New York Journal of Mathematics

New York J. Math. **20** (2014) 1–25.

Arithmetic dynamics on smooth cubic surfaces

Solomon Vishkautsan

Abstract. We study dynamical systems induced by birational automorphisms on smooth cubic surfaces defined over a number field K. In particular we are interested in the product of noncommuting birational Geiser involutions of the cubic surface. We present results describing the sets of K and $\bar{K}$-periodic points of the system, and give a necessary and sufficient condition for a dynamical local-global property called strong residual periodicity. Finally, we give a dynamical result relating to the Mordell–Weil problem on cubic surfaces.

Contents

1. Introduction

In this article we study arithmetic dynamics on smooth cubic surfaces over a number field K. The setup is quite simple: Take X/K a smooth

Received August 2, 2013.

2010 *Mathematics Subject Classification.* Primary: 37P55; Secondary: 37P35, 37P05, 14G25, 14J26, 11G05.

Key words and phrases. Dynamical systems, cubic surfaces, periodic points, residual periodicity, arithmetic dynamics.

The author's research was supported by the Israel Science Foundation, grants 657/09 and 1207/12, and by the Skirball Foundation via the Center for Advanced Studies in Mathematics at Ben-Gurion University of the Negev.

ISSN 1076-9803/2014

cubic surface over a number field K, and f a birational automorphism of X, also defined over K. A dynamical system is induced by applying iterations of f to points in $X(K)$ or $X(\bar{K})$ (where $\bar{K}$ is the algebraic closure of K). Such a dynamical system is an example of an *arithmetic-geometric dynamical system* (described formally in Section 3). We are interested in two questions: What can be said about the K- and $\bar{K}$-periodic points of f? What can be said about the interplay between global dynamics over K and local dynamics when the system is reduced modulo p, for all but finitely many primes p in K's ring of integers?

In particular, we focus on dynamical systems induced by a simple type of birational automorphism on smooth cubic surfaces, defined by taking the composition of two Geiser involutions of the cubic surface (see Section 4). Such automorphisms are examples of *Halphen twists* (cf. Brown and Ryder[6], Blanc and Cantat [4]). By a theorem of Manin ([14, Example 39.8.4]), the composition of two Geiser involutions is of infinite order in the group of birational automorphisms of the cubic surface, and has the nice property of preserving an elliptic fibration of the cubic surface (by *preserve* we mean that every fiber is mapped to itself under the birational automorphism). Even for this simple type of birational automorphisms, the dynamical properties are not entirely trivial and deserve to be studied carefully.

A complication in studying the dynamics of a birational map φ of an algebraic variety X is the *locus of indeterminacy* $\mathcal{Z}(\varphi)$, the set of points where the map φ is not defined. Even worse is the fact that the set of points on the variety whose iterations under φ land in $\mathcal{Z}(\varphi)$, which we denote by $\mathcal{Z}_\infty(\varphi)$, can *a priori* be the set of all rational points of X defined over $\bar{K}$. A recent result by Amerik [1, Corollary 9] states that this in fact cannot happen, but does not guarantee any periodic points lying outside of this set. We also need to define what we mean by periodic points in this setup, since for example for a birational involution φ of the projective plane, the image of a point can be undefined for the first iteration of φ, but fixed under the second iteration. We do not wish to consider points of this type to be periodic, so in this article we will only consider a point to be periodic if it lies outside of $\mathcal{Z}_\infty(\varphi)$.

An arithmetic-geometric dynamical system D (such as the one induced by a birational automorphism of a smooth cubic surface) can be reduced modulo p for all but finitely many primes p, inducing *residual dynamical systems* D_p (see Section 3). In some systems, an interesting local-global behavior occurs when the system D has no periodic points defined over K, but there exist periodic points of bounded period modulo all but finitely many primes p, where the bound on the periods is independent of p. We consider the more general case, when there exist periodic points of bounded period modulo all but finitely many primes p that are not reductions modulo p of any periodic points over K, with the bound on the periods independent of p. This property was first described by Bandman, Grunewald and Kunyavskiĭ [2, Section 6], and is called *strong residual periodicity.* In the above-mentioned article one can find motivating examples.

Our results in this article are as follows: Let f denote a birational automorphism defined by taking the composition of two Geiser involutions on a smooth cubic surface X. We show that the $\bar{K}$-periodic points of f (lying outside of $\mathcal{Z}_\infty(f)$) are Zariski-dense in $X(\bar{K})$ (Corollary 6.6). The set of K-periodic points is contained in the union of finitely many fibers of the elliptic fibration preserved by f (Corollary 6.11), and the number of these fibers is bounded by a number depending only on the degree of the extension $K/\mathbb{Q}$. We further show that if $K = \mathbb{Q}$ then the period of $\mathbb{Q}$-periodic points is bounded by 12, and cannot equal 11 (Theorem 6.12). The fibers containing all periodic points can be found using a sequence of recursively defined polynomials that relate to division polynomials of elliptic curves. We define and use these polynomials to study local-global dynamics of the system and provide a necessary and sufficient condition for strong residual periodicity (Theorem 7.6). Finally, we provide a result relating to the Mordell–Weil problem on cubic surfaces (see Section 8): We prove that under mild conditions, the set of periodic points of f is finitely generated by tangents and secants (Theorem 8.2). We also call the reader's attention to the very useful Lemma 3.9, which proves that group translations are never strongly residually periodic.

Let us briefly describe the structure of the article: In Sections 2–4 we provide the notations and preliminaries required to prove our results. In Section 5 we describe the dynamics of a product of Geiser involutions. In Section 6 we present a method for counting periodic fibers of such birational automorphisms. In Section 7 we prove a necessary and sufficient condition for strong residual periodicity of a product of Geiser involutions. In Section 8 we discuss the Mordell–Weil problem on cubic surfaces. In Section 9 we provide examples illustrating the various results of the article.

Acknowledgments. This article contains some of the results from the author's Ph.D. thesis under the joint advisorship of Tatiana Bandman and Boris Kunyavskiĭ of Bar-Ilan University. Their tremendous help and advice during the writing of the dissertation and this article are greatly appreciated. The author also thanks (in chronological order) Michael Friedman, Igor Dolgachev and Serge Cantat for fruitful correspondence and discussions relating to this article and its results. The author gratefully thanks the referee for his helpful comments and corrections.

2. Notations

Notation 2.1.

- K is a number field, and $\bar{K}$ its algebraic closure.
- $\mathcal{O}_K$ is the ring of integers of K.

- p is a prime ideal in $\mathcal{O}_K$.
- $\mathcal{O}_p$ is the localization of $\mathcal{O}_K$ at the prime p.
- $\mathfrak{m}_p$ is the maximal ideal in $\mathcal{O}_p$.
- κ_p is the residue field of the prime p (i.e., $\mathcal{O}_p/\mathfrak{m}_p$).
- $\mathcal{L}(x, y)$ is the projective line going through two distinct points x, y in $\mathbb{P}^3$.
- $\mathcal{P}(x, y, z)$ is the projective plane through noncollinear $x, y, z \in \mathbb{P}^3$.
- $T_x(S)$ is the tangent plane at x for a smooth projective surface S in $\mathbb{P}^3$.

Definition 2.2. Given a rational map $\varphi : X \to Y$ between quasiprojective varieties X, Y, the *domain* of φ is the largest open subset of X for which the restriction of φ is a morphism. The complement of the domain is called the *locus of indeterminacy* (or *indeterminacy set*), and is denoted by $\mathcal{Z}(\varphi)$.

Notation 2.3. Let φ be a dominant rational self-map $\varphi : X \to X$ of a projective variety $X \subset \mathbb{P}_k^N$. For an integer $n \geq 1$ we denote

$$\mathcal{Z}_n(\varphi) = \bigcup_{i=0}^{n-1} \varphi^{-i}(\mathcal{Z}(\varphi)).$$

We remark that $\mathcal{Z}_n(\varphi) \neq \mathcal{Z}(\varphi^n)$ (e.g., $\mathcal{Z}_n(\varphi)$ may be an infinite set for a rational map φ from a smooth projective surface, but $\mathcal{Z}(\varphi^n)$ is finite, since the locus of indeterminacy of such a map has codimension ≥ 2). We also denote

$$\mathcal{Z}_\infty(\varphi) = \bigcup_{n=1}^{\infty} \mathcal{Z}_n(\varphi) = \bigcup_{i=0}^{\infty} \varphi^{-i}(\mathcal{Z}(\varphi)).$$

Thus, $\mathcal{Z}_\infty(\varphi)$ is the set of all points whose orbit intersects the locus of indeterminacy $\mathcal{Z}(\varphi)$ (the Zariski-closure of this set is called the *extended indeterminacy set*, cf. Diller [10, Definition 2.1]).

3. Preliminaries on arithmetic-geometric dynamical systems

In this section, we recall the definitions and properties of arithmetic dynamical systems. We follow Silverman [24, Section 1], Hutz [12, Section 2] and Bandman, Grunewald and Kunyavskiĭ [2, Section 6] unless otherwise stated.

Definition 3.1. Let K be a number field. A triple $D = (X, \varphi, F)$ is called an *arithmetic-geometric dynamical system* over K (or K*-dynamical system* or *AG dynamical system*) if:

- X is an algebraic K-variety.
- $\varphi : X \to X$ is a dominant K-endomorphism (or a dominant K-rational self-map; note that in this case we allow the function in the dynamical system to be partially defined).

- $F \subset X(K)$ is a subset of rational points which we call the *forbidden set* of the dynamical system D (the forbidden set will include points the dynamical behavior of which we wish to ignore, cf. Remark 3.7 below).

The dynamics are induced by the components of the system D: we study iterations $\varphi^n(x)$ for points $x \in X(\bar{K})$. We are particularly interested in *periodic points*, i.e., points $x \in X(\bar{K}) \setminus \mathcal{Z}_\infty(\varphi)$ such that $\varphi^n(x) = x$ for some positive integer n. The minimal such n is called the *exact period* of x.

Definition 3.2. Let $\mathcal{O}_K$ be the ring of integers of a number field K. A triple $\mathcal{D} = (\mathcal{X}, \Phi, \mathcal{F})$ is called an $\mathcal{O}_K$*-dynamical system* if:

- $\mathcal{X}$ is an $\mathcal{O}_K$-scheme of finite type.
- $\Phi : \mathcal{X} \to \mathcal{X}$ is a dominant $\mathcal{O}_K$-endomorphism (or a dominant $\mathcal{O}_K$-rational self-map).
- $\mathcal{F} \subset \mathcal{X}(\mathcal{O}_K)$ is the *forbidden set* of the dynamical system $\mathcal{D}$ (cf. Remark 3.7 below).

Definition 3.3. We say that an $\mathcal{O}_K$-dynamical system $\mathcal{D} = (\mathcal{X}, \Phi, \mathcal{F})$ is an *integral model* of the K-dynamical system $D = (X, \varphi, F)$ if:

- $\mathcal{X} \times_{\mathcal{O}_K} K = X$ (this means X is the generic fiber of $\mathcal{X}$).
- The restriction of Φ to the generic fiber of $\mathcal{X}$ coincides with φ.
- $\rho(\mathcal{F}) = F$, where $\rho\colon \mathcal{X}(\mathcal{O}_K) \to X(K)$ is the restriction to the generic fiber.

Definition 3.4. Consider a K-AG dynamical system $D = (X, \varphi, F)$ and an integral model $\mathcal{D} = (\mathcal{X}, \Phi, \mathcal{F})$, as described in the previous section. Let p be a prime of $\mathcal{O}_K$. Then:

- X_p, the special fiber of $\mathcal{X}$ at p, is called the *reduction of X modulo p*. We have $X_p = \mathcal{X} \times_{\mathcal{O}_K} \kappa_p$.
- Let $\rho_p\colon \mathcal{X} \to X_p$ be the reduction map (restriction to the special fiber). The image of $a \in \mathcal{X}(\mathcal{O}_K)$ under ρ_p is the *reduction modulo p of a*.
- $\varphi_p\colon X_p \to X_p$, the restriction of Φ to the special fiber over p, is an endomorphism (or rational self-map) of κ_p-schemes. This is the *reduction of φ modulo p*.
- $F_p = \rho_p(\mathcal{F}) \subset X_p(\kappa_p)$ is the reduction of the forbidden set $\mathcal{F}$.

We call the triple $D_p = (X_p, \varphi_p, F_p)$ the *residual system* of D modulo p.

Definition 3.5. Let $D = (X, \varphi, F)$ be a K-AG dynamical system such that X is a smooth and proper K-variety and φ is a dominant endomorphism. Let $\mathcal{D} = (\mathcal{X}, \Phi, \mathcal{F})$ be an integral model. Then for a place p of K we say X has *good reduction at a prime p* if X_p is a smooth and proper scheme; we say that φ has *good reduction at a prime p* if φ_p extends to a dominant κ_p-morphism. If both X and φ have good reductions modulo p, we say that D has *good reduction* modulo p.

Let us recall some important facts about good reduction: A smooth projective variety X defined over a number field K has good reduction at all but finitely many primes of $\mathcal{O}_K$ (see Hindry and Silverman [11, Proposition A.9.1.6]). A similar statement is true for a morphism of a projective variety defined over a number field K (see Hutz [13, Proposition 1]). For a prime p of good reduction of a dynamical system D, reduction modulo p commutes nicely with a morphism, i.e., $\rho_p(\varphi^n(a)) = \varphi_p^n(\rho_p(a))$ (see Hutz [12, Theorem 7]). Therefore we can discuss the reductions of orbits, etc.

Definition 3.6. Let $D = (X, \varphi, F)$ be a K-AG dynamical system, and let $D_p = (X_p, \varphi_p, F_p)$ be the reduction of D modulo p with respect to some integral model. Let $a \in X_p(\kappa_p) \setminus F_p$ be a periodic point of φ_p. Let $\ell_p(\varphi, a)$ be the orbit size of a. Set $\underline{\ell}_p := \min\{\ell_p(\varphi, a)\}$ where the minimum is taken over all a. If there are no periodic points in $X_p(\kappa_p) \setminus F_p$, we set $\underline{\ell}_p = \infty$. Let M denote the collection of primes p such that $\underline{\ell}_p = \infty$. Let $N = \{\underline{\ell}_p\}_{p \notin M}$. We say that a K-dynamical system $D = (X, \varphi, F)$ or an $\mathcal{O}_K$-dynamical system $\mathcal{D} = (\mathcal{X}, \Phi, \mathcal{F})$ is *residually aperiodic* if the set M is infinite, *residually periodic* if M is finite, and *strongly residually periodic* (SRP) if the sets M and N are both finite. We denote by *SRP(n)* a dynamical system that is strongly residually periodic with minimal periods bounded by an integer n for all but finitely many primes.

Remark 3.7. Usually we will take the forbidden set $F \subset X(K)$ to be the set of all periodic points in $X(K)$ (or the Zariski-closure of this set), so that SRP describes the situation where we have bounded residual periods that cannot be explained by periodic points in $X(K)$. In case φ is rational, we include $\mathcal{Z}_\infty$ in F so that we can exclude points with bad dynamics.

Given a dynamical system $D = (X/K, \varphi, \emptyset)$ (for now we ignore the forbidden set), one can ask about the orbit size of a point $a \in X(K)$ when reduced modulo p. If $a \in X(\mathcal{O}_K)$ is periodic of exact period n, then the orbit size of $\rho_p(a)$ divides n (cf. Hutz [12, Theorem 1]). If a is of an infinite orbit, we would expect that when reducing the point modulo primes p, the reduced point $\rho_p(a)$ will have periods that grow together with the cardinality of κ_p. This is a direct corollary from a theorem of Silverman (see [24, Theorem 2]):

Corollary 3.8 (Corollary to Silverman's Theorem)**.** *Let $D = (X, \varphi, F)$ be an AG dynamical system, and let $a \in X(K) \setminus \mathcal{Z}_\infty$ be a point of an infinite orbit. Then the residual periods of a are unbounded over the primes in $\mathcal{O}_K$.*

From the corollary we see that strong residual periodicity cannot be explained by one global point of infinite orbit, and in fact we can deduce from Silverman's theorem that it cannot be explained by a finite set of points of infinite orbit in $X(K)$. The corollary allows us to prove the following simple yet useful lemma:

Lemma 3.9. *Let G/K be an algebraic group over a number field K, and let D be the dynamical system induced by the group translation $\varphi_g(x) = gx$, for some element $g \in G(K)$ of infinite order. Then D is not SRP.*

Proof. The iterations of φ_g are very simple: $\varphi_g^n(x) = g^n x$. We see that the following are equivalent:

(a) There exists a periodic point $x \in G(K)$ of exact period n.
(b) The element g is of finite order n.
(c) The element g is a periodic point of φ_g of exact period n: i.e.,

$$\varphi_g^n(g) = g$$

(and $n \geq 1$ is the minimal positive integer satisfying this).
(d) The map φ_g is of finite order n in the automorphism group of the underlying variety of G/K.

Now, if g is of infinite order in G/K, then by the properties above it is of infinite orbit, and we can use the corollary to Silverman's Theorem (Corollary 3.8) to see that the φ_g-periods of g modulo primes p are unbounded over the primes. This means that the minimal periods are unbounded (because the equivalent conditions above are also relevant for the reduced system D_p when there is good reduction), so that φ_g is not SRP. $\square$

4. Preliminaries on cubic surfaces

In order to study arithmetic dynamics on smooth cubic surfaces, we need to recall several classical geometric properties and theorems related to them.

We briefly recall the group structure on absolutely irreducible cubic plane curves (cf. Manin [14, Chapter I, Section 1, page 7] and Silverman [25, Chapter III, Section 2]). Let C be an absolutely irreducible cubic curve in the projective plane $\mathbb{P}^2$, defined over a field k. Let $C_{ns}(k)$ denote its set of nonsingular rational points over k. Assuming $C_{ns}(k) \neq \emptyset$, we define a binary composition law $\circ : C_{ns}(k) \times C_{ns}(k) \to C_{ns}(k)$, by setting $x \circ y$ for $x \neq y$ to be the third point of intersection of the line $L = \mathcal{L}(x, y)$ with the curve C. If $x = y$ then we take L to be the tangent to C at x. We can then turn $C_{ns}(k)$ into a group by choosing an element $u \in C_{ns}(k)$ and defining $xy := u \circ (x \circ y)$ for $x, y \in C_{ns}(k)$. With this multiplication, $C_{ns}(k)$ is an abelian group with unit u . If C is smooth, this gives the usual composition law on elliptic curves, and we denote it by $x + y$.

Similarly, we can define a composition law $\circ : S(\bar{k}) \times S(\bar{k}) \to S(\bar{k})$ on a smooth cubic surface $S \subset \mathbb{P}^3_k$ defined over a field k (cf. Manin [14, Chapter I, Section 1, page 7]). This composition is only partially defined. Given two distinct points $x, y \in S(\bar{k})$ such that $\mathcal{L}(x, y)$ does not lie on S, we define $x \circ y$ to be the third point of the intersection of the line $\mathcal{L}(x, y)$ with S (this line has three points of intersection with S, by Bezout's theorem). We note that this operation is commutative but not necessarily associative.

Definition 4.1. A point $x \in S(\bar{k})$ on a smooth cubic surface S/k is a *good point* if it does not lie on the union of the lines of $S \times_k \bar{k}$ (recall that there are 27 lines over $\bar{k}$ on a smooth cubic surface, cf. Shafarevich [21, Chapter IV, Section 2.5, Theorem]). An unordered pair of distinct points $x, y \in S(\bar{k})$ is called a *good pair* if the line containing these points is not tangent to $S \times_k \bar{k}$ and does not intersect the union of the lines on $S \times_k \bar{k}$ in $\mathbb{P}^3$ (cf. Manin [14, Chapter V, Section 33.6]).

It is clear from the definition that a pair of distinct points $x, y \in S(\bar{k})$ on a smooth cubic surface is a good pair if and only if $x \circ y$ is defined, the three points x, y and $x \circ y$ are distinct and all three of them are good.

The *Geiser involution* of a smooth cubic surface S through a point $x \in S(k)$, is a map $t_x : S \to S$ sending each $y \in S(\bar{k})$ to $x \circ y$, when defined (cf. Brown and Ryder [6, Section 2.2] and Corti, Pukhlikov and Reid [7, Section 2.6]). We define t_x for absolutely irreducible cubic curves in the same way. It is clear that t_x is a birational involution (it is generally not defined at x itself). A theorem of Manin [14, Theorems 33.7, 33.8] says that the Geiser involutions together with the Bertini involutions and the projective automorphisms generate $\mathrm{Bir}(S)$ for a minimal smooth cubic surface S defined over a perfect nonclosed field. Some other useful properties of the Geiser involution are that $t_x(y) = t_y(x)$ for a good pair x, y, and its locus of indeterminacy is $\mathcal{Z}(t_x) = \{x\}$. Also, t_x is an automorphism when restricted to $S \setminus C_x$, where $C_x = T_x(S) \cap S$.

Theorem 4.2. *Let $C \subset \mathbb{P}^2$ be an absolutely irreducible plane cubic curve defined over a field k. Then:*

(a) *The product of any two Geiser involutions $t_x t_y$ is a group translation: Given the choice of a group structure on the nonsingular points on the cubic curve, then for any nonsingular point $z \in C_{ns}(\bar{k})$ we get $t_x t_y(z) = (y - x) + z$ (or $t_x t_y(z) = x^{-1} y z$ if the group is multiplicative.*

(b) *For any $x, y, z \in C$ we have $t_x t_y t_z = t_w$, where $w = y \circ (x \circ z)$.*

Proof. See the proof of Theorem 2.1 in Manin [14]. □

Theorem 4.3. *Let S be a smooth cubic surface over a perfect field k, and let $x, y \in S(k)$ be a good pair. Then the birational map $t_x t_y$ is of infinite order in* $\mathrm{Bir}(S)$*.*

Proof. See Manin [14, Example 39.8.4]. □

We recall some facts about hyperplane sections of a smooth surface S in $\mathbb{P}^3$ defined over a perfect field k. If H is a hyperplane in $\mathbb{P}^3$, then a point $x \in S \cap H$ is singular (on $S \cap H$) if and only if $H = T_x$ (here $S \cap H$ is viewed scheme-theoretically, since the intersection may not be reduced, cf. Beltrametti et al. [3, Chapter 3, Section 1.8]). For a smooth cubic surface S in $\mathbb{P}^3$ we know that any hyperplane section will be one of the following (see Reid [20, Chapter 7, Section 1, Proposition]):

(a) an absolutely irreducible smooth plane cubic curve;
(b) a cuspidal plane cubic;
(c) a nodal plane cubic;
(d) an absolutely irreducible conic and a line;
(e) three distinct lines.

By using these properties it is easy to prove the following list of statements about hyperplane sections of cubic surfaces:

Proposition 4.4. *Let $S \subset \mathbb{P}^3$ be a smooth cubic surface over a perfect field k.*

(a) *The point $x \in S(\bar{k})$ is a good point if and only if the curve*
$$C_x = T_x(S) \cap S$$
is absolutely irreducible.

(b) *Let x, y be distinct good points on S. Then C_x and C_y do not have any common components.*

(c) *Let x, y be a good pair on S. Then any plane $H \subset \mathbb{P}^3$ passing through x, y intersects S in an absolutely irreducible cubic curve C, and the three (distinct) points x, y, z in $\mathcal{L}(x, y) \cap S$ are nonsingular on C.*

5. Dynamics of a product of Geiser involutions

In this section we study the global dynamics of a product of two Geiser involutions $t_x t_y$, where x, y is a good pair on S. We will show that the dynamics of $t_x t_y$ are determined by its restrictions to the fibers of the elliptic fibration preserved by $t_x t_y$. Using Theorem 4.2 we see that $t_x t_y$ restricts to a group translation on the nonsingular points of each fiber, making the dynamics of $t_x t_y$ particularly easy to study. As a slight disclaimer, we mention that some of the proofs in this section are classical in nature, so no originality is claimed here (other than applying them to the dynamical setting). Our main results in this section are Proposition 5.5, characterizing the periodic fibers of exact period n, and Proposition 5.8, proving the existence of $\bar{K}$-periodic points lying outside of $\mathcal{Z}_\infty(t_x t_y)$.

Proposition 5.1. *Let S be a smooth cubic surface, and x, y a good pair. Let H be a hyperplane going through x, y. Let C be the hyperplane section $H \cap S$ (absolutely irreducible by Proposition 4.4). Then C is invariant under $t_x t_y$ and the restriction of $t_x t_y$ to C is a group translation on C_{ns}.*

Proof. That C is invariant is clear from the definition of t_x and $t_x t_y$ is a group translation by Theorem 4.2. □

Let $S \subset \mathbb{P}^3$ be a smooth cubic surface over a perfect field k. An *elliptic fibration* on S is a rational map $\varphi : S \to B$ defined over k, such that the geometric generic fiber is birational to a curve of genus 1. For a field k of characteristic 0 the base of an elliptic fibration must be of genus 0 and has a rational point, so it is isomorphic to $\mathbb{P}^1$(see Brown and Ryder

[6, Section 1] for the definition, and a proof of the last statement). Given a good pair x, y on S, we can define an elliptic fibration by taking the pencil of planes through the line $L = \mathcal{L}(x, y)$: we choose two distinct planes $H_1 = \{f = 0\}, H_2 = \{g = 0\}$ passing through L (where f, g are linear forms); then the rational map $\varphi = (f, g)$ is an elliptic fibration. We call such a fibration the *linear fibration* associated with the good pair x, y. The following is immediate from Proposition 5.1.

Proposition 5.2. *Let $S \subset \mathbb{P}^3$ be a smooth cubic surface. Given a good pair x, y on S, the fibers of the linear fibration through x, y are invariant under the birational automorphism $t_x t_y$.*

From Proposition 5.1 and the proof of Lemma 3.9, we see that the only fibers containing periodic points are those for which $t_x t_y$ restricts to a group translation of finite order (aside from the singular points of the singular fibers, which we will show to be fixed points). Denote by $\mathrm{Fixed}(\varphi)$ the set of fixed points of a rational map φ, then:

Proposition 5.3. *Let x, y be a good pair on a smooth cubic surface S over a perfect field k, then* $\mathrm{Fixed}(t_x t_y) = \mathrm{Fixed}(t_x) \cap \mathrm{Fixed}(t_y)$*.*

Proof. Obviously, if $w \in \mathrm{Fixed}(t_x) \cap \mathrm{Fixed}(t_y)$, then $w \in \mathrm{Fixed}(t_x t_y)$. In the other direction, suppose $t_x t_y(w) = w$. Assume $w \neq x$; we apply t_x to both sides of the equation and get $t_x(w) = t_y(w)$ (since $w \notin \{x\} = \mathcal{Z}(t_x)$). We know that $t_x(w) = t_w(x)$, so that we get $t_w(x) = t_w(y)$. Now, if $t_w(x) \neq w$, we can apply t_w to both sides of the equation and get $x = y$, a contradiction. Therefore, still under the assumption of $w \neq x$, we get $t_w(x) = t_x(w) = w$ and also $t_y(w) = w$ as required. If $w = x$, then we have $t_x t_y(x) = x$, which implies $t_y(x) \in C_x$ since $t_x^{-1}(x) = C_x$. The points $x, y, t_y(x)$ are collinear, and since $x, t_y(x) \in C_x$, we get that $y \in C_x$ as well, which implies $t_y(x) = x$; but then $t_x t_y(x) = t_x(x)$ is indeterminate, a contradiction. $\square$

Corollary 5.4. *Let S, x, y be as in Proposition* 5.3*. Then:*

(a) *A point $w \in S(\bar{k})$ is a fixed point of $t_x t_y$ if and only if w is a singular point of the curve $C = \mathcal{P}(x, y, w) \cap S$.*
(b) *The map $t_x t_y$ has at most* 12 *fixed points over $\bar{k}$.*

Proof. (a) We saw in the proof of Proposition 5.3 that w is a fixed point of $t_x t_y$ if and only if $x, y \in C_w$. Therefore $C = C_w$, and w is singular on C_w (by Proposition 4.4).

(b) The linear fibration π associated with x, y can be blown up at the three points x, y, z in $\mathcal{L}(x, y) \cap S$ to give a rational elliptic surface, which only has at most 12 singular fibers (see Miranda [18, Section 1]) (Note that no singularities on the fibers of π are resolved by the blowup, since x, y, z are smooth on all fibers by Proposition 4.4). Each of these singular fibers is associated with a fixed point of $t_x t_y$ by Corollary 5.4. $\square$

We will say that a fiber C in the linear fibration associated with a good pair $\{x, y\}$ is a *periodic fiber* of period $n > 0$ if $(t_x t_y)^n$ is the identity when restricted to the fiber C, and n is the minimal positive integer satisfying this.

Proposition 5.5. *Let x, y be a good pair on a smooth cubic surface $S \subset \mathbb{P}^3$ defined over a perfect field k. Let $w \in S(\bar{k}) \setminus \mathcal{Z}_\infty(t_x t_y)$ be noncollinear with x, y, and denote $C = \mathcal{P}(x, y, w) \cap S$. Then the following are equivalent:*

(a) *The point w is a periodic point of exact period $n > 1$ of $t_x t_y$.*
(b) *The curve C is $t_x t_y$-periodic of period n (which is the same as saying $t_x t_y$ is of order n in $Aut(C)$), and w is a nonsingular point of C.*
(c) *The point y is of order n in the group $C_{ns}(k)$ with x chosen to be the unit element (the point y is nonsingular on C by Proposition* 4.4*).*

Proof. Let $w \in S$ be periodic of exact period $n > 1$. By Proposition 5.1, the birational automorphism $t_x t_y$ restricts to an automorphism of C. We choose x to be the unit element of the group structure on $C_{ns}(k)$ (note that $w \in C_{ns}(k)$ since the period of w is greater than 1, and then by Corollary 5.4 it is nonsingular), and get

$$w = (t_x t_y)^n(w) = ny + w \tag{1}$$

(see Theorem 4.2), from which we get $ny = 0$, meaning that the order of y on the cubic curve is n and that $(t_x t_y)^n = id$. If the order of $t_x t_y$ was less than n, we would get a contradiction to n being the exact period of w. So we have proved that (a) implies (b) and (c). Similarly, one uses equation (1) to prove the other implications. $\square$

We can say more for the period $n = 2$:

Proposition 5.6. *Let S, x, y, φ, w and C be as in Proposition* 5.5*. We restrict $\circ$ to the curve C, where it is fully defined. Then the following are equivalent:*

(a) *The point $w \in S(\bar{k})$ is a periodic point of exact period $n = 2$ of $t_x t_y$.*
(b) *$x \circ x = y \circ y$.*
(c) *$x \circ x \in C_x \cap C_y$.*

Proof. The statements (b) and (c) are equivalent, because $x \circ x \in C_y$ means that the line through y and $x \circ x$ has a double point at y, and as this line is contained in $\mathcal{P}(x, y, w)$, it must mean that this is the tangent line to C at y, but then by definition $x \circ x = y \circ y$. The statements (a) and (b) are equivalent since

$$(t_x t_y)^2(w) = w \iff 2y + w = w \iff 2y = 0 \iff x \circ (y \circ y) = x,$$

and we can apply x to both sides of the last equation. $\square$

Corollary 5.7. *Let S, x, y, φ be as in Proposition* 5.5*; then there are three periodic fibers of period 2 defined over $\bar{k}$, counted with multiplicity, in the* *linear fibration of S through the points x, y (and these contain all periodic points of period 2).*

Proof. We show that the period 2 fibers of φ are determined by the intersection of the line $L = T_x(S) \cap T_y(S)$ with S. The line L cannot lie on S, since otherwise it lies on $T_x(S)$ and therefore is contained in $C_x = T_x(S) \cap S$; but C_x is absolutely irreducible by Proposition 4.4. Therefore the line L intersects S at three points (counted with multiplicity). None of these three points are collinear with x, y (otherwise $\mathcal{L}(x, y)$ has a double point at both y and x). Each point $w \in S \cap L$ then determines a fiber of the linear fibration, and on this fiber we get $w = x \circ x = y \circ y$, since $\mathcal{L}(w, x) \subset T_x(S)$ and $\mathcal{L}(w, y) \subset T_y(S)$. The result then follows from Proposition 5.6. □

Proposition 5.8. *Let S be a smooth cubic surface over a perfect field k. Let x, y be a good pair on S, and let C be a fiber of the linear fibration through x, y. Then:*

(a) *For any positive integer n, the set $C(\bar{k}) \cap \mathcal{Z}_n(t_x t_y)$ is finite (see Notation 2.3).*
(b) *If C is periodic of period n, then the set $C(\bar{k}) \cap \mathcal{Z}_\infty(t_x t_y)$ is finite, and this implies the existence of $\bar{k}$-periodic points outside of $\mathcal{Z}_\infty(t_x t_y)$.*

Proof. To make notations simpler, we identify all algebraic sets with their underlying set of $\bar{k}$-points. Denote $f = t_x t_y$, and let z be the third point in $\mathcal{L}(x, y) \cap S$. We prove the proposition by induction on n. For $n = 1$ we have $\mathcal{Z}_1(f) = \mathcal{Z}(f) = \{y, z\}$, so the assertion is true. Let $n > 1$, and assume that the statement is true for any $m < n$. For $n \geq 2$ we have $\mathcal{Z}_n(f) = \mathcal{Z}(f) \cup f^{-1}[\mathcal{Z}_{n-1}(f)]$, so that

$$C \cap \mathcal{Z}_n(f) = (C \cap \mathcal{Z}(f)) \cup (C \cap f^{-1}[\mathcal{Z}_{n-1}(f)]).$$

The first set in the union is finite; it remains to prove that $C \cap f^{-1}[\mathcal{Z}_{n-1}(f)]$ is finite. It is easy to see that $C \subset f^{-1}[C]$, so that

$$C \cap f^{-1}[\mathcal{Z}_{n-1}(f)] \subset C \cap f^{-1}[C \cap \mathcal{Z}_{n-1}(f)].$$

The set $C \cap \mathcal{Z}_{n-1}(f)$ is finite by the induction hypothesis, so

$$C \cap \mathcal{Z}_{n-1}(f) \subseteq \{x, y, z, A_1, \ldots, A_K\},$$

where $A_1, \ldots, A_K$ are points in $C(\bar{k}) \setminus \{x, y, z\}$. The inverse image

$$f^{-1}(\{y, A_1, \ldots, A_K\})$$

is finite (as can be checked readily from the definition of t_x and t_y), so it remains to show that $C \cap f^{-1}[\{x, z\}]$ is finite. Now $f^{-1}[\{z\}] = C_y$, which is an irreducible hyperplane section singular at y by Proposition 4.4, and therefore has no common components with C (the curve C is irreducible and cannot have a singularity at x, y, z by Proposition 4.4), so that their intersection is finite. Finally, $f^{-1}[\{x\}] = t_y^{-1}(C_x)$. As before $C \subset t_y^{-1}[C]$, so that

$$C \cap t_y^{-1}[C_x] \subset t_y^{-1}[C \cap C_x].$$

The set $C \cap C_x$ is finite, so $C \cap C_x \subseteq \{x, B_1, \ldots, B_M\}$, where $B_1, \ldots, B_M$ are points in $C(\bar{k}) \setminus \{x, y, z\}$ (The curve C_x does not contain y and z, since otherwise x is a double point of $\mathcal{L}(x, y) \cap S$, which is impossible, since x, y and z are distinct). The inverse image of $\{x, B_1, \ldots, B_M\}$ under t_y is finite. This proves (a).

To prove (b), we note that any point of C not in $\mathcal{Z}_n(t_x t_y)$ must be periodic of period n, and therefore cannot lie in $\mathcal{Z}_\infty(t_x t_y)$; but $C \cap \mathcal{Z}_n(t_x t_y)$ is finite by (a), so that $C \cap \mathcal{Z}_\infty(t_x t_y)$ is finite as well. □

6. Division polynomials associated with linear fibration

We have seen in Section 5 that finding periodic points of $t_x t_y$ for a good pair x, y on a smooth cubic surface S defined over a number field K, is equivalent to studying periodicity on the fibers of the linear fibration defined by the points x, y (Proposition 5.2). We have also seen that for a fiber to have periodic points of exact period n, the fiber itself must be periodic of period n, and this is equivalent to y being of order n in the group structure induced by choosing x as the unit element (Proposition 5.5). We want to find all the fibers of the linear fibration that are periodic of finite period. In order to do so we employ *division polynomials* of elliptic curves. We first recall the definition and basic properties of these polynomials.

Definition 6.1. Given an elliptic curve E in Weierstrass form

$$y^2 = x^3 + Ax + B,$$

we associate to it the *division polynomials* $\psi_n, n \geq 0$ in $\mathbb{Z}[x, y, A, B]$:

$$\begin{aligned}
\psi_0 &= 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2y, \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_m^3 + 1, \qquad \text{for } m \geq 2, \\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \qquad \text{for } m \geq 3.
\end{aligned}$$

Theorem 6.2. *Let E be an elliptic curve defined over a number field K. Then the division polynomials have the following properties ($E[n]$ is the set of points in $E(\bar{K})$ with order dividing n):*

(a) *$\psi_{2n+1}, y^{-1}\psi_{2n}$ are polynomials in $\mathbb{Z}[x, A, B]$.*
(b) *The roots of ψ_{2n+1} are the x-coordinates of the points in*

$$E[2n+1] \setminus \{\mathcal{O}\}.$$

(c) *The roots of $y^{-1}\psi_{2n}$ are the x-coordinates of the points in $E[2n] \setminus E[2]$.*

Proof. See Washington [27, Chapter 3, Section 2]. □

Remark 6.3. To make the notations easier, we replace ψ_n for even n with $y^{-1}\psi_n$.

Proposition 6.4. *Let S be a smooth cubic surface defined over a number field K, let $x, y \in S(K)$ be a good pair, and denote by $\pi : S \to \mathbb{P}^1$ the linear fibration associated with the good pair x, y. There exist polynomials $\gamma_n(t)$ in $K[t]$, for $n \geq 3$, whose roots in $\bar{K}$ lying outside a finite set $\mathcal{B} \subset \mathbb{P}^1$ correspond to fibers of π that are $t_x t_y$-periodic of period ≥ 3 and dividing n.*

Proof. We can ensure that the fiber at infinity is nonperiodic and nonsingular. Outside this fiber π induces a cubic pencil with parameter t, whose generic fiber is a smooth cubic curve C in the projective plane $\mathbb{P}^2$ over the function field $K(t)$. The points x, y induce two rational points (which we still denote by x, y) on the cubic curve C. We choose x to be the unit element of the cubic curve C, which induces an elliptic curve group structure on C. We note that it is impossible for y on C to be of finite order when x is chosen as unit element, since otherwise $t_x t_y$ is of finite order in $\mathrm{Bir}(X)$, contradicting Theorem 4.3.

We now use a Weierstrass transformation (see Shioda [22, Section 2]) to map our elliptic curve (C, x) to an isomorphic elliptic curve in Weierstrass form over $K(t)$

$$E : v^2 = u^3 + A(t)u + B(t).$$

We denote the Weierstrass transformation by $\omega : (C, x) \to (E, \mathcal{O})$. The point y is mapped to a rational point on E, and we still denote this point by y. We can ensure that the Weierstrass form E has coefficients in $\mathcal{O}_K[t]$: This is done by transforming E to a *minimal Weierstrass form* (cf. Silverman [25, Chapter VII, Section 1]), i.e., an isomorphic copy of E such that the valuation of A and B is nonnegative and minimal (in its isomorphism class) at all places of $K(t)$; then it is possible to get rid of the denominators so that all the coefficients of $A(t)$ and $B(t)$ are in $\mathcal{O}_K$.

There exists an open subset $U \subseteq \mathbb{P}^1$ such that for each $t \in U$, the specialization of the Weierstrass transformation ω to the fiber over a specific t will remain an isomorphism of irreducible cubic curves. We include the complement of U in $\mathcal{B}$.

We now have an infinite sequence of division polynomials $\psi_n \in \mathcal{O}_K[t][u]$, $n \geq 3$, of the elliptic curve $E/K(t)$. We evaluate these polynomials at the u-coordinate of the point y, and get an element $\tilde{\gamma}_n(t)$ in $K(t)$. The denominator of $\tilde{\gamma}_n$ depends only on $y \in E$; thus there are finitely many values of t at which $\tilde{\gamma}_n(t)$ might have poles, which we include in $\mathcal{B}$. We now define γ_n to be the numerator of $\tilde{\gamma}_n$, for $n \geq 3$.

It is clear that the fibers of π lying over the roots of $\gamma_n(t)$ not in $\mathcal{B}$, are fibers where y is of finite order $\neq 2$ and dividing n. Thus by Proposition 5.5 these fibers are periodic of period $\neq 2$ and dividing n. □

Corollary 6.5. *Let $S/K, x, y$ and π be as in Proposition 6.4. There exist polynomials $\Psi_n(t)$ in $K[t]$, for $n \geq 3$, whose roots in $\bar{K}$ correspond to all the fibers of π that are periodic under the birational map $t_x t_y$, of period $\neq 2$ and dividing n.*

Proof. We only need to check the order of y on the finite number of fibers over the points in $\mathcal{B}$. If a fiber over a point $a \in \mathcal{B}$ is nonperiodic, then we factor out a as a root from the polynomials $\gamma_n(t)$. If it is periodic, then we need to make sure it appears as a root of the polynomials $\gamma_n(t)$. It remains to prove that the resulting polynomials have coefficients in K. This is true because if we have a point a on whose corresponding fiber we have y of finite order n, then the order of y on the fibers over the conjugates of a will be the same, and therefore they will be roots of the same polynomials. □

Corollary 6.6. *Under the assumptions of the last corollary, the $\bar{K}$-periodic points of $t_x t_y$ are Zariski-dense in $S(\bar{K})$.*

Proof. By Corollary 6.5, there are infinitely many periodic fibers of $t_x t_y$ over $\bar{K}$ (the polynomials Ψ_p, Ψ_q have no common roots for distinct primes p and q). By Proposition 5.8, these fibers must contain $\bar{K}$-rational points lying outside of $\mathcal{Z}_\infty(t_x t_y)$. □

Definition 6.7. We call the polynomials $\Psi_n, n \geq 3$ in the last corollary the *division polynomials* of the smooth cubic surface S with respect to the good pair x, y (this definition is nonstandard). We now define the 1st and 2nd division polynomials:

(1) $\Psi_1(t)$ is defined to be the discriminant of Weierstrass form $E/K(t)$ from the proof of Proposition 6.4.
(2) $\Psi_2(t)$ is defined to be the numerator of the v coordinate of the point y on $E/K(t)$.

Proposition 6.8. *Let S be a smooth cubic surface defined over a number field K, and let $x, y \in S(K)$ be a good pair.*

(a) *The roots of Ψ_1 in $\bar{K}$ correspond to the fibers of π that contain fixed points of $t_x t_y$. This polynomial is of degree at most* 12.
(b) *The roots of Ψ_2 in $\bar{K}$ correspond to the fibers of π that are periodic of period* 2. *This polynomial is of degree at most* 3.

Proof. (a) The discriminant of a cubic curve in Weierstrass form is 0 if and only if the curve is singular. A point w on the surface S is fixed under $t_x t_y$ if and only if the fiber $C = \mathcal{P}(x, y, w) \cap S$ is singular, by Corollary 5.4. There are at most 12 fixed points of $t_x t_y$ on the surface S, by Corollary 5.4, which explains the degree.

(b) A point on an elliptic curve in Weierstrass form is of order 2 if and only if its v coordinate is 0. By Proposition 5.7 there are at most 3 curves of period 2. □

Notation 6.9. Let S be a smooth cubic surface defined over a number field K, let $x, y \in S(K)$ be a good pair and let Ψ_n be the division polynomials associated with x, y. For $n \geq 1$ define the polynomials

$$\Phi_n(t) = \Psi_n(t) \prod_{d|n, d>2} \Psi_d(t)^{-1}.$$

The roots of $\Phi_n(t), n \geq 2$, in $\bar{K}$ correspond to periodic fibers of π of *exact* period n.

Proposition 6.10. *Let S be a smooth cubic surface defined over a number field K and let $x, y \in S(K)$ be a good pair.*

(a) *For the case $K = \mathbb{Q}$, the polynomials $\Phi_n(t)$ do not have roots in $\mathbb{Q}$ for $n > 12$ or $n = 11$.*
(b) *For a general number field K there exists a positive integer N such that $\Phi_n(t)$ does not have roots in K for $n > N$. The bound N depends only on the degree of the extension $K/\mathbb{Q}$.*

Proof. (a) Mazur's torsion theorem [16, Theorem 8] lists the possible $\mathbb{Q}$-rational torsion subgroups of elliptic curves over $\mathbb{Q}$. The maximal order of an element of finite order is bounded by 12. If $\Phi_n(t)$ has a root in $\mathbb{Q}$ for $n > 12$, then the fiber over this root is an elliptic curve over $\mathbb{Q}$ with a rational point of order n, a contradiction.

(b) Merel's torsion theorem (see Merel [17, Corollary]), guarantees a bound on the order of the K-rational torsion subgroup that depends only on the degree of the field extension. An explicit bound on the order of the torsion subgroup can be found in Parent [19, Corollary 1.8] (this bound is exponential in the degree of the extension of $K/\mathbb{Q}$). $\square$

Corollary 6.11. *Let S be a smooth cubic surface defined over a number field K and let $x, y \in S(K)$ be a good pair. The set of all periodic points of $t_x t_y$ in $S(K)$ is contained in a finite number of fibers of π.*

Proof. All periodic points must be contained in the fibers of the linear fibration lying over the K-roots of the polynomials Ψ_n. Therefore, by Proposition 6.10, there are only finitely many fibers that can contain K-periodic points. $\square$

Theorem 6.12. *Under the assumptions of Proposition 6.10, for $K = \mathbb{Q}$ the birational automorphism $t_x t_y$ can only have $\mathbb{Q}$-periodic points of exact period $1, \ldots, 10, 12$. For a general number field K, the birational automorphism $t_x t_y$ can only have periodic points of exact period bounded by a number depending only on the degree of the extension $K/\mathbb{Q}$.*

The division polynomials of the linear fibration give us an effective method for "finding" all K-periodic points of a birational automorphism $t_x t_y$:

(1) First we find the K-roots of all division polynomials up to the bounds described in the proof of Proposition 6.10.
(2) For the nonsingular periodic fibers, we can then use algorithms to find the generators of the Mordell-Weil of the elliptic curve (cf. Cremona [8, Chapter 3, Section 5]).
(3) We can parametrize the periodic points on the singular periodic fibers.
(4) For each periodic fiber, we can find all the points in $\mathcal{Z}_\infty(t_x t_y)$ in a finite number of steps (see Proposition 5.8).

7. SRP on cubic surface

We are now ready to prove some results about strong residual periodicity of the AG dynamical system of type $D = (S, t_x t_y, F)$ on a smooth cubic surface S defined over a number field K, whose global dynamics were described in the previous two sections. We take the forbidden set F to be union of the Zariski-closure of the set of all periodic points in $X(K)$ and the set of K-rational points in $\mathcal{Z}_\infty(t_x t_y)$. In this section we prove two sufficient conditions for SRP, and then we prove that when put together, they are necessary and sufficient.

Proposition 7.1. *Let S be a smooth cubic surface defined over a number field K and let $x, y \in S(K)$ be a good pair. If there exists a fiber C, defined over K, of the linear fibration through the good pair $x, y \in S(K)$ such that the set of K-rational points $C(K)$ is finite, then $D = (S, \varphi = t_x t_y, F)$ is strongly residually periodic.*

Proof. The curve C must be smooth, since absolutely irreducible singular cubic curves with a rational point are rational, and therefore have infinitely many rational points. The point y must be of finite order in the group induced by choosing x as the unit element on C. All points in $C(K)$, outside of $\mathcal{Z}_\infty(t_x t_y)$, are $t_x t_y$-periodic with period equal to the order of y. Denote by N the order of y in $C(K)$. To prove the proposition we will show that for primes p for whom the cardinality of κ_p is large enough, there exists a point $w \in C_p(\kappa_p)$ that satisfies:

1. The point w is not a reduction of any periodic point in the Zariski-closure of the subset of periodic points in $S(K)$.
2. The point w is not a reduction of any point in $\mathcal{Z}_\infty(\varphi)$.
3. The point w is not in $\mathcal{Z}_\infty(\varphi_p)$ (in particular w is defined under φ_p^N, and is therefore a periodic point of period at most N).

We restrict ourselves to primes p where the system D has good reduction. In particular the elliptic curve $E = (C, x)$ is reduced to an elliptic curve $E_p = (C_p, x_p)$. We can then use Hasse's theorem on elliptic curves (see Silverman [25, Thm V.1.1]) to guarantee that the number of rational points in $C_p(\kappa_p)$ is as large as we desire. We can thus guarantee that for all but finitely many primes p there exists a point $w \in C_p(\kappa_p)$ such that w is not a reduction of any point in $C(K)$. The Zariski-closure of the subset of periodic points in $S(K)$ is contained in a finite number of fibers of the linear fibration through x, y, so that it is enough to choose p such that C_p intersects the reductions of the other fibers only at the points $\{x, y, z\} = \mathcal{L}(x, y) \cap S$ (this is true for any prime p such that κ_p is large enough). This proves (1).

We proved in Proposition 5.8 that the intersection of $C(\bar{K})$ with $\mathcal{Z}_\infty(\varphi)$ is finite. We use this and the same reasoning as in the previous paragraph to prove (2).

The set $\mathcal{Z}_\infty(\varphi_p)$ is the set of points whose orbit intersects $\mathcal{Z}(\varphi_p)$. Now, $\mathcal{Z}(\varphi_p) \subseteq \{y_p = \rho_p(y), z_p = \rho_p(z)\}$, so that any point $v \in C_p(\kappa_p)$ not in

$\mathcal{Z}(\varphi_p)$ that lies in $\mathcal{Z}_\infty(\varphi_p)$, satisfies $ny_p + v = y_p$ or $ny_p + v = z_p$, for some integer $1 \leq n \leq N$. Rewriting this, we get $v = (1-n)y_p$ or $v = z_p - ny_p$, for some integer $1 \leq n \leq N$. In other words, there are at most $2N$ points in $C_p(\kappa_p) \cap \mathcal{Z}_\infty(\varphi_p)$. The bound $2N$ is independent of the prime p, and therefore for primes p such that κ_p is large enough, we can find points in $C_p(\kappa_p)$ that are not in $\mathcal{Z}_\infty(\varphi_p)$, so that (3) is proved. □

Remark 7.2.

(i) The order of y on $C(K)$ is bounded by Theorem 6.12.
(ii) See Example 9.1 for a dynamical system satisfying the conditions of Proposition 7.1.

Proposition 7.3. *Let S be a smooth cubic surface defined over a number field K and let $x, y \in S(K)$ be a good pair. The minimal periods of the residual systems of $D = (S, \varphi = t_x t_y, \mathcal{F})$ are bounded (as in Definition* 3.6*) if and only if there exists a positive integer N such that the polynomial $\Theta_N(t) = \Phi_1(t) \cdots \Phi_N(t)$ (see Notation* 6.9*) has a root modulo all but finitely many primes p.*

Proof. Let $\pi : S \to \mathbb{P}^1$ be the linear fibration through the pair x, y. The polynomial Θ_N has roots modulo all but finitely many primes if and only if there exist either periodic fibers of π of period at most N or fixed points for all but finitely primes. The set of $\mathcal{Z}_\infty(\varphi_p)$ is bounded on periodic curves of period at most N by a bound depending only on N, as we have seen in the proof of Proposition 7.1. Thus for primes p such that κ_p is large enough, the fiber must contain points outside $\mathcal{Z}_\infty(\varphi_p)$. Therefore, the condition that there exist either periodic fibers of π of period at most N or fixed points for all but finitely many primes, is equivalent to the boundedness of the minimal periods of the residual systems D_p. □

Proposition 7.4. *Let S be a smooth cubic surface defined over a number field K, and let $x, y \in S(K)$ be a good pair. If there exists a positive integer N such that the polynomial $\Theta_N(t) = \Phi_1(t) \cdots \Phi_N(t)$ divided by all linear factors defined over K (i.e., all K-roots are removed), has no roots over K, and for all but finitely many primes p the polynomial $\Theta_N(t)$ has a root modulo p, then $D = (S, \varphi = t_x t_y, F)$ is strongly residually periodic.*

Proof. By Proposition 7.3, we know that the minimal residual periods are bounded by N for all but finitely many primes. We need to check that our points of minimal period modulo p are not all reductions of points from the forbidden set.

First we check reductions of K-periodic points. We know that the minimal period for all but finitely many primes is at most N, and any periodic point over K must either be of larger period than N, or belong to a fiber corresponding to a K-root of $\Theta_N(t)$. Let C be a K-periodic fiber of period $m > N$, then y is of order m on C. For all but finitely many primes, the reduction of the point y modulo p will have the same order $m > N$ on the reduced fiber (cf. Silverman [25, Proposition VII.3.1]). Therefore the reduction of such a fiber cannot give us points of period at most N (by Proposition 5.5). Now suppose we have a fiber C of the linear fibration that corresponds to a root $a \in K$ of $\Theta_N(t)$. Denote by $\tilde{\Theta}_N(t) \in K[t]$ the polynomial obtained from $\Theta_N(t)$ after dividing by all linear factors defined over K. Then a is not a root of $\tilde{\Theta}_N(t)$. Fu rther, $\rho_p(a)$ can only be a root of $\tilde{\Theta}_N(t)$ modulo p for a finite number of primes p. Therefore the fiber C_p can only agree with the fibers lying over the roots of $\tilde{\Theta}_N(t)$ modulo p for finitely many primes p. Thus, periodic points obtained from roots of $\tilde{\Theta}_N(t)$ will not be reductions modulo p of points from the fiber C.

Finally, we check the reduction of points in $\mathcal{Z}_\infty(\varphi)$: Given a κ_p periodic fiber of period at most N, it can contain only a bounded amount of periodic points whose orbit goes through $\mathcal{Z}(\varphi_p)$. The bound for this type of points does not depend on p but only on N. Therefore, for primes p such that κ_p is large enough, there will be κ_p-periodic points on the fiber that are not reductions of points from $\mathcal{Z}_\infty(\varphi)$ (the orbit of the reduction of such a point must go through $\mathcal{Z}(\varphi_p)$). □

Corollary 7.5. *Let S be a smooth cubic surface defined over a number field K and let $x, y \in S(K)$ be a good pair. If there exists a number N such that the polynomial $\Theta_N(t) = \Phi_1(t) \cdots \Phi_N(t)$ has no roots over K, and for all but finitely many primes p the polynomial $\Theta_N(t)$ has a root modulo p, then $D = (S, \varphi = t_x t_y, F)$ is strongly residually periodic.*

Theorem 7.6. *Let S be a smooth cubic surface defined over a number field K and let $x, y \in S(K)$ be a good pair. The system $D = (X, \varphi = t_x t_y, F)$ is strongly residually periodic if and only if one of the following is true:*

(a) *There exists a K-fiber in the linear fibration through x, y with finitely many rational points.*
(b) *There exists a positive integer N such that $\Theta_N = \Phi_1 \cdots \Phi_N$ divided by all linear factors over K, has roots modulo all but finitely many primes p.*

Proof. The if part is true by Propositions 7.1 and 7.4. If D is strongly residually periodic, then the periods are bounded, and this means there exists a positive integer N such that Θ_N has roots modulo all but finitely many primes (by Proposition 7.3). If we divide Θ_N by all the linear factors over K, and we have roots modulo all but finitely many primes, then the second condition is satisfied. Otherwise strong residual periodicity must be explained by a fiber that is defined over K, but if such a fiber has infinitely many periodic points, then the entire fiber is in the forbidden set — therefore if the second condition is not met the first condition must be true. □

8. Finite generation of a subset of rational points on a smooth cubic surface

In this section we recall the Mordell–Weil problem for cubic surfaces, and prove a dynamical theorem in a Mordell–Weil flavor, using results we obtained in the previous sections.

Let S be a smooth cubic surface defined over a field k. Given a subset of points $\mathcal{S}_0 \subseteq S(k)$ we can define recursively an increasing sequence of sets

$$\mathcal{S}_0 \subseteq \mathcal{S}_1 \subseteq \mathcal{S}_2 \subseteq \cdots , \tag{2}$$

where $\mathcal{S}_{i+1}$ is defined by adding to $\mathcal{S}_i$ all the points of the form $w \circ z \in S(k)$ obtained by taking any two distinct points $w, z \in \mathcal{S}_i$. This is called *drawing secants* through the points in $\mathcal{S}_i$. We can modify this sequence by also including in $\mathcal{S}_{i+1}$ all the points $w \in S(k)$ such that $w \in C_x(k)$ (recall that $C_x = T_x(S) \cap S$) for some $x \in \mathcal{S}_i$. This is called *drawing tangents* through the points in $\mathcal{S}_i$. The *span* of $\mathcal{S}_0$ (denoted by $\mathrm{Span}(\mathcal{S}_0)$) by tangents and secants (or only secants) is defined as the union of all the sets in the sequence in (2).

Question 8.1 (The Mordell–Weil problem for cubic surfaces)**.** Given a smooth cubic surface S over a field k such that $S(k) \neq \emptyset$, does there exist a finite subset $\mathcal{S} \subset \mathcal{S}(k)$ such that $\mathrm{Span}(\mathcal{S}) = S(k)$? If so, then we say $S(k)$ is *finitely generated*.

The Mordell–Weil problem for cubic surfaces is still open, and partial results can be found in Manin [15] and Siksek [23]. Of course, the answer to the question may very well depend on whether we allow tangents or not, and in fact Manin considers an alternative composition rule in the above-mentioned article.

We proceed to prove a Mordell–Weil like theorem for the set of K-periodic points of $t_x t_y$ where K is a number field. In order to obtain "true" finite generation, we restrict ourselves to taking tangents only inside the nonsingular fibers of the linear fibration associated to x and y.

Theorem 8.2. *Let K be a number field, S/K a smooth cubic surface and $x, y \in S(K)$ a good pair. If there do not exist singular fibers in the linear fibration through x, y that are periodic of finite period, then the set of K-periodic points of the birational automorphism $t_x t_y$ is finitely generated by secants and tangents.*

Proof. By Corollary 6.11, there are only finitely many fibers of the linear fibration containing all periodic points. There are two types of such fibers: the first is a singular fiber containing only one singular point, which is fixed under $t_x t_y$ (the rest of the points on the fiber are nonperiodic due to the assumption in the theorem). The second is a smooth fiber that is periodic. The first type is surely finitely generated, and the second is finitely generated by the Mordell–Weil theorem for elliptic curves (see Silverman [25, Chapter

VIII]). Thus we can choose a finite number of generators on each periodic fiber, take the union with all the singular points on the singular fibers, and we are done. □

Corollary 8.3. *If $K = \mathbb{Q}$ in Theorem 8.2, and the resultants* $\mathrm{Res}(\Psi_1, \Psi_n) \neq 0$ *for $n = 2, 3, 4, 6$, then the set of $\mathbb{Q}$-periodic points of $t_x t_y$ is finitely generated.*

Proof. The condition $\mathrm{Res}(\Psi_1, \Psi_n) \neq 0$ means there are no fibers that are both singular and of period n (by Proposition 6.8). If a singular fiber C of the linear fibration is periodic, then y is of finite order in the group (C_{ns}, x). Singular cubics over $\mathbb{Q}$ have group structure on C_{ns} isomorphic to either $\mathbb{Q}^+$ or a subgroup of L^*, where L is a quadratic extension of $\mathbb{Q}$ (see Silverman [25, Exercise III.3.5]). In either case there are no nontrivial torsion elements of an order not in $\{2, 3, 4, 6\}$. □

Remark 8.4. We show in Example 9.4 that there exist dynamical systems on smooth cubic surfaces where $\mathrm{Res}(\Psi_1, \Psi_2) = 0$. Of course, this does not mean that the consequence of the corollary is untrue for such examples (i.e., the set of periodic points might still be finitely generated).

9. Examples

In this section we present some examples, illustrating the ideas and theorems presented in the paper. Finding the division polynomials associated with a good pair x, y is unreasonable without the use of a computer. We have implemented the necessary MAGMA [5] functions to calculate the division polynomials associated with the birational map $t_x t_y$. The code package also contains functions that check the minimal residual periods of $t_x t_y$ for primes up to a given bound (this can provide an indication as to whether a given example is SRP or not). The code can be downloaded at the author's website `http://www.wishcow.com`. The results of our package can be verified using the MAGMA code package provided by Brown and Ryder [6], which can generate Geiser involutions for a smooth cubic surface. We start with an example of a strongly residually periodic dynamical system on a smooth cubic surface:

Example 9.1. Let $S/\mathbb{Q}$ be the smooth cubic surface defined by the equation

$$S : YW^2 + Y^2Z - X^3 - 4Z^3 = 0. \tag{3}$$

The points $x = [0 : 1 : 0 : 0], y = [0 : -2 : 1 : 0]$ are a good pair on S. We denote by φ the birational automorphism $t_x t_y$ on S. The forbidden set is defined as in Section 7. We will show that the dynamical system $D = (S/\mathbb{Q}, \varphi, F)$ is $SRP(3)$, i.e., there exists a number M such that for any prime $p > M$, the dynamical system has periodic points of period 3 modulo p.

Intersecting the hyperplane $\{W = 0\}$ with S gives the cubic curve $C : Y^2Z - X^3 - 4Z^3$, which is a smooth cubic. This hyperplane goes through the points x and y, and therefore the curve C is invariant under the map $t_x t_y$ (see Proposition 5.1). Choosing the identity of the elliptic group structure to be $x = [0 : 1 : 0]$ (or more accurately, the point induced by x), we get an elliptic curve with Weierstrass form $v^2 = u^3 + 4$. Consulting the Cremona database of elliptic curves [9], we see that $E = (C, x)$ is an elliptic curve with Mordell–Weil rank 0, and the torsion subgroup is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. The three rational points are $x = [0 : 1 : 0], y = [0 : -2 : 1]$ and $z = [0 : 2 : 1]$. Since the group is $\mathbb{Z}/3\mathbb{Z}$, the point y is of order 3 on the elliptic curve. We have already seen (Proposition 5.5) that the order of y is the same as the order of $t_x t_y$ in the group $\mathrm{Bir}(E)$. Thus we get that even though $t_x t_y$ is of infinite order in $\mathrm{Bir}(S)$, it is of finite order 3 when restricted to the hyperplane section. By Proposition 7.1 we get that the dynamical system D is SRP(3).

Let us describe a method for constructing examples with desired dynamical properties (e.g., SRP). We choose an elliptic curve $E : v^2 = u^3 + Au + B$ with particular properties, for instance with a finite number of rational points as was done in Example 9.1. We then choose two points $x, y \in E(K)$ to play the roles of the points x, y on the surface S, and search for a smooth surface S containing this curve. We can do this by running over surfaces of the form

$$S : W \cdot H(X, Y, Z, W) - Y^2 Z - X^3 - AXZ^2 - BZ^3 = 0$$

where H is a quadratic form, and searching for ones that are smooth and in which x, y is a good pair. Then this surface will have $C = \{W = 0\} \cap S$ as a fiber in the linear fibration induced by x, y, and this fiber C is exactly our curve E.

Example 9.2. We continue Example 9.1, by proving that the dynamical system D has no periodic points over $\mathbb{Q}$. We use this example to illustrate the method of using the division polynomials of the linear fibration induced by the good pair x, y. To find the cubic pencil of the linear fibration of S induced by x, y, we set $W = tX$ in equation (3). This is because the line passing through x, y is $\mathcal{L}(x, y) = \{W = 0, X = 0\}$. We get the cubic pencil $C : t^2 X^2 Y + Y^2 Z - X^3 - 4Z^3 = 0$.

The fiber at infinity that we have removed is $X = 0$, which is the curve $C_\infty : YW^2 + Y^2 Z - 4Z^3 = 0$. We bring this curve to Weierstrass form and get $E_\infty : v^2 = u^3 - 4u$. This curve can be checked in the Cremona database [9] to have Mordell–Weil rank 0, and torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. All four rational points on C_∞ can be checked to be in $\mathcal{Z}_\infty(t_x t_y)$ (and therefore are not periodic and are in the forbidden set). The point y has order 2 in the group $E_\infty(\mathbb{Q})$, so that by Proposition 7.1 the dynamical system D is in fact $SRP(2)$.

We can check that the Weierstrass form of the cubic pencil C is $E : v^2 = u^3 - 4t^4 u + 4$. The discriminant of E is $\Delta(t) = 4096t^{12} - 6912$. The zeros of the discriminant, as a polynomial in t, give us 12 distinct singular fibers of the linear fibration, all of which are nodal cubics (the coefficient of u is nonzero at all roots of $\Delta(t)$, see Silverman [25, Proposition III.1.4]). None of the roots of $\Delta(t)$ are rational, so there are no fixed points of $t_x t_y$ defined over $\mathbb{Q}$ (See Corollary 5.4).

The dynamical system is $SRP(1)$ only if the polynomial Δ has roots modulo all but finitely many primes p. We show this is not true. We can check using MAGMA [5] that the Galois group of the polynomial Δ has an element of order 12. Then by the Frobenius density theorem (see Lenstra and Stevenhagen [26, page 32]), there are infinitely many primes p for which the polynomial Δ remains irreducible when reduced modulo p, so that residual periodicity cannot be explained by the fixed points.

To get a fiber of the linear fibration that is periodic of period 2, we need the v coordinate of the point y to be 0 when evaluated at t. However, the image of y in E is $[0:2:1]$, so we get that outside of the fiber at ∞ there are no fibers of period 2.

We can calculate the division polynomials $\Psi_n, n \geq 3$ for $t_x t_y$. To find them we take the division polynomials ψ_n for E, and evaluate them at $v = 0$, since $y = [0:2:1]$. We only need the polynomials $\Psi_n(t)$ for $n \leq 12, n \neq 11$ (See Proposition 6.10 for why we can skip Ψ_{11}, and stop at Ψ_{12}). The polynomials are quite large so we do not list them here. A quick check shows that none of these polynomials have roots in $\mathbb{Q}$ outside of $t = 0$, which is the fiber of period 3. This means that there are no fibers of finite period $n \geq 3$. As we have checked all possibilities, we have proved that $t_x t_y$ has no periodic points over $\mathbb{Q}$.

Example 9.3. We show an example of a dynamical system on a smooth cubic surface that has infinitely many periodic points. Let $S/\mathbb{Q}$ be the smooth cubic surface defined by the equation

$$S : X^3 - 3024XZ^2 - Y^2Z - YW^2 + 81216Z^3 = 0. \tag{4}$$

The points $x = [0, 1, 0, 0], y = [12, 216, 1, 0]$ form a good pair on S. The hyperplane section $C = \{W = 0\} \cap S$ is a fiber of the linear fibration induced by x, y. This cubic curve has the Weierstrass form $E : v^2 = u^3 - 3024u + 81216$. This curve can be checked in the Cremona database [9] to have Mordell–Weil rank 1, and $y = (12, 216)$ has order 3 in the elliptic curve E. This means that the fiber C is periodic of period 3 under $t_x t_y$, which proves there are infinitely many $\mathbb{Q}$-periodic points for $t_x t_y$ on S.

Example 9.4. We show an example of a dynamical system on a smooth cubic surface with a singular fiber in the linear fibration containing infinitely many periodic points. This example demonstrates that the condition in Theorem 8.2 is not redundant (in the sense that such systems exist, not that the condition is necessary). Let $S/\mathbb{Q}$ be the smooth cubic surface defined by the equation

$$S : X^3 + X^2Z - XYW - Y^2Z - Z^2W - W^3 = 0. \tag{5}$$

The points $x = [0,1,0,0], y = [-1,0,1,0]$ form a good pair on S. The hyperplane section $C = \{W = 0\} \cap S$ is a fiber of the linear fibration induced by x, y. This cubic curve has the Weierstrass form $E : v^2 = u^3 + u^2$, which is the classic nodal cubic. The point $y = (-1,0)$ on E is the unique point of order 2 of this curve. This means that S has a singular curve of period 2 under $t_x t_y$.

References

[1] Amerik, Ekaterina. Existence of non-preperiodic algebraic points for a rational self-map of infinite order. *Math. Res. Lett.* **18** (2011), no. 2, 251–256. MR2784670 (2012e:37182), Zbl 1241.14011, arXiv:1007.1635, doi: 10.4310/MRL.2011.v18.n2.a5.

[2] Bandman, Tatiana; Grunewald, Fritz; Kunyavskiĭ, Boris. Geometry and arithmetic of verbal dynamical systems on simple groups. *Groups Geom. Dyn.* **4** (2010), no. 4, 607–655. MR2727656 (2011k:14020), Zbl 1276.14037, arXiv:0809.0369, doi: 10.4171/GGD/98.

[3] Beltrametti, Mauro C.; Carletti, Ettore; Gallarati, Dionisio; Monti Bragadin, Giacomo. Lectures on curves, surfaces and projective varieties. A classical view of algebraic geometry. Translated from the 2003 Italian original by Francis Sullivan. EMS Textbooks in Mathematics. *European Mathematical Society (EMS), Zürich*, 2009. MR2549804 (2010k:14001), Zbl 1180.14001, doi: 10.4171/064.

[4] Blanc, Jèrèmy; Cantat, Serge. Dynamical degrees of birational transformations of projective surfaces. Preprint, 2013. arXiv:1307.0361.

[5] Bosma, Wieb; Cannon, John; Playoust, Catherine. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265. MR1484478, Zbl 0898.68039, doi: 10.1006/jsco.1996.0125.

[6] Brown, Gavin; Ryder, Daniel. Elliptic fibrations on cubic surfaces. *J. Pure Appl. Algebra* **214** (2010), no. 4, 410–421. MR2558749 (2011a:14023), Zbl 1197.14045, arXiv:0807.0696, doi: 10.1016/j.jpaa.2009.06.014.

[7] Corti, Alessio; Pukhlikov, Aleksandr; Reid, Miles. Fano 3-fold hypersurfaces. *Explicit birational geometry of* 3*-folds*, 175–258. London Math. Soc. Lecture Note Ser., 281. *Cambridge Univ. Press, Cambridge*, 2000. MR1798983 (2001k:14034), Zbl 0960.14020, doi: 10.1017/CBO9780511758942.006.

[8] Cremona, J. E. Algorithms for modular elliptic curves. Second edition. *Cambridge University Press, Cambridge*, 1997. vi+376 pp. ISBN: 0-521-59820-6 MR1628193 (99e:11068), Zbl 0872.14041.

[9] Cremona, John. The elliptic curve database for conductors to 130000. *Algorithmic number theory*, 11–29. Lecture Notes in Comput. Sci., 4076, *Springer, Berlin*, 2006. MR2282912 (2007k:11087), Zbl 1143.11324, doi: 10.1007/11792086_2.

[10] Diller, Jeffrey. Dynamics of birational maps of $\mathbf{P}^2$. *Indiana Univ. Math. J.* **45** (1996), no. 3, 721–772. MR1422105 (97k:32044), Zbl 0874.58022, doi: 10.1512/iumj.1996.45.1331.

[11] Hindry, Marc; Silverman, Joseph H. Diophantine geometry. An introduction. Graduate Texts in Mathematics, 201. *Springer-Verlag, New York*, 2000. xiv+558 pp. ISBN: 0-387-98975-7; 0-387-98981-1. MR1745599 (2001e:11058), Zbl 0948.11023.

[12] Hutz, Benjamin. Good reduction of periodic points on projective varieties. *Illinois J. Math.* **53** (2009), no. 4, 1109–1126. MR2741181 (2012e:37184), Zbl 1226.37060.

[13] Hutz, Benjamin. Determination of all rational preperiodic points for morphisms of $\mathbb{P}^N$. Preprint, 2012. arXiv:1210.6246.

[14] Manin, Yu. I. Cubic forms. Algebra, geometry, arithmetic. Translated from the Russian by M. Hazewinkel. Second edition. North–Holland Mathematical Library,

4. *North-Holland Publishing Co., Amsterdam*, 1986. x+326 pp. ISBN: 0-444-87823-8 MR833513 (87d:11037), Zbl 0582.14010.

[15] Manin, Yu. I. Mordell–Weil problem for cubic surfaces. *Advances in mathematical sciences: CRM's 25 years (Montreal, PQ, 1994)*, 313–318, CRM Proc. Lecture Notes, 11. *Amer. Math. Soc., Providence, RI*, 1997. MR1479681 (99a:14029), Zbl 1053.14508, arXiv:alg-geom/9407009.

[16] Mazur, B. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186 (1978). MR488287 (80c:14015), Zbl 0394.14008.

[17] Merel, Loïc. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124** (1996), no. 1-3, 437–449. MR1369424 (96i:11057), Zbl 0936.11037, doi: 10.1007/s002220050059.

[18] Miranda, Rick. Persson's list of singular fibers for a rational elliptic surface. *Math. Z.* **205** (1990), no. 2, 191–211. MR1076128 (92a:14035), Zbl 0722.14022, doi: 10.1007/BF02571235,

[19] Parent, Pierre. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.* **506** (1999), 85–116. MR1665681 (99k:11080), Zbl 0919.11040, arXiv:alg-geom/9611022, doi: 10.1515/crll.1999.506.85.

[20] Reid, Miles. Undergraduate algebraic geometry. London Mathematical Society Student Texts, 12. *Cambridge University Press, Cambridge*, 1988. viii+129 pp. ISBN: 0-521-35559-1; 0-521-35662-8. MR982494 (90a:14001), Zbl 0701.14001, doi: 10.1017/CBO9781139163699.

[21] Shafarevich, Igor R. Basic algebraic geometry. 1. Varieties in projective space. Second edition. Translated from the 1988 Russian edition and with notes by Miles Reid. *Springer-Verlag, Berlin*, 1994. xiv+269 pp. ISBN: 3-540-57554-5. MR1328833 (95m:14001), Zbl 0797.14001.

[22] Shioda, Tetsuji. Weierstrass transformations and cubic surfaces. *Comment. Math. Univ. St. Paul.* **44** (1995), no. 1, 109–128. MR1336422 (96h:14046), Zbl 0861.14025.

[23] Siksek, Samir. On the number of Mordell–Weil generators for cubic surfaces. *J. Number Theory* **132** (2012), no. 11, 2610–2629. MR2954995, Zbl 1253.14023, arXiv:1012.1838, doi: 10.1016/j.jnt.2012.05.020.

[24] Silverman, Joseph H. Variation of periods modulo p in arithmetic dynamics. *New York J. Math.* **14** (2008), 601–616. MR2448661 (2009h:11100), Zbl 1153.11028, arXiv:0707.1505, `http://nyjm.albany.edu/j/2008/14-27.pdf`.

[25] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. MR2514094 (2010i:11005), Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6.

[26] Stevenhagen, P.; Lenstra, H. W., Jr. Chebotarëv and his density theorem. *Math. Intelligencer* **18** (1996), no. 2, 26–37. MR1395088 (97e:11144), Zbl 0885.11005, doi: 10.1007/BF03027290.

[27] Washington, Lawrence C. Elliptic curves. Number theory and cryptography. Second edition. Discrete Mathematics and its Applications (Boca Raton), *Chapman & Hall/CRC, Boca Raton, FL*, 2008. xviii+513 pp. ISBN: 978-1-4200-7146-7; 1-4200-7146-7. MR2404461 (2009b:11101), Zbl 1200.11043.

Department of Mathematics, Ben-Gurion University of the Negev, P.O.B. 653 Beer-Sheva 8410501 Israel
`wishcow@gmail.com`

This paper is available via `http://nyjm.albany.edu/j/2014/20-1.html`.