DIOPHANTINE TRIPLES AND K3 SURFACES

MATIJA KAZALICKI AND BARTOSZ NASKRĘCKI

ABSTRACT. A Diophantine m-tuple with elements in the field K is a set of m non-zero (distinct) elements of K with the property that the product of any two distinct elements is one less than a square in K. Let $X : (x^2-1)(y^2-1)(z^2-1) = k^2$, be an affine variety over K. Its K-rational points parametrize Diophantine triples over K such that the product of the elements of the triple that corresponds to the point $(x, y, z, k) \in X(K)$ is equal to k. We denote by $\overline{X}$ the projective closure of X and for a fixed k by X_k a variety defined by the same equation as X.

In this paper, we try to understand what can the geometry of varieties X_k, X and $\overline{X}$ tell us about the arithmetic of Diophantine triples.

First, we prove that the variety $\overline{X}$ is birational to $\mathbb{P}^3$ which leads us to a new rational parametrization of the set of Diophantine triples.

Next, specializing to finite fields, we find a correspondence between a K3 surface X_k for a given $k \in \mathbb{F}_p^\times$ in the prime field $\mathbb{F}_p$ of odd characteristic and an abelian surface which is a product of two elliptic curves $E_k \times E_k$ where $E_k : y^2 = x(k^2(1 + k^2)^3 + 2(1 + k^2)^2 x + x^2)$. We derive an explicit formula for $N(p, k)$, the number of Diophantine triples over $\mathbb{F}_p$ with the product of elements equal to k. Moreover, we show that the variety $\overline{X}$ admits a fibration by rational elliptic surfaces and from it we derive the formula for the number of points on $\overline{X}$ over an arbitrary finite field $\mathbb{F}_q$. Using it we reprove the formula for the number of Diophantine triples over $\mathbb{F}_q$ from [DK21].

Curiously, from the interplay of the two (K3 and rational) fibrations of $\overline{X}$, we derive the formula for the second moment of the elliptic surface E_k (and thus confirming Steven J. Miller's Bias conjecture in this particular case) which we describe in terms of Fourier coefficients of a rational newform generating $S_4(\Gamma_0(8))$.

Finally, in the Appendix, Luka Lasić defines circular Diophantine m-tuples, and describes the parametrization of these sets. For $m = 3$ this method provides an elegant parametrization of Diophantine triples.

CONTENTS

1. Introduction

A Diophantine m-tuple with elements in a commutative unital ring $\mathcal{R}$ is a set of m non-zero (distinct) elements of $\mathcal{R}$ with the property that the product of any two of its distinct elements is one less than a square. Diophantus of Alexandria found the first example of a rational Diophantine quadruple $\{1/16, 33/16, 17/4, 105/16\}$, while the first Diophantine quadruple in integers was found by Fermat, and it was the set $\{1, 3, 8, 120\}$. Recently, He, Togbé and Ziegler [HTZ19] building upon the work of Dujella [Duj04] proved that there does not exist an integer Diophantine quintuple. On the other hand, it was shown in [DKMS17] that there are infinitely many rational Diophantine sextuples (for more constructions see [DK17], [DKP20] and [DKP19]), and it is not known if there are rational Diophantine septuples. For a short survey on Diophantine m-tuples see [Duj16].

In this paper, we focus on Diophantine triples over the field K of odd characteristic that we describe as follows. Let

$$\mathcal{D} : ab + 1 = r^2, ac + 1 = s^2, bc + 1 = t^2$$

be an affine variety in $\mathbb{A}^6$, and let $\widetilde{\mathcal{D}} = \mathcal{D} \setminus \{abc(a-b)(a-c)(b-c) = 0\}$. The group $(\mathbb{Z}/2\mathbb{Z})^3$ acts on the set of points $\mathcal{D}(K)$ (and also on $\widetilde{\mathcal{D}}(K)$) by multiplying r, s, t coordinates by ± 1, $(a, b, c, r, s, t) \mapsto (a, b, c, \pm r, \pm s, \pm t)$. It follows from the definition of Diophantine triples that the map $d : \widetilde{D}(K) \to \mathbb{A}^3$, $d(a, b, c, r, s, t) = (a, b, c)$ induces a bijection between the set of ordered Diophantine triples over K and the orbits of the $(\mathbb{Z}/2\mathbb{Z})^3$-action on the set $\widetilde{D}(K)$.

Moreover, we define

$$X : (x^2 - 1)(y^2 - 1)(z^2 - 1) = k^2$$

to be an affine threefold in $\mathbb{A}^4$, and let $\widetilde{X} = X \setminus \{k(x^2 - y^2)(x^2 - z^2)(y^2 - z^2) = 0\}$.

Our starting point is an observation that the birational map $p : \mathcal{D} \to X$, $p(a, b, c, r, s, t) = (r, s, t, abc)$ and its inverse $q : X \to \mathcal{D}$, $q(x, y, z, k) = (\frac{k}{z^2-1}, \frac{k}{y^2-1}, \frac{k}{x^2-1}, x, y, z)$ define a bijection between the sets $\widetilde{\mathcal{D}}(K)$ and $\widetilde{X}(K)$, hence the following proposition follows.

Proposition 1.1. There is one to one correspondence between ordered Diophantine triples over the field K (char(K) $\neq 2$) and K-rational points $(\pm r, \pm s, \pm t, k)$ on X with the property that $k(r^2 - s^2)(r^2 - t^2)(s^2 - t^2) \neq 0$.

Note that, if we fix $k \in K^\times$, then K-rational points on affine variety $X_k : (x^2 - 1)(y^2 - 1)(z^2 - 1) = k^2$ parametrize Diophantine triples with the fixed product k.

Our main objective in this paper is to study the geometry of varieties X and X_k in order to investigate possible applications to the theory of Diophantine triples.

Denote by $\overline{X}$ a projective closure of X. We prove in Proposition 2.1 that the projective threefold $\overline{X}$ is birational to $\mathbb{P}^3$. Combining Proposition 2.1 with the correspondence described above, we obtain the following rational parametrization of the Diophantine triples

$$a_1 = \frac{2(t_1 - 1)(t_1 + 1)t_3}{t_1^2 t_3^2 - t_2^2 - t_3^2 + 1}$$
$$a_2 = \frac{2(t_2 - 1)(t_2 + 1)t_3}{t_1^2 t_3^2 - t_2^2 - t_3^2 + 1},$$
$$a_3 = \frac{t_1^2 t_3^2 - t_2^2 - t_3^2 + 1}{2t_3}.$$

In Appendix, Luka Lasić defines and studies circular Diophantine m-tuples, and describes another, aesthetically very pleasing symmetric parametrization of Diophantine triples

$$a_1 = \frac{2t_1(1 + t_1t_2(1 + t_2t_3))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)},$$

$$a_2 = \frac{2t_2(1 + t_2t_3(1 + t_3t_1))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)},$$

$$a_3 = \frac{2t_3(1 + t_3t_1(1 + t_1t_2))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)}.$$

Parametric formulas for Diophantine triples can be useful as a starting point in the construction of Diophantine sets and the corresponding elliptic curves of high rank. See Section 2 in [Duj09] for the first such application to rational Diophantine sextuples, and [DKP20], [DP20b] and [DP20a] for three interesting applications of Luka's formulas.

Next, we switch our attention to Diophantine triples over finite fields. Diophantine m-tuples over the finite fields were first studied in [DK21] where the authors derived a formula for the number of Diophantine triples and quadruples over $\mathbb{F}_p$.

In Section 3.1, we construct a fibration on the threefold $\overline{X}$ whose fibers are rational elliptic surfaces. For a prime power $q = p^m$, we count $\mathbb{F}_q$-rational points on those fibers, and summing them up derive in Lemma 3.2 the formula for $\#\overline{X}(\mathbb{F}_q)$

$$(1.1) \qquad \#\overline{X}(\mathbb{F}_q) = q^3 + 3q^2 + \max\{3 - p, 0\}.$$

Using this formula together with Proposition 1.1, in Section 4 we reprove the formula for the number of Diophantine triples from [DK21].

For $k \neq 0$, X_k is a singular model of a K3 surface, cf. Lemma 3.4. In Section 3.2 we show that X_k admits a correspondence with an abelian surface which is a product of two elliptic curves $E_k \times E_k$, where

$$E_k : y^2 = x(k^2(1 + k^2)^3 + 2(1 + k^2)^2 x + x^2)$$

if $k^2 \neq -1$. When $k^2 = -1$ the curve E_k is $y^2 = x^3 - x$. Using this structure, in Proposition 3.13 and Theorem 3.15 we derive a formula for $\#X_k(\mathbb{F}_p)$, e.g. if $k^2 \neq -1$ then

$$(1.2) \qquad \#X_k(\mathbb{F}_p) = 7 - 5p + p^2 + \left(\frac{k^2 + 1}{p}\right)(a_{k,p}^2 - p),$$

where $a_{k,p} = p + 1 - \#E_k(\mathbb{F}_p)$ and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. From (1.2) and Proposition 1.1, in Corollary 4.3 we derive the formula for $N(p, k)$ - the number of Diophantine triples over $\mathbb{F}_p$ whose product of elements is equal to k.

Since surfaces X_k define a fibration of the threefold X, we can express $\#X(\mathbb{F}_p)$ as a sum of $\#X_k(\mathbb{F}_p)'s$, hence from (1.1) and (1.2) in Sections 3.3 and 3.4 we obtain the following curious formula

Theorem 1.2. *Let p be an odd prime number. Then*

$$(1.3) \qquad \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1, 0\}}} a_{k,p}^2 = -c_f(p) + p^2 - 3p - 2\left(\frac{-1}{p}\right)p - 2,$$

where

$$f(\tau) = \sum_{n=1}^{\infty} c_f(n)q^n = q - 4q^3 - 2q^5 + 24q^7 - 11q^9 - 44q^{11} + \ldots \in S_4(\Gamma_0(8)), q = e^{2\pi i\tau}$$

is a newform which generates the space of cuspforms $S_4(\Gamma_0(8))$ of weight 4 and level $\Gamma_0(8)$.

Remark 1.3. The newform f is an eta product equal to $\eta(2\tau)^4\eta(4\tau)^4$, where $\eta(\tau) = q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)$ is the Dedekind eta function. We note that this modular form is up to factor at 2 a Mellin transform of the L-series attached to $H_{\text{ét}}^3(X, \mathbb{Q}_\ell)$ cohomology group of certain Calabi-Yau rigid threefold X, cf. [Ver00], [CM07].

We can rephrase formula (1.3) in the language of Galois representations. In Section 3.4, following Deligne [Del71, N° 3], to the elliptic surface with generic fiber E_k we associate a compatible family $(\rho_{1,\ell}^2)$ of ℓ-adic Galois representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with the property that the trace of Frobenius $Trace(\rho_{1,\ell}^2(\text{Frob}_p))$ is up to some polynomial in p equal to $\sum\limits_{\substack{k\in\mathbb{F}_p \\ k^2\notin\{-1,0\}}} a_{k,p}^2$. Now (1.3) is equivalent to the fact that $Trace(\rho_{1,\ell}^2(\text{Frob}_p))$ is equal to the trace of Hecke operator T_p acting on one dimensional space $S_4(\Gamma_0(8))$ generated by $f(\tau)$. This could be readily explained by Deligne's theorem [Del71, N° 5] if E_k were universal elliptic curve for $\Gamma_0(8)$, but this is not the case. The elliptic surfaces $\mathcal{E}$ of which the curve E_k is a generic fiber is a K3 surface. Its non-equivalent elliptic fibrations have been classified in [BL13]. Elliptic fibration E_k is described in Section 8.0.9 [BL13]. The surface $\mathcal{E}$ has another elliptic fibration which corresponds to the universal family of elliptic curves over $X_1(8)$. However, the existence of these two non-equivalent elliptic fibrations on the K3 surface $\mathcal{E}$ is not enough to deduce directly our claims.

We can also rephrase the formula (1.3) in terms of the second moment sum associated to the elliptic surface E_k.

In general, let $\mathcal{F}_k$ be a 1-parametric family of elliptic curves over $\mathbb{Q}$, i.e. a generic fiber of an elliptic surface $\mathcal{F} \to \mathbb{P}^1$ defined over $\mathbb{Q}$ with a section. For every $k \in \mathbb{P}^1(\mathbb{Q})$ let $\tilde{\mathcal{F}}_{k,p}$ be a minimal model at a rational prime p of $\mathcal{F}_k$, and denote by $a_{k,p}$ the number $p+1-\#\tilde{\mathcal{F}}_{k,p}(\mathbb{F}_p)$.

We define the r-th moment sum associated with the $\mathcal{F}_k$ and prime p

$$M_{r,p}(\mathcal{F}_k) = \sum_{k\in\mathbb{F}_p} a_{k,p}^r,$$

thus it follows from formula (1.3) that for every prime $p \geq 3$ we have

$$(1.4) \qquad M_{2,p}(E_k) = p^2 - c_f(p) - \left(3 + 2\left(\frac{-1}{p}\right)\right)p - 1.$$

The difference of 1 between (1.4) and (1.3) follows from the following calculation. For any prime number $p > 2$ the model E_k is minimal and singular for $k = 0$ (of Kodaira type I_4). The projective closure of $E_0 : y^2 = x^2(x+2)$ has $p+1+\left(\frac{2}{p}\right)$ points over $\mathbb{F}_p$, hence $a_{0,p}^2 = 1$. If for a given prime p there exists an element $i \in \mathbb{F}_p$ such that $i^2 = -1$, then at $k = \pm i$ the model E_k is minimal and singular of type III^*. The equation of its reduction is $y^2 = x^3$, hence $a_{\pm i,p} = 0$.

Rosen and Silverman [RS98] have proved a conjecture of Nagao which implies that the first moment $M_{1,p}(\mathcal{F})$ of a rational elliptic surface is related to the Mordell-Weil rank of the group $\mathcal{F}_k(\mathbb{Q}(k))$. In precise terms the limit of $\frac{1}{X}\sum_{p\leq X} M_{1,p}(\mathcal{F}_k)\frac{\log p}{p}$ for $X \to \infty$ exists and is equal to $-\text{rank }\mathcal{F}_k(\mathbb{Q}(k))$. It follows that the numbers $M_{1,p}(\mathcal{F}_k)/p$ (i.e. the coefficients $a_{k,p}$) have negative bias (and the larger the rank of the family, the greater the bias).

It is known from the work of Michel [Mic95] that for non-isotrivial families $\mathcal{F}_k$ we have

$$M_{2,p}(\mathcal{F}_k) = p^2 + O(p^{3/2}),$$

More precisely, $M_{2,p}(\mathcal{F}_k) = p^2 + f_3(p) + f_2(p) + f_1(p) + f_0(p)$ and $|f_i(p)| \leq Cp^{i/2}$ for all primes p and a constant which depends only on the family $\mathcal{F}_k$. Each term $f_i(p)$ for $i < 4$ is a sum of all Galois conjugates of certain algebraic integers of norm $p^{i/2}$. More precisely, following [Mic95] we deduce that $M_{2,p}(\mathcal{F}_k) = p^2 + pS_1(p) + pS_2(p) + S_3(p)$. A function $S_3(p) = O(1)$ depends only on the places of bad reduction of $\mathcal{F}_k$, $S_2(p) = -\#\{\Delta(\mathcal{F}_k) = 0\}$ is the number of $\mathbb{F}_p$ points of the minimal discriminant of $\mathcal{F}_k$. Finally $S_1 = -\text{tr}(\text{Frob}_p \mid H_c^1(U_p, \text{Sym}_2(\mathcal{G}_p)))$ where U_p is a

certain open $\mathbb{F}_p$-curve computed from $\mathcal{F}_k$ and $\mathcal{G}_p$ is a rank 2 lisse sheaf on U_p built from the relative family $\mathcal{F}_k$, [Mic95, §3]. The sum $S_1(p) = S_1^{(0)}(p) + S_1^{(1/2)}(p)$ is such that $S_1^{(0)}(p)$ is a sum of algebraic numbers of norm 1 and $S_1^{(1/2)}(p)$ is a sum of algebraic numbers of norm $1/2$. Hence, $f_0(p) = S_3(p)$, $f_1(p) = 0$, $f_2(p) = p(S_2(p) + S_1^{(0)}(p))$ and $f_3 = pS_1^{(1/2)}$. We notice that the latter two factorizations are not in the ring of integers, since the sheaf $\mathrm{Sym}_2(\mathcal{G}_p)$ is obtained in the normalization process involving a Tate twist by $1/2$, cf. [Mic95, §3].

Let $\pi(x)$ denote the number of primes up to x. We are interested in the averages

$$\mu_i = \mu_i(f_i(p)) = \lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} \frac{f_i(p)}{p^{i/2}}$$

of sequences $(f_i(p))$.

Inspired by the work of Michel, Steven J. Miller in his thesis [Mil02] and subsequently with his co-authors in [ACF+18] initiated a more detailed study of bias for the second moments $M_{2,p}(\mathcal{F}_k)$. They calculated the second moments for certain pencils of cubic of the form $\mathcal{G}_k$: $y^2 = P(x)k + Q(x)$ where $\deg P(x), \deg Q(x) \leq 3$, and based on their findings proposed the following conjecture.

Conjecture (Bias Conjecture). *Let $\mathcal{F}_k$ be a one-parameter family of elliptic curves over $\mathbb{Q}$. The largest index i of the terms $f_i(p)$ in the second moment expansion of $M_{2,p}(\mathcal{F}_k)$ for which $\mu_i \neq 0$ satisfies the condition $\mu_i < 0$.*

For a precise statement of the conjecture see the introduction of [KN20] where we proved the conjecture for the family $\mathcal{G}_k$ for generic choice of polynomials $P(x)$ and $Q(x)$.

Theorem 1.4. *The Bias conjecture is true for the family E_k.*

Proof. It follows from (1.4) that $f_0 = -1$, $f_1(p) = 0$, $f_2(p) = -\left(3 + 2\left(\frac{-1}{p}\right)\right)p$ and $f_3(p) = -c_f(p)$.

Sato-Tate conjecture [BLGHT11, Theorem B.3] implies that the sequence of numbers $\{\theta_p = c_f(p)/(2p^{3/2})\}_p$ is equidistributed in the interval $[-1, 1]$ with respect to the Sato-Tate measure $\mathrm{ST}(t) = 2/\pi\sqrt{1 - t^2}dt$, i.e. for any continuous function f on $[-1, 1]$ we have

$$\lim_{x \to \infty} \frac{\sum_{p \leq x} f(\theta_p)}{\pi(x)} = \int_{-1}^{1} f(t)\mathrm{ST}(t).$$

In particular, when $f(t) = t$, the integral on the right vanishes and the average of $\frac{c_f(p)}{2\sqrt{p}}$ is zero, hence $\mu_3 = 0$.

As a consequence of the effective version of Dirichlet's theorem on arithmetic progression, since $(-1/p) = \pm 1$ if and only if $p \equiv \pm 1 \pmod 4$, we have that $\lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{p \leq x} \frac{\left(\frac{-1}{p}\right)p}{p} = 0$, thus the highest order lower term of the second moment with a non-vanishing average is $f_2(p)$ term and its average μ_2 is equal to -3, hence the bias conjecture holds. $\qquad\square$

Acknowledgements

2. Parametrization of the triples

Let $X_k : (x^2 - 1)(y^2 - 1)(z^2 - 1) = k^2$ be an affine variety defined over a field K of characteristic $\neq 2$. For $k = 0$ this is a union of six planes. For $k \neq 0$ it is a singular model of a K3 surface as we will prove in Lemma 3.4.

When char $K = 2$ the variety X_k is not reduced. The reduced scheme $X_{k,red} : (x - 1)(y - 1)(z - 1) = k$ is either a union of three lines for $k = 0$ or a rational cubic surface for $k \neq 0$.

Let X denote the total space of the fibration $\pi_{K3} : X \to \mathbb{A}^1$, $\pi_{K3}(x, y, z, k) = k$ where the fibers are varieties X_k. We have another fibration $\pi_{rat} : X \to \mathbb{A}^1$, $\pi_{rat}(x, y, z, k) = z$, where the fibers are denoted Y_z. Let $\overline{X}$ denote the projective closure of the variety X

$$\overline{X} : (x^2 - w^2)(y^2 - w^2)(z^2 - w^2) - k^2 \cdot w^4 = 0.$$

We have natural extensions $\pi_{K3} : \overline{X} \to \mathbb{P}^1$, $\pi_{K3}([x : y : z : k : w]) = [k : w]$ and $\pi_{rat} : \overline{X} \to \mathbb{P}^1$, $\pi_{rat}([x : y : z : k : w]) = [z : w]$.

Proposition 2.1. The projective threefold $\overline{X}$ is birational to $\mathbb{P}^3$.

Proof. Let $\phi : \overline{X} \to \mathbb{P}^3$ denote the following rational map

$$(2.1) \qquad \phi([x : y : z : k : w]) = [(x + w)y : (x + w)z : kw : (x + w)w]$$

and let $\psi : \mathbb{P}^3 \to \overline{X}$ denote the map

$$
\begin{aligned}
(2.2) \qquad \psi([t_1 : t_2 : t_3 : u]) = [&\left(t_1^2 + t_2^2 - t_3^2\right) u^3 - t_1^2 t_2^2 u - u^5 : \\
& -t_1 u^4 + t_1 \left(t_1^2 + t_2^2 + t_3^2\right) u^2 - t_1^3 t_2^2 : \\
& -t_2 u^4 + t_2 \left(t_1^2 + t_2^2 + t_3^2\right) u^2 - t_1^2 t_2^3 : \\
& 2t_3 \left(t_1 - u\right) \left(t_1 + u\right) \left(u - t_2\right) \left(t_2 + u\right) : \\
& \left(t_1^2 + t_2^2 + t_3^2\right) u^3 - t_1^2 t_2^2 u - u^5]
\end{aligned}
$$

We check by a direct computation that $\psi \circ \phi$ and $\phi \circ \psi$ are identity maps, hence both are birational and the proof is complete. $\square$

Remark 2.2. To construct a map ψ we observe that, for fixed A, $(x^2 - 1)A = k^2$ defines a conic which goes through the point $x = -1$, $k = 0$. The pencil $k = T_3(x + 1)$ of lines determines a parametrization $x = \frac{A + T_3^2}{A - T_3^2}$, $k = \frac{2AT_3}{A - T_3^2}$. We set $y = T_1$, $z = T_2$ and $A = (T_1^2 - 1)(T_2^2 - 1)$. Map ψ is obtained by homogenizing the variables $T_i = t_i/u$ and the formula for its inverse ϕ follows from the equation of the pencil of lines.

3. Counting points in $\overline{X}(\mathbb{F}_p)$

In this section, we calculate the formula for $\#\overline{X}(\mathbb{F}_p)$ in two different ways - by using two fibrations of the threefold $\overline{X}$. In Section 3.1, we consider a fibration by rational elliptic surfaces, while in Section 3.3 we use a fibration by K3 surfaces X_k. Using a certain correspondence between X_k and a split abelian surface we describe $\#X_k(\mathbb{F}_p)$ in terms of the p-th Fourier coefficient of a certain modular form. Later in Section 4 we use this result to derive a formula for the number of Diophantine triples over $\mathbb{F}_p$.

Let $q = p^m$, for a prime $p > 2$ and $m \geq 1$. Let ϕ_q denote the unique multiplicative character $\phi_q : \mathbb{F}_q^\times \to \mathbb{C}^\times$ of order 2. We need the following technical result.

Proposition 3.1 ([BEW98, Thm. 2.1.2]). *Let q be a prime power such that $2 \nmid q$. Let $\alpha, \beta, \gamma \in \mathbb{F}_q$ be given elements. Let $\Delta = 4\alpha\gamma - \beta^2$, then*

$$\sum_{t \in \mathbb{F}_q} \phi_q(\alpha t^2 + \beta t + \gamma) = \begin{cases} -\phi_q(\alpha), & \alpha \neq 0, \Delta \neq 0 \\ (q-1)\phi_q(\alpha), & \alpha \neq 0, \Delta = 0 \\ q\phi_q(\gamma) & \alpha = 0, \Delta = 0 \end{cases}$$

For a field K of characteristic not equal to 2 and two elements $k, z \in K$ such that $k \neq 0$ and $z^2 \neq 1$ we have an affine curve

$$X_{k,z} : (x^2 - 1)(y^2 - 1) = \frac{k^2}{z^2 - 1}.$$

Let $a = \sqrt[4]{1 - \frac{k^2}{z^2 - 1}}$. Under the substitution $x \mapsto x' \cdot a$, $y \mapsto y' \cdot a$, the curve $X_{k,z}$ is isomorphic to $(x')^2 + (y')^2 = a^2(1 + (x')^2(y')^2)$ which is famously known as the Edwards normal form [Edw07]. The curve of such form has geometric genus 1, hence is elliptic. In fact, we have a birational map $\phi_{k,z} : X_{k,z} \dashrightarrow Y_{k,z}$ defined over K to a Weierstrass model [Sil09, III.1]

(3.1) $\qquad Y_{k,z} : Y^2 = X^3 + (4z^4 + (-2k^2 - 8)z^2 + (2k^2 + 4))X^2 + k^4(z^2 - 1)^2 X.$

where

$$\phi_{k,z}(x, y) = \left(\frac{k^2(x+1)(z^2-1)}{x-1}, \frac{2k^2(x+1)y(z^2-1)^2}{1-x} \right),$$

$$\phi_{k,z}^{-1}(X, Y) = \left(\frac{2X}{k^2(1-z^2) + X} - 1, \frac{Y}{2X(1-z^2)} \right)$$

The map $\phi_{k,z}$ induces a morphism of degree 1

$$\phi_{k,z} : X_{k,z} \to Y_{k,z} \setminus \{P_1, P_2, P_3\},$$

where $P_1 = (0, 0)$, $P_2 = (k^2(z^2 - 1), -2k^2(z^2 - 1)^2)$ and $P_3 = (k^2(z^2 - 1), 2k^2(z^2 - 1)^2)$.

3.1. **Fibration with rational elliptic surfaces.** In this part, we are going to present proof of the following proposition

Lemma 3.2. *Let p be a prime and let $q = p^m$ for any $m \geq 1$. It follows that*

(3.2) $\qquad\qquad\qquad \#\overline{X}(\mathbb{F}_q) = q^3 + 3q^2 + \max\{3 - p, 0\}$

and

(3.3) $\qquad\qquad \#(X \setminus X_{k=0})(\mathbb{F}_q) = \begin{cases} q^3 - 6q^2 + 12q - 9, & p > 2 \\ q^3 - 3q^2 + 3q - 1, & p = 2 \end{cases}$

Proof. Let $\overline{X}$ denote a projective closure of the threefold X. We have

$$\overline{X} : (x^2 - w^2)(y^2 - w^2)(z^2 - w^2) - k^2 \cdot w^4 = 0.$$

The intersection of $\overline{X}$ with a hyperplane $w = 0$ is a union three planes $P_x : x = w = 0$, $P_y : y = w = 0$ and $P_z : z = w = 0$. The planes meet at three distinct lines, which in turn meet at a unique point $[0 : 0 : 0 : 0 : 1]$. Hence

$$\#\overline{X}(\mathbb{F}_q) = \#X(\mathbb{F}_q) + 3q^2 + 1.$$

For $p = 2$ the scheme X is non-reduced. Its reduced subscheme is $(x - 1)(y - 1)(z - 1) = k$, hence $\#X(\mathbb{F}_q) = q^3$. The subscheme $X_{k=0}$ is again non-reduced and its reduced subscheme is a union of three planes which intersect at three distinct lines and such that have a common point of intersection. Altogether we have $\#X_{k=0}(\mathbb{F}_q) = 3q^2 - 3q + 1$ and $\#(X \setminus X_{k=0})(\mathbb{F}_q) = q^3 - 3q^2 + 3q - 1$.

Assume that $p > 2$. We are going to prove that $\#X(\mathbb{F}_q) = q^3 - 1$. We consider the fibration $\pi_{rat} : \overline{X} \to \mathbb{P}^1$ such that $[x : y : z : w] \mapsto [z : w]$.

Let $z \neq \pm 1$. Let $\tilde{Y}_z$ denote a smooth projective relatively minimal model of Y_z with a natural fibration $\pi_z : \tilde{Y}_z \to \mathbb{P}^1$. This is a rational elliptic surface [SS19, Chap. 7] which is at $k = 0$ of split type I_8 and at $k = \infty$ of non-split type I_2. At $k = \pm\sqrt{z^2 - 1}$ there is a singular fiber of type I_1. The fibers cannot coincide under condition $z \neq \pm 1$. The Néron-Severi group of $\tilde{Y}_z$ is free of rank 10 and is spanned entirely by the image of the zero section, general fiber and components of the special fibers which is a consequence of the Shioda-Tate formula [Shi90]. For any prime $\ell \neq p$ it follows that $H^2_{\text{ét}}((\tilde{Y}_z)_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ is spanned entirely by the images of curves from the Néron-Severi group. Since all the components are defined over $\mathbb{F}_p$ it follows from the Grothendieck-Lefschetz trace formula [Har77, C.4] that

$$\#\tilde{Y}_z(\mathbb{F}_q) = 1 + 10q + q^2.$$

Let $\tilde{Y}_{k,z}$ denote a fiber $\pi_z^{-1}(k)$. For $k = \infty$ we have a fiber of type I_2 which is non-split, hence

$$(3.4) \qquad \#\tilde{Y}_{\infty,z}(\mathbb{F}_q) = 2q + 1 - \phi_q(z^2 - 1).$$

For $k = 0$ we have a fiber of type I_8 which is split, hence

$$(3.5) \qquad \#\tilde{Y}_{0,z}(\mathbb{F}_q) = 8q.$$

If $\phi_q(z^2 - 1) = 1$ there are two fibers above $\pm\alpha$, where $\alpha^2 = z^2 - 1$ in $\mathbb{F}_q$. Both fibers $\tilde{Y}_{\pm\alpha,z}$ are isomorphic over $\mathbb{F}_q$ to the nodal projective curve $ZY^2 = X^3 - X^2Z$, hence

$$(3.6) \qquad \#\tilde{Y}_{\pm\alpha,z}(\mathbb{F}_q) = q + 1 - \phi_q(-1).$$

From the existence of the fibration π_z it follows that

$$(3.7) \quad \#\tilde{Y}_z(\mathbb{F}_q) = \#\tilde{Y}_{\infty,z}(\mathbb{F}_q) + \#\tilde{Y}_{0,z}(\mathbb{F}_q) + (1 + \phi_q(z^2 - 1))\#\tilde{Y}_{\alpha,z}(\mathbb{F}_q) + \sum_{\substack{k \in \mathbb{F}_q \\ k(k^2 - z^2 + 1) \neq 0}} \#\tilde{Y}_{k,z}(\mathbb{F}_q).$$

For $k \in \mathbb{F}_q$ such that $k(k^2 - z^2 + 1) \neq 0$ we have the equality $\#X_{k,z}(\mathbb{F}_q) = \#\tilde{Y}_{k,z}(\mathbb{F}_q) - 4$ since the map $\phi_{k,z}$ is a morphism of degree 1 onto $\tilde{Y}_{k,z} \setminus \{P_1, P_2, P_3, \mathcal{O}\}$.

On the other hand, the fibration π_{rat} on X provides us with the equality

$$\#X(\mathbb{F}_q) = \#X_{z=1}(\mathbb{F}_q) + \#X_{z=-1}(\mathbb{F}_q) + \sum_{z \in \mathbb{F}_q, z^2 \neq 1} \#X_z(\mathbb{F}_q).$$

For $z = \pm 1$ the variety X_z is isomorphic to $\mathbb{A}^2$, so $\#X_{z=\pm 1}(\mathbb{F}_q) = q^2$.

For $z \neq \pm 1$ it follows that

$$\#X_z(\mathbb{F}_q) = \#X_{0,z}(\mathbb{F}_q) + (1 + \phi_q(z^2 - 1))\#X_{\alpha,z}(\mathbb{F}_q) + \sum_{\substack{k \in \mathbb{F}_q, \\ k(k^2 - z^2 + 1) \neq 0}} \#X_{k,z}(\mathbb{F}_q).$$

Variety $X_{0,z}$ is a union of four affine lines with a circular arrangement (type I_4), hence $\#X_{0,z}(\mathbb{F}_q) = 4q - 4$.

For an α such that $\alpha^2 = z^2 - 1$ in $\mathbb{F}_q$ we have that $X_{\alpha,z}$ is a genus 0 curve with equation $(x^2 - 1)(y^2 - 1) = 1$. It follows that

$$\#X_{\alpha,z}(\mathbb{F}_q) = q - 3 - \phi_q(-1).$$

It is easy to check that $\#X_{k=0}(\mathbb{F}_q) = 6q^2 - 12q + 8$ since the scheme $X_{k=0}$ is a configuration of 6 planes which intersect in the cubical arrangement. The formulas above lead us to the conclusion that

$$\#X(\mathbb{F}_q) = 2q^2 + \sum_{z^2 \neq 1} (q^2 + \phi_q(z^2 - 1)) = q^3 - 1.$$

$\square$

Remark 3.3. It is possible to provide a very short computational proof of the formula (3.2) of Lemma 3.2 using only Proposition 2.1. We compute (in Magma) the explicit schemes S_ϕ and S_ψ such that $\phi, \psi^{-1} : \overline{X} \setminus S_\phi \to \mathbb{P}^3 \setminus S_\psi$ are isomorphisms of schemes. Scheme S_ψ is a union of five projective planes

$$u = 0; \quad t_2 = \pm u; \quad t_1 = \pm u$$

and a rational surface $\mathcal{P}$

$$t_1^2 t_3^2 - t_2^2 u^2 - t_3^2 u^2 + u^4 = 0.$$

Scheme S_ϕ is a union of 8 projective planes

$$x - w = k = 0; \quad x = w = 0; \quad y = w = 0; \quad z = w = 0; \quad y \pm w = k = 0; \quad z \pm w = k = 0.$$

It follows that $|S_\phi(\mathbb{F}_q)| = 8(q^2 + q + 1) - 16(q+1) + 13$ and $|S_\psi(\mathbb{F}_q)| = 5(q^2 + p + 1) - 16(q+1) + 15 + \underbrace{(q^2 + 4q + 2)}_{=|\mathcal{P}(\mathbb{F}_q)|}$ and the formula (3.2) easily follows for every field $\mathbb{F}_q$ of odd characteristic.

3.2. Correspondence between X_k and an abelian surface.

Let Z denote a K3 surface defined over the complex numbers. The surface Z admits a correspondence with an abelian surface A if there is a diagram of finite maps
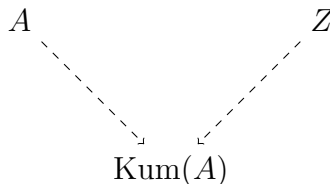

FIGURE 1. Correspondence between Z and A.

where $\mathrm{Kum}(A)$ denotes the Kummer surface attached to A, i.e. a resolution of singularities of the quotient surface $A/\langle \pm 1 \rangle$.

Lemma 3.4. *Let K be a field of characteristic not equal to 2 and let $k \in K$ be a nonzero element. A surface X_k has a projective smooth minimal model $\widetilde{X}_k$ over K which is a K3 surface, i.e. $H^1(\widetilde{X}_k, \mathcal{O}_{\widetilde{X}_k}) = 0$ and the canonical class $K_{\widetilde{X}_k}$ is trivial.*

Proof. Surface X_k is birational to an elliptic surface $\mathcal{Y}_k$ with general fiber $Y_k : Y^2 = f(X, z)$ from (3.1). An application of the Tate algorithm [Sil94, IV §9] shows that the Weierstrass model Y_k over $K(z)$ is globally minimal in the sense of [SS19, §5.10]. The elliptic discriminant of the model Y_k equals $-16k^8 (z^2 - 1)^7 (k^2 - z^2 + 1)$ which is of degree 16 with respect to the fibration variable z. Hence, the Euler characteristic of the elliptic surface $\mathcal{Y}_k$ equals 2 (cf. [SS19, §5.13]) proving that $\mathcal{Y}_k$ is a K3 surface [SS19, Chap. 11]. It follows from the adjunction formula that for any smooth curve C on a K3 surface $2g(C) - 2 = C^2$, hence there are no -1 curves. This proves that the surface $\mathcal{Y}_k$ is minimal, hence we take for $\widetilde{X}_k$ the surface $\mathcal{Y}_k$. $\qquad\square$

Remark 3.5. Equation $B : f(X, z) = 0$ defines a reducible sextic curve on the affine plane. Its projective closure has degree 6 and all singular points are simple, i.e. at most of multiplicity 3. Projectivized equation $Y^2 = \tilde{f}(X, z, w)$ defines a surface in the weighted projective space $\mathbb{P}(1, 1, 1, 3)$ and determines a normal double cover $T_k \to \mathbb{P}^2$ branched along the sextic curve B. Its canonical resolution of singularities $\widetilde{T}_k$ has plurigenus $p_g(\widetilde{T}_k) = 1$ and irregularity $q(\widetilde{T}_k) = 0$, proving that $\widetilde{T}_k$ is a $K3$ surface [BHPVdV04, V.22].

In what follows we prove that for each $k \in K$, $k \neq 0$ and K not of characteristic 2, the elliptic K3 surface $Z = \widetilde{X}_k$ admits a correspondence with an abelian surface $A = E \times E$ which is a square of the elliptic curve $E = E_k$. In consequence, we obtain an explicit description of

the transcendental part of $H^2(Z)$ cohomology (either singular or ℓ-adic) of Z in terms of the cohomology of $H^1(E)$ cohomology of a given elliptic curve E.

Convention: We use the notation $\mathcal{F}$ to denote an elliptic surface with a generic fiber F, which is an elliptic curve over a rational function field.

Lemma 3.6. *Let $k \in K^\times$ be an element of a field K of characteristic not equal to 2. There exists a finite rational map $f : X_k \to Kum(E_k \times E_k)$ defined over $K(\sqrt{k^2+1})$ where E_k is an elliptic curve over K which depends on k. Thus the K3 surface $\widetilde{X}_k$ which corresponds to X_k admits a correspondence with the abelian variety $E_k \times E_k$.*

Proof. Let $\psi_k : Y_k \to W_k$ denote the following 2-isogeny of two elliptic curves over $K(z)$ with kernel spanned by the point $(0,0)$

$$\psi(x,y) : (x,y) \mapsto \left(\frac{k^4 \left(z^2-1\right)^2}{x} - 2k^2 \left(z^2-1\right) + x + 4 \left(z^2-1\right)^2, \frac{y \left(x^2 - k^4 \left(z^2-1\right)^2\right)}{x^2} \right)$$

where

$$W_k : Y^2 = X^3 + 4 \left(z^2-1\right) \left(k^2 - 2z^2 + 2\right) X^2 - 16 \left(z^2-1\right)^3 \left(k^2 - z^2 + 1\right) X.$$

The surface $\mathcal{W}_k$ is isomorphic to a surface $\mathcal{Z}_k$ via the isomorphism $(X,Y,z) \mapsto (X,Y,\frac{z+1}{z-1})$ and the generic fiber of the latter has a Weierstrass model

$$Z_k : Y^2 = X^3 + \frac{16z \left(k^2z^2 - 2k^2z + k^2 - 8z\right)}{(z-1)^4} X^2 - \frac{1024z^3 \left(k^2z^2 - 2k^2z + k^2 - 4z\right)}{(z-1)^8} X.$$

The surface $\mathcal{Z}_k$ has singular fibers of the following types ($\sharp$):

$$I_2^* : z = 0, \infty,$$
$$I_4 : z = 1,$$
$$I_2 : z = \frac{k^2 + 2 \pm 2\sqrt{k^2+1}}{k^2}.$$

We identify this elliptic fibration with the fibration $\mathscr{J}_6$ from [KS08, §2.4].

Let us assume for now that $k^2 \neq -1$. Let

$$(3.8) \qquad E_k : y^2 = x(k^2(1+k^2)^3 + 2(1+k^2)^2 x + x^2)$$

be an elliptic curve. We have a natural elliptic fibration $(x_1, x_2, t) \mapsto t$ on the Kummer surface $\mathrm{Kum}(E_k \times E_k)$

$$x_1(k^2(1+k^2)^3 + 2(1+k^2)^2 x_1 + x_1^2)t^2 = x_2(k^2(1+k^2)^3 + 2(1+k^2)^2 x_2 + x_2^2).$$

We find an elliptic fibration with reduction types ($\sharp$) when we consider an elliptic parameter $u = \frac{x_1}{x_2}$. Elimination of the variable x_1 provides a model

$$(3.9) \qquad k^2 \left(k^2+1\right)^3 \left(t^2u - 1\right) + 2 \left(k^2+1\right)^2 x_2(tu-1)(tu+1) + x_2^2 \left(t^2u^3 - 1\right) = 0.$$

Change of variables $(t, x_2) = \left(X, -\frac{\left(k^2+1\right)\left(k^2u^2X^2 - k^2 + u^2X^2 - Y - 1\right)}{u^3X^2 - 1} \right)$ produces a Weierstrass model

$$Y^2 = (1+k^2)(1 + \left(u \left(k^2(u-1)^2 - 2u\right)\right) X^2 + u^4 X^4)$$

This is a quadratic twist by $(1 + k^2)$ of the quartic singular model of the elliptic curve Z_k. In fact, the substitution

$$(X,Y) = \left(-\frac{2y}{x \left(4u^2 - x\right)}, \frac{(x - 4u^2)^2 - 2k^2(u-1)^2u \left(2u^2 - x\right)}{x \left(4u^2 - x\right)} \right)$$

produces a model (after twisting by $1 + k^2$)

$$(3.10) \qquad y^2 = x^3 + u\left(k^2u^2 - 2k^2u + k^2 - 8u\right)x^2 - 4u^3\left(k^2u^2 - 2k^2u + k^2 - 4u\right)x.$$

A linear change of variables $(x, y, u) = (X \cdot d^2, Y \cdot d^3, z)$ where $d = (z-1)^2/4$ provides an isomorphism with the model Z_k.

Let $k^2 = -1$. In this case, Y_k is 2-isogenous to a curve which is a generic fiber of the Kummer surface $\mathrm{Kum}(E \times E)$ where $E : y^2 = x^3 - x$. Calculations are analogous to the general case and so we skip them. A composition of the maps defined above provides the rational map f. $\qquad \square$

For a given K3 surface X over the complex numbers, we denote by T_X the cup-product orthogonal complement in the Betti cohomology $H^2(X, \mathbb{Z})$ of the image N of the Néron-Severi group via the cocycle map $c_{Betti} : \mathrm{NS}(X) \to H^2(X, \mathbb{Z})$. By the Lefschetz (1,1)-theorem it follows that $N = H^2(X, \mathbb{Z}) \cap H^{1,1}(X)$. When $X \to Y$ is a finite map between two K3 surfaces X, Y which induces a non-zero map $H^{2,0}(Y) \to H^{2,0}(X)$, it follows that T_X is Hodge isometric to T_Y. To check that the former map is non-zero it is enough to verify that a holomorphic two-differential on Y pulls back to a non-zero differential on X, cf. [SS19, Thm. 12.5].

For a Kummer surface $\mathrm{Kum}(A)$ attached to an abelian variety A, the transcendental lattice $T_A \otimes \mathbb{Q}$ is isomorphic to $T_{\mathrm{Kum}(A)} \otimes \mathbb{Q}$ [Mor84, Prop.4.3]. When $A = E \times E$ is a square of an elliptic curve, the group $T_A \otimes \mathbb{Q}$ can be identified with a subgroup of $\mathrm{Sym}^2(H^1(E, \mathbb{Q}))$ due to Künneth formula and the identification $\mathrm{NS}(A) \cong \mathbb{Z}^2 \oplus \mathrm{Hom}(E, E)$. When E has no complex multiplication $T_A \otimes \mathbb{Q} = \mathrm{Sym}^2(H^1(E, \mathbb{Q}))$. By the comparison between Betti and ℓ-adic cohomology we can transfer these results to the etale cohomology.

The cocycle map induces a $\mathrm{Gal}(\overline{K}/K)$-equivariant injection of the Néron-Severi group

$$c : \mathrm{NS}((X)_{\overline{K}}) \otimes \mathbb{Q}_\ell \hookrightarrow H = H^2_{\text{ét}}((X)_{\overline{K}}, \mathbb{Q}_\ell).$$

The comparison theorem identifies $T_X \otimes \mathbb{Q}_\ell$ with the complement of $im(c)$ in H, denoted by H^{tr}.

For the K3 surface X that has a correspondence with $A = E \times E$ over K, the group H^{tr} is a Galois submodule in $\mathrm{Sym}^2(H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_\ell))$. The two groups are equal when E has no complex multiplication, [SS19, §12.2.4].

Let $X = \mathcal{Y}_k$ and $k \in K \subset \mathbb{C}$, $k \neq 0$. It follows from the Tate algorithm and the discriminant formula for the generic fiber of the elliptic surface $\mathcal{Y}_k$ that we have the following bad fibers. For k such that $k^2 \neq -1$ we have

$$I_1^* : z = \pm 1$$
$$I_8 : z = \infty$$
$$I_1 : z = \pm\sqrt{k^2 + 1}.$$

For $k^2 = -1$ two fibers of type I_1 merge into one fiber above $z = 0$ of type I_2.

The fibers of type I_8 and I_1^* have all components defined over K. Let ℓ be a prime. The image of $\mathrm{NS}((\mathcal{Y}_k)_{\overline{K}}) \otimes \mathbb{Q}_\ell$ via the cocycle map c is a subspace $N \subset H^2_{\text{ét}}((\mathcal{Y}_k)_{\overline{K}}, \mathbb{Q}_\ell)$. The subspace $V \subset N$ of the image of c which is spanned by the components of reducible fibers, the image of the zero section and the general fiber has rank equal to at least 19 due to [SS19, Cor. 6.7]. Since $\mathcal{Y}_k$ is a K3 surface it follows that $\dim_{\mathbb{Q}_\ell} H^2_{\text{ét}}((\mathcal{Y}_k)_{\overline{K}}, \mathbb{Q}_\ell) = 22$. The subgroup V is a trivial $\mathrm{Gal}(\overline{K}/K)$-representation in H.

Proposition 3.7. Let $K \subset \mathbb{C}$. Let $k \in K^\times$, $k^2 \neq -1$ and $E = E_k$ be the elliptic curve (3.8) with $\mathrm{End}(E) = \mathbb{Z}$. Let ℓ be a prime. It follows that the rank $\mathrm{NS}((\mathcal{Y}_k)_{\overline{K}}) = 19$. The G-representation H is equal to $V \oplus T$, where $T = \mathrm{Sym}^2(H^1_{\text{ét}}(E)_{\overline{K}}, \mathbb{Q}_\ell) \otimes \chi$ and χ is a character associated with the extension $K(\sqrt{k^2 + 1})/K$.

Proof. Since there is a finite map between $\mathcal{Y}_k$ and $\mathrm{Kum}(E_k \times E_k)$ it follows from [SS19, Thm. 12.2.5] that rank $\mathrm{NS}((\mathcal{Y}_k)_{\overline{K}}) = $ rank $\mathrm{NS}((\mathrm{Kum}(E_k \times E_k))_{\overline{K}})$. Next, the formula [SS19, Eq. 12.9]

implies that the latter group has rank 19, concluding that $T = T_{\mathcal{Y}_k} \otimes \mathbb{Q}_\ell$ has rank 3. The discussion before the proposition implies that in that case T is isomorphic as $\mathrm{Gal}(\overline{K}/K(\sqrt{k^2+1}))$-module with $S = \mathrm{Sym}^2(H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_\ell))$. By the formula (3.10) T is isomorphic to $S \otimes \chi$ as $\mathrm{Gal}(\overline{K}/K)$-modules for the quadratic character χ associated with $K(\sqrt{k^2+1})/K$. $\qquad\square$

Remark 3.8. Analogous statements were discussed in [vGT06] and [Nas17].

Proposition 3.9. Let $K \subset \mathbb{C}$ and $-1 \notin K$. Let $L = K(i)$, where $i^2 = -1$. The elliptic surface $\mathcal{Y}_i$ is defined over K. Its satisfies $\mathrm{rank}\,\mathrm{NS}((\mathcal{Y}_i)_{\overline{K}}) = 20$ and as $\mathrm{Gal}(\overline{K}/K)$-module $\mathrm{NS}((\mathcal{Y}_i)_{\overline{K}})$ is a direct sum of rank 19 trivial representation and a rank 1-module with basis $< e >$ such that $\sigma(e) = -e$ for the automorphism $\sigma(i) = -i$. The transcendental part of $H^2_{\text{ét}}((\mathcal{Y}_k)_{\overline{K}}, \mathbb{Q}_\ell)$ has rank 2 and is a proper submodule of $\mathrm{Sym}^2(H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_\ell))$ where $E : y^2 = x^3 - x$.

Proof. The elliptic surface $\mathcal{Y}_i$ has a fiber of type I_2 at $z = 0$. This fiber is isomorphic over K is a union of two components F_1, F_2 defined over $K(i)$, which satisfy the relation $F_1 + F_2 = F$ in the $\mathrm{NS}((\mathcal{Y}_i)_{\overline{K}})$, where F is a general fiber. Hence, the representation $\mathrm{NS}((\mathcal{Y}_i)_{\overline{K}}) \otimes \mathbb{Q}$ has a basis $e_1, \ldots, e_{18} = O, e_{19} = F, e = 2F_1 - F$. On that basis the action of σ is $\sigma(e_i) = e_i$ and $\sigma(e) = -e$, since the elements e_i are defined over K and $\sigma(F_1) = F_2$.

In this case, the passage from the Kummer model (3.9) to the Weierstrass model does not require any twisting, and the argument of Proposition 3.7 proves that the transcendental part of $H^2_{\text{ét}}((\mathcal{Y}_k)_{\overline{K}}, \mathbb{Q}_\ell)$ is a rank 2 submodule in $\mathrm{Sym}^2(H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_\ell))$. $\qquad\square$

Remark 3.10. We point out that the correspondence between $\widetilde{X}_k$ and $E_k \times E_k$ that we have constructed is not the Shioda-Inose structure [Mor84]. In fact, one can prove that the discriminants of the transcendental lattices of $\widetilde{X}_k$ and $\mathcal{W}_k$ do not satisfy the necessary condition $\mathrm{disc}\,T(\widetilde{X}_k)[2] = \mathrm{disc}\,T(\mathcal{W}_k)$.

3.3. Fibration with K3 surfaces.

In this section we derive formula (3.3) (see Lemma 3.2) by counting points on fibers X_k and evaluating the sum

$$\#(X \backslash X_{k=0})(\mathbb{F}_p) = \sum_{\substack{k \in \mathbb{F}_p \\ k \neq 0}} \#X_k(\mathbb{F}_p).$$

We denote by $\tilde{Y}_k$ a minimal smooth projective model of

$$Y_k : Y^2 = X^3 + (4z^4 + (-2k^2 - 8)z^2 + (2k^2 + 4))X^2 + k^4(z^2 - 1)^2 X,$$

which is an elliptic surface $\pi : \tilde{Y}_k \to \mathbb{P}^1$ with projection π obtained from the natural projection $(X, Y, z) \mapsto z$. The following proposition relates $\#X_k(\mathbb{F}_p)$ to $\#\tilde{Y}_k(\mathbb{F}_p)$.

An elliptic surface $N \to \mathbb{P}^1$ which is defined over $\mathbb{Q}$ is said to have a good reduction at a rational prime p when there exists a model $\mathcal{N} \to \mathrm{Spec}\,\mathbb{Z}_{(p)} = \{g, s\}$ which is smooth projective of relative dimension 2 and such that the generic fiber $\mathcal{N}_g$ is isomorphic with N, there exists a factorization

$$\mathcal{N} \to \mathbb{P}^1_{\mathbb{Z}_{(p)}} \to \mathrm{Spec}\,\mathbb{Z}_{(p)}$$

and the induced morphisms $\mathcal{N}_x \to \mathbb{P}^1$ for $x \in \mathrm{Spec}\,\mathbb{Z}_{(p)}$ define an elliptic surface over $\mathbb{Q}$ and $\mathbb{F}_p$, respectively.

For a polynomial $f \in \mathbb{Z}[t]$, let $\mathrm{rad}(f)$ denote a radical of that polynomial and $\mathrm{disc}(f)$, the discriminant of f.

We say that a Weierstrass model $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ of an elliptic curve N over $\mathbb{Q}(t)$ is globally minimal if $a_i \in \mathbb{Z}[t]$, the model is minimal at all finite places and is also minimal at infinity [SS19, §5.10].

Lemma 3.11. *Let N be a globally minimal model of an elliptic curve over $\mathbb{Q}(t)$. Let Δ be the discriminant of N and let $j = \frac{f}{g}$ be its j-invariant with f, g coprime and in $\mathbb{Z}[t]$. Let $p > 5$*

be a rational prime such that for every polynomial $h \in \{\mathrm{rad}(a_i), \mathrm{rad}(\Delta), \mathrm{rad}(f), \mathrm{rad}(g)\}$ *we have* $p \nmid \mathrm{disc}(h)$ *and the modulo* p *reduction of the equation of* N *defines an elliptic curve over* $\mathbb{F}_p(t)$ *with Weierstrass coefficients* $\tilde{a}_i \in \mathbb{F}_p[t]$ *defining a globally minimal model over* $\mathbb{F}_p(t)$, *then* p *is a prime of good reduction for the elliptic surface attached to* N.

Proof. This is a translation of a theorem proved by one of the authors in [Nas14, Tw. 2.2.12].

The conditions imposed in the theorem imply that two elliptic curves $N/\mathbb{Q}(t)$ and $\tilde{N}/\mathbb{F}_p(t)$ satisfy the same steps in Tate's algorithm, hence the associated elliptic curves over $\mathbb{Q}$ and $\mathbb{F}_p$, respectively have the same configuration of singular fibers at places which correspond to each other under reduction modulo p.

The Weierastrass model $W_N \to \mathbb{P}^1_{\mathbb{Z}_{(p)}}$ treated as a relative surface has only isolated double points as singularities [CD89, §0.2] in the fibers above both the generic and special fiber. In both characteristics, 0 and p, the types of singularities are the same [CD89, Prop. 0.2.6] and hence the Tate's algorithm provides a simultaneous resolution of singularities on $W_N \to \mathbb{P}^1_{\mathbb{Z}_{(p)}}$ leading to a smooth model $\mathcal{N} \to \mathrm{Spec}\,\mathbb{Z}_{(p)}$. □

Corollary 3.12. *Elliptic curve* Y_k *over* $\mathbb{Q}(z)$ *has good reduction at every prime* $p > 5$ *and for every* $k \in \mathbb{Z}$ *which satisfies* $p \nmid k$. *In particular, elliptic surfaces* $\mathcal{Y} = \mathcal{Y}_k$ *over* $\mathbb{Q}$ *and* $\widetilde{\mathcal{Y}} = \tilde{Y}_k$ *over* $\mathbb{F}_p$ *satisfy the equality as* $D_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-*modules*

$$H^2_{\text{ét}}((\mathcal{Y})_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell) = H^2_{\text{ét}}((\widetilde{\mathcal{Y}})_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$$

for every prime $\ell \neq p$.

Proof. The good reduction for primes $p > 5$ follows from Lemma 3.11 and a direct calculation with the globally minimal model of Y_k. The equality of the cohomology groups as representations of the decomposition group at p follows as a standard fact for ℓ-adic cohomology of a smooth scheme $\mathcal{Y} \to \mathrm{Spec}\,\mathbb{Z}_{(p)}$. □

Proposition 3.13. *Let* p *be an odd prime and* $k \in \mathbb{F}_p$. *If* $k^2 \notin \{-1, 0\}$ *then*

$$\#X_k(\mathbb{F}_p) = \#\tilde{Y}_k(\mathbb{F}_p) - 24p + 6.$$

If $k^2 = -1$ *then* $\#X_k(\mathbb{F}_p) = \#\tilde{Y}_k(\mathbb{F}_p) - 25p + 6$.

Proof. When $z \neq \pm 1$ and $z^2 \neq k^2 + 1$, then $\#X_{k,z}(\mathbb{F}_p) = \#\tilde{Y}_{k,z} - 4$ since the fiber $\tilde{Y}_{k,z}$ is an elliptic curve and the model $Y_{k,z}$ has a point at infinity removed.

When $z = \pm 1$ it follows from the equation of $X_{k,z}$ that $\#X_{k,z}(\mathbb{F}_p) = 0$, while $\#\tilde{Y}_{k,\pm 1}(\mathbb{F}_p) = 6p+1$ because the reduction type at $z = \pm 1$ of the elliptic curve $\tilde{Y}_{k,z}$ is I_1^* and all the components of the Kodaira fiber are defined over $\mathbb{F}_p$.

At $z = \infty$ we have a split reduction type I_8 for $\tilde{Y}_{k,z}$, hence $\#\tilde{Y}_{k,z}(\mathbb{F}_p) = 8p$.

For each z such that $z^2 = k^2 + 1 \neq 0$ we have a reduction type I_1, hence $\#\tilde{Y}_{k,z}(\mathbb{F}_p) = p + 1 - \phi_p(-1)$. On the other hand for such z the curve $X_{k,z}$ is $x^2y^2 - x^2 - y^2 = 0$ and $\#X_{k,z}(\mathbb{F}_p) = p - 3 - \phi_p(-1)$.

When $k^2 = -1$, then at $z = 0$ we have a non-split reduction of type I_2 and $\#\tilde{Y}_{k,0}(\mathbb{F}_p) = 2p + 1 - (-1/p)$ while $\#X_{k,0}(\mathbb{F}_p) = p - 3 - \phi_p(-1)$. □

Using the correspondence from Section 3.2 attached to X_k (or on Y_k directly) we can derive explicit formula for $\#\tilde{Y}_k(\mathbb{F}_p)$.

Remark 3.14. Let p be an odd prime. Let $\lambda(p)$ denote $p + 1 - \#E(\mathbb{F}_p)$ where $E : y^2 = x^3 - x$. Notice that

$$\lambda(p)^2 = \begin{cases} 4b^2, & \text{if } p \equiv 1 \pmod 4; p = a^2 + b^2 \text{ with } b \text{ odd,} \\ 0, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

which follows from [IR90, Chap.18, Thm. 5].

Theorem 3.15. *Let p be an odd prime, and $k \in \mathbb{F}_p$. If $k^2 \notin \{-1, 0\}$ then*

$$\#\tilde{Y}_k(\mathbb{F}_p) = 1 + 19p + p^2 + \phi_p(k^2 + 1)(a_{k,p}^2 - p),$$

where $E_k : y^2 = x(k^2(1 + k^2)^3 + 2(1 + k^2)^2 x + x^2)$ and $a_{k,p} = p + 1 - \#E_k(\mathbb{F}_p)$. Moreover, if $k^2 = -1$ then

$$\#\tilde{Y}_k(\mathbb{F}_p) = 1 + (20 - \phi_p(-1))p + p^2 + (\lambda(p)^2 - p).$$

Proof. For primes $p = 3$ and $p = 5$ we verify the claims by a direct calculation. Suppose that $p > 5$ and k_0 be a lift of $k \in \mathbb{F}_p$, $k^2 \neq -1$ to integers which satisfies $k_0 > p$. Under such assumption the elliptic curve E_{k_0} cannot have complex multiplication since the list of CM j-invariants is finite and explicit [Sil94, App. A §3]. The conclusion follows from Proposition 3.7 and the trace formula applied to Corollary 3.12.

Let $k^2 = -1$ in $\mathbb{F}_p$. Let $\mathcal{Y}_i$ be an elliptic surface over $\mathbb{Q}$ as defined in Proposition 3.9 and let E_i denote the elliptic curve $y^2 = x^3 - x$. Our claim follows from Proposition 3.9, Corollary 3.12 and Remark 3.14. $\square$

Proposition 3.13 and Theorem 3.15 now reduce a derivation of the formula (3.3) to the evaluation of the sum

$$\sum_{\substack{k \in \mathbb{F}_p, \\ k^2 \notin \{-1,0\}}} \phi_p(k^2 + 1)a_{k,p}^2 = - \sum_{\substack{k \in \mathbb{F}_p, \\ k^2 \notin \{-1,0\}}} a_{k,p}^2 + 2 \sum_{\substack{k \in \mathbb{F}_p, \\ k^2 \notin \{-1,0\}, \\ k^2 + 1 = \square}} a_{k,p}^2,$$

where $x = \square$ means that x is a square in $\mathbb{F}_p$. The main idea is to interpret two sums on the right-hand side as traces of Frobenii $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of certain Galois representations attached to the elliptic surfaces with generic fibers $E_k : y^2 = x(k^2(1 + k^2)^3 + 2(1 + k^2)^2 x + x^2)$ and $F_k : y^2 = (x - (k-1)^2)(x - (k+1)^2)x$.

To motivate the curve F_k, we start with the following observation. Let p be an odd prime and for $k \in \mathbb{F}_p \setminus \{-1, 0, 1\}$ let $b_{k,p} = p + 1 - \#F_k(\mathbb{F}_p)$.

Proposition 3.16. *If p is an odd prime, then*

$$2\lambda(p)^2 + 2 \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\} \\ k^2 + 1 = \square}} a_{k,p}^2 = \sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b_{k,p}^2.$$

Proof. Let H_k denote the elliptic curve obtained from E_k by the pullback through a quadratic map $\phi : k \mapsto \frac{1-k^2}{2k}$. The curve H_k is a quadratic twist by $-(k^2 + 1)$ of the curve F_k. Indeed, we have the following models of those curves over $\mathbb{Q}(k)$

$$E_k : \; y^2 = x^3 + 2x^2 + \frac{k^2}{k^2 + 1}x,$$

$$H_k : \; y^2 = x^3 + 2x^2 + \frac{(k^2 - 1)^2}{(k^2 + 1)^2}x,$$

$$F_k : \; y^2 = x^3 - 2(k^2 + 1)x^2 + \left(k^2 - 1\right)^2 x.$$

Let $S = \{k \in \mathbb{F}_p : k(k^2 - 1)(k^2 + 1) \neq 0\}$. Notice that we have an involution $\iota : S \to S$ with $\iota(k) = -\frac{1}{k}$ without a fixed point on S. Hence, there exists two sets $B, \tilde{B}$ such that $B \cap \tilde{B} = \emptyset$ and $S = B \cup \tilde{B}$. It follows that $\phi(k) = \phi(\iota(k))$, hence $\phi(B) = \phi(\tilde{B})$.

Claim: $\phi(B) = \{k \in \mathbb{F}_p : k^2 \notin \{-1, 0\}, k^2 + 1 = \square\}$. Indeed, for an element s we have $\phi(s)^2 \in \{-1, 0\}$ if and only if $s \in \{\pm 1, \pm\sqrt{-1}\}$ but $\{\pm 1, \pm\sqrt{-1}\} \cap B = \emptyset$. If $k^2 + 1 = r^2$ for some non-zero r, then there exists an element $s \in B$ such that $k = \frac{1-s^2}{2s} = \phi(s)$ and $r = \frac{1+s^2}{2s}$.

Let

$$\mathcal{S} = \sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b_{k,p}^2 = \sum_{k \in \{\pm\sqrt{-1}\}} b_{k,p}^2 + \sum_{k \in S} b_{k,p}^2$$

We have that $F_{\pm\sqrt{-1}} : y^2 = x^3 + 4x$, so $b_{\pm\sqrt{-1},p}^2 = \lambda(p)^2$ since the curves $F_{\pm\sqrt{-1}}$ are quadratic twists of $\tilde{E}_{1728}$. Finally, notice that for $s \in S$ we have the equalities

$$b_{s,p}^2 = a_p(F_s)^2 = a_p(H_s)^2 = a_p(E_{\phi(s)})^2 = a_{\phi(s),p}^2,$$

$$b_{\iota(s),p}^2 = a_{\phi(\iota(s)),p}^2 = a_{\phi(s),p}^2$$

and so

$$\mathcal{S} - 2\lambda(p)^2 = \sum_{s \in B} b_{s,p}^2 + \sum_{s \in \tilde{B}} b_{s,p}^2 = \sum_{s \in B} b_{s,p}^2 + \sum_{s \in B} b_{\iota(s),p}^2 = 2 \sum_{s \in B} a_{\phi(s),p}^2 = 2 \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\} \\ k^2+1=\square}} a_{k,p}^2.$$

$\square$

3.4. **Compatible families of ℓ-adic Galois representations of** $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $h_1 : \mathcal{E} \to \mathbb{P}^1$ and $h_2 : \mathcal{F} \to \mathbb{P}^1$ denote two elliptic surfaces with generic fibers E_k and F_k, respectively. We will associate to each elliptic surface a compatible family of ℓ-adic Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as follows.

Denote by $h_1' : \mathcal{E} \to \mathbb{P}_1^1$ and $h_2' : \mathcal{F} \to \mathbb{P}_2^1$ the restrictions of elliptic surfaces h_1 and h_2 to the complements $\mathbb{P}_i^1 = \mathbb{P}^1 \setminus \{t \in \mathbb{P}^1 : h_i^{-1}(t) \text{ is singular}\}$.

For $j = 1, 2$, a prime ℓ, and a positive integer m, we obtain a sheaf

$$\mathcal{F}_\ell^j = R^1 h_{j*}' \mathbb{Q}_\ell$$

on $\mathbb{P}_j^1$, and also a sheaf $i_* \mathrm{Sym}^m \mathcal{F}_\ell$ on $\mathbb{P}_j^1$ (here $\mathbb{Q}_\ell$ is the constant sheaf on the elliptic surface h_j, R^1 is derived functor and $i : \mathbb{P}_j^1 \to \mathbb{P}^1$ the inclusion). The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{Q}_\ell$-space

$$W_{m,\ell}^j = H_{\text{ét}}^1(\mathbb{P}_j^1 \otimes \overline{\mathbb{Q}}, i_* \mathrm{Sym}^m \mathcal{F}_\ell^j)$$

defines an ℓ-adic representation $\rho_{j,\ell}^m$ which is pure of weight $m + 1$.

It follows from Lemma 3.11 and a direct computation with globally minimal models of $\mathcal{E}$ and $\mathcal{F}$ that representations $\rho_{j,\ell}^m$ are unramified for $p > 5$. We denote by $Frob_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ a geometric Frobenius at p. Using the following well known result, for $p > 5$, we can express the trace of $\rho_{j,\ell}^m(Frob_p)$ in terms of $\#E_k(\mathbb{F}_p)$ or $\#F_k(\mathbb{F}_p)$.

Theorem 3.17. *Let $p > 5$ be a prime. For $j = 1, 2$ and any positive integer m the following are true:*

(1) *We have that*

$$Trace(Frob_p | W_{m,\ell}^j) = - \sum_{t \in \mathbb{P}_j^1(\mathbb{F}_p)} Trace(Frob_p | (i_* \mathrm{Sym}^m \mathcal{F}_\ell^j)_t).$$

(2) *If the fiber $E_t^j := h_j^{-1}(t)$ (i.e. E_t^j is either equal to E_t or F_t) is smooth, then*

$$Trace(Frob_p | (i_* \mathrm{Sym}^1 \mathcal{F}_\ell)_t) = Trace(Frob_p | H^1(E_t^j, \mathbb{Q}_\ell)) = p + 1 - \#E_t^j(\mathbb{F}_p).$$

Furthermore,

$$Trace(Frob_p | (i_* \mathrm{Sym}^2 \mathcal{F}_\ell)_t) = Trace(Frob_p | (i_* \mathrm{Sym}^1 \mathcal{F}_\ell^j)_t)^2 - p.$$

(3) *If the fiber $E_t^j := h_j^{-1}(t)$ is singular, then $Trace(Frob_p | (i_* \mathrm{Sym}^2 \mathcal{F}_\ell)_t) = 1$ if the fiber is multiplicative or potentially multiplicative.*

(4) *If $p \equiv 1 \pmod 4$ and $t = \pm\sqrt{-1} \in \mathbb{F}_p$, then $Trace(Frob_p | (i_* \mathrm{Sym}^2 \mathcal{F}_\ell^1)_t) = p$.*

Proof. Points (1)-(3) follow from [DK21, Thm. 11.]. We proceed to the proof of point (4).

In order to calculate the trace of $Frob_p|(i_*\text{Sym}^2\mathcal{F}_\ell^1)_t$ at $t = \pm\sqrt{-1} \in \mathbb{F}_p$, we follow 3.7 of [Sch88]. Let $K = \mathbb{F}_p(T)$ be the function field of rational function in T. Let v be the discrete valuation of K corresponding to $T - t$, and K_v the completion. Let G_v be the absolute Galois group $\text{Gal}(K_v^{\text{sep}}/K_v)$, I_v the inertia group, and F_v a geometric Frobenius. Let H_v denote $H^1(E^1 \otimes K_v^{\text{sep}}, \mathbb{Q}_\ell)$. The space H_v is a G_v-module and

$$Trace(Frob_p|(i_*\text{Sym}^2\mathcal{F}_\ell^2)_t) = Trace(F_v|(Sym^2 H_v)^{I_v}).$$

First we note that elliptic surface $\mathcal{E}$ has a reduction of type III^* at fibers $t^2 = -1$ which is potentially good. We use the fact that for primes $p > 5$ the elliptic surface in characteristic p has the same reduction types as the one in characteristic 0, cf. Lemma 3.11. So over the local field $K = \mathbb{F}_p((v = t - \alpha))$ for $\alpha^2 = -1$, $\alpha \in \mathbb{F}_p$ we can check that the base change of E to the field $L = K(\sqrt{\sqrt{v} - v})$ has good reduction. It follows from [Sil09, Prop. 4.1] that the inertia group $I_{\overline{L}/L}$ acts trivially on the Tate module $T_\ell(E)$. The Galois group $\text{Gal}(L/K)$ is cyclic of order 4. One can check that the inertia group $I_{L/K}$ has order 4 since the inertia order equals the ramification degree above the point $[0 : 1]$ (totally ramified) in the map $f : C \to \mathbb{P}^1$, where $C : Y^2 = XZ - X^2$ is a conic and the map $f([X : Y : Z]) = [X^2 : Z^2]$.

It follows that the image of inertia subgroup I_v in $\text{GL}(H_v)$ is a cyclic group of order 4. Since $\Lambda^2 H_v = \mathbb{Q}_\ell(-1)$ is unramified, there is a basis $\{X, Y\}$ of $H_v \otimes \overline{\mathbb{Q}_\ell}$ on which I_v acts as $\pm i$. Hence, $(Sym^2 H_v)^{I_v}$ is one-dimensional vector space spanned by XY.

Since $p \equiv 1 \pmod 4$, we have that $\sqrt{-1} \in \mathbb{F}_p$, hence the image of G_v in $\text{GL}(H_v)$ is commutative. In particular, $F_v(X) = \beta X$ and $F_v(Y) = \overline{\beta} Y$, where β is an algebraic integer with $\beta\overline{\beta} = p$. It follows that $F_v(XY) = pXY$, and the claim follows. $\square$

Corollary 3.18. *For a prime $p > 5$, we have that*

a)
$$Trace(\rho_{1,\ell}^2(\text{Frob}_p)) = p^2 - 3p - 2\phi_p(-1)p - 2 - \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\}}} a_{k,p}^2,$$

b)
$$Trace(\rho_{2,\ell}^2(\text{Frob}_p)) = p^2 - 3p - 4 - \sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b_{k,p}^2.$$

Proof. The claim follows directly from the previous theorem and the information about the reduction types of the singular fibers of elliptic surfaces $\mathcal{E}$ and $\mathcal{F}$. Namely, $\mathcal{E}$ has multiplicative singular fibers at $k = 0, \infty$ (of types I_4 and I_2 respectively) and potentially good singular fibers at $k^2 + 1 = 0$ (of types III^*), while $\mathcal{F}$ has has multiplicative singular fibers at $k = 0, \infty, -1, 1$ (of types I_2, I_2, I_4 and I_4 respectively). $\square$

Consider the newform

$$f(\tau) = \sum_{n=1}^\infty c_f(n)q^n = q - 4q^3 - 2q^5 + 24q^7 - 11q^9 - 44q^{11} + \dots \in S_4(\Gamma_0(8)).$$

Now we state the main result of this section.

Theorem 3.19. *Let $p > 5$ be a prime, and $\ell \neq p$. We have that*

$$Trace(\rho_{1,\ell}^2(\text{Frob}_p)) = Trace(\rho_{2,\ell}^2(\text{Frob}_p)) = c_f(p).$$

Proof. **Second equality** $Trace(\rho_{2,\ell}^2(\text{Frob}_p)) = c_f(p)$: the equality follows from Deligne's formula [Del71, N° 5] relating the trace of Frobenius acting on Galois representation of a universal family of elliptic curves over a modular curve and the trace of Hecke operator T_p acting on

corresponding space of cusp forms. In this particular case, the family F_k is a twist by $\sqrt{-1}$ of a universal family [Kub76, Table 3]

$$y^2 + xy + \left(-\frac{1}{16}k^2 + \frac{1}{16}\right)y = x^3 + \left(-\frac{1}{16}k^2 + \frac{1}{16}\right)x^2$$

of elliptic curves with $\mathbb{Z}/2 \oplus \mathbb{Z}/4$ torsion subgroup. The corresponding modular curve is $X(\Gamma)$ for $\Gamma = \Gamma_1(4) \cap \Gamma^0(2)$, a congruence subgroup of index 12, with cusps $\{\infty, 0, 1/3, 1/2\}$. The following equalities

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \sqrt{2} \end{bmatrix}^{-1} \Gamma_0(8) \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \sqrt{2} \end{bmatrix} = \Gamma_0(4) \cap \Gamma^0(2) = \{\pm I\}\Gamma,$$

imply that the map $S_4(\Gamma_0(8)) \to S_4(\Gamma)$, $g(\tau) \mapsto g(\tau/2)$ is an isomorphism. Hence, the space $S_4(\Gamma)$ is 1-dimensional and spanned by $f(\tau/2)$.

First equality $Trace(\rho_{1,\ell}^2(\mathrm{Frob}_p)) = Trace(\rho_{2,\ell}^2(\mathrm{Frob}_p))$:

Corollary 3.18 shows that our claim is equivalent to:

$$\sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b_{k,p}^2 - 2\phi_p(-1)p + 2 = \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\}}} a_{k,p}^2.$$

Due to Proposition 3.16, we need to prove:

$$\sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\}}} \phi_p(k^2 + 1)a_{k,p}^2 = -2 - 2\lambda(p)^2 + 2\phi_p(-1)p. \quad (*)$$

For p an odd prime and $k \in \mathbb{F}_p$ such that $k^2 \notin \{-1,0\}$ Proposition 3.13 implies that

$$\#X_k(\mathbb{F}_p) = \#\tilde{Y}_k(\mathbb{F}_p) - 24p + 6.$$

If $k^2 \notin \{-1,0\}$, then it follows from Theorem 3.15 that

$$\#X_k(\mathbb{F}_p) = 7 - 5p + p^2 + \phi_p(k^2 + 1)(a_{k,p}^2 - p).$$

For $k^2 = -1$:

$$\#X_k(\mathbb{F}_p) = 7 - (6 + \phi_p(-1))p + p^2 + \lambda(p)^2.$$

It follows from (3.3) that

$$\sum_{\substack{k \in \mathbb{F}_p \\ k \neq 0}} \#X_k(\mathbb{F}_p) = p^3 - 6p^2 + 12p - 9.$$

The following sum

$$\sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\}}} (7 - 5p + p^2 + \phi_p(k^2 + 1)(a_{k,p}^2 - p)) + (1 + \phi_p(-1))(7 - (6 + \phi_p(-1))p + p^2 + \lambda(p)^2)$$

equals $p^3 - 6p^2 + 12p - 9$ which is equivalent to

$$\sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\}}} \phi_p(k^2 + 1)a_{k,p}^2 = -2 - \lambda(p)^2(1 + \phi_p(-1)) + 2\phi_p(-1)p \quad (**)$$

Equality $(**)$ is equivalent to $(*)$ since $-2\lambda(p)^2 = -\lambda(p)^2(1 + \phi_p(-1))$ is equivalent to

$$\lambda(p)^2(\phi_p(-1) - 1) = 0$$

which holds for every odd prime p. Indeed, if $p \equiv 1 \pmod 4$, we have $\phi_p(-1) = 1$ and for $p \equiv -1 \pmod 4$ we have $\lambda(p) = 0$ by Remark 3.14. $\qquad \square$

Theorem 3.20. *Let p be an odd prime. Then*

$$\sum_{\substack{k \in \mathbb{F}_p \ k^2 \notin \{-1,0\}}} a_{k,p}^2 = \begin{cases} p^2 - 5p - 2 - c_f(p), & \text{if } p \equiv 1 \pmod 4, \\ p^2 - p - 2 - c_f(p), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

and

$$\sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b_{k,p}^2 = p^2 - 3p - 4 - c_f(p).$$

Proof. If $p > 5$ then the claim follows directly from Corollary 3.18 and Theorem 3.19. In other cases, the claim follows by direct computation. $\qquad\square$

Remark 3.21. Note that, arguing as in the proof of Theorem 1.4, it follows from the previous theorem that the second moment formula for the family F_k is

$$(3.11) \qquad\qquad M_{2,p}(F_k) = p^2 - c_f(p) - 3p - 1.$$

So the family satisfies the Bias conjecture. For the family H_k we obtain the formula

$$(3.12) \qquad\qquad M_{2,p}(H_k) = p^2 - c_f(p) - 3p - 2\lambda(p)^2 - 1.$$

In this case we have the additional contribution of $-2\lambda(p)^2$ which contributes to $f_2(p)$ due to Hasse bound. By the Sato-Tate conjecture for the CM elliptic curve $y^2 = x^3 - x$ the average of $\lambda(p)^2/p$ equals 1, hence the Bias conjecture holds for H_k as well.

4. Diophantine triples over finite fields

In this section, by using Lemma 3.2 we prove the following theorem which was first proved in [DK21] using different methods.

Theorem 4.1. *Let p be an odd prime and let $q = p^m$ for any $m \geq 1$. The number of Diophantine triples in $\mathbb{F}_q$ is equal to*

$$N(q) = \begin{cases} \frac{(q-1)(q-3)(q-5)}{48}, & \text{if } q \equiv 1 \pmod 4, \\ \frac{(q-3)(q^2-6q+17)}{48}, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Remark 4.2. If $q = 2^m$ then every element in $\mathbb{F}_q$ is a square (since Frobenius map $x \mapsto x^2$ is an automorphism of $\mathbb{F}_q$), hence every triple in $\mathbb{F}_q$ will have Diophantine property.

Proof. Assume that $q = p$. We will start by carefully studying the correspondence between the points on $(X \setminus X_{k=0})(\mathbb{F}_p)$ and Diophantine triples in $\mathbb{F}_p$. To the point $(x, y, z, k) \in (X \setminus X_{k=0})(\mathbb{F}_p)$, we associate two different triples $\{\frac{k}{x^2-1}, \frac{k}{y^2-1}, \frac{k}{z^2-1}\}$ and $\{\frac{-k}{x^2-1}, \frac{-k}{y^2-1}, \frac{-k}{z^2-1}\}$ (they are different since the product of the elements of the first triple is k and of the second is $-k$). These are Diophantine triples if x^2, y^2 and z^2 are pairwise distinct.

Denote by $N_1(p)$ and $N_2(p)$ the number of points in $(X \setminus X_{k=0})(\mathbb{F}_p)$ for which x^2, y^2 and z^2 are pairwise distinct and such that $xyz = 0$ and $xyz \neq 0$ respectively. Since the points $(\pm x, \pm y, \pm z, \pm k)$ all give rise to the same Diophantine triples (as well as the points we get by permuting coordinates x, y and z), we have that

$$N(p) = \frac{2N_1(p) + N_2(p)}{48}.$$

First, we count the points $(x, y, z, k) \in (X \setminus X_{k=0})(\mathbb{F}_p)$, with $x^2 = y^2 = z^2$. This condition is equivalent to $x^2 - 1 = k^2 \neq 0$. It follows from Proposition 3.1 that the number of such point is equal to

$$N_3(p) = \begin{cases} 4(p-5) + 2, & \text{if } p \equiv 1 \pmod 4 \\ 4(p-3), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

In the similar way, the number of points $(x, y, z, k) \in (X \setminus X_{k=0})(\mathbb{F}_p)$ with $x^2 = y^2 \neq z^2$ for some permutation of x, y and z is equal to

$$N_4(p) = \begin{cases} 6p^2 - 45p + 99, & \text{if } p \equiv 1 \pmod 4 \\ 6p^2 - 45p + 81, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Finally, to calculate $N_1(p)$ we need to count solutions $(x, y, k) \in \mathbb{F}_p^3$ of equation $(x^2 - 1)(y^2 - 1) = -k^2$ with $xyk \neq 0$ and $x^2 \neq y^2$. Since the product $(x^2 - 1)(y^2 - 1)$ is a square if both factors are either squares or non-squares, from the previous results it follows that

$$N_1(p) = \begin{cases} 3(p^2 - 10p + 25), & \text{if } p \equiv 1 \pmod 4 \\ 3(p^2 - 6p + 9), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Since $N_2(p) = \#(X \setminus X_{k=0})(\mathbb{F}_p) - N_1(p) - N_3(p) - N_4(p)$ from Lemma 3.2 we obtain

$$N_2(p) = \begin{cases} p^3 - 15p^2 + 83p - 165, & \text{if } p \equiv 1 \pmod 4 \\ (p - 7)(p - 5)(p - 3), & \text{if } p \equiv 3 \pmod 4 \end{cases},$$

and the formula for $N(p)$ follows.

The general case $q = p^m$ is proved analogously. $\qquad\square$

Following the proof of the previous theorem, for a prime $p > 2$, we can derive the number $N(p, k)$ of Diophantine triples in $\mathbb{F}_p$ with the fixed product $k \in \mathbb{F}_p^\times$. For $k \in \mathbb{F}_p$ such that $(k^2 + 1)k \neq 0$, let

$$G_k : y^2 = x^3 + x^2 - \frac{k^2}{4}x$$

be an elliptic curve over $\mathbb{F}_p$ which is birationally equivalent to the genus one curve $(x^2 - 1)^2(y^2 - 1) = k^2$, and let

$$H_k : y^2 = x^3 + (2k^2 + 4)x^2 + k^4 x,$$

be an elliptic curve over $\mathbb{F}_p$ birationally equivalent to the genus one curve $(x^2 - 1)(y^2 - 1) = -k^2$. Denote by $c_{k,p} = p + 1 - \#G_k(\mathbb{F}_p)$ and $d_{k,p} = p + 1 - \#H_k(\mathbb{F}_p)$. Also, denote by $e_{k,p}$ the number of distinct $\mathbb{F}_p$-rational solutions of the equation $(x^2 - 1)^2 = -k^2$, and by $f_{k,p}$ the number of distinct $\mathbb{F}_p$-rational solutions of the equation $(x^2 - 1)^3 = k^2$.

Corollary 4.3. *Let $p > 3$ be a prime, and let $k \in \mathbb{F}_p^\times$. Then*

a) If $k^2 \neq -1$, then

$$96 \cdot N(p, k) = 2p^2 + \underbrace{2\phi_p(k^2 + 1)(a_{k,p}^2 - p) - 16p}_{=O(p)}$$

$$+ \underbrace{12c_{k,p} - 6d_{k,p}}_{=O(\sqrt{p})} + \underbrace{50 - 12e_{k,p} + 16f_{k,p} - 6\phi_p(k^2 + 1)}_{=O(1)}.$$

b) If $k^2 = -1$, then

$$48 \cdot N(p, k) = p^2 + \underbrace{(4b^2 - 10p)}_{=O(p)} + \underbrace{8f_{k,p} + 13}_{=O(1)},$$

where $p = a^2 + b^2$ with b odd.

APPENDIX - CIRCULAR DIOPHANTINE m-TUPLES BY LUKA LASIĆ

In this appendix, we describe a parametrization of circular Diophantine m-tuples. For $m = 3$ we obtain a parametrization of rational Diophantine triples for which we show that it is equivalent to the one defined in Section 2.

Definition 4.4. A sequence of m rational numbers $(a_1, a_2, \ldots, a_m)$ is called a circular Diophantine m-tuple if $a_{i-1}a_i + 1$ is a perfect square for all $i \in \{1, 2, \ldots, m\}$ (we use "circular" notation: $a_k := a_{k \bmod m+1}$ for all $k \in \mathbb{Z}$).

Given a circular Diophantine m-tuple with non-zero elements $(a_1, a_2, \ldots, a_m)$, we define rational numbers $t_i = \frac{1 \pm \sqrt{1 + a_{i-1}a_i}}{a_i}$ for all $i \in \{1, 2, \ldots, m\}$ and for any choice of signs. Define rational functions $F_m = F_m(T_1, T_2, \ldots, T_m)$ and $G_m = G_m(T_1, T_2, \ldots, T_m)$ by

$$F_m = \frac{2T_1(1 + T_1 T_2(1 + T_2 T_3(1 + \ldots (1 + T_{m-2}T_{m-1}(1 + T_{m-1}T_m))\ldots)))}{(T_1 T_2 \cdots T_m)^2 - 1},$$

$$G_m = \frac{1 + T_1 T_2(2 + T_2 T_3(2 + T_3 T_4(2 + \ldots (2 + T_{m-1}T_m(2 + T_m T_1))\ldots)))}{(T_1 T_2 \cdots T_m)^2 - 1}.$$

One can check that $a_i = F_m(t_i, t_{i+1}, \ldots, t_{i+m-1})$, if $t_1 t_2 \cdots t_m \neq \pm 1$.
Conversely, since

$$F_m(T_i, \ldots, T_{i+m-1})F_m(T_{i+1}, \ldots, T_{i+m}) + 1 = G_m(T_i, \ldots, T_{i+m-1})^2,$$

for any choice of $T_i \in \mathbb{Q}$ such that $T_1 T_2 \cdots T_m \neq \pm 1$ it follows that

$$(F_m(T_1, T_2, \ldots, T_m), F_m(T_2, T_3, \ldots, T_1), \ldots, F_m(T_m, T_1, \ldots, T_{m-1}))$$

is a circular Diophantine m-tuple.

In particular, when $m = 3$ circular Diophantine triple (a_1, a_2, a_3) is actually a rational Diophantine triple (provided that elements of the triple are distinct and non-zero). Hence, the parametrization of circular Diophantine triples provides us with the parametrization of rational Diophantine triples

$$a_1 = \frac{2t_1\left((t_2 t_3 + 1) t_1 t_2 + 1\right)}{t_1^2 t_2^2 t_3^2 - 1},$$

$$a_2 = \frac{2t_2\left((t_1 t_3 + 1) t_2 t_3 + 1\right)}{t_1^2 t_2^2 t_3^2 - 1},$$

$$a_3 = \frac{2t_3\left((t_1 t_2 + 1) t_1 t_3 + 1\right)}{t_1^2 t_2^2 t_3^2 - 1}.$$

Moreover,

$$r = G_3(t_1, t_2, t_3) = \frac{((t_1 t_3 + 2) t_2 t_3 + 2) t_1 t_2 + 1}{t_1^2 t_2^2 t_3^2 - 1},$$

$$s = G_3(t_2, t_3, t_1) = \frac{((t_1 t_2 + 2) t_1 t_3 + 2) t_2 t_3 + 1}{t_1^2 t_2^2 t_3^2 - 1},$$

$$t = G_3(t_3, t_1, t_2) = \frac{((t_2 t_3 + 2) t_1 t_2 + 2) t_1 t_3 + 1}{t_1^2 t_2^2 t_3^2 - 1}$$

and

$$\Delta = \frac{8t_1 t_2 t_3 \left((t_1 t_2 + 1) t_1 t_3 + 1\right)\left((t_1 t_3 + 1) t_2 t_3 + 1\right)\left((t_2 t_3 + 1) t_1 t_2 + 1\right)}{(t_1^2 t_2^2 t_3^2 - 1)^3}.$$

It follows that

$$(r^2 - 1)(s^2 - 1)(t^2 - 1) = \Delta^2,$$

hence we can define a birational map $\mathcal{L} : \mathbb{A}^3 \to X$

$$\mathcal{L}(t_1, t_2, t_3) = (G_3(t_1, t_2, t_3), G_3(t_2, t_3, t_1), G_3(t_3, t_1, t_2), \Delta(t_1, t_2, t_3)).$$

The parametrization $\mathcal{L}$ is equivalent to the one we have defined in Section 2.

Corollary 4.5. *The map $\mathcal{L}$ is equal up to a birational automorphism μ of $\mathbb{A}^3$ to the affine restriction $\psi|_{\mathbb{A}^3}$ to the first chart of the map ψ from Proposition 2.1, i.e.*

$$\mathcal{L} = \psi|_{\mathbb{A}^3} \circ \mu$$

where

$$\mu(t_1, t_2, t_3) = (s, t, a_1 a_2 / t_2).$$

References

[ACF+18]   Megumi Asada, Ryan C. Chen, Eva Fourakis, Yujin Hong Kim, Andrew Kwon, Jared Duker Lichtman, Blake Mackall, Steven J. Miller, Eric Winsor, Karl Winsor, Jianing Yang, and Kevin Yang. Lower-order biases in the second moment of Dirichlet coefficients in families of L-functions (with appendices by Steven J. Miller and Jiefei Wu, and Steven J. Miller and Yan Weng). arXiv:1808.06056, 2018.

[BEW98]   Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[BHPVdV04]   Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius Van de Ven. *Compact complex surfaces*, volume 4 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, second edition, 2004.

[BL13]   Marie-José Bertin and Odile Lecacheux. Elliptic fibrations on the modular surface associated to $\Gamma_1(8)$. In *Arithmetic and geometry of K3 surfaces and Calabi-Yau threefolds*, volume 67 of *Fields Inst. Commun.*, pages 153–199. Springer, New York, 2013.

[BLGHT11]   Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi-Yau varieties and potential automorphy II. *Publ. Res. Inst. Math. Sci.*, 47(1):29–98, 2011.

[CD89]   François R. Cossec and Igor V. Dolgachev. *Enriques surfaces. I*, volume 76 of *Progress in Mathematics.* Birkhäuser Boston, Inc., Boston, MA, 1989.

[CM07]   Slawomir Cynk and Christian Meyer. Modular Calabi-Yau threefolds of level eight. *Internat. J. Math.*, 18(3):331–347, 2007.

[Del71]   Pierre Deligne. Formes modulaires et représentations l-adiques. In *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, volume 175 of *Lecture Notes in Math.*, pages Exp. No. 355, 139–172. Springer, Berlin, 1971.

[DK17]   Andrej Dujella and Matija Kazalicki. More on Diophantine sextuples. In *Number theory— Diophantine problems, uniform distribution and applications*, pages 227–235. Springer, Cham, 2017.

[DK21]   Andrej Dujella and Matija Kazalicki. Diophantine m-tuples in finite fields and modular forms. *Research in Number Theory*, 7, 3, 2021.

[DKMS17]   Andrej Dujella, Matija Kazalicki, Miljen Mikić, and Márton Szikszai. There are infinitely many rational Diophantine sextuples. *Int. Math. Res. Not. IMRN*, (2):490–508, 2017.

[DKP19]   Andrej Dujella, Matija Kazalicki, and Vinko Petričević. Rational Diophantine sextuples with square denominators. *J. Number Theory*, 205:340–346, 2019.

[DKP20]   Andrej Dujella, Matija Kazalicki, and Vinko Petričević. Rational Diophantine sextuples containing two regular quadruples and one regular quintuple. *Acta Mathematica Spalatensia*, 1:19–27, 2020.

[DP20a]   Andrej Dujella and Juan Carlos Peral. High rank elliptic curves induced by rational Diophantine triples. *Glas. Mat. Ser. III*, 55(4):237–252, 2020.

[DP20b]   Andrej Dujella and Vinko Petričević. Doubly regular Diophantine quadruples. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM*, 114(4):Paper No. 189, 8, 2020.

[Duj04]   Andrej Dujella. There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.*, 566:183–214, 2004.

[Duj09]   Andrej Dujella. Rational Diophantine sextuples with mixed signs. *Proc. Japan Acad. Ser. A Math. Sci.*, 85(4):27–30, 2009.

[Duj16]   Andrej Dujella. What is . . . a Diophantine *m*-tuple? *Notices Amer. Math. Soc.*, 63(7):772–774, 2016.

[Edw07]   Harold M. Edwards. A normal form for elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 44(3):393–422, 2007.

[Har77]   Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[HTZ19]   Bo He, Alain Togbé, and Volker Ziegler. There is no Diophantine quintuple. *Trans. Amer. Math. Soc.*, 371(9):6665–6709, 2019.

[IR90]   Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[KN20]   Matija Kazalicki and Bartosz Naskręcki. Second moments and the bias conjecture for the family of cubic pencils. arXiv:2012.11306, 2020.

[KS08]   Masato Kuwata and Tetsuji Shioda. Elliptic parameters and defining equations for elliptic fibrations on a Kummer surface. In *Algebraic geometry in East Asia—Hanoi 2005*, volume 50 of *Adv. Stud. Pure Math.*, pages 177–215. Math. Soc. Japan, Tokyo, 2008.

[Kub76]   Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[Mic95]   Philippe Michel. Rang moyen de familles de courbes elliptiques et lois de Sato-Tate. *Monatsh. Math.*, 120(2):127–136, 1995.

[Mil02]   Steven Joel Miller. *1- and 2-level densities for families of elliptic curves: Evidence for the underlying group symmetries.* ProQuest LLC, Ann Arbor, MI, 2002. Thesis (Ph.D.)–Princeton University.

[Mor84]   David R. Morrison. On K3 surfaces with large Picard number. *Invent. Math.*, 75(1):105–121, 1984.

[Nas14]   Bartosz Naskręcki. Ranks in families of elliptic curves and modular forms. *Adam Mickiewicz University in Poznań*, 2014. Ph.D. thesis.

[Nas17]   Bartosz Naskręcki. On a certain hypergeometric motive of weight 2 and rank 3. arXiv:1702.07738, 2017.

[RS98]   Michael Rosen and Joseph H. Silverman. On the rank of an elliptic surface. *Invent. Math.*, 133(1):43–67, 1998.

[Sch88]   Anthony J. Scholl. The *l*-adic representations attached to a certain noncongruence subgroup. *J. Reine Angew. Math.*, 392:1–15, 1988.

[Shi90]   Tetsuji Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990.

[Sil94]   Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09]   Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[SS19]   Matthias Schütt and Tetsuji Shioda. *Mordell-Weil lattices*, volume 70 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer, Singapore, 2019.

[Ver00]   H. A. Verrill. The *L*-series of certain rigid Calabi-Yau threefolds. *J. Number Theory*, 81(2):310–334, 2000.

[vGT06]   Bert van Geemen and Jaap Top. An isogeny of K3 surfaces. *Bull. London Math. Soc.*, 38(2):209–223, 2006.

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

Email address: matija.kazalicki@math.hr

Faculty of Mathematics and Computer Science, Adam Mickiewicz University in Poznań, ul. Uniwersytetu Poznańskiego 4, 61-614, Poznań, Poland

Email address: bartnas@amu.edu.pl