Journal of Pure and Applied Algebra 227 (2023) 107323

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

On the geometry of elliptic pairs

Elizabeth Pratt

ARTICLE INFO

Article history:
Received 2 September 2022
Received in revised form 21 November 2022
Available online 16 January 2023
Communicated by I. Coskun

MSC:
14Exx; 14Jxx

ABSTRACT

An *elliptic pair* (X, C) is a projective rational surface X with log terminal singularities, and an irreducible curve C contained in the smooth locus of X, with arithmetic genus 1 and self-intersection 0. They are a useful tool for determining whether the pseudo-effective cone of X is polyhedral [1], and interesting algebraic and geometric objects in their own right. Especially of interest are toric elliptic pairs, where X is the blow-up of a projective toric surface at the identity element of the torus. In this paper, we classify all toric elliptic pairs of Picard number two. Strikingly, it turns out that there are only three of these. Furthermore, we study a class of non-toric elliptic pairs coming from the blow-up of $\mathbb{P}^2$ at nine points on a nodal cubic, in characteristic p. This construction gives us examples of surfaces where the pseudo-effective cone is non-polyhedral for a set of primes p of positive density, and, assuming the generalized Riemann hypothesis, polyhedral for a set of primes p of positive density.

1. Introduction

The effective cone of a projective variety X and its closure, $\overline{\mathrm{Eff}}(X)$, are well-studied invariants of X. In particularly nice cases $\overline{\mathrm{Eff}}(X)$ is polyhedral. This is true, for example, when X is a projective toric variety. However, in general it is difficult to determine for an arbitrary projective surface X whether $\overline{\mathrm{Eff}}(X)$ is polyhedral. Recent work by Castravet, Laface, Tevelev, and Ugaglia [1] has shown that in the presence of a curve C on X satisfying certain properties, a polyhedrality criterion can be obtained in terms of the group structure of $\mathrm{Pic}(C)$. Using this criterion, they were able to prove that the Grothendieck-Knutsen moduli space $\overline{M_{0,n}}$ of stable rational curves has a non-polyhedral effective cone for $n \geq 10$, by proving the corresponding statement for blow-ups of certain toric surfaces $\mathbb{P}$.

More precisely, an *elliptic pair* (X, C) is a projective rational surface X with log terminal singularities, and an irreducible curve C contained in the smooth locus of X, such that the arithmetic genus of C is one and $C^2 = 0$. These elliptic pairs are not only useful for determining the polyhedrality of $\overline{\mathrm{Eff}}(X)$, but are also interesting geometric and arithmetic objects in their own right. In this paper we will construct elliptic

E-mail address: epratt@berkeley.edu.

https://doi.org/10.1016/j.jpaa.2023.107323

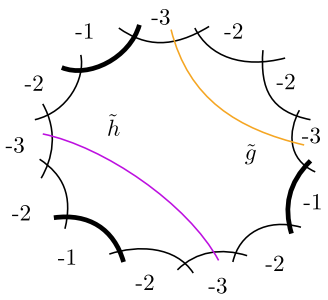

Fig. 1. Intersections of curves on $\widetilde{X_\Delta}$, where $\Delta = \{(0,0),(2,0),(5,8)\}$.

pairs in two ways: first from blow-ups of toric surfaces of Picard number one, and then from blow-ups of $\mathbb{P}^2$ at nine points on a nodal cubic.

In Section 2 we follow the procedure given in [1] to construct *toric elliptic pairs* (X, C), which arise from lattice polygons Δ satisfying certain combinatorial properties. In this case X will be the blow-up of $\mathbb{P}(\Delta)$ at the identity element e of the torus. We may denote X instead by X_Δ if we wish to emphasize an underlying lattice polygon of X.

In [1] a number of interesting classification questions were raised. For instance, it is known that there are infinitely many pentagons which give rise to toric elliptic pairs with non-polyhedral effective cone. However, classification of quadrilaterals giving toric elliptic pairs is not known. Moreover, we do not have any examples of toric elliptic pairs (X, C) where X has Picard number three and $\overline{\mathrm{Eff}}(X)$ is non-polyhedral (see Remark 4.5 of [1]).

In this paper we completely classify all toric elliptic pairs coming from triangles, i.e. where X has Picard number two, the smallest possible. Strikingly, unlike the pentagon case, we prove that combinatorial restrictions allow only three such pairs.

Theorem 1.1. *There are only three toric elliptic pairs (X, C) where X has Picard number two. They are given by lattice triangles Δ with vertices $\{(0,0),(2,0),(5,8)\}$ with $m = 4$, $\{(0,0),(5,0),(12,20)\}$ with $m = 10$, and $\{(0,0),(5,0),(18,45)\}$ with $m = 15$, where m is the width of Δ.*

Remark 1.2. Since X has Picard number two in all of these cases, the effective cone is two-dimensional and generated by C and the exceptional divisor E over the identity element of the torus. Thus in this case the polyhedrality question is trivial and we are really only interested in the problem of classifying these pairs.

In Section 3 we show for each lattice triangle Δ in Theorem 1.1 that Δ gives rise to an extremal elliptic fibration. We will compute the singular fibers and Kodaira type. Fig. 1 shows the curves on the minimal resolution $\widetilde{X}$ of X for the $m = 4$ case. Here the underlying elliptic pair is (X, C). The curve C, which is not pictured in Fig. 1, passes through each boundary divisor given by a side of Δ with multiplicity equal to the lattice length of that side.

The curves $\tilde{g}$ and $\tilde{h}$ in Fig. 1 are additional curves of self-intersection -1 on X, which are obtained by analyzing curves on X as in will be described in Section 3.

By Castelnuovo's contraction criterion, we can then contract $\tilde{g}$ and $\tilde{h}$ to obtain the minimal model Z of $\widetilde{X}$. Fig. 2 shows the singular fibers obtained for the $m = 4$ case.

Sections 2 and 3 also answer a question posed by González-Anaya, González, and Karu in [8] and Kurano in [9]: are there negative curves with positive genus on $\mathrm{Bl}_e\mathbb{P}(\Delta)$ where Δ is a lattice triangle? A negative curve C in X is defined as a curve on $\mathrm{Bl}_e\mathbb{P}(\Delta)$ of non-positive self-intersection. Our toric elliptic pairs $(\mathrm{Bl}_e\mathbb{P}(\Delta)), C)$ provide an example of such curves, since by the definition of an elliptic pair we have $C^2 = 0$ and $p_a(C) = 1$.

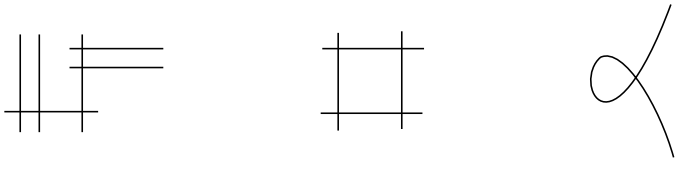

Fig. 2. The singular fibers of the minimal elliptic fibration Z_Δ, where $\Delta = \{(0,0),(2,0),(5,8)\}$.

The paper [1] also studies the distribution of primes p such that the reduction of the toric elliptic pair (X, C) modulo p, where C is an elliptic curve, has non-polyhedral effective cone. This is related to deep conjectures in arithmetic geometry of elliptic curves, including the Lang-Trotter conjecture [10].

In Section 4, we study an analogous question for a class of (non-toric) elliptic pairs, which come from blow-up of $\mathbb{P}^2$ at nine points on a nodal cubic C. Instead of the Lang-Trotter conjecture, which concerns the arithmetic of elliptic curves, we will study connections to Artin's conjecture, which can be interpreted in terms of the arithmetic of nodal cubics. This construction gives us examples of surfaces where the pseudo-effective cone is non-polyhedral for a set of primes p of positive density, and, assuming the generalized Riemann hypothesis, polyhedral for a set of primes p of positive density.

For our construction, we identify the smooth locus of the nodal cubic C with $\mathrm{Pic}^0(C)$, and $\mathrm{Pic}^0(C)$ with $\mathbb{G}_m$ in such a way that $1 \in \mathbb{G}_m$ is a flex point of C. We say that $a, q \in \mathbb{Q}$ are *multiplicatively independent* in $\mathbb{Q}^*$ if $a^x q^y = 1$ implies that $x = y = 0$. Let $z_1 = ... = z_7 = 1, z_8 = a, z_9 = qa^{-1}$ with $a, q \in \mathbb{Q}$ multiplicatively independent. We construct X to be the blow-up of $\mathbb{P}^2$ at the nine points $z_1, ..., z_9$, which is an infinitely near blow up for $z_1, ..., z_7$. That is, we consecutively blow up the point of intersection of the proper transform of C with the exceptional divisor of the previous blow-up. Let $\bar{a}$ and $\bar{q}$ be the reductions of a and q modulo p.

The surface X defined this way and the proper transform of C give an arithmetic elliptic pair $(\mathcal{C}, \mathcal{X})$ [1]. That is, $(\mathcal{C}, \mathcal{X})$ are a pair of schemes which are flat over a nonempty open subset $\mathcal{U}$ of Spec $\mathbb{Z}$, such that the geometric fiber (C_p, X_p) is an elliptic pair for every p in $\mathcal{U}$. In this setting, we derive the following arithmetic condition for polyhedrality.

Theorem 1.3. *The pair $(\mathcal{C}, \mathcal{X})$ gives an arithmetic elliptic pair [1] over a nonempty open subset $\mathcal{U}$ of* Spec $\mathbb{Z}$*, such that the geometric fiber (C_p, X_p) is an elliptic pair for every p in $\mathcal{U}$. Then $\overline{\mathrm{Eff}}(X_p)$ is polyhedral if and only if $\bar{a}^2 \in \langle \bar{q} \rangle \subset \mathbb{F}_p^*$.*

The question of when the condition in Theorem 1.3 holds has been studied extensively in number theory. More precisely, consider the set of primes p for which the condition is satisfied:

$$S(a, q) = \{p \text{ prime: } \bar{a} \in \langle \bar{q} \rangle \subset \mathbb{F}_p^*\}.$$

We show in Lemma 4.2 that the set $S(a, q)^c$ contains a set of prime numbers of positive density. That is, there is a set of primes of positive density for which $\overline{\mathrm{Eff}}(X_p)$ is not polyhedral.

We also mention some known results about $S(a, q)$. First, by a theorem of Pólya [6], $S(a, q)$ is infinite. Therefore, $\overline{\mathrm{Eff}}(X_p)$ is polyhedral for infinitely many primes. Furthermore, by Moree and Stevenhagen [7], assuming the generalized Riemann hypothesis, $S(a, q)$ has positive density in the set of all prime numbers.

Another useful result is Artin's conjecture on primitive roots, which states that if $q \in \mathbb{Z}$ is neither a perfect square nor -1, then $\bar{q} \mod p$ generates $\mathbb{F}_p^*$ for a set of primes p of positive density. If Artin's conjecture holds, we see that $S(a, q)$ will contain a set of positive density in the prime numbers.

By work of Hooley [4], Artin's conjecture follows from the generalized Riemann hypothesis. Thus by either Artin's conjecture or the work of Moree and Stevenhagen, if we accept the generalized Riemann hypothesis, there exists a set of primes of positive density for which $\overline{\mathrm{Eff}}(X_p)$ is polyhedral.

Finally, a theorem of Heath-Brown tells us that for any three primes (a, b, c), Artin's conjecture is true for at least one of a, b, and c [5]. Combined with Lemma 4.2, this allows us to construct surfaces with a polyhedral effective cone for a set of primes of positive density, and a non-polyhedral effective cone for a set of primes of positive density. We construct such a surface concretely in Lemma 4.3.

1.1. Acknowledgments

I am grateful to my senior thesis advisor, Jenia Tevelev, for his guidance and extensive feedback throughout this work. I would also like to thank Tom Weston for helpful discussions. This project has been partially supported by the NSF grant DMS-2101726 (PI Jenia Tevelev).

2. Toric elliptic pairs from triangles

We make preparations to define a toric elliptic pair, as in [1]. First, given a lattice polygon Δ, we define a morphism

$$\begin{aligned} g_\Delta : \mathbb{G}_2^m &\to \mathbb{P}^{|\Delta \cap \mathbb{Z}^2|-1} \\ x &\mapsto [x^i y^j : (i,j) \in \Delta \cap \mathbb{Z}^2] \end{aligned}$$

We let $\mathbb{P}(\Delta)$ be the closure of the image of g_Δ, and $e = g_\Delta(1,1)$. We denote by $\mathcal{L}_\Delta$ the linear system of hyperplane sections. Then any f in $\mathcal{L}_\Delta$ can be written as a Laurent polynomial with exponent vectors in Δ. That is,

$$f = \sum_{(i,j)\in\Delta} a_{ij} x^i y^j \in k[x^{\pm 1}, y^{\pm 1}].$$

Given a positive integer m, we define $\mathcal{L}_\Delta(m)$ to be the linear subspace of $\mathcal{L}_\Delta$ consisting of the curves having multiplicity at least m at e. Finally, we let $\mathrm{Vol}(\Delta)$ be twice the Euclidean area of Δ, so that $\mathrm{Vol}(\Delta)$ will be an integer.

Definition 2.1. Suppose there exist Δ and m such that the following conditions hold:

(i) $\mathrm{Vol}(\Delta) = m^2$;
(ii) $|\partial\Delta \cap \mathbb{Z}^2| = m$;
(iii) There is an irreducible curve Γ in $\mathcal{L}_\Delta(m)$ such that
  (a) Γ has multiplicity m at e
  (b) The Newton polygon of Γ coincides with Δ.

Let C be the proper transform of Γ under the blow-up. Then we call $(\mathrm{Bl}_e(\mathbb{P}(\Delta), C)$ a *toric elliptic pair*.

Remark 2.2. Theorem 4.4 of [1] proves that $(\mathrm{Bl}_e\mathbb{P}(\Delta), C)$ is an elliptic pair. In particular, (i), (ii), and (iiia) tell us that C has arithmetic genus 1, and (iiib) tells us that Γ does not pass through the singularities of $\mathbb{P}(\Delta)$. Thus C does not pass through the singularities of $\mathrm{Bl}_e\mathbb{P}(\Delta)$. Also, note that in the definition of toric elliptic pair given in [1] the authors additionally require that $\dim \mathcal{L}_\Delta(m) = 1$. However, their proof of Theorem 4.4 does not use this fact, so we have dropped this assumption in Definition 2.1.

We call a lattice triangle *primitive* if $\gcd(a, b, c) = 1$. Now we can state our main theorem. In this section we will prove that there are at most three toric elliptic pairs of Picard number two, given by a primitive

lattice triangle. In the next section we will verify that each of the lattice triangles in Theorem 2 actually gives us a toric elliptic pair, and show that non-primitive triangles cannot give toric elliptic pairs. In the rest of this paper we will take "triangle" to mean "lattice triangle."

As one may see from Definition 2.1, not all lattice polygons give toric elliptic pairs. In Lemma 2.3 we prove an additional arithmetic condition on the triangles Δ which do give toric elliptic pairs, in terms of the width of Δ. Theorem 2.4 shows that the arithmetic conditions from Lemma 2.3 and (i) and (ii) of Definition 2.1 are only satisfied for three primitive lattice triangles, up to $\mathrm{SL}_2(\mathbb{Z})$ transformation.

Lemma 2.3. *Let Δ be a lattice polygon, let $X = \mathrm{Bl}_e\mathbb{P}(\Delta)$ and suppose (X, C) is a toric elliptic pair. Let $m = |\partial\Delta \cap \mathbb{Z}^2|$. Then the width of Δ is $\geq m$.*

Proof. Pick a primitive vector λ in the lattice $\mathbb{Z}^2$ of one-parameter subgroups. Let D_λ be the prime divisor of $\mathbb{P}(\Delta)$ given by the closure of the corresponding one-parameter subgroup. More explicitly, if $\lambda = (i, j)$ the corresponding one-parameter subgroup is (t^i, t^j), which is given by the equation $x^j = y^i$.

Let H be a very ample divisor on $\mathbb{P}(\Delta)$ that gives a linear system $\mathcal{L}_\Delta$. Let w_λ be the width of Δ along λ. Then $w_\lambda = H \cdot D_\lambda$.

Now, consider the proper transform $\widetilde{D_\lambda}$ in the blow-up $\mathrm{Bl}_e\mathbb{P}(\Delta)$. Since D_λ goes through the identity with multiplicity one, we have $E \cdot \widetilde{D_\lambda} = 1$. We also have $\pi^* H \sim C + mE$.

By the projection formula,

$$w_\lambda = H \cdot D_\lambda = \pi^* H \cdot \widetilde{D_\lambda}.$$

So we have

$$\begin{aligned} w_\lambda &= (C + mE) \cdot \widetilde{D_\lambda} = C \cdot \widetilde{D_\lambda} + m(E \cdot \widetilde{D_\lambda}) \\ &= C \cdot \widetilde{D_\lambda} + m. \end{aligned}$$

The Newton polygon of C is Δ by (iii) of Definition 2.1. However, the Newton polygon of D_λ is a line segment. Thus they are not translates of one other. This tells us that the proper transforms of C and D_λ are two different irreducible curves on the blow-up. Thus $C \cdot \widetilde{D_\lambda} \geq 0$, giving us that $w_\lambda \geq m$. □

We begin by choosing representatives for equivalence classes of polygons under transformations in $\mathrm{SL}_2(\mathbb{Z})$. Every triangle is equivalent to a triangle with vertex set $\{(0,0), (a,0), (b,c)\}$ such that $a > 0$ and $0 \leq b < c$.

Theorem 2.4. *Let Δ be a primitive lattice triangle with width w. Let $m = |\delta\Delta \cap \mathbb{Z}^2|$. Suppose*

(i) $w \geq m$;
(ii) m^2 is twice the Euclidean area of Δ.

Then Δ can be obtained via an $SL_2(\mathbb{Z})$ transformation from one of $\{(0,0), (2,0), (5,8)\}$ with $m = 4$, $\{(0,0), (5,0), (12,20)\}$ with $m = 10$, and $\{(0,0), (5,0), (18,45)\}$ with $m = 15$.

Proof. Note that by definition of the area of Δ we have $m^2 = ac$. Also, the lattice lengths of the sides of Δ are $a, \gcd(b,c)$, and $\gcd(a-b,c)$. Thus $a + \gcd(b,c) + \gcd(a-b,c) = m$.

By assumption, the width of Δ is at least m. Let $\lambda = (1,-1)$ and $\nu = (1,0)$. Then we have $w_\lambda = a - (b-c) = a - b + c$ and $w_\nu = \max\{a,b\}$. Then $a - (b-c) \geq m$ and $\max\{a,b\} \geq m$. But we know $a < m$, so $\max\{a,b\} = b \geq m$. Rearranging, we get that $m - a \leq c - b \leq c - m$.

Let $b' = c - b$. Observe that we can impose any ordering on the lattice lengths of the sides of Δ. Then we have the following conditions, where (3) is the ordering of side lengths we impose:

$$m^2 = ac \tag{1}$$

$$a + \gcd(b', c) + \gcd(b' + a, c) = m \tag{2}$$

$$a \geq \gcd(b', c) \geq \gcd(b' + a, c) \tag{3}$$

$$m - a \leq b' \leq c - m. \tag{4}$$

In particular, by the ordering encoded by (2) and (3), we have $\frac{a}{m} \geq \frac{1}{3}$. We proceed by cases, considering different possible values of $\frac{a}{m}$.

Case 1: $\frac{a}{m} > \frac{2}{3}$.

We will prove an upper bound for an expression involving a, m, and c. First, observe that $\frac{c-m}{m-a} = \frac{m}{a} < \frac{3}{2}$. Thus by (4) we have

$$m - a \leq b' < \frac{3}{2}(m - a). \tag{5}$$

Also, by (2) and (3) we have $m - a > \gcd(b', c) \geq \frac{m-a}{2}$. Since by (4) we have $b' \geq m - a$, we cannot have $b' = \gcd(b', c)$. But by (5) we also have $b' < \frac{3}{2}(m - a) \leq 3\gcd(b', c)$. Thus $b' = 2\gcd(b', c)$.

Let $d = \gcd(b', c)$. Then $b' = 2d$ and $c = kd$ for some odd k in $\mathbb{Z}$. By (4) we have

$$\frac{d}{m - a} \leq \frac{1}{2} \cdot \frac{c - m}{m - a} = \frac{1}{2} \cdot \frac{m}{a} < \frac{1}{2} \cdot \frac{3}{2} = \frac{3}{4}.$$

Then by (2), $\gcd(b' + a, c) > \frac{1}{4}(m - a)$. On the other hand, $\gcd(a, d) = 1$ implies $\gcd(b' + a, c) = \gcd(2d + a, k)$. Thus we have $k > \frac{m-a}{4}$.

Also, from condition (2) we have $d + \gcd(b' + a, c) = m - a$. Combining this with (3) we get $d \geq \frac{m-a}{2}$.

Thus we obtain

$$c = kd > \frac{(m - a)^2}{8} = \frac{1}{8} \cdot a(c - 2m + a). \tag{6}$$

We also have $\frac{c}{a} = \left(\frac{m}{a}\right)^2 < \frac{9}{4}$. Combining this with (6) we see $\frac{1}{8}(c - 2m + a) < \frac{c}{a} < \frac{9}{4}$. Clearing denominators we obtain our promised upper bound:

$$c - 2m + a < 18. \tag{7}$$

Now, consider the following parameterization of the equation $ac = m^2$: $a = es^2, c = et^2$, and $m = ets$, where $e, t, s \in \mathbb{Z}$ and $\gcd(t, s) = 1$. Then our inequality (7) becomes $(t - s)^2 e < 18$. This leaves finitely many pairs $(t - s, e)$ to consider.

Let $x = t - s$. Then inequality (4) becomes

$$esx \leq 2d \leq e(s + x)x. \tag{8}$$

Thus we can write $2d = esx + p$ where $0 \leq p \leq ex^2 < 18$. From the equation $c = kd$ we get

$$2e(s + x)^2 = k(esx + p). \tag{9}$$

Equation (9) gives us a family of diophantine equations in s and k with a finite set of parameters (e, x, p). We will proceed by solving this family of diophantine equations abstractly in terms of e, x, and p, and using a computer to substitute particular values of (e, x, p).

We rearrange equation (9) into quadratic form with respect to s, obtaining $2es^2+ex(4-k)s+2ex^2-pk=0$. Solving for s, we obtain

$$s = \frac{1}{4e}(-ex(4-k) \pm \sqrt{D}), \qquad D := e^2x^2(4-k)^2 - 8e(2ex^2 - pk).$$

Since $-ex(4-k) \pm \sqrt{D}$ is in $4\mathbb{Z}$, we see that $\sqrt{D}$ must be in $\mathbb{Z}$. Let $y = \sqrt{D}$. Then we solve

$$\begin{aligned} y^2 &= D \\ &= e^2x^2(4-k)^2 - 8e(2ex^2 - pk) \\ &= (ex)^2k^2 - 8e(ex^2 - p)k. \end{aligned}$$

Completing the square with respect to k gives us

$$\left(exk - \left(ex - \frac{p}{x}\right)\right)^2 = y^2 + 16\left(ex - \frac{p}{x}\right)^2.$$

Multiplying by x^2 on each side to clear denominators gives us $(ex^2k-4(ex^2-p))^2 = y^2x^2+16(ex^2-p)^2$. We can then factor the difference of squares to obtain

$$(ex^2k - 4(ex^2 - p) - xy)(ex^2k - (ex^2 - p) + xy) = 16(ex^2 - p)^2. \tag{10}$$

Now we simply need to plug in values of e, x, and p such that $0 \leq p \leq ex^2 < 18$ and factor the right hand side of (10). We will obtain a finite list of options for k and y for each choice of (e, x, p) by solving two linear equations in two variables. We can further subject (k, y) to the conditions that k is odd and that $\gcd(a, d) = 1$. Each choice of (k, y) will give us two options for s (corresponding to $\pm\sqrt{D}$). Thus we can completely check all possible triangles.

Finally, by condition (2), we have $m - a - d = \gcd(2d + a, c)$. Without this condition, we have five candidate triangles. With this condition added, we have none. Sage code which executes the algorithm just described is included in Section 5.1.

Case 2: $\frac{1}{2} < \frac{a}{m} \leq \frac{2}{3}$.

Observe that $\frac{c-m}{m-a} = \frac{m}{a} < 2$. Thus by condition (4) we have $m - a \leq b' < 2(m - a)$. Also, by conditions (2) and (3) we have $m - a > \gcd(b', c) \geq \frac{m-a}{2}$. Thus we have $b' = 2d$ or $b' = 3d$.

We will use the bounds on $\frac{a}{m}$ to bound possible k, where $k = \frac{c}{d}$ is as in case 1.

By conditions (2) and (3) we obtain $\frac{m}{2} > d \geq \frac{m}{6}$. Re-arranging and substituting $k = \frac{c}{d}$, we obtain

$$6\left(\frac{c}{m}\right) \geq k > 2\left(\frac{c}{m}\right).$$

Now recall that $m^2 = ac$. Thus $\frac{a}{m} \cdot \frac{c}{m} = 1$. But we also have $\frac{1}{2} < \frac{a}{m} \leq \frac{2}{3}$. Thus $2 > \frac{c}{m} \geq \frac{3}{2}$. Substituting these inequalities into our bounds on k, we obtain

$$12 > k > 3. \tag{11}$$

Suppose $b' = 2d$. Since $(b', c) = d$, we know k must be odd. Thus we obtain a finite list of options: $k = 5, 7, 9, 11$.

Next, suppose $b' = 3d$. Then k cannot be divisible by 3. Thus we obtain a finite list of options: $k = 4, 5, 7, 8, 10, 11$.

Furthermore, by condition (2) and $\gcd(a,d)=1$, we have that $d = m - a - \gcd(2d+a,k)$. Let $x = \gcd(2d+a,k)$. Then x must divide k. Thus we obtain a finite family of diophantine equations in (a,m) with parameters (k,x):

$$m^2 = ac = kda = ka(m-a-x). \tag{12}$$

Putting equation (12) into quadratic form with respect to $\frac{m}{a}$ and solving gives us

$$2\left(\frac{m}{a}\right) = k \pm \sqrt{k^2 - 4k - 4\frac{kx}{a}}. \tag{13}$$

But recall we have $\frac{1}{2} < \frac{a}{m} \leq \frac{2}{3}$, so

$$3 \leq 2\left(\frac{m}{a}\right) < 4. \tag{14}$$

Since $k \geq 4$ by equation (11) we have $k + \sqrt{k^2 - 4k - 4\frac{kx}{a}} \geq 4$. Thus the larger root in (13) will always fall outside the bound given in (14), and we can restrict our attention to the smaller root.

Suppose that $k = 4$. Then equation (11) has no real solutions. Thus we must have $k > 4$.

Since $k > 4$ we have that $2k - 9 > 0$. Now, suppose that $a > \frac{4kx}{2k-9}$. Then $2k - 4\frac{kx}{a} > 9$. Adding k^2 to both sides, we get $k^2 - 6k + 9 < k^2 - 4k - 4\frac{kx}{a}$. Thus $k - 3 < \sqrt{k^2 - 4k - 4\frac{kx}{a}}$. Finally, we see $3 > k - \sqrt{k^2 - 4k - 4\frac{kx}{a}}$, which falls outside of our bound in (14). Thus if (14) is satisfied, we must have

$$a \leq \frac{4kx}{2k-9}. \tag{15}$$

We thus have a finite family of triples (k,a,x), which we can use to solve the equation $m^2 = ka(m-a-x)$ for possible m. We can then check for each m obtained this way that m is in an integer, and that $\frac{a}{m} > \frac{1}{2}$. The code for this procedure is included in Section 5.2.

Running the code results in the candidates:

$$k = 5,\ a = 9,\ x = 1,\ m = 15$$
$$k = 5,\ a = 45,\ x = 5,\ m = 75.$$

Finally, we determine whether candidate triangles (m,a,c) listed above are primitive lattice triangles satisfying the conditions (1) through (4).

Candidate 1: We calculate $d = m - a - \gcd(2d+a,k) = 5$. Then $c = kd = 5 \cdot 5 = 25$. Next, suppose $b' = 2d$. Then $b = c - 2d = 25 - 2 \cdot 5 = 15$. Thus we get the triangle $\{(0,0),(9,0),(15,25)\}$. This triangle is $\mathrm{SL}_2(\mathbb{Z})$ equivalent to $\{(0,0),(5,0),(18,45)\}$, and the remaining conditions can be easily checked.

If we instead suppose that $b' = 3d$, we get $b = 10$. Thus we get the triangle $\{(0,0),(9,0),(10,25)\}$. However, this does not satisfy (4), as $10 = b \not\geq m = 15$.

Candidate 2: We calculate $d = m - a - \gcd(2d+a,k) = 25$. Thus $c = kd = 125$. Then $b' = 2d$ or $b' = 3d$. Thus $b = 50$ or 75. In either case, the lattice triangle we obtain is not primitive, i.e. $\gcd(a,b,c) > 1$.

Case 3: $\frac{1}{3} \leq \frac{a}{m} \leq \frac{1}{2}$.

Observe that $\gcd(b,c) = \gcd(b',c) = d$. Let $b = b_0 d$ and $c = c_0 d$. Recall that by condition (3), we have $d \geq \gcd(b'+a,c)$. So by condition (2) we get that $d \geq \frac{m-a}{2}$. But since $a \leq \frac{m}{2}$ we get $d \geq \frac{m}{4}$. Also, using $a \geq \frac{m}{3}$ and condition (1), we get $c = \left(\frac{m}{a}\right) m \leq 3m$. Thus we have

$$c_0 d \leq 3m = 12\left(\frac{m}{4}\right) \leq 12d.$$

We also have that $b \geq m > 2d$. Thus $b_0 \geq 3$. To summarize, we've obtained the finite list of possibilities

$$3 \leq b_0 < c_0 \leq 12.$$

From condition (4) we also have $c_0 - b_0 \geq \frac{m}{d}$. From condition (3) we have $m \geq 2a \geq 2d$, so $\frac{m}{d} \leq 2$. So $c_0 - b_0 \geq 2$.

Let $x = \gcd(b' + a, c)\gcd(b - a, c)$. Since $1 = \gcd(a, b, c) = (a, d)$, we get

$$x = \gcd(b_0 d - a, c_0 d) = \gcd(b_0 d - a, c_0)|c_0.$$

Thus we have a finite list of possible x. By condition (2), we have $d = m - a - x$. From this and condition (3) we get that $m \geq 2d = 2(m - a - x)$. Simplifying, we obtain

$$\frac{m}{2} \geq a \geq \frac{m - 2x}{2}.$$

Thus we can consider the finite list $a = \frac{m}{2}, ..., \frac{m-2x}{2}$. Suppose $a = \frac{m-y}{2}$ where $0 \leq y \leq 2x$. We also have $c = c_0 d = c_0(m - a - x)$. Substituting for a and c into the equation $ac = m^2$, we obtain

$$\left(\frac{m - y}{2}\right) c_0 \left(m - \frac{m - y}{2} - x\right) = m^2.$$

Simplifying, we obtain the following quadratic equation in m:

$$(c_0 - 4)m^2 - 2c_0 xm - c_0 y(y - 2x) = 0. \tag{16}$$

We can solve equation (16) for m for each of a finite family of parameters (b_0, c_0, x, y) subject to the conditions $0 \leq y \leq 2x$, x divides c_0, $3 \leq b_0 \leq c_0 \leq 12$, and $c_0 - b_0 \geq 2$. Then we check whether the m obtained is an integer and whether the lattice triangle is primitive. The code for the procedure described in this paragraph is given in Section 5.3. Finally, we check that our candidate triples (a, b, c) satisfy (1) through (4).

By running the code in Section 5.3, we obtain the triples

$$m = 3 : (1, 5, 9)$$
$$m = 4 : (2, 3, 8), (2, 5, 8)$$
$$m = 6 : (3, 8, 12)$$
$$m = 10 : (5, 12, 20).$$

We eliminate $(1, 5, 9)$, since the width of the corresponding triangle is 2. We eliminate $(2, 3, 8)$, since the width of the corresponding triangle is 3. We eliminate $(3, 8, 12)$ because the number of lattice points on the boundary is 8. The other two triples satisfy all of conditions (1) through (4).

Example 2.5. We include an example of how the code in Section 5.3 will proceed for a particular choice of (b_0, c_0, x, y). Suppose $b_0 = 5$ and $c_0 = 8$. Then $x = 1, 2, 4, 8$ are possibilities. Equation (16) gives us

$$4m^2 - 16xm + 8(2xy - y^2) = 0.$$

Suppose $x = 1$ and $y = 0$. Then we obtain $m^2 - 4m = 0$. Thus $m = 4$. Then $a = \frac{m}{2} = 2$. To calculate d, we solve $4^2 = m^2 = c_0 da = 8 \cdot d \cdot 2$. Thus $d = 1$.

The code produces the candidate triple $(2, 5, 8)$. We manually check the lattice perimeter: $a + d + x = 2 + 1 + 1 = 4$. Indeed, this triangle is one of the three triangles in the statement of Theorem 2.4. □

3. Elliptic fibrations

Definition 3.1. An elliptic fibration is a morphism from an irreducible projective surface S to a smooth curve, e.g. $\mathbb{P}^1$, such that a general fiber is an elliptic curve. An elliptic fibration is called *extremal* if it has a section and the Mordell-Weil group of sections is finite.

Theorem 3.2. *Each of the three lattice triangles with vertex sets* $\{(0,0),(2,0),(5,8)\}$, $\{(0,0),(5,0),(12,20)\}$, *and* $\{(0,0),(5,0),(18,45)\}$ *of Theorem 2.4 gives us a rational extremal elliptic fibration. The corresponding minimal rational elliptic fibrations are surfaces of types* X_{141}, X_{211}, *and* X_{211} *respectively [3]. That is, they have singular fibers of types* $I_1^* I_4 I_1, II^* I_1 I_1$, *and* $II^* I_1 I_1$ *in Kodaira's classification.*

Proof. We show that if Δ is one of the three triangles above, then $\mathcal{L}_\Delta(m)$ is an elliptic fibration, i.e. a pencil which contains an elliptic curve. We then compute the minimal resolutions of each $\mathrm{Bl}_e\mathbb{P}(\Delta)$ and find the minimal model of the corresponding smooth rational elliptic fibration, and compute its Kodaira type. Since Δ has a side of lattice length one, the toric boundary divisor corresponding to this side intersects the elliptic curve in exactly one point. Thus we have at least one section of the fibration. Table 1 in [3] then shows that the elliptic fibration is extremal.

Suppose that Δ is one of our three triangles. Then m is equal to the width of Δ. Let $(v, -u)$ be a vector which achieves m. Then the curve $(x^u y^v - 1)^m$ given by m copies of the one parameter subgroup has multiplicity m at e. Now, let $s = b - mu$ and consider the curve $g(x, y) = x^s(x^u y^v - 1)^m$, which also has multiplicity m at e.

We claim that the exponents of monomials in Supp g are in Δ. To see this, write

$$g(x,y) = \sum_{i=1}^{m} (-1)^i x^s (x^u y^v)^i.$$

So all of the exponents of monomials in g lie along the line from $(s, 0)$ to $m \cdot (u, v) + (s, 0) = (b, mv)$. In each of our examples, $(a, 0) \cdot (v, -u) = m$, so $c = \frac{m^2}{a} = \frac{amv}{a} = mv$. Thus the endpoints of the line segment are in the convex polygon Δ, so the entire line segment lies in Δ. We conclude that g is in $\mathcal{L}_\Delta(m)$. We will use the existence of g to find curves on $\mathrm{Bl}_e\mathbb{P}(\Delta)$ which we can contract to compute its minimal resolution.

Example 3.3. Consider the triangle $\Delta = \{(0,0),(2,0),(5,8)\}$ with $m = 4$. By Computation 3.4 below, the width of Δ is achieved in the direction $(2, -1)$. We expand $g(x, y) = x(xy^2 - 1)^4 = x((xy^2)^4 - (xy^2)^3 + (xy^2)^2 - xy^2 + 1)$. One can verify visually that each of these monomials have exponents in Δ, as in Fig. 3.

Next, we compute using the Magma package "non-polyhedral" which is available on Github [2] that for each of our surfaces $\mathbb{P}(\Delta)$, there is an curve Γ in $\mathcal{L}_\Delta(m)$ whose Newton polytope coincides with Δ. We include the $m = 4$ case as an example.

Computation 3.4. *Let* $\Delta = \{(0,0),(2,0),(5,8)\}$. *We find a curve* Γ *on* X_Δ *which goes through the identity element of the torus with multiplicity* 4. *Our* Γ *is denoted* f *in the computation below. Here the command "Genus" gives the geometric genus of* f.

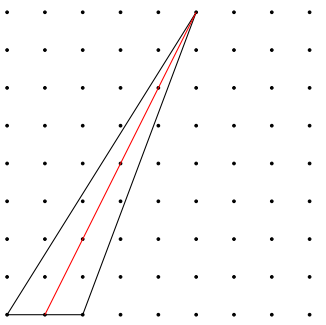

Fig. 3. The triangle Δ for $m = 4$. All monomials in g are lattice points along the median.

```
> pol:=Polytope([[0,0],[2,0],[5,8]]);
> Width(pol);
4 {
    (2, -1),
    (-2, 1)
}
> f:=FindCurve(pol, 4, Rationals());
> f;
Curve over Rational Field defined by
9/4*x[1]^5*x[2]^8 - 8*x[1]^4*x[2]^6 + 15/2*x[1]^3*x[2]^4 + 2*x[1]^3*x[2]^3 +
    2*x[1]^2*x[2]^3 - 6*x[1]^2*x[2] + x[1]^2 - 6*x[1]*x[2] + 17/4*x[1] + 1
> Genus(f);
1
```

We know that $p_a(C) = 1$ by Proposition 4.2 of [1]. Thus we have that C is smooth, irreducible, and genus one, hence an elliptic curve.

We also need to check that Γ does not pass through the singularities of $\mathbb{P}(\Delta)$. As observed in Section 2, this is equivalent to the Newton polytope of Γ being equal to Δ. Again, we include the $m = 4$ case as an example.

Computation 3.5. *We compute the Newton polytope of* Γ.

```
> pol:=Polytope([[0,0],[2,0],[5,8]]);
> f:=FindCurves(pol, 4, Rationals())[1];
> Transpose(Matrix(Vertices(NPolytope(f))));
[5 2 0]
[8 0 0]
```

Let $X = \mathrm{Bl}_e\mathbb{P}(\Delta))$, and C be the proper transform of Γ. Then both C and the proper transform $\tilde{g}$ of g are in $H^0(X, C)$, and they are not the same curve, since one is an elliptic curve and the other is a rational curve. Thus for each of our surfaces, $h^0(X, C) \geq 2$. By Lemma 3.2 in [1], $h^0(X, C) = 2$. Thus (X, C) gives an elliptic fibration.

To show that (X, C) is extremal, we compute the minimal resolution $\widetilde{X}$ of X, and the minimal elliptic fibration Z of $\widetilde{X}$. We recover the Kodaira type of Z, showing that the fibration is extremal.

Triangle 1: $\Delta = \{(0, 0), (2, 0), (5, 8)\}$ with $m = 4$.

We compute the minimal resolution of $\widetilde{X}$ of X, which is given by Fig. 4. The number on each curve in Fig. 4 indicates its self-intersection. The lines in bold are the curves of self intersection -1 given by the sides of Δ.

The curve $\tilde{g}$ in Fig. 4 is the proper transform of $g(x, y) = x(xy^2 - 1)^4$. The curve $\tilde{h}$ is the proper transform of the curve $h(x, y) = x^2y^3 - 3xy + x + 1$. We obtain h by factoring the adjoint linear system $|K + C|$ into prime components as in Computation 3.6, where K is the canonical divisor on X.

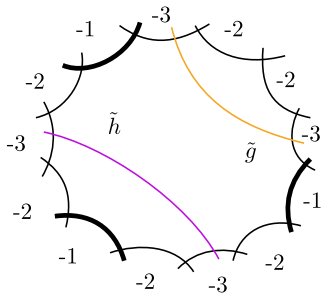

Fig. 4. Intersections of curves on $\widetilde{X_\Delta}$, where $\Delta = \{(0,0),(2,0),(5,8)\}$.

Computation 3.6. *Finding the factorization of* $|K+C|$ *for* $\Delta = \{(0,0),(2,0),(5,8)\}$.

```
> pol := Polytope([[0,0],[2,0],[5,8]]);
> PolsAdjSys(pol);
[x[1]*x[2]^2 - 1, x[1]^2*x[2]^3 - 3*x[1]*x[2] + x[1] + 1]
```

By adjunction, $(K+C)\cdot C = 0$, so $\tilde{h}$ and C are disjoint. In Computation 3.7 we check using Magma that $\tilde{g}$ and $\tilde{h}$ are curves of self-intersection -1 on $\widetilde{X}$. This will later allow us to contract $\tilde{g}$ and $\tilde{h}$ using Castelnuovo's contraction criterion.

Computation 3.7. *Computing the self-intersection of* C, $\tilde{g}$, *and* $\tilde{h}$ *on* $\widetilde{X_\Delta}$. *The rows in the matrix return by AdjSys represent the classes of* C, $\tilde{g}$, *and* $\tilde{h}$, *respectively, in the Picard group of* $\widetilde{X_\Delta}$. *The last number in each row gives the multiplicity of the curve at* e.

```
> adjsysmatrix := Matrix(Rationals(), #AdjSys(pol), #AdjSys(pol)[1], AdjSys(pol));
> adjsysmatrix;
[ 8  5  2  1  0  0  0  0  0  0  1  2  5 -4]
[ 2  1  0  0  0  0  0  0  0  0  0  0  1 -1]
[ 3  2  1  1  1  0  0  0  0  1  1  1  2 -2]
> matrix := imatS(pol);
> adjsysmatrix*matrix*Transpose(adjsysmatrix);
[ 0  0  0]
[ 0 -1  0]
[ 0  0 -1]
```

We also use Magma to calculate the intersections between $\tilde{g}, \tilde{h}$, and the proper transforms of the toric boundary divisors of X_Δ, which are depicted in Fig. 4.

Computation 3.8. *The intersection matrix of the minimal resolution* $\widetilde{X_\Delta}$ *of* X_Δ.

```
> Transpose(Matrix(Reorder(Rays(Resolution(NormalFan(pol))))));
[ 0 -1 -2 -5 -8 -3 -1  1  3  8  5  2  1]
[ 1  1  1  2  3  1  0 -1 -2 -5 -3 -1  0]
> imatS(pol);
[-1  1  0  0  0  0  0  0  0  0  0  0  1  0]
[ 1 -2  1  0  0  0  0  0  0  0  0  0  0  0]
[ 0  1 -3  1  0  0  0  0  0  0  0  0  0  0]
[ 0  0  1 -2  1  0  0  0  0  0  0  0  0  0]
[ 0  0  0  1 -1  1  0  0  0  0  0  0  0  0]
[ 0  0  0  0  1 -3  1  0  0  0  0  0  0  0]
[ 0  0  0  0  0  1 -2  1  0  0  0  0  0  0]
[ 0  0  0  0  0  0  1 -2  1  0  0  0  0  0]
[ 0  0  0  0  0  0  0  1 -3  1  0  0  0  0]
[ 0  0  0  0  0  0  0  0  1 -1  1  0  0  0]
[ 0  0  0  0  0  0  0  0  0  1 -2  1  0  0]
[ 0  0  0  0  0  0  0  0  0  0  1 -3  1  0]
```

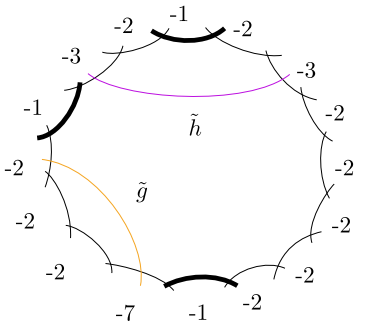

Fig. 5. Intersections of curves on $\widetilde{X_\Delta}$, with $\Delta = \{(0,0),(5,0),(12,20)\}$.

```
[ 1  0  0  0  0  0  0  0  0  0  0  1 -2  0]
[ 0  0  0  0  0  0  0  0  0  0  0  0  0 -1]
```

Each ray of the normal fan corresponds to a divisor in $\widetilde{X_\Delta}$. The toric boundary divisors corresponding to the sides of Δ are given by $(0,1),(8,-3)$, and $(8,-5)$ in the normal fan, which correspond to the curves of self-intersection -1 in the 14×14 intersection matrix given by Computation 3.8. We see from the exponents of g that $\tilde{g}$ intersects the curves given by $\pm(2,-1)$ in the normal fan, which correspond to rows 6 and 9 in the intersection matrix, thus allowing us to place $\tilde{g}$ in Fig. 4.

We can also see from the exponents of h that $\tilde{h}$ intersects the curves in the minimal resolution which given by $(2,3)$ and $(1,1)$ in the normal fan, thus allowing us to place it in Fig. 4.

The elliptic curve C, which is not pictured in Fig. 4, passes through each boundary divisor given by a side of Δ with multiplicity equal to the lattice length of that side.

Since $\tilde{g}$ and $\tilde{h}$ each have self-intersection -1 on X_Δ, we can contract them using Castelnuovo's contraction criterion. We obtain a configuration of -2 curves with Dynkin diagram D_5 from contracting $\tilde{g}$, and A_3 by contracting $\tilde{h}$, which correspond to singular fibers of Kodaira type I_1^* and I_4. These fibers are pictured in Fig. 2. Since we have an elliptic fibration, the sum of the Euler characteristics of the singular fibers must be 12. So we must also have a singular fiber of type I_1. Thus the Kodaira type is X_{141}, and consequently the elliptic fibration is extremal [3].

Triangle 2: $\Delta = \{(0,0),(5,0),(12,20)\}$ with $m = 10$.

As in Computation 3.8, we obtain Fig. 5 by computing the normal fan and intersection matrix of Δ. By a Magma calculation, the width of Δ is achieved in the direction $(2,-1)$. The curve $\tilde{g}$ in Fig. 5 is the proper transform of $g(x,y) = x^2(xy^2-1)^{10}$.

The curve $\tilde{h}$ in Fig. 5 is the proper transform of $h(x,y) = x^2y^3 - 3xy + x + 1$. As in the Triangle 1 case, $h(x,y)$ is a curve on $\mathbb{P}(\Delta)$ which is obtained by factoring the adjoint linear system $|K+C|$ (see Computation 3.9).

Computation 3.9. *Finding the factorization of* $|K+C|$ *for* $\Delta = \{(0,0),(5,0),(12,20)\}$.

```
> pol := Polytope([[0,0],[5,0],[12,20]]);
> PolsAdjSys(pol);
[x[1]*x[2]^2 - 1, x[1]^2*x[2]^3 - 3*x[1]*x[2] + x[1] + 1]
```

The computation that $\tilde{g}$ and $\tilde{h}$ are disjoint and each have self-intersection -1 is identical to that of Computation 3.7, with the vertices of "pol" replaced by the vertices of Triangle 2.

Again, we can contract $\tilde{g}$ and $\tilde{h}$ using Castelnuovo's contraction criterion. We obtain a configuration of -2 curves with Dynkin diagram E_8 by contracting $\tilde{g}$. Similarly, we obtain a configuration of curves with

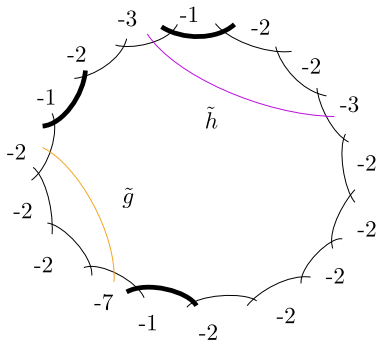

Fig. 6. Intersections of curves on $\widetilde{X_\Delta}$, with $\Delta = \{(0,0),(5,0),(18,45)\}$.

Dynkin diagram A_1 by contracting $\tilde{h}$. These correspond to singular fibers of Kodaira type II^* and I_1, respectively. Thus the Kodaira type is X_{211}, and consequently the elliptic fibration is extremal [3].

Triangle 3: $\Delta = \{(0,0),(5,0),(18,45)\}$ with $m = 15$.

By a Magma calculation, the width of Δ is achieved in the direction $(3,-1)$. The curve $\tilde{g}$ in Fig. 6 is the proper transform of $g(x,y) = x^3(xy^5-1)^{15}$. As in Computation 3.8, we obtain Fig. 5 by computing the normal fan and intersection matrix of Δ.

The curve $\tilde{h}$ in Fig. 6 is the proper transform of $h(x,y) = x^3y^7 - 2x^2y^5 - x^2y^4 + 5xy^2 - 3xy + x - 1$, which is obtained by factoring the adjoint linear system $|K+C|$ (see Computation 3.10). The computation that $\tilde{g}$ and $\tilde{h}$ are disjoint and each self-intersection -1 is identical to that of Computation 3.7, with the vertices of "pol" replaced by the vertices of Triangle 3.

Computation 3.10. *Finding the factorization of $K+C$ for $\Delta = \{(0,0),(5,0),(18,45)\}$.*

```
> pol := Polytope([[0,0],[5,0],[18,45]]);
> PolsAdjSys(pol);
[x[1]*x[2]^3 - 1, x[1]^3*x[2]^7 - 2*x[1]^2*x[2]^5 - x[1]^2*x[2]^4 + 5*x[1]*x[2]^2
    - 3*x[1]*x[2] + x[1] - 1]
```

Again, we can contract $\tilde{g}$ and $\tilde{h}$ using Castelnuovo's contraction criterion. We obtain E_8 by contracting $\tilde{g}$, and A_1 by contracting $\tilde{h}$, which correspond to singular fibers of Kodaira type II^* and I_1, respectively. Thus the Kodaira type is X_{211}, as in Triangle 2, and consequently the elliptic fibration is extremal [3]. □

Now that we know that (X_Δ, C) are elliptic pairs for each of our triangles Δ, we can combine this result with Theorem 2.4 to completely classify all toric elliptic pairs of Picard number two.

Theorem 3.11. *Suppose that (X,C) is a toric elliptic pair, where $X = \mathrm{Bl}_e(\mathbb{P}(\Delta)$ for some lattice triangle Δ. Then Δ is one of $\{(0,0),(2,0),(5,8)\}$ with $m=4$, $\{(0,0),(5,0),(12,20)\}$ with $m=10$, and $\{(0,0),(5,0),(18,45)\}$ with $m=15$.*

Proof. First, recall that $\mathrm{SL}_2(\mathbb{Z})$-equivalent polygons give rise to isomorphic toric surfaces. Thus Theorem 2.4 tells us that if Δ is primitive, then Δ can be transformed via an $\mathrm{SL}_2(\mathbb{Z})$ transformation to one of the triangles listed in the theorem.

Write $\Delta = \{(0,0),(a,0),(b,c)\}$ where $(\gcd(a,b,c) = k$ and $m = |\delta\Delta \cap \mathbb{Z}^2|$. Then $m = kn$ for some $n \in \mathbb{N}$.

Let Δ/k be $\{(0,0),(a/k,0),(b/k,c/k)\}$. Then Δ/k is primitive and satisfies the hypothesis of Theorem 2.4. So Δ/k is one of the three triangles listed in the theorem.

Since each of our triangles Δ/k gives an elliptic fibration, we know that $\dim \mathcal{L}_{\Delta/k}(n) = 2$. Let $\{g,h\}$ be a basis of $\mathcal{L}_{\Delta/k}(n)$. Then g^k and h^k are two linearly independent curves in $\mathcal{L}_\Delta(m)$, so $\dim \mathcal{L}_\Delta(m) \geq 2$.

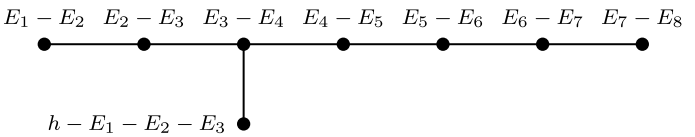

Fig. 7. Dynkin diagram of $\mathbb{E}_8$ labeled with simple roots.

Thus by Lemma-Definition 3.2 of [1], we have that $\dim \mathcal{L}_\Delta(m) = 2$. Therefore, every member of $\mathcal{L}_\Delta(m)$ is a linear combination of g^k and h^k, and thus factors nontrivally over $\mathbb{C}$. But there must be an irreducible curve in $\mathcal{L}_\Delta(m)$ by definition of a toric elliptic pair. Thus we have $k = 1$ and $\Delta/k = \Delta$. □

4. Elliptic pairs from a nodal cubic in $\mathbb{P}^2$

In this section, we will consider non-toric elliptic pairs coming from blow-ups of $\mathbb{P}^2$ at nine points on the nodal cubic over an algebraically closed field of prime characteristic p.

Let C be the nodal cubic $y^2z = x^2(x + z)$ in $\mathbb{P}^2$. We will identify the smooth locus of C with $\mathrm{Pic}^0(C)$, and $\mathrm{Pic}^0(C)$ with $\mathbb{G}_m$. We choose $1 \in \mathbb{G}_m$ to be the flex point $[0 : 1 : 0]$ of C. We say that $a, q \in \mathbb{Q}$ are *multiplicatively independent* in $\mathbb{Q}^*$ if $a^x q^y = 1$ implies that $x = y = 0$.

Let $z_1 = ... = z_7 = 1, z_8 = a, z_9 = qa^{-1}$ with $a, q \in \mathbb{Q}$ multiplicatively independent. Let X be the blow-up of $\mathbb{P}^2$ at the nine points $z_1, ..., z_9$, which is an infinitely near blow up for $z_1, ..., z_7$. That is, we consecutively blow up the point of intersection of the proper transform of C with the exceptional divisor of the previous blow-up. Let $\bar{a}$ and $\bar{q}$ be the reductions of a and q modulo p. Then (C, X) is an elliptic pair defined over $\mathbb{Q}$. Thus by Definition 3.19 of [1], (C, X) gives rise to an *arithmetic elliptic pair* $(\mathcal{C}, \mathcal{X})$ over a nonempty open subset $\mathcal{U}$ of Spec $\mathbb{Z}$, where the geometric fiber (C_p, X_p) is an elliptic pair for every p in $\mathcal{U}$.

Theorem 4.1. *Let $(\mathcal{C}, \mathcal{X})$ be the arithmetic elliptic pair [1] given by the procedure above, and defined over a nonempty open subset $\mathcal{U}$ of* Spec $\mathbb{Z}$*, such that the geometric fiber (C_p, X_p) is an elliptic pair for every p in $\mathcal{U}$. Then $\overline{\mathrm{Eff}}(X_p)$ is polyhedral if and only if $\bar{a}^2 \in \langle \bar{q} \rangle \subset \mathbb{F}_p^*$.*

Proof. There is a restriction map

$$\mathrm{res} : \mathrm{Pic}(X) \to \mathrm{Pic}(C)$$

which sends $C^\perp$ into $\mathrm{Pic}^0(C)$. Also, observe that $C^\perp/\langle C \rangle$ with an intersection pairing gives rise to the root lattice $\mathbb{E}_8$. In particular, the curves of self-intersection -2 on X are effective roots in $\mathbb{E}_8$. We will show that a certain subset of these effective roots generates a root sublattice of rank 7.

Let E_i be the exceptional divisor of the ith blow-up. For ease of notation, we will allow ourselves to denote the proper transform of $\widetilde{E_i}$ after the $(i + 2)$th blow-up as $\widetilde{E_i}$, because $\widetilde{E_i}$ is disjoint from E_{i+2} and is thus unchanged by the $(i + 2)$th blow-up. Thus $E_i = \widetilde{E_i} + ... + \widetilde{E_6} + E_7$ for $i \leq 7$. Then $E_i^2 = -1$ and $E_i \cdot E_j = 0$ if $|j - i| \geq 1$.

Let h be the class of a line in $\mathrm{Pic}^0(C)$. We can label the Dynkin diagram of $\mathbb{E}_8$ with roots as in Fig. 7, all of which are effective except $E_7 - E_8$.

Since 1 is a flex point of C, the root $(h - E_1 - E_2 - E_3)$ is realized by the class of a proper transform of a tangent line at 1, so it is indeed an effective root. Also, $E_i - E_{i+1} = \widetilde{E_i}$ are effective roots for all $1 \leq i \leq 7$. Computing the self-intersections, we see that $(E_i - E_{i+1})^2 = -2$. Also, since h is disjoint from E_1, E_2, and E_3, we have $(h - E_1 - E_2 - E_3)^2 = h^2 - 2h(E_1 + E_2 + E_3) + (E_1 + E_2 + E_3)^2 = 1 + 0 - 3 = -2$. Finally, curves that correspond to adjacent nodes have intersection 1: $(E_i - E_{i+1})(E_{i+1} - E_{i+2}) = -E_{i+1}^2 = 1$.

Because $\mathrm{res}(C^\perp)$ lies in $\mathrm{Pic}^0(C)$, we obtain an induced map

$$\overline{\mathrm{res}} : C^\perp/\langle C \rangle \to \mathrm{Pic}^0(C)/\langle \mathrm{res}(C) \rangle.$$

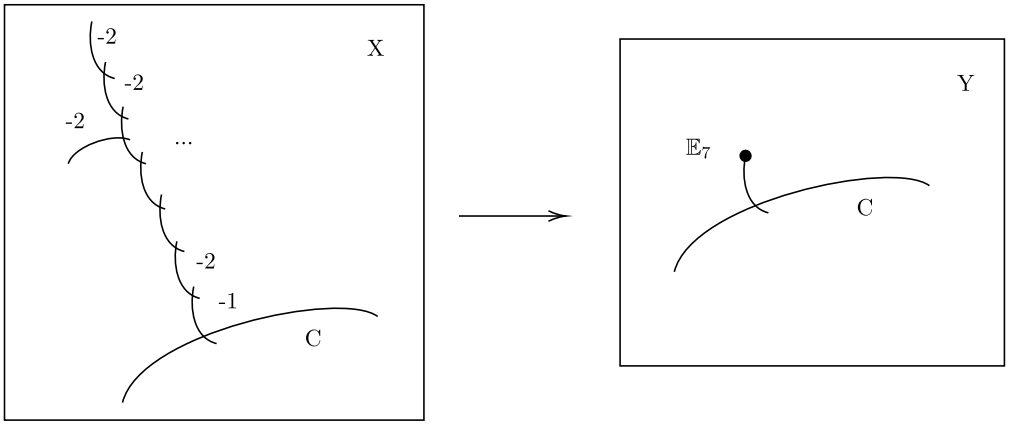

Fig. 8. Contracting the $\mathbb{E}_7$ sublattice in X to obtain Y.

Table 1
Images of roots under the map $\overline{\text{res}}$.

Roots	Image in $\text{Pic}^0(C)/\langle \text{res}(C)\rangle$
$E_i - E_8,\ i < 8$	a^{-1}
$E_i - E_9,\ i < 9$	a
$E_8 - E_9$	a^2
$h - E_i - E_j - E_8,\ i < j < 8$	a^{-1}
$h - E_i - E_j - E_9,\ i < j < 8$	a

Now, consider the root sublattice $\mathbb{E}_7$ of $\mathbb{E}_8$ generated by $E_1 - E_2, ..., E_6 - E_7$ and $h - E_1 - E_2 - E_3$. The roots in $\mathbb{E}_7$ are mapped to 0 by $\overline{\text{res}}$, because the corresponding curves are disjoint from C.

Furthermore, we can contract the effective roots in $\mathbb{E}_7$ to get a surface Y with a single Du Val singularity, as shown in Fig. 8.

From Corollary 3.14 in [1], $\overline{\text{Eff}}(X)$ is polyhedral if and only if $\overline{\text{Eff}}(Y)$ is polyhedral. Since $p(X) = 10$, we see $p(Y) = 3$. This allows us to use Corollary 3.18 in [1] to obtain a criterion for polyhedrality in our case: $\overline{\text{Eff}}(Y)$ is polyhedral if and only if $\overline{\text{res}}(\beta) = 0$ for some root $\beta \in \mathbb{E}_8 \setminus \mathbb{E}_7$.

We will interpret the condition $\overline{\text{res}}(\beta) = 0$ in terms of a and q. First, we compute $\text{res}(C)$ as follows:

$$\text{res}(C) = \text{res}(3h - \sum_{i=1}^{9} E_i) = 3 \cdot \text{res}(h - E_1 - E_2 - E_3) + 2(E_1 + E_2 + E_3) - \sum_{i=4}^{9} E_i.$$

Since $h - E_1 - E_2 - E_3$ is represented by a curve of self-intersection -2 disjoint from C, we have $\text{res}(h - E_1 - E_2 - E_3) = 0$. Restricting each E_i to C gives $E_i \cap C = [z_i]$, i.e. the class of the point z_i in $\text{Pic}^0(C)$. Thus

$$\text{res}(C) = 2([z_1] + [z_2] + [z_3]) - \sum_{i=4}^{9} [z_i].$$

From our identification of $\text{Pic}^0(C)$ with $\mathbb{G}_m$, we have

$$\text{res}(C) = (z_1 z_2 z_3)^2 (z_4 ... z_9)^{-1} = (aqa^{-1})^{-1} = q^{-1}.$$

Thus $\overline{\text{res}}(\beta) = 0$ if and only if $\text{res}(\beta) \in \langle q \rangle$ in $\mathbb{F}_p^*$. In Table 1, we analyze the image of the remaining roots of $\mathbb{E}_8 = C^\perp / \langle C \rangle$ which are not in $\mathbb{E}_7$, again using the identification with $\mathbb{G}_m$. Note that since 1 is a flex point, we can identify h with the tangent line to C at $1 = z_0$. Then $\overline{\text{res}}(h) = 3[z_0]$.

Thus $\overline{\mathrm{Eff}}(X)$ is polyhedral if and only if at least one of a and a^2 is in $\langle q \rangle$. But if a is in $\langle q \rangle$, then so is a^2. □

Next, we prove a lemma which tells us that the polyhedrality condition of Theorem 4.1 fails for a set of primes of positive density. This lemma is known to experts, but we could not find a reference.

Lemma 4.2. *Let $a, q \in \mathbb{Q}$ be multiplicatively independent in $\mathbb{Q}^*$. Consider the set*

$$S(a,q)^c = \{p \text{ prime: } \bar{a} \notin \langle \bar{q} \rangle \text{ in } \mathbb{F}_p^*\}.$$

Then $S(a,q)^c$ contains a set of prime numbers of positive density.

Proof. For ease of notation, we switch to writing a, q for the reductions of a, q modulo p. Observe that $a \in \langle q \rangle$ if and only if $\langle a \rangle \in \langle q \rangle$ in $\mathbb{F}_p^*$. Let $o(x)$ denote the order of x in $\mathbb{F}_p^*$. Since $\mathbb{F}_p^*$ is cyclic, $\langle a \rangle$ is in $\langle q \rangle$ if and only if $o(a)$ divides $o(q)$, if and only if $[\mathbb{F}_p^* : \langle q \rangle] \mid [\mathbb{F}_p^* : \langle a \rangle]$.

Now, suppose $l \in \mathbb{Z}$ is a prime satisfying the conditions (i) $l \mid [\mathbb{F}_p^* : \langle q \rangle]$ and (ii) $l \nmid [\mathbb{F}_p^* : \langle a \rangle]$. Then $[\mathbb{F}_p^* : \langle q \rangle] \nmid [\mathbb{F}_p^* : \langle a \rangle]$. Thus (i) and (ii) are sufficient conditions for a prime p to lie in $S(a,q)^c$. The conditions (i) and (ii) can be rewritten by multiplying both sides by $o(q)/l$, $o(a)/l$ respectively to get (i) $q^{\frac{p-1}{l}} = 1$ in $\mathbb{F}_p^*$ and (ii) $a^{\frac{(p-1)}{l}} \neq 1$ in $\mathbb{F}_p^*$.

Let $K = \mathbb{Q}(\zeta_l, a^{\frac{1}{l}}, q^{\frac{1}{l}})$. We will proceed by encoding (i) and (ii) as conditions on the class of the Frobenius element of p in the Galois group of K over $\mathbb{Q}$, and invoking Chebotarev's density theorem.

By the assumption that a and q are multiplicatively independent in $\mathbb{Q}^*$, we have $(a,q) = 1$ and that a, q are not lth powers. Then the Galois group G of $K/\mathbb{Q}$ is isomorphic to $\mathbb{Z}_l^\times \ltimes (\mathbb{Z}_l \times \mathbb{Z}_l)$. Let ζ denote the lth root of unity. Then G is generated by elements of the form

$$\sigma_s : \zeta \mapsto \zeta^s$$
$$\tau_t : q^{\frac{1}{l}} \mapsto \zeta^t q^{\frac{1}{l}}$$
$$\rho_r : a^{\frac{1}{l}} \mapsto \zeta^r a^{\frac{1}{l}},$$

where if the action of $\sigma \in G$ on an element $\alpha \in K$ is not written, then σ acts as the identity on α. We can thus identify G with $\langle \sigma_1 \rangle \ltimes (\langle \tau_1 \rangle \times \langle \rho_1 \rangle)$.

We proceed by writing $\mathrm{Frob}_p = (\sigma_s, \tau_t, \rho_r)$ and determining what s, t, and r must be. By definition of the Frobenius element, we have $\mathrm{Frob}_p(\zeta) = \zeta^p$. But by condition (i) we have $p = 0 \mod l$. So if $\mathrm{Frob}_p(\zeta) = \zeta^s$, then $s = 0$. Similarly, we have $\mathrm{Frob}_p(q^{\frac{1}{l}}) = q^{\frac{p}{l}}$. Suppose that condition (i) holds, i.e. $q^{\frac{p-1}{l}} = 1$ in $\mathbb{F}_p^*$. Then $\mathrm{Frob}_p(q^{\frac{1}{l}}) = q^{\frac{1}{l}}$. So $t = 0$. By condition (ii), $\mathrm{Frob}_p(a^{\frac{1}{l}}) \neq a^{\frac{1}{l}}$. So $r \neq 0$. Thus p satisfies (i) and (ii) if and only if in the Galois group G, Frob_p is of the form $(\sigma_1, \tau_0, \rho_{\neq 0})$.

We check that these elements form a conjugacy class. Any element $(\sigma_{s_0}, \tau_{t_0}, \rho_{r_0})$ in G is fixed by elements of the form τ_t, ρ_r. Conjugating by an element of the form σ_s gives $(\sigma_{s_0}, \tau_{st_0}, \rho_{sr_0})$. But since $1 \leq s \leq p-1$, we remain in the conjugacy class.

Applying the Chebotarev density theorem, we see that there are asymptotically $(l-1)/((l-1) \cdot l \cdot l)$ such primes. □

In general, it is difficult to "patch" together different values of l to obtain an asymptotic density for $S(a,q)^c$, since the probabilities given by the Chebotarev density theorem are not statistically independent [7]. However, Moree and Stevenhagen showed in Theorem 2 of [7] that assuming the generalized Riemann hypothesis, the density of $S(a,q)$ can be precisely calculated to be

$$c_{a,q} \cdot \prod_{p \text{ prime}} \left(1 - \frac{p}{p^3 - 1}\right)$$

where $c_{a,q}$ is a constant depending on a and q. The product $\prod_{p \text{ prime}} \left(1 - \frac{p}{p^3-1}\right)$ converges to the Stephens constant S, whose approximation to 50 decimal places is

$$S \approx 0.57595996889294543964316337549249669250651396717649.$$

In the case that $\mathbb{Q}^*/\langle -1, a, b\rangle$ is torsion-free, then $c_{a,b}$ is between 0.981 and 1.024. Thus in this case (X_p, C_p) has polyhedral effective cone for roughly 57% of primes, and non-polyhedral effective cone for roughly 43% of primes.

Furthermore, a theorem of Heath-Brown tells us that for any three primes (a, b, c), Artin's conjecture is true for at least one of a, b, and c [5]. Combined with Lemma 4.2, this allows us to explicitly construct surfaces with a polyhedral effective cone for a set of primes of positive density, and a non-polyhedral effective cone for a set of primes of positive density.

Corollary 4.3. *Let C be the nodal cubic, with $\mathrm{Pic}^0(C)$ identified with $\mathbb{G}_m$. Let $a, q \in \mathbb{Q}$ be multiplicatively independent. Consider the surface X_p^q given by the blow-up of $\mathbb{P}^2$ at $z_1 = \ldots = z_7 = 1$ and $z_8 = a, z_9 = qa^{-1}$, where z_i are points on the nodal cubic. Then at least one of X_p^2, X_p^3, and X_p^5 has both a polyhedral effective cone for a set of primes of positive density, and a non-polyhedral effective cone for a set of primes of positive density.*

5. Sage code for Section 2

5.1. Code for Section 2, Case 1

The following code finds triangles for which $\frac{a}{m} > \frac{2}{3}$.

```
# Check gcd conditions and bounds on a/m
def check(e, x, p, s, k):
    d=(e*s*x+p)/2
    a = e*s^2
    c = e*(s+x)^2
    m = e*s*(s+x)
    return s>0 and gcd(a,d)==1 and (s-x)/s > 2/3 and m-a-d==gcd(2*d+a,c)

def check_integrality(k, y):
    return k.is_integer() and int(k)%2==1 and y.is_integer() and y >= 0

# Loop over parameters (e, x, p)
k, y = var('k,y')
for x in range(1,5):
    print("Solutions for t - s = %s" %x)
    for e in range (1, floor(18/(x^2))):
        for p in range (0, e*x^2):
            rhs = 16*(e*x^2 -p)^2
            divs = divisors(rhs)
            for div in divs:
                eqn1 = (e*x^2*k - 4*(e*x^2-p) - x*y == div)
                eqn2 = (e*x^2*k - 4*(e*x^2-p) + x*y == rhs/div)
                sol = solve([eqn1,eqn2],k,y, solution_dict=True)
                k1 = sol[0][k]
                y1 = sol[0][y]
                if check_integrality(k1, y1):
                    D =  e^2*x^2*(4-k1)^2 -8*e*(2*e*x^2 - p*k1)
                    s1 = 1/(4*e)*(-e*x*(4 -k1) + sqrt(D))
                    s2 = 1/(4*e)*(-e*x*(4 -k1) - sqrt(D))
                    for s in [s1,s2]:
                        if s.is_integer() and check(e,x,p,s,k1): print(sol)
```

5.2. Code for Section 2, Case 2

The following code finds triangles for which $\frac{1}{2} < \frac{a}{m} \leq \frac{2}{3}$.

```
# Loop over parameter k
possiblek = [4,5,7,8,9,10, 11]
for k in possiblek:
    divs = divisors(k)
    for x in divs:
        for a in range(1, floor((4*k*x)/(2*k-9))):
            m1 = 1/2*(k*a + sqrt((k*a)^2 - 4*k*a*(a + x)))
            m2 = 1/2*(k*a - sqrt((k*a)^2 - 4*k*a*(a + x)))
            for m in [m1, m2]:
                if m.is_integer() and a/m > 1/2:
                    print("k,a,x,m = %s,%s,%s,%s" %(k,a,x,m))
```

5.3. Code for Section 2, Case 3

The following code finds triangles for which $\frac{1}{3} \leq \frac{a}{m} \leq \frac{1}{2}$.

```
# Check that the lattice triangle is primitive
def primitive(b, c, x, y, m):
    a = (m1-y)/2
    d = m1-a-x
    b = b*d
    c = c*d
    return m>0 and gcd(a, gcd(b, c)) == 1

# Loop over parameters (b = b0, c = c0, x, y)
for b in range(3, 12):
    for c in range(b+2, 12):
        divs = divisors(c)
        for x in divs:
            for y in range(0, 2*x):
                D = (2*c*x)^2 + 4*(c-4)*c*y*(y - 2*x)
                m1 = 1/(2*(c-4))*(2*c*x + sqrt(D))
                m2 = 1/(2*(c-4))*(2*c*x - sqrt(D))
                for m in [m1, m2]:
                    if m.is_integer() and gcd(b,c)==1 and primitive(b,c,x,y,m):
                        a = (m-y)/2
                        d = m-a-x
                        if x == gcd(b*d - a, c*d):
                            print("m,a,b,c= %s,%s,%s,%s" %(m,a,b*d,c*d))
```

References

[1] Blown-up toric surfaces with non-polyhedral effective cone Ana-Maria Castravet, Antonio Laface, Jenia Tevelev, Luca Ugaglia, arXiv:2009.14298, 2021, available at https://arxiv.org/pdf/2009.14298.pdf.

[2] non-polyhedral Ana-Maria Castravet, Antonio Laface, Jenia Tevelev, Luca Ugaglia, available at https://github.com/alaface/non-polyhedral.

[3] Cox rings of extremal rational elliptic surfaces Michela Artebani, Alice Garbagnati, Antonio Laface, arXiv:1302.4361, 2013, available at https://arxiv.org/pdf/1302.4361.pdf.

[4] Christopher Hooley, On Artin's conjecture 1967 (225) (1967) 209–220, https://doi.org/10.1515/crll.1967.225.209.

[5] D.R. Heath-Brown, Artin's conjecture for primitive roots, Q. J. Math. 37 (1) (1986) 27–38, https://doi.org/10.1093/qmath/37.1.27.

[6] Georg Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, J. Reine Angew. Math. (Crelles J.) (1921) 1–31.

[7] Pieter Moree, Peter Stevenhagen, A two-variable Artin conjecture, J. Number Theory 85 (2000) 291–304, https://doi.org/10.1006/jnth.2000.2547.

[8] Javier González-Anaya, José Luis González, Kalle Karu, The geography of negative curves, arXiv:2104.03950, available at https://arxiv.org/pdf/2104.03950.pdf.

[9] Kazuhiko Kurano, Equations of negative curves of blow-ups of Ehrhart rings of rational convex polygons, arXiv:2101.02448, available at https://arxiv.org/pdf/2101.02448.pdf.

[10] S. Lang, H. Trotter, Bull. Am. Math. Soc. 83 (2) (1977) 289–292, https://doi.org/10.1090/S0002-9904-1977-14310-3.