & 0 & 6 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 7 & 5 & 2 \\ 5 & 2 & 7 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 5 & 7 & 7 & 6 & 1 \\ 6 & 6 & 7 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 7 & 7 & 2 & 2 & 0 \\ 5 & 4 & 1 & 7 & 1 \end{bmatrix}$
	$\begin{bmatrix} 4 & 1 & 7 & 1 & 0 \\ 0 & 4 & 5 & 7 & 6 \end{bmatrix}$	$\begin{bmatrix} 4 & 5 & 6 & 7 & 1 \\ 7 & 7 & 0 & 0 & 5 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 7 & 5 & 3 \\ 7 & 4 & 5 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 4 & 6 & 0 & 6 \\ 7 & 0 & 3 & 7 & 6 \end{bmatrix}$	$\begin{bmatrix} 6 & 1 & 7 & 2 & 0 \\ 2 & 5 & 0 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 7 & 6 & 2 & 0 \\ 6 & 7 & 3 & 5 & 4 \end{bmatrix}$
	$\begin{bmatrix} 5 & 1 & 7 & 4 & 0 \\ 3 & 4 & 6 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 5 & 7 & 6 & 5 & 1 \\ 6 & 7 & 1 & 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 1 & 0 & 2 & 2 \\ 7 & 0 & 3 & 6 & 0 \end{bmatrix}$	$\begin{bmatrix} 6 & 7 & 1 & 5 & 1 \\ 0 & 0 & 5 & 7 & 3 \end{bmatrix}$	$\begin{bmatrix} 5 & 1 & 0 & 3 & 5 \\ 2 & 7 & 7 & 0 & 6 \end{bmatrix}$	$\begin{bmatrix} 1 & 5 & 4 & 7 & 0 \\ 4 & 2 & 6 & 4 & 0 \end{bmatrix}$
	$\begin{bmatrix} 3 & 1 & 6 & 0 & 5 \\ 0 & 6 & 5 & 5 & 7 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 & 6 & 0 & 7 \\ 0 & 0 & 3 & 6 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 0 & 7 & 4 \\ 5 & 1 & 2 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 5 & 2 & 7 & 3 \\ 3 & 5 & 0 & 3 & 6 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 7 & 6 & 7 \\ 1 & 0 & 4 & 6 & 2 \end{bmatrix}$	$\begin{bmatrix} 7 & 6 & 1 & 0 & 4 \\ 1 & 5 & 0 & 0 & 6 \end{bmatrix}$
	$\begin{bmatrix} 6 & 2 & 5 & 0 & 6 \\ 1 & 7 & 0 & 7 & 6 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 & 7 & 5 \\ 1 & 0 & 3 & 2 & 6 \end{bmatrix}$	$\begin{bmatrix} 4 & 3 & 3 & 0 & 5 \\ 6 & 7 & 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 4 & 7 & 1 & 1 \\ 6 & 7 & 2 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 6 & 7 & 0 & 1 & 3 \\ 2 & 0 & 3 & 1 & 6 \end{bmatrix}$	$\begin{bmatrix} 6 & 5 & 0 & 7 & 6 \\ 5 & 7 & 4 & 1 & 0 \end{bmatrix}$
	$\begin{bmatrix} 6 & 7 & 2 & 4 & 1 \\ 6 & 5 & 3 & 0 & 7 \end{bmatrix}$	$\begin{bmatrix} 6 & 7 & 2 & 1 & 0 \\ 4 & 2 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 6 & 7 & 4 & 0 & 1 \\ 4 & 3 & 1 & 6 & 7 \end{bmatrix}$	$\begin{bmatrix} 7 & 0 & 6 & 0 & 4 \\ 7 & 2 & 3 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 2 & 7 & 6 & 7 \\ 2 & 6 & 2 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 7 & 7 & 5 \\ 2 & 0 & 3 & 2 & 7 \end{bmatrix}$
	$\begin{bmatrix} 3 & 0 & 5 & 2 & 3 \\ 6 & 5 & 3 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 5 & 2 & 0 & 7 & 3 \\ 2 & 5 & 1 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 & 6 & 7 & 7 \\ 5 & 7 & 2 & 4 & 3 \end{bmatrix}$	$\begin{bmatrix} 7 & 1 & 7 & 0 & 4 \\ 5 & 1 & 7 & 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 & 7 & 6 & 7 \\ 6 & 5 & 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 6 & 7 & 5 \\ 3 & 5 & 4 & 7 & 2 \end{bmatrix}$
	$\begin{bmatrix} 0 & 2 & 7 & 5 & 3 \\ 4 & 1 & 7 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 6 & 5 & 0 & 3 \\ 4 & 5 & 7 & 5 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 & 4 & 5 & 0 \\ 6 & 7 & 0 & 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 6 & 3 & 7 \\ 5 & 7 & 3 & 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 4 & 7 & 6 & 1 & 0 \\ 1 & 0 & 4 & 5 & 4 \end{bmatrix}$	$\begin{bmatrix} 7 & 7 & 1 & 0 & 3 \\ 2 & 0 & 6 & 5 & 7 \end{bmatrix}$
	$\begin{bmatrix} 5 & 7 & 1 & 4 & 3 \\ 6 & 5 & 4 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 3 & 0 & 7 & 7 \\ 6 & 1 & 3 & 6 & 7 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 & 5 & 0 & 7 \\ 0 & 0 & 4 & 7 & 1 \end{bmatrix}$	$\begin{bmatrix} 6 & 4 & 5 & 1 & 0 \\ 2 & 0 & 0 & 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 & 3 & 7 & 0 \\ 5 & 7 & 1 & 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 & 1 & 0 & 7 \\ 5 & 0 & 0 & 5 & 2 \end{bmatrix}$
	$\begin{bmatrix} 2 & 3 & 5 & 7 & 3 \\ 5 & 7 & 2 & 6 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 5 & 4 & 6 \\ 0 & 0 & 6 & 7 & 1 \end{bmatrix}$	$\begin{bmatrix} 5 & 2 & 0 & 7 & 0 \\ 3 & 7 & 2 & 5 & 1 \end{bmatrix}$	$\begin{bmatrix} 4 & 3 & 0 & 6 & 7 \\ 6 & 7 & 2 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 5 & 0 & 7 & 2 \\ 2 & 6 & 0 & 5 & 7 \end{bmatrix}$	$\begin{bmatrix} 7 & 3 & 1 & 0 & 6 \\ 2 & 5 & 2 & 0 & 7 \end{bmatrix}$
	$\begin{bmatrix} 3 & 4 & 3 & 1 & 0 \\ 5 & 0 & 0 & 1 & 6 \end{bmatrix}$	$\begin{bmatrix} 6 & 4 & 2 & 5 & 0 \\ 5 & 6 & 0 & 7 & 1 \end{bmatrix}$	$\begin{bmatrix} 6 & 1 & 7 & 0 & 0 \\ 4 & 3 & 2 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 7 & 2 & 3 & 2 \\ 5 & 4 & 1 & 7 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 4 & 6 & 0 & 7 \\ 5 & 1 & 4 & 4 & 1 \end{bmatrix}$	$\begin{bmatrix} 5 & 1 & 4 & 4 & 1 \\ 1 & 4 & 6 & 0 & 7 \end{bmatrix}$
	$\begin{bmatrix} 1 & 6 & 0 & 5 & 7 \\ 1 & 3 & 3 & 6 & 6 \end{bmatrix}$	$\begin{bmatrix} 6 & 5 & 1 & 0 & 4 \\ 4 & 7 & 3 & 4 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 7 & 1 & 6 & 0 \\ 1 & 6 & 3 & 7 & 2 \end{bmatrix}$	$\begin{bmatrix} 3 & 0 & 2 & 0 & 5 \\ 2 & 1 & 7 & 0 & 6 \end{bmatrix}$	$\begin{bmatrix} 6 & 5 & 1 & 8 & 0 \\ 1 & 4 & 3 & 2 & 6 \end{bmatrix}$	$\begin{bmatrix} 1 & 4 & 5 & 4 & 7 \\ 6 & 1 & 5 & 7 & 0 \end{bmatrix}$
	$\begin{bmatrix} 0 & 0 & 6 & 4 & 7 \\ 1 & 0 & 6 & 7 & 5 \end{bmatrix}$	$\begin{bmatrix} 1 & 3 & 6 & 2 & 7 \\ 2 & 6 & 5 & 0 & 7 \end{bmatrix}$	$\begin{bmatrix} 2 & 6 & 7 & 6 & 1 \\ 1 & 7 & 7 & 2 & 3 \end{bmatrix}$	$\begin{bmatrix} 5 & 4 & 4 & 1 & 0 \\ 1 & 0 & 6 & 4 & 3 \end{bmatrix}$	$\begin{bmatrix} 5 & 1 & 4 & 4 & 2 \\ 2 & 1 & 6 & 0 & 5 \end{bmatrix}$	$\begin{bmatrix} 1 & 7 & 2 & 3 & 3 \\ 1 & 7 & 0 & 6 & 0 \end{bmatrix}$

$\begin{bmatrix} 5 & 6 & 1 & 7 & 0 & 2 & 0 \\ 2 & 4 & 5 & 3 & 1 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 0 & 4 & 6 & 3 & 7 & 7 \\ 1 & 3 & 6 & 3 & 7 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 5 & 5 & 7 & 1 & 0 & 0 \\ 6 & 7 & 1 & 2 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 & 0 & 6 & 7 & 6 & 4 \\ 2 & 0 & 0 & 6 & 4 & 2 & 7 \end{bmatrix}$	$\begin{bmatrix} 2 & 6 & 7 & 4 & 1 & 3 & 0 \\ 5 & 3 & 5 & 7 & 0 & 7 & 0 \end{bmatrix}$	$\begin{bmatrix} 6 & 0 & 0 & 1 & 6 & 3 & 7 \\ 2 & 5 & 4 & 2 & 0 & 7 & 0 \end{bmatrix}$
$\begin{bmatrix} 3 & 3 & 6 & 0 & 6 & 7 & 7 \\ 1 & 7 & 3 & 3 & 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 6 & 7 & 7 & 4 & 2 \\ 4 & 3 & 3 & 1 & 0 & 6 & 7 \end{bmatrix}$	$\begin{bmatrix} 4 & 6 & 1 & 5 & 0 & 4 & 7 \\ 6 & 1 & 5 & 0 & 7 & 0 & 4 \end{bmatrix}$	$\begin{bmatrix} 1 & 6 & 6 & 7 & 1 & 0 & 3 \\ 3 & 5 & 7 & 7 & 6 & 5 & 0 \end{bmatrix}$	$\begin{bmatrix} 6 & 5 & 1 & 5 & 0 & 7 & 7 \\ 0 & 0 & 7 & 6 & 7 & 4 & 5 \end{bmatrix}$	$\begin{bmatrix} 2 & 7 & 6 & 7 & 0 & 6 & 5 \\ 3 & 3 & 1 & 2 & 0 & 6 & 7 \end{bmatrix}$
$\begin{bmatrix} 5 & 6 & 1 & 4 & 7 & 5 & 0 \\ 6 & 2 & 2 & 0 & 7 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 6 & 7 & 6 & 4 & 5 \\ 6 & 5 & 0 & 0 & 4 & 7 & 7 \end{bmatrix}$	$\begin{bmatrix} 6 & 2 & 5 & 1 & 0 & 5 & 7 \\ 3 & 4 & 0 & 3 & 1 & 6 & 7 \end{bmatrix}$	$\begin{bmatrix} 6 & 4 & 4 & 5 & 0 & 0 & 7 \\ 2 & 5 & 0 & 0 & 1 & 2 & 7 \end{bmatrix}$	$\begin{bmatrix} 5 & 6 & 4 & 1 & 0 & 4 & 7 \\ 6 & 4 & 7 & 3 & 4 & 1 & 0 \end{bmatrix}$	

Table 4: List of Lang–Trotter polygons for $m \leq 7$

Database 10.2. A database of Lang–Trotter polygons that can be used to show that the pseudo-effective cone of $\overline{M}_{0,n}$ is not polyhedral for $n \geq 10$ in characteristic p for any prime $p < 2000$ (see Remark 9.8). For each polygon, the corresponding non-polyhedral primes are displayed.

vertices	non-polyhedral primes
$\begin{bmatrix} 0 & 6 & 9 & 10 & 9 & 3 & 1 \\ 0 & 2 & 4 & 5 & 6 & 10 & 4 \end{bmatrix}$	2, 19, 29, 31, 53, 71, 83, 97, 103, 131, 167, 211, 233, 257, 263, 269, 277, 313, 347, 373, 419, 439, 461, 487, 491, 577, 593, 619, 643, 653, 661, 709, 761, 827, 907, 919, 941, 953, 991, 1013, 1061, 1097, 1123, 1213, 1223, 1231, 1249, 1289, 1367, 1451, 1481, 1483, 1499, 1543, 1549, 1583, 1721, 1723, 1741, 1787, 1871, 1873
$\begin{bmatrix} 10 & 10 & 9 & 6 & 3 & 0 & 2 & 7 \\ 4 & 3 & 1 & 0 & 1 & 10 & 9 & 6 \end{bmatrix}$	7, 11, 13, 53, 59, 71, 107, 109, 127, 149, 157, 167, 173, 179, 181, 263, 271, 277, 283, 293, 337, 419, 421, 443, 449, 463, 487, 593, 601, 619, 643, 653, 677, 727, 751, 757, 761, 773, 797, 857, 859, 877, 887, 911, 929, 937, 997, 1019, 1031, 1049, 1061, 1069, 1087, 1091, 1103, 1163, 1231, 1249, 1291, 1301, 1319, 1373, 1427, 1439, 1447, 1451, 1459, 1489, 1493, 1523, 1553, 1559, 1571, 1609, 1613, 1669, 1721, 1741, 1747, 1777, 1787, 1811, 1871, 1889, 1901, 1933, 1973, 1987, 1993, 1997
$\begin{bmatrix} 5 & 6 & 9 & 11 & 12 & 2 & 0 & 2 & 3 \\ 0 & 0 & 1 & 2 & 4 & 10 & 11 & 5 & 3 \end{bmatrix}$	23, 29, 41, 59, 67, 71, 131, 139, 179, 181, 191, 199, 223, 229, 241, 251, 307, 311, 331, 337, 349, 379, 401, 409, 419, 421, 443, 461, 491, 547, 571, 577, 587, 601, 631, 647, 661, 673, 701, 733, 739, 751, 787, 827, 839, 857, 859, 911, 919, 937, 971, 977, 983, 991, 1013, 1019, 1021, 1039, 1061, 1063, 1087, 1109, 1123, 1129, 1171, 1187, 1213, 1223, 1229, 1237, 1249, 1259, 1277, 1279, 1307, 1327, 1381, 1409, 1429, 1447, 1459, 1493, 1511, 1549, 1571, 1579, 1583, 1597, 1619, 1621, 1699, 1723, 1741, 1759, 1811, 1823, 1831, 1847, 1873, 1913, 1931, 1933, 1979, 1987
$\begin{bmatrix} 0 & 5 & 9 & 10 & 12 & 11 & 5 & 4 \\ 12 & 10 & 7 & 6 & 3 & 2 & 0 & 0 \end{bmatrix}$	23, 31, 37, 41, 47, 53, 73, 101, 131, 139, 197, 199, 223, 233, 307, 317, 331, 383, 389, 401, 421, 439, 449, 461, 479, 487, 499, 509, 569, 571, 593, 599, 607, 631, 641, 673, 701, 709, 743, 787, 811, 829, 857, 863, 877, 881, 907, 911, 941, 1019, 1021, 1123, 1151, 1153, 1171, 1217, 1231, 1237, 1259, 1291, 1297, 1423, 1429, 1481, 1583, 1609, 1657, 1723, 1753, 1783, 1823, 1871, 1879, 1889, 1901, 1907, 1973, 1979, 1987, 1997
$\begin{bmatrix} 0 & 2 & 12 & 13 & 13 & 11 & 9 & 4 \\ 0 & 1 & 7 & 9 & 10 & 12 & 13 & 12 \end{bmatrix}$	31, 37, 47, 79, 131, 139, 151, 181, 211, 223, 239, 257, 271, 281, 307, 331, 373, 389, 409, 433, 457, 461, 479, 523, 569, 577, 587, 641, 659, 683, 709, 719, 733, 743, 761, 769, 809, 821, 823, 853, 859, 863, 887, 953, 997, 1013, 1063, 1093, 1103, 1117, 1129, 1153, 1163, 1181, 1201, 1237, 1249, 1283, 1361, 1367, 1439, 1471, 1531, 1553, 1601, 1609, 1699, 1721, 1741, 1789, 1867, 1871, 1873, 1889, 1907, 1931, 1973, 1979, 1997
$\begin{bmatrix} 0 & 2 & 12 & 13 & 12 & 11 & 8 & 7 & 4 \\ 0 & 1 & 7 & 9 & 11 & 12 & 13 & 13 & 12 \end{bmatrix}$	31, 61, 71, 89, 97, 109, 127, 139, 149, 163, 173, 191, 193, 227, 233, 257, 271, 281, 311, 313, 347, 349, 353, 389, 421, 433, 457, 463, 467, 479, 491, 499, 541, 563, 571, 587, 607, 613, 631, 643, 683, 733, 743, 751, 757, 769, 797, 809, 821, 853, 857, 863, 907, 941, 967, 971, 991, 997, 1013, 1019, 1031, 1049, 1051, 1063, 1087, 1091, 1093, 1097, 1109, 1153, 1163, 1193, 1217, 1279, 1283, 1303, 1321, 1433, 1439, 1451, 1481, 1483, 1493, 1499, 1511, 1543, 1559, 1571, 1597, 1621, 1667, 1693, 1723, 1759, 1823, 1867, 1913, 1931, 1973, 1979, 1987
$\begin{bmatrix} 13 & 9 & 5 & 4 & 2 & 1 & 0 & 1 & 11 \\ 8 & 0 & 3 & 4 & 7 & 9 & 12 & 13 & 9 \end{bmatrix}$	11, 19, 59, 83, 101, 107, 113, 163, 167, 181, 197, 269, 293, 307, 313, 317, 337, 347, 349, 359, 373, 401, 461, 491, 499, 509, 521, 569, 617, 643, 647, 661, 677, 683, 739, 787, 797, 809, 821, 827, 829, 839, 859, 883, 887, 941, 983, 1087, 1109, 1117, 1163, 1213, 1237, 1277, 1283, 1291, 1303, 1307, 1429, 1451, 1483, 1493, 1553, 1597, 1621, 1637, 1667, 1733, 1801, 1901, 1933, 1993, 1997
$\begin{bmatrix} 0 & 1 & 10 & 12 & 13 & 12 & 10 & 7 & 1 \\ 0 & 0 & 3 & 4 & 6 & 9 & 13 & 12 & 2 \end{bmatrix}$	11, 23, 29, 31, 43, 59, 67, 73, 137, 149, 157, 223, 229, 271, 277, 281, 283, 293, 353, 367, 439, 457, 461, 491, 503, 577, 599, 601, 641, 643, 647, 653, 661, 691, 733, 757, 941, 977, 997, 1019, 1049, 1051, 1061, 1069, 1193, 1249, 1301, 1303, 1327, 1373, 1451, 1471, 1487, 1543, 1553, 1559, 1579, 1597, 1607, 1627, 1669, 1699, 1723, 1753, 1777, 1789, 1831, 1847, 1877, 1913, 1933, 1949, 1997, 1999
$\begin{bmatrix} 0 & 12 & 13 & 13 & 11 & 9 & 7 & 1 \\ 0 & 4 & 9 & 10 & 12 & 13 & 12 & 2 \end{bmatrix}$	7, 11, 67, 101, 139, 199, 251, 313, 331, 337, 353, 373, 383, 419, 421, 431, 503, 541, 557, 571, 587, 601, 607, 617, 619, 659, 709, 719, 733, 751, 857, 877, 883, 911, 947, 967, 1033, 1093, 1123, 1163, 1193, 1277, 1279, 1283, 1289, 1303, 1319, 1327, 1381, 1409, 1423, 1429, 1439, 1453, 1459, 1499, 1531, 1549, 1621, 1657, 1663, 1667, 1787, 1879, 1913, 1951

$\begin{bmatrix} 0 & 2 & 12 & 13 & 13 & 12 & 11 & 9 & 4 \\ 0 & 1 & 7 & 8 & 9 & 11 & 12 & 13 & 12 \end{bmatrix}$	5, 17, 23, 29, 41, 43, 67, 73, 79, 101, 103, 107, 113, 157, 173, 179, 191, 193, 227, 229, 239, 251, 263, 277, 281, 283, 313, 331, 337, 349, 353, 367, 379, 389, 397, 443, 449, 457, 463, 467, 479, 487, 503, 509, 521, 557, 563, 587, 617, 641, 643, 647, 653, 659, 701, 773, 787, 809, 823, 859, 887, 907, 911, 937, 941, 947, 983, 991, 1009, 1013, 1019, 1039, 1049, 1087, 1091, 1097, 1103, 1187, 1217, 1279, 1289, 1303, 1307, 1321, 1327, 1373, 1399, 1409, 1427, 1429, 1453, 1471, 1483, 1487, 1493, 1511, 1523, 1553, 1579, 1619, 1621, 1663, 1667, 1693, 1697, 1709, 1721, 1723, 1733, 1759, 1777, 1831, 1867, 1871, 1873, 1877, 1889, 1907, 1931, 1951, 1973, 1993, 1997
$\begin{bmatrix} 0 & 5 & 10 & 12 & 14 & 14 & 5 & 4 \\ 0 & 2 & 5 & 7 & 10 & 11 & 14 & 12 \end{bmatrix}$	31, 37, 47, 79, 103, 127, 137, 149, 151, 163, 199, 211, 223, 229, 257, 269, 271, 311, 347, 353, 359, 389, 397, 401, 419, 439, 443, 457, 461, 463, 487, 499, 503, 523, 569, 571, 631, 677, 701, 727, 751, 773, 823, 853, 883, 911, 919, 947, 953, 967, 991, 1019, 1039, 1063, 1097, 1123, 1151, 1153, 1171, 1193, 1201, 1217, 1223, 1231, 1279, 1283, 1289, 1303, 1307, 1327, 1373, 1423, 1447, 1453, 1471, 1499, 1511, 1523, 1543, 1567, 1571, 1607, 1693, 1699, 1723, 1733, 1753, 1759, 1777, 1783, 1801, 1831, 1861, 1877, 1879, 1889, 1913, 1951, 1987, 1999
$\begin{bmatrix} 0 & 5 & 7 & 12 & 13 & 14 & 12 & 6 & 2 \\ 0 & 2 & 3 & 6 & 8 & 11 & 12 & 14 & 6 \end{bmatrix}$	3, 17, 19, 61, 67, 127, 197, 223, 241, 251, 263, 271, 277, 307, 359, 367, 431, 463, 487, 563, 641, 659, 701, 719, 733, 751, 761, 797, 823, 829, 839, 877, 887, 911, 967, 977, 1031, 1049, 1093, 1123, 1153, 1163, 1223, 1249, 1277, 1321, 1327, 1433, 1447, 1453, 1481, 1571, 1613, 1627, 1663, 1709, 1733, 1759, 1787, 1801, 1847, 1901, 1997

Table 5:

We give an overview of the MAGMA package, which can be downloaded from:

<https://github.com/alaface/non-polyhedral>

and contains descriptions of all functions. We first use Polygon 111 as a running example, then we study infinite families of pentagons and heptagons from Section 6. After that we find non-polyhedral primes up to 2000 for the polygon of Section 7, and finally we study Halphen polygons, in particular the one in Example 8.5.

Computation 10.3. Normal fan of the lattice polygon Δ , the fan of the minimal resolution of the toric surface \mathbb{P}_Δ , $\text{Vol}(\Delta)$, number of boundary points.

```
> pol := Polytope([[6,1],[5,4],[1,3],[8,2],[0,6],[0,7],[3,0]]);
  Transpose(Matrix(Reorder(Rays(NormalFan(pol)))));
[ 3 -1 -1 -2 -3 1 3]
[ 2 3 2 -3 -5 0 1]
> Transpose(Matrix(Reorder(Rays(Resolution(NormalFan(pol))))));
[ 3 1 0 -1 -1 -1 -1 -2 -3 -1 0 1 3 2]
[ 2 1 1 3 2 1 0 -1 -3 -5 -2 -1 0 1 1]
> [Volume(pol),#BoundaryPoints(pol)];
[ 49, 7 ]
```

Computation 10.4. Dimension of linear systems $\mathcal{L}_\Delta(m)$ and $\mathcal{L}_{k\Delta}(km)$ (over different fields), equation f of $\Gamma \subset \mathbb{G}_m^2$, Newton polytope of f .

```
> m := Width(pol);
  #FindCurves(pol,m,Rationals());
1
> #FindCurves(2*pol,2*m,GF(5));
2
> f := FindCurves(pol,m,Rationals())[1];
  Transpose(Matrix(Vertices(NPolytope(f))));
[8 6 5 3 1 0 0]
[2 1 4 0 3 7 6]
```

Computation 10.5. Irreducibility and geometric genus of Γ .


```

> IsIrreducible(FindCurve(pol,m,Rationals()));
true
> Genus(FindCurve(pol,m,Rationals()));
1

```

Computation 10.6. In the minimal resolution \tilde{X} of X , a divisor linearly equivalent to the pullback of C together with the prime components of the pullback of $K_X + C$, their multiplicities, Newton polygons and equations.

```

> AdjSys(pol);
[
  [ 19, 7, 2, 1, 0, 0, 0, 0, 0, 0, 1, 2, 5, 8, 20, 13, -7 ],
  [ 3, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 3, 2, -1 ],
  [ 1, 0, 0, 0, 0, 0, 0, 0, 1, 2, 1, 1, 1, 2, 1, -1 ],
  [ 8, 3, 1, 1, 0, 0, 0, 0, 0, 1, 1, 2, 3, 8, 5, -3 ]
]
> MultAdjSys(pol);
[ 2, 1, 1 ]
> PolsAdjSys(pol);
[
  x[1] - 1,
  x[1] - x[2],
  x[1]^3*x[2] - 3*x[1]^2*x[2] - x[1]*x[2]^2 + 5*x[1]*x[2] - x[1] + x[2]^3 -
    2*x[2]^2
]

```

Computation 10.7. Root lattice of Δ , the map $\text{Cl}(X) \rightarrow \text{Cl}(Y)$, intersection matrices of X and Y (the latter is not with respect to a basis).

```

> RootLat(pol);
A6 A1
> Cl,g := MapToY(pol);
Cl;
Full Quotient RSpace of degree 3 over Integer Ring
Column moduli:
[ 0, 0, 0 ]
> imatX(pol);
[-10/33  1/11    0    0    0    0    1/3    0]
[  1/11 -8/11    1    0    0    0    0    0]
[    0    1  -9/7   1/7    0    0    0    0]
[    0    0   1/7  -11/7    1    0    0    0]
[    0    0    0    1  -3/5   1/5    0    0]
[    0    0    0    0   1/5  -12/5    1    0]
[  1/3    0    0    0    0    1  -2/3    0]
[    0    0    0    0    0    0    0   -1]
> imatY(pol);
[ 17/14  8/7  13/14  25/14  4/7  31/14  1/2 103/14]
[  8/7  3/7  9/7  6/7  5/7  15/7  0  39/7]
[ 13/14  9/7  5/14 29/14  1/7 27/14  1/2 87/14]
[ 25/14  6/7 29/14 17/14 10/7 39/14  1/2 135/14]
[  4/7  5/7  1/7  10/7 -1/7 11/7  0  23/7]
[ 31/14 15/7 27/14 39/14 11/7 45/14 3/2 201/14]
[  1/2  0  1/2  1/2  0  3/2 -1/2  3/2]
[103/14 39/7 87/14 135/14 23/7 201/14 3/2 573/14]

```

Computation 10.8. Minimal equation of C and images of intersection points with the toric boundary divisors using the standard MAGMA algorithm, $\text{res}(C)$ and images of roots in $\text{Pic}^0(C)$ (identified with C), polyhedrality of specific primes. The algorithm constructs a birational map $u : C \dashrightarrow E$, with E given by a minimal Weierstrass equation in \mathbb{P}^2 . We consider only examples where E is smooth and the map u is defined everywhere in characteristic 0. Since C has arithmetic genus 1, it follows that C is smooth and the map u is an isomorphism. Similarly, for specific primes p , we discard those primes for which E is not smooth, or for which the map u is not defined everywhere.

```

> E,u := EllCur(pol);
E;
Elliptic Curve defined by y^2 + x*y = x^3 - x^2 - 4*x + 4 over Rational Field
> Cl,g := MapToY(pol);
C := FindCurve(pol,Width(pol),Rationals());
A := Ambient(C);
f := Equation(C);
h := map<A->Ambient(E) | [Evaluate(p,[A.1,A.2,1]) :
p in DefiningEquations(u)]>;
ff := [i : i in [1..#Vertices(pol)] | Volume(OrdFacets(pol)[i]) eq 1];
pts := [E!PtsCur(h,f,u,pol,i) : i in ff];
B := resC(pol,E,ff,pts);
pts;
[ (6 : 10 : 1), (-3/16 : -133/64 : 1), (0 : 2 : 1), (496 : -11286 : 1),
(1 : -1 : 1), (32/49 : -510/343 : 1), (16/9 : -14/27 : 1) ]
> res := resC(pol,E,ff,pts);
res;
[ (16/9 : -14/27 : 1), (1 : -1 : 1), (2 : 0 : 1) ]
> roots := FindRoots(pol);
ImgRoots := [&+[Eltseq(v)[i]*B[i] : i in [1..#B]] : v in roots];
ImgRoots;
[ (-2 : 2 : 1), (0 : 2 : 1), (85/49 : -244/343 : 1), (-19/16 : -119/64 : 1),
(394519648/356869881 : -4479186863510/6741628921971 : 1), (4303/4489 :
-323950/300763 : 1), (0 : -2 : 1), (-19/16 : 195/64 : 1) ]
> C := g(CinS(pol));
ImgC := [&+[Eltseq(C)[i]*B[i] : i in [1..#B]];
ImgC;
(-1 : -2 : 1)
> NonPolyhedralPrimes(pol,2000);
{ 47, 71, 103, 197, 233, 239, 277, 313, 367, 379, 409, 503, 563, 599, 647,
677, 683, 691, 719, 727, 761, 829, 911, 997, 1103, 1123, 1151, 1171, 1187, 1231,
1283, 1327, 1481, 1493, 1709, 1723, 1861, 1907, 1997 }

```

Computation 10.9. For the sequence of polygons Δ_k (we use pentagons from §6 and $k > 0$ as an example), verify that $\mathcal{O}(C)|_C$ is not torsion using Mazur's theorem. Find the type of the rational elliptic fibration with fibers C_k (when k varies).

```

> K<t> := FunctionField(Rationals());
a := -(12*t^2+24*t+11);
b := 4*(t+1)^2*(3*t+2)*(3*t+4);
E := EllipticCurve([0,a,0,b,0]);
P<x,y,z> := Ambient(E);
< p := E!(Points(Scheme(E,x-2*(t+1)*(3*t+2)*z))[2]);
KodairaSymbols(E);

```

```

[ <I2, 1>, <I2, 1>, <I2, 1>, <I4, 1>, <I1, 2> ]
> val := {};
for n in [1..12] do
  q := n*p;
  d := Lcm([Denominator(r) : r in Eltseq(q)]);
  M := Matrix([[a*d : a in Eltseq(q)], [0,1,0]]);
  g := Gcd([Numerator(f) : f in Minors(M,2)]);
  val := val join {r[1] : r in Roots(g)};
end for;
val;
{ -2, -4/3, -1, -2/3, 0 }

```

For the heptagons in §6 (and $k > 1$) we use the following variation:

```

> K<k> := FunctionField(Rationals());
a := -k*(2*k+1)/(k+2);
e := -(4*k+2);
x0 := 2*k*(k+1)^2/((k-1)*(k+2));
y0 := x0*(5*k+3)/(1-k);
b := -2*x0*(2*k+1)*(k+1)^2/((k+2)*(1-k));
E := EllipticCurve([e,a,b,0,0]);
q := E![x0,y0];
r := E![0,0];
s := q+q;
p := s-r;
Order(p);
0
> KodairaSymbols(E);
[ <IV, 1>, <I4, 1>, <I4, 1>, <I4, 1>, <IV, 1>, <IV, 1> ]

> val := {};
for n in [1..12] do
  q := n*p;
  d := Lcm([Denominator(r) : r in Eltseq(q)]);
  M := Matrix([[a*d : a in Eltseq(q)], [0,1,0]]);
  g := Gcd([Numerator(f) : f in Minors(M,2)]);
  val := val join {r[1] : r in Roots(g)};
end for;
val;
{ -2, 1 }

```

Computation 10.10. We find the non-polyhedral primes for the polygon of §7 with a smooth minimal model Y . The function DP3 computes the smooth cubic surface contraction of Y and its hyperplane section, the elliptic curve.

```

> pol := Polytope([
  [3,0], [6,1], [8,2], [23,12], [27,15], [30,18], [30,19],
  [29,20], [21,26], [18,28], [16,29], [13,30], [12,30],
  [11,29], [9,25], [7,20], [1,4], [0,1], [0,0]
]);
MX := imatX(pol);
MY := imatY(pol);
ind := [i : i in [1..#Vertices(pol)] | MX[i,i] eq MY[i,i]];
vv,E,pts := DP3(pol,ind);

```

```

roots := FindRoots(pol);
B := resC(pol,E,vv,pts);
ImgRoots := [&+[Eltseq(v)[i]*B[i] : i in [1..#B]] : v in roots];
Cl,g := MapToY(pol);
C := g(CinS(pol));
ImgC := &+[Eltseq(C)[i]*B[i] : i in [1..#B]];
{p : p in PrimesInInterval(2,2000) | p notin BadPrimes(E) and
not IsPolyhedralPrime(roots,ImgRoots,C,ImgC,p)};
{ 29, 43, 67, 71, 89, 101, 113, 167, 179, 181, 191, 197, 211, 233, 239, 241,
263, 269, 313, 337, 349, 359, 379, 383, 409, 449, 461, 491, 557, 587, 617, 701,
727, 733, 751, 769, 773, 809, 811, 829, 857, 877, 911, 929, 937, 977, 1031,
1039, 1051, 1087, 1091, 1093, 1097, 1117, 1129, 1153, 1187, 1193, 1223, 1229,
1231, 1237, 1249, 1259, 1303, 1319, 1321, 1433, 1481, 1489, 1511, 1523, 1553,
1583, 1607, 1609, 1663, 1669, 1709, 1753, 1873, 1877, 1907, 1949, 1999 }

```

Computation 10.11. For a Halphen polygon Δ such that the corresponding curve C is smooth in characteristic 0, the function `Bprimes` computes the set of “bad primes”, namely, for any other prime p , in characteristic p we have that:

- The Newton polygon of C is equal to Δ .
- The curve C is smooth, with the same (smooth) Weierstrass model.
- $K_X + C$ admits a uniform (over p) Zariski decomposition $N + P$, with

$$P = 0, \quad N = \sum a_i C_i,$$

with the curves C_i irreducible. In particular, Y has du Val singularities.

- If $Z \rightarrow Y$ is the minimal resolution, the roots in $\mathbb{E}_8 = \text{Cl}_0(Z)$ that lie in $\text{Ker}(\overline{\text{res}})$ stay the same as in characteristic 0.

For the Halphen polygon in Example 8.5 we obtain:

```

> pol := Polytope([[0,0],[1,0],[6,1],[8,2],[7,5],[5,8],[1,2]]);
> Bprimes(pol);
{ 2, 3, 5, 7, 11, 19, 71 }

```

Computation 10.12. We fix the prime $p := 2$ and the integer e such that $|eC|$ is a pencil in characteristic p . We then compute the cardinality of reducible fibers of the fibration $\pi: X \rightarrow \mathbb{P}^1$ associated to $|eC|$ (by the proof of Theorem 1.2, it is enough to consider fibers over points defined on \mathbb{F}_p).

```

> p := 2;
> e := 1;
> pol := Polytope([[0,0],[6,2],[9,4],[10,5],[9,6],[3,10],[1,4]]);
> ls := FindCurves(e*pol,e*Width(pol),GF(p));
> pencil := [ls[2]] cat [ls[1]+t*ls[2] : t in GF(p)];
> red := [];
> for g in pencil do
mu := #[f : f in Factorization(g) | #Monomials(f[1]) gt 1];
if mu gt 1 then Append(~red,mu); end if;
end for;
> red;
[ 3, 2 ]

```

REFERENCES

- [ABC⁺15] N. Arkani-Hamed, J. Bourjaily, F. Cachazo, A. Postnikov, and J. Trnka, *On-shell structures of MHV amplitudes beyond the planar limit*, J. of High Energy Physics **2015** (2015), no. 6, 179.
- [ADHL15] I. Arzhantsev, U. Derenthal, J. Hausen, and A. Laface, *Cox rings*, Cambridge Studies in Advanced Mathematics, vol. 144, Cambridge University Press, Cambridge, 2015.
- [Art62] M. Artin, *Some numerical criteria for contractibility of curves on algebraic surfaces*, Amer. J. Math. **84** (1962), 485–496.
- [AS12] V. Alexeev and D. Swinarski, *Nef divisors on $\overline{M}_{0,n}$ from GIT*, Geometry and arithmetic, 2012, pp. 1–21.
- [Bal20] G. Ballelli, *Enumeration of Lattice Polytopes by Their Volume*, Discrete Comput. Geom. (2020).
- [Bas72] M. Bashmakov, *The cohomology of abelian varieties over a number field*, Russian Mathematical Surveys **27** (1972), no. 6, 25–70.
- [Bau09] T. Bauer, *A simple proof for the existence of Zariski decompositions on surfaces*, J. Algebraic Geom. **18** (2009), no. 4, 789–793.
- [BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).
- [BDPP13] S. Boucksom, J.-P. Demailly, M. Păun, and T. Peternell, *The pseudo-effective cone of a compact Kähler manifold and varieties of negative Kodaira dimension*, J. Algebraic Geom. **22** (2013), no. 2, 201–248.
- [BG21] P. Belkale and A. Gibney, *Basepoint free cycles on $\overline{M}_{0,n}$ from Gromov-Witten theory*, Int. Math. Res. Not. IMRN **2** (2021), 855–884.
- [BGM15] P. Belkale, A. Gibney, and S. Mukhopadhyay, *Vanishing and identities of conformal blocks divisors*, Algebr. Geom. **2** (2015), no. 1, 62–90.
- [BM76] E. Bombieri and D. Mumford, *Enriques’ classification of surfaces in char. p . Part III*, Invent. Math. **35** (1976), 197–232.
- [BM77] ———, *Enriques’ classification of surfaces in char. p . Part II*, Complex analysis and algebraic geometry, 1977, pp. 23–42.
- [Cas09] A.-M. Castravet, *The Cox ring of $\overline{M}_{0,6}$* , Trans. Amer. Math. Soc. **361** (2009), no. 7, 3851–3878.
- [Cas18] ———, *Mori dream spaces and blow-ups*, Algebraic geometry: Salt Lake City 2015, 2018, pp. 143–167.
- [CD12] S. Cantat and I. Dolgachev, *Rational surfaces with a large group of automorphisms*, J. Amer. Math. Soc. **25** (2012), no. 3, 863–905.
- [CLS11] D. A. Cox, J. B. Little, and H. K. Schenck, *Toric varieties*, Graduate Studies in Mathematics, vol. 124, American Mathematical Society, Providence, RI, 2011.
- [Cox95] D. A. Cox, *The homogeneous coordinate ring of a toric variety*, J. Algebraic Geom. **4** (1995), no. 1, 17–50.
- [CT12] A.-M. Castravet and J. Tevelev, *Rigid Curves on $\overline{M}_{0,n}$ and Arithmetic Breaks*, Contemporary Math. **564** (2012), 19–67.
- [CT13] ———, *Hypertrees, projections, and moduli of stable rational curves*, J. Reine Angew. Math. **675** (2013), 121–180.
- [CT15] ———, *$\overline{M}_{0,n}$ is not a Mori dream space*, Duke Math. J. **164** (2015), no. 8, 1641–1667.
- [CT20] ———, *Derived category of moduli of pointed curves. I*, Algebr. Geom. **7** (2020), no. 6, 722–757.
- [Deb01] O. Debarre, *Higher-dimensional algebraic geometry*, Universitext, Springer-Verlag, New York, 2001.
- [DGJ17] B. Doran, N. Giansiracusa, and D. Jensen, *A simplicial approach to effective divisors in $\overline{M}_{0,n}$* , Int. Math. Res. Not. IMRN **2** (2017), 529–565.
- [Dyn57] E. B. Dynkin, *Semisimple subalgebras of semisimple Lie algebras*, Trans. Am. Math. Soc. **6** (1957), 111–244.
- [FL17] M. Fulger and B. Lehmann, *Zariski decompositions of numerical cycle classes*, J. Algebraic Geom. **26** (2017), no. 1, 43–106.
- [Fed20] M. Fedorchuk, *Symmetric F -conjecture for $g \leq 35$* , arXiv:2007.13457 (2020).

- [FS11] M. Fedorchuk and D. I. Smyth, *Ample divisors on moduli spaces of pointed rational curves*, J. Algebraic Geom. **20** (2011), no. 4, 599–629.
- [FT12] O. Fujino and H. Tanaka, *On log surfaces*, Proc. Japan Acad. Ser. A Math. Sci. **88** (2012), no. 8, 109–114.
- [Fuj20] O. Fujino, *On minimal model theory for algebraic log surfaces*, arXiv:2004.00246 (2020).
- [Ful17] M. Fulger, *Seshadri constants for curve classes*, arXiv:1707.00734 (2017).
- [GG12] N. Giansiracusa and A. Gibney, *The cone of type A, level 1, conformal blocks divisors*, Adv. Math. **231** (2012), no. 2, 798–814.
- [Gib09] A. Gibney, *Numerical criteria for divisors on \overline{M}_g to be ample*, Compos. Math. **145** (2009), no. 5, 1227–1248.
- [GJM13] N. Giansiracusa, D. Jensen, and H.-B. Moon, *GIT compactifications of $M_{0,n}$ and flips*, Adv. Math. **248** (2013), 242–278.
- [GK16] J. L. González and K. Karu, *Some non-finitely generated Cox rings*, Compos. Math. **152** (2016), no. 5, 984–996.
- [GKM02] A. Gibney, S. Keel, and I. Morrison, *Towards the ample cone of $\overline{M}_{g,n}$* , J. Amer. Math. Soc. **15** (2002), no. 2, 273–294.
- [GM86] R. Gupta and M. R. Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), no. 1, 13–44.
- [GM90] ———, *Cyclicity and generation of points mod p on elliptic curves*, Inventiones mathematicae **101** (1990), no. 1, 225–235.
- [GM12] A. Gibney and D. Maclagan, *Lower and upper bounds for nef cones*, Int. Math. Res. Not. IMRN **14** (2012), 3224–3255.
- [GNW94] S. Goto, K. Nishida, and K. Watanabe, *Non-Cohen-Macaulay symbolic blow-ups for space monomial curves and counterexamples to Cowsik’s question*, Proc. Amer. Math. Soc. **120** (1994), no. 2, 383–392.
- [Gri16] J. Grivaux, *Parabolic automorphisms of projective surfaces (after M. H. Gizatullin)*, Mosc. Math. J. **16** (2016), no. 2, 275–298.
- [HK00] Y. Hu and S. Keel, *Mori dream spaces and GIT*, Michigan Math. J. **48** (2000), 331–348. Dedicated to William Fulton on the occasion of his 60th birthday.
- [HKL16] J. Hausen, S. Keicher, and A. Laface, *Computing Cox rings*, Math. Comp. **85** (2016), no. 297, 467–502.
- [HKL18] ———, *On blowing up the weighted projective plane*, Math. Z. **290** (2018), no. 3-4, 1339–1358.
- [HM82] J. Harris and D. Mumford, *On the Kodaira dimension of the moduli space of curves*, Invent. Math. **67** (1982), no. 1, 23–88. With an appendix by William Fulton.
- [HT02] B. Hassett and Y. Tschinkel, *On the effective cone of the moduli space of pointed rational curves*, Topology and geometry: commemorating SISTAG, 2002, pp. 83–96.
- [HY21] Z. He and L. Yang, *Birational geometry of blow-ups of projective spaces along points and lines*, Int. Math. Res. Not. IMRN **9** (2021), 6442–6497.
- [KM96] S. Keel and J. McKernan, *Contractible Extremal Rays on $\overline{M}_{0,n}$* (1996), available at [arXiv:alg-geom/9607009v1](https://arxiv.org/abs/alg-geom/9607009v1).
- [KM98] J. Kollár and S. Mori, *Birational geometry of algebraic varieties*, Cambridge Tracts in Mathematics, vol. 134, Cambridge University Press, Cambridge, 1998.
- [Kol92] J. Kollár (ed.), *Flips and abundance for algebraic threefolds - A summer seminar at the University of Utah (Salt Lake City, 1991)*, Astérisque, 1992.
- [Laz04a] R. Lazarsfeld, *Positivity in algebraic geometry. I*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 49, Springer-Verlag, Berlin, 2004.
- [Laz04b] ———, *Positivity in algebraic geometry. II*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 49, Springer-Verlag, Berlin, 2004.
- [LM00] A. Losev and Y. Manin, *New moduli spaces of pointed curves and pencils of flat connections*, Michigan Math. J. **48** (2000), 443–472.
- [LMF20] LMFDB, *The L-functions and Modular Forms Database*, 2020. available at <http://www.lmfdb.org>.
- [LT77] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292.

- [LU20] A. Laface and L. Ugaglia, *On base loci of higher fundamental forms of toric varieties*, J. Pure Appl. Algebra **224** (2020), no. 12, 106447, 18.
- [Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHÉS **47** (1977), 33–186.
- [Nik00] V. V. Nikulin, *A remark on algebraic surfaces with polyhedral Mori cone*, Nagoya Math. J. **157** (2000), 73–92.
- [Obi17] S. Obinna, *Database of blow-ups of toric surfaces of Picard number 2*, University of Massachusetts, 2017. <https://people.math.umass.edu/~tevelev/obinna/>.
- [OS91] K. Oguiso and T. Shioda, *The Mordell-Weil lattice of a rational elliptic surface*, Rikkyo Daigaku sugaku zasshi **40** (1991), no. 1, 83–99.
- [OP91] T. Oda and H. S. Park, *Linear Gale transforms and Gel'fand–Kapranov–Zelevinskij decompositions*, Tohoku Math. J. (2) **43** (1991), no. 3, 375–399.
- [Opi16] M. Opie, *Extremal divisors on moduli spaces of rational curves with marked points*, Michigan Math. J. **65** (2016), no. 2, 251–285.
- [Ser71] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae **15** (1971), no. 4, 259–331.
- [Sil83] J. H. Silverman, *Heights and the specialization map for families of abelian varieties*, Journal für die reine und angewandte Mathematik **342** (1983), 197–211.
- [Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
- [Sil09] ———, *The arithmetic of elliptic curves*, Second, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
- [ST15] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015.
- [Tan14] H. Tanaka, *Minimal models and abundance for positive characteristic log surfaces*, Nagoya Math. J. **216** (2014), 1–70.
- [Tev20] J. Tevelev, *Scattering amplitudes of stable curves*, arXiv:2007.03831 (2020), available at <https://arxiv.org/pdf/2007.03831.pdf>.
- [Tsc26] N. Tschebotareff, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95** (1926), 191–228.
- [Ver02] P. Vermeire, *A counterexample to Fulton's conjecture on $\overline{M}_{0,n}$* , J. Algebra **248** (2002), no. 2, 780–784.
- [Wes03] T. Weston, *Kummer theory of abelian varieties and reductions of Mordell-Weil groups*, Acta Arithmetica **110** (2003), 77–88.

UNIVERSITÉ PARIS-SACLAY, UVSQ, CNRS, LABORATOIRE DE MATHÉMATIQUES DE VERSAILLES,
78000, VERSAILLES, FRANCE

Email address: ana-maria.castravet@uvsq.fr

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDAD DE CONCEPCIÓN, CASILLA 160-C, CONCEPCIÓN,
CHILE

Email address: alaface@udec.cl

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS AMHERST,
710 NORTH PLEASANT STREET, AMHERST, MA 01003, USA AND LABORATORY OF ALGEBRAIC
GEOMETRY AND ITS APPLICATIONS, HSE, MOSCOW, RUSSIA

Email address: tevelev@math.umass.edu

DIPARTIMENTO DI MATEMATICA E INFORMATICA, UNIVERSITÀ DEGLI STUDI DI PALERMO, VIA
ARCHIRAFI 34, 90123 PALERMO, ITALY

Email address: luca.ugaglia@unipa.it