THE HILBERT PROPERTY FOR INTEGRAL POINTS OF AFFINE SMOOTH CUBIC SURFACES

SIMONE COCCIA

Abstract. In this paper we prove that the set of S-integral points of the smooth cubic surfaces in \mathbb{A}^3 over a number field k is not thin, for suitable k and S. As a corollary, we obtain results on the complement in \mathbb{P}^2 of a smooth cubic curve, improving on Beukers' proof that the S-integral points are Zariski dense, for suitable S and k. With our method we reprove Zariski density, but our result is more powerful since it is a stronger form of Zariski density. We moreover prove that the rational integer points on the Fermat cubic surface $x^3 + y^3 + z^3 = 1$ form a non-thin set and we link our methods to previous results of Lehmer, Miller-Woollett and Mordell.

1. INTRODUCTION

In order to state our results, we recall the basic terminology and theorems about thin sets of rational points. Our main references are [3], [5], [7], [13], [16], [21], [23], [24].

In this paper we assume that algebraic varieties are integral over k and quasi-projective, where k is a number field. By *cover* of algebraic varieties $\pi : Y \to X$ we shall mean a *dominant rational map of finite degree* with Y irreducible.

Definition 1.1. Let X be an irreducible k-algebraic variety of dimension n and let $\Omega \subseteq X(k)$. We say that Ω is a *thin* subset of X(k) if there are finitely many irreducible k-covers $\pi_i \colon Y_i \to X$ with π_i of degree ≥ 2 , such that $\Omega \subseteq \bigcup \pi_i(Y_i(k))$.

One can easily prove that if a set of rational points lies in a proper closed subvariety, then it is thin, so that being non-thin is a stronger version of Zariski-density.

Definition 1.2. We say that an algebraic variety X over k has the *Hilbert property* (HP) if X(k) is not thin.

It is easy to see that the Hilbert property is a birational invariant. The classical Hilbert irreducibility theorem can be formulated in this language as the following:

Theorem 1.3. The projective line \mathbb{P}^1_k over a number field k has the Hilbert property.

From this result one can deduce that all projective spaces (and so all rational varieties) have the HP.

The main inspiration for this work comes from the recent paper [9] of Corvaja and Zannier, where they unveil a relation between the HP and the topology of algebraic varieties, more specifically the ramification of its covers. They prove that for a variety X to have the HP, it is necessary that its non-trivial covers ramify somewhere, i.e. that X is algebraically simply connected. This is a consequence of the Chevalley-Weil theorem, which to the contrary predicts the lifting of all rational points in presence of an unramified cover: the Hilbert property is then an "opposite" of the Chevalley-Weil theorem. Building on this analogy Corvaja and Zannier asked the following:

Problem 1.4 ([9]). Does every smooth projective algebraically simply connected variety over a number field k with a Zariski dense set of rational points have the HP over k?

See also §3.8 of [7] for more discussions about the problem. In order to understand the power of an affirmative answer, let us say that in the special case of unirational varieties it would imply a positive solution to the Inverse Galois Problem. Moreover, Corvaja and Zannier gave the first example of non (uni)-rational variety with the HP:

Theorem 1.5 ([9]). The K3 surface defined in \mathbb{P}^3 by

$$x^4 + y^4 = z^4 + w^4$$

is not (uni)rational over \mathbb{C} and has the Hilbert property over \mathbb{Q} .

In the recent preprint [10] J. L. Demeio provided further examples of varieties with the HP, such as K3 surfaces or quotients of varieties under the action of a finite group. Corvaja and Zannier formulated analogous definitions and conjectures for the integer case, which are the object of this paper.

Definition 1.6. We say that an algebraic variety X/k has the *S*-integral Hilbert property (IHP) if $X(\mathcal{O}_S)$ is not thin.

Equivalently, X has the IHP if given finitely many k-covers $\pi_i \colon Y_i \to X$, each without rational sections defined over \bar{k} , the set $X(\mathcal{O}_S) \setminus \bigcup \pi_i(Y_i(k))$ is Zariski-dense.¹

Remark 1.7. One typical assumption is that the covers are given by finite maps $\pi: Y \to X$ where Y is a normal absolutely irreducible variety. In fact, consider a cover $\pi: Y \to X$ where Y is an absolutely irreducible variety. By removing a closed set, we can assume that π is a dominant morphism. We can mutually decompose Y and X in affine open sets such that π restricts to $\pi: V \to U$. The map π is still a dominant morphism and so it defines an inclusion $\pi^*: k[U] \hookrightarrow k[V] \subset k(V) = k(Y)$. Taking the integral closure A of $\pi^*(k[U])$ in k(Y) one obtains a normal absolutely irreducible affine variety $\tilde{V} = \text{Spec}(A)$ equipped with a finite morphism $\tilde{\pi}: \tilde{V} \to U$ and a birational isomorphism $f: V \dashrightarrow \tilde{V}$ such that $\pi = \tilde{\pi} \circ f$. Gluing these affine spectra we obtain the desired finite map, which differs from π only on a closed set, thus proving that this reduction is possible.

The original version of Hilbert's Irreducibility theorem then becomes:

Theorem 1.8. The affine line \mathbb{A}^1 has the IHP over \mathbb{Z} .

The natural analogue of Problem 1.4 is then:

Problem 1.9. Any smooth quasi-projective variety topologically simply connected and with a Zariski-dense set of S-integral points has the IHP.

In order to ask a similar question for non-simply connected varieties, one is led to the following definition.

Definition 1.10 (Weak integral Hilbert property). A normal quasi-projective algebraic variety X/k has the *weak integral Hilbert property* (WIHP) if, given finitely many covers $\pi_i: Y_i \to X$ each ramified above a non-empty divisor, the set $X(\mathcal{O}_S) \setminus \bigcup \pi_i(Y_i(k))$ is Zariski dense.

Problem 1.11. If a normal quasi-projective algebraic variety has a Zariski dense set of S-integral points then it has the WIHP.

Remark 1.12. Clearly for simply connected varieties the IHP is equivalent to the WIHP.

Remark 1.13. It could be possible that we should allow an enlargement of k and S to have a positive solution to the problems, as in our result on smooth cubic surfaces. However in the special case of the Fermat cubic surface we will prove the IHP over \mathbb{Z} .

Let us analyze these problems in the case of curves, as a basic example. For \mathbb{A}^1 it is exactly the statement of Theorem 1.8. An interesting example showing the difference between the two is \mathbb{G}_m , which is not topologically simply connected, since $\pi_1(\mathbb{G}_m) = \pi_1(\mathbb{C}^*) = \mathbb{Z}$. In fact \mathbb{G}_m is not an instance of Problem 1.9, as one can see applying the Chevalley-Weil theorem to the unramified morphism $x \mapsto x^n$ from \mathbb{G}_m to \mathbb{G}_m . However it is a positive example for Problem 1.11, since a ramified cover of \mathbb{G}_m has always finitely many *S*-integral points. This is a consequence of Siegel's theorem. For any other curve

¹ It is immaterial to require that the points are lifted to integral ones, because there is always a finite map which differs from the cover for a closed set, and by Proposition 2.3 pre-images through finite maps of S-integral points are S'-integral for an enlargement S' of S.

Siegel's theorem provides a complete solution, since the S-integral points are finite and so the IHP cannot hold.

We finally state the first result of this paper, which is an instance of Problem 1.9 (in its potential version).

Theorem 1.14. Let $\widetilde{F} \subset \mathbb{P}^3$ be a smooth cubic surface defined over a number field k and let H be a smooth hyperplane section of \widetilde{F} (which is a planar cubic curve contained in \widetilde{F}). We define $F \coloneqq \widetilde{F} \setminus H$. Then there exists an extension K of k and a finite set of places S of K such that $F(\mathcal{O}_S)$ is Zariski-dense and F has the IHP for the S-integral points.

It will be proven in the next section, following the method of Corvaja and Zannier of the two elliptic fibrations, which in our case are substituted with conic fibrations. This is a potential result since it could be possible that $F(\mathcal{O}_S)$ is Zariski-dense for smaller Kand S, but we could have to take a finite extension of the field and enlarge S to ensure that it is non-thin. However the Fermat cubic surface, i.e. the surface in \mathbb{A}^3 defined by

(1)
$$x^3 + y^3 + z^3 = 1$$

will provide a non-trivial instance of a surface satisfying the statement of Problem 1.9 in its full form. This is the content of the following

Theorem 1.15. The rational integer points on the Fermat cubic surface form a non thin set.

The study of the diophantine equation (1) dates back to Euler, who proved the rationality of the Fermat cubic surface (see section 13.7 of [14]). The interest for this equation was renewed in the fifties by Mordell ([20]) who analyzed more general cubic equations, such as

$$x^3 + y^3 + z^3 = k$$

At Mordell's suggestion, Millet and Woollett ([18]) found all solutions for $0 \le k \le 100$ and $|z| \le |y| \le |x| \le 3164$ with the help of the electronic computer EDSAC at the Cambridge University Mathematical Laboratory. In the case of the Fermat cubic surface they found 21 non-trivial solutions, i.e. satisfying $(x + y)(y + z)(z + x) \ne 0$, of which 8 are given by the parametric solution

(2)
$$x = 9t^4, \quad y = -9t^4 + 3t, \quad z = -9t^3 + 1$$

where t is an integer. It followed another paper of Mordell ([19]) where he proved the infinitude of integer solutions of

$$ax^3 + ay^3 + bz^3 = bc^3$$

and observed that four of the solution of Miller-Woollett satisfied

$$z - 1 = -7(x + y)$$

suggesting that these could be found by the method of his paper. Finally in [17] Lehmer exhibited an infinite sequence of parametric solutions of which (2) is the first. All these solutions satisfy the relation

$$1 - z = 3t^2(x + y)$$

where t is an integer. He pushed forward the observation of Mordell, noticing that the table contains 9 solutions of the form

$$\alpha(x+y) = 1-z$$

where α is an integer. With our method we are able to find three families of rational curves with infinitely many integral points. As we will see later, equation (3) corresponds to one of these families, so that our method subsumes the one of Lehmer and Mordell. It is interesting to note that their method to produce parametric solutions is based on the theory of Pell's equations, as ours, tough implicitly. In fact Theorem 3.2 is just a generalization to rational curves of the infinitude of integral solutions of the Pell's equations.

In the last section we are going to prove the WIHP for the complement in \mathbb{P}^2 of a smooth cubic, which will be a consequence of Theorem 1.14. The Zariski density of the

S-integral points was already proved by Beukers in [2] by constructing a family of conics with infinitely many S-integral points. However they form a thin set for a cover ramified outside the cubic, so that our result is stronger.

Acknowledgements. My deepest thanks go to my advisor Prof. Pietro Corvaja, for having suggested me this topic as my Tesi di laurea and having guided me with endless support through the literature and the pitfalls in which I ended up. I would also like to thank Julian Demeio and Prof. Francesco Zucconi for helpful discussions and for the interest shown in this work.

2. Some results on integral points

Here we briefly recall the basic definitions and results on integral points on varieties. Our main reference is [5].

Let v be a finite place of a number field k and \mathcal{O}_v be the valuation ring at v, i.e. $\mathcal{O}_v = \{x \in k \colon |x|_v \leq 1\}$. We denote by $\mathfrak{m}_v = \{x \in k \colon |x|_v < 1\}$ its maximal ideal and by $k(v) = \mathcal{O}_v/\mathfrak{m}_v$ its residue field (which is finite). Let us then choose a finite set S of places containing the archimedean ones and define as

$$\mathcal{O}_S = \{ x \in k \colon |x|_v \le 1, \forall v \notin S \}$$

the ring of S-integers. Let $D \subset \mathbb{P}^n$ be a closed subvariety over k which is defined by a homogeneous ideal $I_D \subset k[X_0, \ldots, X_n]$. We can consider $I_{D,v} \coloneqq I_D \cap \mathcal{O}_v[X_0, \ldots, X_n]$ and its image in the quotient ring $\mathcal{O}_v[X_0,\ldots,X_n]/\mathfrak{m}_v = k(v)[X_0,\ldots,X_n]$. It is still a homogeneous ideal and so it defines a closed subvariety D_v of \mathbb{P}^n over k(v). We say that P reduces modulo v to D if $P_v \in D_v$, where P_v is the reduction modulo v of P.

Let \widetilde{X} be a projective k-variety in \mathbb{P}^n and $D \subset \widetilde{X}$ a subvariety. We say that $P \in \widetilde{X}$ is integral with respect to D if for no finite place v the point P reduces to D. If S is a finite set of places containing the archimedean ones, we say that P is S-integral with respect to D if it never reduces to D for any prime *outside* S. Usually one writes $X = \overline{X} \setminus D$ and by $X(\mathcal{O}_S)$ we mean the set of S-integral points of \tilde{X} with respect to D. If D is a divisor, it is called *divisor at infinity*, in the sense that one completes the quasi-projective variety X to \tilde{X} adding the "points at infinity" contained in D. When $X \subset \mathbb{A}^n \subset \mathbb{P}^n$ is an affine variety, we recover the naive definition using coordinates. Indeed, considering the completion \widetilde{X} under the canonical embedding $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ and defining $D = \widetilde{X} \setminus X$, the S-integral points of \widetilde{X} with respect to D will be the points of X with coordinates in \mathcal{O}_S .

We now study the behavior of integral points under morphisms, allowing if necessary an enlargement of S. Let X_1 and X_2 be quasi-projective algebraic varieties defined over a number field k and let $\pi: X_1 \to X_2$ be a k-morphism. We can complete both varieties to projective varieties \widetilde{X}_1 and \widetilde{X}_2 in such a way that π can be continued to a morphism $\pi: \widetilde{X}_1 \to \widetilde{X}_2$ with $\pi^{-1}(D_2) = D_1$, where $D_i := \widetilde{X}_i \setminus X_i$. Usually we will omit any reference to X and D: any time we will have a morphism between (quasi-projective) varieties it will be implicit that it has been continued to the completions and the divisors at infinity.

We now list some results that we will use in our proofs.

Proposition 2.1. Let X_1 and X_2 be quasi-projective algebraic varieties defined over a number field k and let $\pi: X_1 \to X_2$ be a k-morphism. Let S be a finite set of places containing the archimedean ones. Enlarging S if necessary, we have $\pi(X_1(\mathcal{O}_S)) \subseteq X_2(\mathcal{O}_S)$.

Corollary 2.2. Let X_1 and X_2 be quasi-projective algebraic varieties defined over a number field k and let $\pi: X_1 \to X_2$ be a k-morphism. Let S be a finite set of places containing the archimedean ones. If π is dominant and $X_1(\mathcal{O}_S)$ is Zariski-dense, then $X_2(\mathcal{O}_S)$ is Zariski-dense, possibly after an enlargement of S. Conversely, if π is dominant and $X_2(\mathcal{O}_S)$ is never Zariski-dense for any S, then $X_1(\mathcal{O}_S)$ cannot be Zariski-dense.

Proposition 2.3. Let X_1 and X_2 be quasi-projective algebraic varieties defined over a number field k. Let $\pi: X_1 \to X_2$ be a finite map and S a finite set of places containing the archimedean ones. Then there is another finite set of places S', containing S, such that $\pi^{-1}(X_2(\mathcal{O}_{S'})) \cap X_1(k) \subseteq X_1(\mathcal{O}_{S'})$. In other terms, the rational preimages of the S'-integral points of X_2 are S'-integral points of X_1 .

Proposition 2.4. Let C be a geometrically irreducible rational curve over k with (at least) two points in the divisor at infinity. Let $\pi: \mathcal{D} \to C$ be a finite k-morphism of geometrically irreducible curves ramified above (at least) one point in the affine part of C. Then \mathcal{D} has only finitely many S-integral points.

Proof. We apply Siegel's theorem: if \mathcal{D} has genus > 0 we are done, otherwise we prove that \mathcal{D} has at least three points at infinity. Using Hurwitz formula, we have $2(d-1) = \sum_{x} (e_x - 1) > 0$, where e_x is the ramification index at x and $d = \deg \pi$, so that d > 1. Moreover the numerical relation implies that we cannot have total ramification in the two points at infinity, since there is a ramification point in the affine part of \mathcal{C} . Then \mathcal{D} has at least three points at infinity.

3. Proof of Theorem 1.14

First, we need to prove the (potential) Zariski density of S-integral points. This result is not new, since it is implicit in Beukers [1] and explicit in [15] of Hassett-Tschinkel, where they proved the following generalization for Del Pezzo surfaces:

Theorem 3.1 ([15]). Let X be a smooth Del Pezzo surface and D a smooth anticanonical divisor. Then integral points for (X, D) are potentially dense.

Here we present our own construction of a Zariski dense set of S-integral points, since it is essential in our proof of Theorems 1.14 and 1.15.

3.1. The density of S-integral points. We recall that a smooth cubic surface in \mathbb{P}^3 can be realized, over a finite extension of k, as the blowup of \mathbb{P}^2 in six points P_1, \ldots, P_6 in general position. By general position we mean that there are no three collinear points and there is no conic passing through all of them. We then have a morphism $\pi: \tilde{F} \to \mathbb{P}^2$ which is one to one everywhere except over the six points, where the exceptional divisors $E_i = \pi^{-1}(P_i)$ are lines contained in the cubic surface. The map π is birational and its inverse

$$\pi^{-1} \colon \mathbb{P}^2 \dashrightarrow \widetilde{F}$$

is given by $[r:s:t] \mapsto [f_0(r,s,t):\cdots:f_3(r,s,t)]$, where f_0,\ldots,f_3 are four linearly independent cubic homogeneous polynomials vanishing at the 6 points. As a consequence, the set of indeterminacy of π^{-1} is given by the six points. The image of H through π is a cubic curve D in \mathbb{P}^2 passing through the six points.

We enlarge k so that P_1, P_2, P_5, P_6 are defined over k and the couple $\{P_3, P_4\}$ is defined over k. Then we have that the blowup is defined over k and the linear systems of conics through P_1, P_2, P_3, P_4 and P_3, P_4, P_5, P_6 are defined over k.

There are 15 lines in \mathbb{P}^2 connecting pairs of points in $\{P_1, \ldots, P_6\}$. The strict transforms of these lines correspond to some of the 27 lines in \tilde{F} and intersect the divisor at infinity H in one point. In fact, if the line is not tangent in any of the two blown-up points, it will intersect D in one more point, which corresponds to a point in H. Otherwise, if it is tangent in one of the two points, there will be no more intersection with D, and the only point at infinity of the strict transform will be the one above the tangency point.

Let ℓ be the line joining P_1 and P_6 (which is then defined over k). Its strict transform L in F is then isomorphic to \mathbb{A}^1 , i.e. to \mathbb{P}^1 with one point at infinity. Enlarging S we can make $L(\mathcal{O}_S)$ infinite and by Hilbert irreducibility theorem $L(\mathcal{O}_S)$ is a non-thin set.

We then consider the morphism $\lambda \colon \widetilde{F} \to \mathbb{P}^1$ given by the composition of the map π and the rational map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^1$ which sends the point $P \in F$ to the intersection of ℓ and the conic of the linear system through P (we shall soon see that λ is indeed a morphism). More precisely we map a point $Q \in F$ to $\pi(Q) \in \mathbb{P}^2$ and consider the conic through P_1, P_2, P_3, P_4 and $\pi(Q)$. The intersection between ℓ and the conic is given by two points, of which one is P_1 , which is defined over k. Then, if Q is defined over k, by the hypotheses on k, also the second intersection point will be defined over k, and we define it to be the image of the map λ . The map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^1$ is not a morphism, since it is not defined in P_1, P_2, P_3, P_4 , but λ is a morphism. To show this, we only have to check that it can be extended to the exceptional divisors over P_1, P_2, P_3, P_4 . In fact, for a given point of, say, E_1 , there passes exactly one strict transform of a conic of the linear system, and we consider this conic for the above construction. Thus λ defines a morphism $\widetilde{F} \to \mathbb{P}^1$ with fibers given by the strict transforms of the conics of the linear system. We will write C_l for the fiber corresponding to the value l.

We can define in an analogous way the fibration $\mu \colon \widetilde{F} \to \mathbb{P}^1$ whose fibers are given by the strict transform of the conics through P_3, P_4, P_5, P_6 . We denote these curves with \mathcal{C}'_m .

We now observe that C_l is a curve with two points at infinity, since the corresponding conic in \mathbb{P}^2 intersects $D \setminus \{P_1, \ldots, P_6\}$ in two points. There are only finitely many exceptions that can occur, namely the conic through P_5 , the one through P_6 and the conics tangent to the cubic. Then we have that the general C_l is isomorphic to \mathbb{G}_m , i.e. to \mathbb{P}^1 minus two points at infinity. It is natural then to study which C_l have infinitely many *S*-integral points. In order to do this, we recall the following well known result.

Theorem 3.2. Let C be a smooth rational curve with two points at infinity P, P'. Suppose that either

- (1) \mathcal{O}_S^* is infinite,
- (2) or the points at infinity P and P' are quadratic conjugates and one place of S splits in the corresponding quadratic extension.

Then if C contains an S-integral point, it has infinitely many ones.

Proof. A smooth rational curve with two points at infinity admits a planar model as a conic C with two points at infinity. We denote by L the line passing through these two points. Then we can use Corollary 5.3.3 of Chapter 5 of [5].

The hypotheses of this theorem are easily verified for every C_l if we enlarge S so to have \mathcal{O}_S^* infinite. Then we will have that any curve \mathcal{C}_l passing through an S-integral point will contain infinitely many other S-integral points. The set of curves \mathcal{C}_l such that $\mathcal{C}_l(\mathcal{O}_S)$ is infinite is parametrized by a non-thin (and thus infinite) set of values $l \in k$, since a curve \mathcal{C}_l through $p \in L(\mathcal{O}_S)$ has infinitely many S-integral points, and $L(\mathcal{O}_S)$ is not thin over k. This gives the Zariski-density of $F(\mathcal{O}_S)$.

Clearly the same properties hold for the curves \mathcal{C}'_m .

Remark 3.3. The reader may ask why we did not use the pencil of lines through a blown-up point. The reason will be clear in the proof, where we will use the simple connectedness of F minus some lines. Still, one can prove the theorem using a system of conics and a system of lines. However, in the case of the Fermat cubic surface, there is no system of lines defined over \mathbb{Q} , so we preferred this proof.

3.2. Topology of complements of curves in smooth cubic surfaces. Let us denote by $L_{3,4}$ the strict transform of the line through P_3 and P_4 . We write

$$X = F \setminus L_{3,4} = F \setminus (H \cup L_{3,4})$$

We want to prove the following:

Theorem 3.4. The surface X is topologically simply connected.

We recall the following two lemmas.

Lemma 3.5. Let X be a (connected) complex manifold, $Z \subset X$ a proper closed complex submanifold, $Y = X \setminus Z$ its complement, $p \in Y$ a point. Then the inclusion $i: Y \hookrightarrow X$ induces a surjective homomorphism $i_*: \pi_1(Y, p) \to \pi_1(X, p)$ between the corresponding fundamental groups.

Proof. See Lemma 2, section 3 of [8].

Lemma 3.6. The surface $U \coloneqq X \setminus (E_1 \cup \cdots \cup E_6)$ has fundamental group isomorphic to \mathbb{Z} .

Proof. The surface U is isomorphic to the complement of a smooth cubic and a transverse line in \mathbb{P}^2 , so that the result is a consequence of the remark following Theorem 2 of [22]. \Box

 $\mathbf{6}$

Lemma 3.7. The surface X admits no finite cyclic unramified connected cover of degree > 1.

Proof. Let $Y \to X$ be a cyclic unramified cover of degree d > 1. By a Theorem of Grauert and Remmert (see [23], Ch.6), Y has a structure of algebraic variety such that the covering map is algebraic. Then the function field of Y is obtained by taking the d-th root of a rational function $f \in \mathbb{C}(\widetilde{X})^* = \mathbb{C}(\widetilde{F})^*$ on \widetilde{F} . The property that $Y \to X$ is unramified means that all zeros and poles of f in X have multiplicity divisible by d. This means that for each irreducible curve $C \subset \widetilde{F}$ outside $L_{3,4} \cup H$ the multiplicity of C in the divisor (f) is divisible by d. Hence we have

$$(f) = aL_{3,4} + bH + dD$$

for a divisor D. For an exceptional divisor E_i with $i \neq 3, 4$ we have the following intersection products

$$L_{3,4}^2 = -1, L_{3,4} \cdot H = 1, L_{3,4} \cdot E_i = 0, E_i \cdot H = 1$$

Multiplying (f) by $L_{3,4}$ and E_i we obtain

$$0 = (f).L_{3,4} = -a + b + dD.L_{3,4}$$

$$0 = (f).E_i = b + dD.E_i$$

so that d must divide both a and b. Then there would not be ramification over $L_{3,4}$ and H and $Y \to X$ would define an unramified cover of all \tilde{F} , which is simply connected, so that the cover would be trivial.

Proof of Theorem 3.4. Let $U \subset X$ be the surface of Lemma 3.6. By Lemma 3.5 the fundamental group of X is a quotient of the fundamental group of U, which is isomorphic to \mathbb{Z} after Lemma 3.6, so that $\pi_1(X)$ is a quotient of \mathbb{Z} . To prove that such a quotient is trivial, it is sufficient to show that it admits no non-trivial finite cyclic quotients. Geometrically, this means that X admits no non-trivial (finite) cyclic cover, which is the content of Lemma 3.7.

Corollary 3.8. The surface F is simply connected.

We then have proved that F satisfies the hypotheses of Problem 1.9, so that we can proceed to the proof of the IHP.

3.3. The IHP for cubic surfaces. Our proof of Theorem 1.14 follows the method developed by Corvaja and Zannier in [9] to prove the Hilbert property for the Fermat quartic surface while now the role of the elliptic fibrations is played by fibrations in conics with two points at infinity. One interesting difference is that here the topology of complements of curves in F is crucial for the success of the strategy. In fact F is simply connected, so that any cover of degree > 1 must ramify outside H. In other terms, for (F, H) the IHP is equivalent to the WIHP. Moreover Theorem 3.4 will be used in an essential step of the following proof.

We argue by contradiction. Suppose we are given finitely many finite maps $\pi_i \colon Y_i \to F$ of degree > 1, where Y_i is an absolutely irreducible variety, such that $F(\mathcal{O}_S) \setminus \bigcup_i (\pi_i(Y_i(k)))$ is not Zariski-dense (and so it is contained in a curve). Then, as we observed, the maps π_i will be ramified over a non-empty divisor of F. We can suppose that the projective continuation $\tilde{\pi}_i \colon \tilde{Y}_i \to \tilde{F}$ are finite², too. In this case, when we speak about S-integral points on Y_i , we mean that $\tilde{\pi}_i^{-1}(H)$ is the divisor at infinity of \tilde{Y}_i . Enlarging the primes $S \subset S'$ we may suppose that if the pre-image through π_i of a point in $F(\mathcal{O}_S)$ lies in $Y_i(k)$, then it actually belongs to $Y_i(\mathcal{O}_{S'})$.

Let us consider one such cover $\pi: Y \to F$. The generic fiber of $\lambda \circ \pi: Y \to \mathbb{P}^1$ can be either reducible or irreducible, i.e. the fiber $Y(l) \coloneqq \pi^{-1}(\mathcal{C}_l)$ is reducible or irreducible for general $l \in \mathbb{C}$. We divide the covers in three types:

(1) Y(l) is generically reducible.

²In fact the usual reduction of Remark 1.7 produces a projective variety because \tilde{F} is projective.

SIMONE COCCIA

- (2) Y(l) is generically irreducible and there exists an irreducible curve in the ramification divisor of π which generically intersects the curves C_l .
- (3) Y(l) is generically irreducible and there exists no such curve as above. More explicitly, the components of the ramification divisor can be irreducible curves of the family C_l , strict transforms of the lines through the four base points of the linear system or the exceptional divisors E_5 and E_6 . To prove this, let us first observe that E_5 and E_6 are the only exceptional divisors which do not generically intersects the curves C_l . Let \mathcal{D} be an irreducible curve in F, distinct from the exceptional divisors, which does not generically intersect the curves C_l . Then $\pi(\mathcal{D})$ is a curve in \mathbb{P}^2 which does not generically intersect the conics $\pi(C_l)$. However these are the conics of a linear system, so they generically intersect every curve which is not part of their linear system. Then $\pi(\mathcal{D})$ can be an irreducible conic $\pi(C_l)$ or a reducible one, i.e. a line through the four base points. Passing to strict transforms we have the assertion.

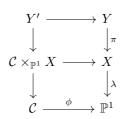
First, we treat the case of generically reducible covers.

Lemma 3.9. If the generic fiber of $\lambda \circ \pi$ is reducible, there exists a cover defined over k of k-irreducible curves $\phi: \mathcal{C} \to \mathbb{P}^1$ such that the pullback of Y over the base change $\mathcal{C} \times_{\mathbb{P}^1} \widetilde{F}$ is reducible over \overline{k} .

Proof. Irreducibility is a birational invariant, hence we reduce to the case of a projection of affine varieties $\pi: Y \to X$ where $X := (f(x, y, \lambda) = 0) \subseteq \mathbb{A}^3$ and $Y := (f(x, y, \lambda) = 0) \cap (g(x, y, z, \lambda) = 0) \subseteq \mathbb{A}^4$, π maps (x, y, z, λ) to (x, y, λ) and $\lambda: X \to \mathbb{P}^1$ maps (x, y, λ) to λ . The fact that $\lambda \circ \pi$ has reducible generic fiber is equivalent to the fact that for all but finitely many $\lambda_0 \in \overline{k}$ the fiber $(f(x, y, \lambda_0) = 0) \cap (g(x, y, z, \lambda_0) = 0)$ is reducible. Up to a birational isomorphism we can eliminate one variable and reduce to a surface defined by P(u, v, t) = 0, projecting (u, v, t) to t, in such a way that for all but finitely many $t_0 \in \overline{k}$ the polynomial $P(u, v, t_0)$ is reducible. This implies that there exists a non-trivial factorization

$$P(u, v, t) = A_t(u, v) \cdot B_t(u, v)$$

where A_t and B_t are polynomials in u and v with coefficients given by algebraic functions of t. Since there are finitely many such coefficients, each providing a finite algebraic extension of the scalars k(t), there is an algebraic element s over k(t), such that the above factorization is valid in k(t, s). Geometrically, this corresponds to a k-cover $\mathcal{C} \to \mathbb{P}^1$, where \mathcal{C} is a k-irreducible curve with function field k(t, s).



From the above discussion, the pullback Y' of Y with respect to this base change is birationally equivalent to (P(u, v, t) = 0), hence reducible over \bar{k} .

Using this Lemma and the fact that Y is geometrically irreducible, we have $\deg(\phi: \mathcal{C} \to \mathbb{P}^1) > 1$. Then the components of Y(l) may be defined over k only for $l \in \phi(\mathcal{C}(k))$, which is a thin set in $\mathbb{P}^1(k)$. That is, for l outside this thin set, the fiber Y(l) is irreducible over k but reducible over \bar{k} , and this implies that Y(l) has only finitely many rational points.³

We denote by T the union of these thin sets, which in the following we will enlarge with finitely many other thin sets, if necessary. We then have obtained that for $l \notin T$ all but finitely many points of $C_l(k)$, and in particular of $C_l(\mathcal{O}_S)$, are not lifted to the generically reducible covers. Then choosing $l \notin T$ with $C_l(\mathcal{O}_S)$ infinite (this always exists since $L(\mathcal{O}_S)$ is not thin), we have that infinitely many integral points do not lift.

8

³See the first remark in Chapter 3 of [23].

Let us examine the covers with generically irreducible fibers. The set of $l \in \mathbb{C}$ for which Y(l) is reducible is a closed set, then it is finite and we can put it in T.

We begin with covers of the second type. Let B be one irreducible curve in the ramification divisor of π , which is not contained in H and generically intersects the curves C_l . We claim that Y(l) has finitely many S'-integral points, except for finitely many l which we put in T. In order to do this, we have to prove that for all but finitely many l, the restriction of π to Y(l) defines a cover of C_l ramified over $B \cap C_l$. We use the following lemma.

Lemma 3.10. Let $\pi: Y \to X$ be a cover of surfaces which is a finite map. Let B be one irreducible component of the ramification divisor. Let C be a curve in X intersecting B transversally at some point p which is smooth for both C and B. Suppose that $\pi^{-1}(C)$ is absolutely irreducible. Then the restriction of π to $\pi^{-1}(C)$ defines a cover $\pi: \pi^{-1}(C) \to C$ ramified above p.

Proof. There is a neighborhood U of p and local analytic coordinates (x, y) for which p = (0, 0), \mathcal{C} is defined by x = 0, B is defined by y = 0 and $U \setminus (U \cap B)$ is biholomorphic to $D \times D^*$ where D is the open unit disc in \mathbb{C} and $D^* = D \setminus \{0\}$. For a ramification point $q \in \pi^{-1}(p)$ there will be local analytic coordinates (u, v) such that $\pi^{-1}(\mathcal{C})$ is defined by u = 0 and the map π is given locally by x = u and $y = v^e$ where e > 1 is the ramification index at q. Then the pre-image of \mathcal{C} is a smooth curve at q and $\pi: \pi^{-1}(\mathcal{C}) \to \mathcal{C}$ ramifies at q.

Clearly the generic C_l intersects transversally the ramification divisor B_i (of the second type cover π_i) in smooth points not contained in the divisor at infinity H. We put the finitely many exceptions in T. Then for $l \notin T$ we can apply Lemma 3.10 to obtain that the restriction $\pi_i : \pi_i^{-1}(C_l) \to C_l$ is a cover of curves ramified above an affine point of C_l . By Proposition 2.4 we have that $\pi_i^{-1}(C_l)$ has only finitely many S'-integral points, for all *i*'s. Recall that we enlarged S so that the k-rational preimages of S-integral points are S'-integral. Then only finitely many points of $C_l(\mathcal{O}_S)$ can lift to the covers of second type. Then, if all the covers were of second type, we would have a contradiction considering the curves C_l with $l \notin T$ and infinitely many S-integral points.

Let us then study the covers of third type. First we observe that the points of total ramification, i.e. with exactly one pre-image through $\tilde{\pi}$, form a closed subset of the ramification locus. Then $\tilde{\pi}$ totally ramifies on all of H or on finitely many points of H. In this last case, if we put in T the l's for which C_l passes through the total ramification points, we have that for $l \notin T$ the absolutely irreducible curve $\pi^{-1}(C_l)$ has more than two points at infinity, and so it has only finitely many S'-integral points.

We can then assume that third type covers are totally ramified over H. For all l, except the finitely many ones for which C_l is tangent to H or it is a component of the ramification locus, Y(l) is an absolutely irreducible curve with two points at infinity and is unramified in the affine part over C_l . Then Y(l) is isomorphic to a multiplicative torus \mathbb{G}_m which we denote by \mathcal{T}_l and $\pi|_{\mathcal{T}_l}$ is the translate of an isogeny. By the assumption on the surjectivity of the covers on integral points, the S-integral points which do not lift are contained in a curve, so that, for $l \in k \setminus T$, all but finitely many S-integral points of C_l lift to rational points of the \mathcal{T}_l 's (of the various covers). Moreover, if $C_l(\mathcal{O}_S)$ is infinite then it is isomorphic to a finitely generated abelian group of positive rank and $\pi(\mathcal{T}_l(O_S))$ is the translate of a subgroup of $C_l(\mathcal{O}_S)$.

Then we have that when $C_l(\mathcal{O}_S)$ is infinite, all the points in $C_l(\mathcal{O}_S)$ are lifted, as it follows from the following (Lemma 3.2 of [9]).

Lemma 3.11 ([9]). Let G be a finitely generated abelian group of positive rank and, for u in a finite set U, let H_u be subgroups of G and let $h_u \in G$. Suppose that $G \setminus \bigcup_{u \in U} (h_u + H_u)$ is finite. Then this complement is actually empty.

We recall that with C'_m we denoted the curves associated to the other fibration μ . By construction C'_m intersects the possible ramification divisors (different from H) of third type covers, with the only exception of the line $L_{3,4}$ through P_3 and P_4 , in a finite set, which is nonempty for all but finitely many m. However any cover of \tilde{F} must ramify on

a curve outside $L_{3,4} \cup H$, since $F \setminus (L_{3,4} \cup H)$ is simply connected, as proved in Theorem 3.4. Then each cover of the third type will be ramified in the affine part of \mathcal{C}'_m for all but finitely many m. Repeating the argument we used for the covers of second type, we have that for m outside a thin set T', only finitely many points in $\mathcal{C}'_m(\mathcal{O}_S)$ lift to rational points of covers of the third type. At the same time any $p \in \mathcal{C}'_m(\mathcal{O}_S)$ lies also on \mathcal{C}_l , where $l = \lambda(p)$, and since it is an S-integral point, if $l \notin T$ then $\mathcal{C}_l(\mathcal{O}_S)$ is infinite. Therefore, if there exists $m \in k \setminus T'$ with $\mathcal{C}'_m(\mathcal{O}_S)$ infinite, such that $\lambda(p) \notin T$ for infinitely many $p \in \mathcal{C}'_m(\mathcal{O}_S)$, we would have a contradiction, since all the points in $\mathcal{C}_{\lambda(p)}(\mathcal{O}_S)$ are lifted.

We can then suppose that, for any given $m \in k \setminus T'$ with $\mathcal{C}'_m(\mathcal{O}_S)$ infinite, all but finitely many points $p \in \mathcal{C}'_m(\mathcal{O}_S)$ are such that $\lambda(p) \in T$. We have that T, being a thin set, is contained in a finite union of sets $\phi_j(Z_j(k))$ where Z_j is an absolutely irreducible curve and $\phi_j: Z_j \to L$ is a finite map of degree > 1, ramified over a finite subset of $L \cong \mathbb{P}^1$. We write \mathcal{R} for the union of those branch points, which is a finite set.

write \mathcal{R} for the union of those branch points, which is a finite set. The set of branch points of λ restricted to \mathcal{C}'_m depends a priori on m. Indeed, it turns out that each branch point depends on m. This is the analogue of Lemma 3.3 of [9].

Lemma 3.12. For all m such that C'_m is smooth, the restriction to C'_m of λ is a map of degree two, having two ramification points. The value of λ at each of these ramification points is a non-constant (algebraic) function of m.

Proof. We provide a geometric proof of this statement. Let us fix an m so that \mathcal{C}'_m is smooth. In order to compute the degree of the map λ restricted to \mathcal{C}'_m , we have to compute the number of points in \mathcal{C}'_m where it takes a generic value. Now, by our opening construction, a 'value' of the map λ is represented by a point of L, i.e. by the curve \mathcal{C}_l passing through this point. Now $\pi(\mathcal{C}_l)$ and $\pi(\mathcal{C}_m)$ are two conics passing through P_3 and P_4 , so they generically intersect in two more points. Taking the strict transform one gets two points of intersection and so the map has degree two. The ramified values of λ are the conics $\pi(\mathcal{C}_l)$ which are tangent to $\pi(\mathcal{C}'_m)$ in points different from P_3 and P_4 , so that we have exactly two ramification points.

We want to prove that these values are not constant as m varies. Now, if a ramified value for λ were fixed, say equal to l, then $\pi(\mathcal{C}_l)$ would be tangent to $\pi(\mathcal{C}'_m)$ for all values of $m \in \mathbb{P}^1$. But this is impossible since reversing the reasoning with μ in place of λ , we have that there are exactly two values of m for which this happens, corresponding to the ramified values of μ .

Analogously, the λ -images of the two points at infinity of \mathcal{C}'_m are given by non-constant functions of m. As a consequence we have that the set of branch points of λ restricted to \mathcal{C}'_m and the set of values of λ at the points at infinity can intersect \mathcal{R} only for finitely many m. Let $m \notin T'$ be one value for which this does not happen and $\mathcal{C}'_m(\mathcal{O}_S)$ is infinite. Let $\phi: Z \to \mathbb{P}^1$ be one of the morphisms above. The fiber product $W \to \mathbb{P}^1$ of $\lambda: \mathcal{C}'_m \to \mathbb{P}^1$ and $\phi: Z \to \mathbb{P}^1$ has the property that the image of W(k) is $\phi(Z(k)) \cap \lambda(\mathcal{C}'_m(k))$. The map ϕ , having degree > 1, must ramify over at least two points which are not branch points for λ , nor images of the two points at infinity, which we denote by Q and Q'. Hence the restriction to any irreducible component $V \subset W$ of the map $\pi: W \to \mathcal{C}'_m$ must ramify somewhere in the affine part of \mathcal{C}'_m . Let $D = \pi^{-1}(Q + Q')$ be the divisor given by the pullback of the divisor at infinity of \mathcal{C}'_m . Then there is a set of places S'' containing S such that the integral points of \mathcal{C}'_m which lifts, actually lift to $V(\mathcal{O}_{S''})$. In symbols, this means $\pi^{-1}(\mathcal{C}'_m(\mathcal{O}_S)) \cap V(k) \subset V(\mathcal{O}_{S''})$. However using Proposition 2.4 we have that $V(\mathcal{O}_{S''})$ is finite, so, repeating the argument for all irreducible components of W, we conclude that only finitely many points of $\mathcal{C}'_m(\mathcal{O}_S)$ lift to rational points of W.

This proves that $\lambda(\mathcal{C}'_m(\mathcal{O}_S)) \cap \phi(Z(k))$ is finite for each morphism ϕ , hence $\lambda(\mathcal{C}'_m(\mathcal{O}_S)) \cap T$ is finite. However this contradicts the assumption that all but finitely many points p in $\mathcal{C}'_m(\mathcal{O}_S)$ (which is an infinite set) satisfy $\lambda(p) \in T$.

In all cases we were able to derive a contradiction, then proving the theorem.

4. Proof of Theorem 1.15

Theorem 1.14 is valid for all smooth cubic surfaces, but it is *potential*, since we had to enlarge the base field and S. Of course, it is still possible that $F(\mathcal{O}_S)$ is not thin for

smaller k and S. This is the case for the Fermat cubic surface, which is the variety defined over the rational numbers \mathbb{Q} by the equation

$$x^3 + y^3 + z^3 + w^3 = 0$$

In the literature it is also referred to as the surface $x^3 + y^3 + z^3 = w^3$, but this is clearly isomorphic to the one above under the involution $w \mapsto -w$, so that it is immaterial to study one or the other. We take $S = \{\infty\}$ and $H \coloneqq (w = 0)$ as the divisor at infinity, so that the S-integral points are exactly the points with integer coordinates on the affine surface

$$x^3 + y^3 + z^3 + 1 = 0$$

First, we provide the explicit formulas of the blowup, which can be found at the link [11] of Noam Elkies' webpage. We denote by r, s, t the homogeneous coordinates in \mathbb{P}^2 . Then the map $\mathbb{P}^2 \dashrightarrow F$ is given by

$$w = -(s+r)t^{2} + (s^{2}+2r^{2})t - s^{3} + rs^{2} - 2r^{2}s - r^{3}$$
$$x = t^{3} - (s+r)t^{2} + (s^{2}+2r^{2})t + rs^{2} - 2r^{2}s + r^{3}$$
$$y = -t^{3} + (s+r)t^{2} - (s^{2}+2r^{2})t + 2rs^{2} - r^{2}s + 2r^{3}$$
$$z = (s-2r)t^{2} + (r^{2} - s^{2})t + s^{3} - rs^{2} + 2r^{2}s - 2r^{3}$$

and its birational inverse $F \to \mathbb{P}^2$ by

$$r = yz - wx$$

$$s = wy - wx + xz + w^{2} - wz + z^{2}$$

$$t = y^{2} - xy + wy + x^{2} - wx + xz$$

unless w + y, x + z are both zero, in which case r, s, t are proportional to x + y, y, x. This map $[w: x: y: z] \mapsto [r: s: t]$ blows down the six disjoint lines, as follows:

- $E_1: w + \zeta z = x + \zeta y = 0$ to $P_1 = [-\zeta : 1 : 1];$ • $E_1: w + \zeta z = x + \zeta y = 0$ to $P_1 = [-\zeta : 1 : 1];$ • $E_2: w + \overline{\zeta} z = x + \overline{\zeta} y = 0$ to $P_2 = [-\overline{\zeta} : 1 : 1];$ • $E_3: x + \zeta z = y + \zeta w = 0$ to $P_3 = [0 : 1 : -\zeta];$ • $E_4: x + \overline{\zeta} z = y + \overline{\zeta} w = 0$ to $P_4 = [0 : 1 : -\overline{\zeta}];$ • $E_5: y + \zeta z = w + \zeta x = 0$ to $P_5 = [1 : -\overline{\zeta} : -\zeta];$ • $E_6: y + \overline{\zeta} z = w + \overline{\zeta} x = 0$ to $P_6 = [1 : -\zeta : -\overline{\zeta}];$

where ζ and $\overline{\zeta}$ are the primitive cubic roots of unity.

Observe that the couples of points $(P_1, P_2), (P_3, P_4)$ and (P_5, P_6) are paired under the action of $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, so that the only lines connecting two blown-up points which are defined over \mathbb{Q} are the three lines connecting these pairs. These are parametrized as

- [r:s:s], which maps to [-x:x:y:-y] with x = -(r+s), y = 2r s,
- [0:s:t], which maps to [s:-t:t:-s],
- [s+t:s:t] which maps to [s:-t:-s:t].

Similarly, of the fifteen pencils of conics passing through four of the six blown-up points, only three are defined over \mathbb{Q} and they are the ones passing through two of the above couples. To produce infinitely many integer points we want to apply Theorem 3.2 to the curves of the blow-up of these three pencils defined over \mathbb{Q} , but we have to check which curves satisfy the hypotheses. In fact, the group of units $\mathbb{Z}^* = \{1, -1\}$ is finite, so we have to use the condition (2) in Theorem 3.2. Since we are searching for the rational integer points, S consists in the archimedean place of \mathbb{Q} , so that we have to hope that the archimedean place splits in the extension at infinity, or equivalently that the extension is real quadratic. This means that the discriminant of the quadratic polynomial defining the extension at infinity is non-square and positive. Of course, since the blow-up is an isomorphism outside the blown-up points, the points at infinity are quadratic conjugates if and only if their images in \mathbb{P}^2 are so. Then we will check the positivity of the discriminant using the equations of the curves in \mathbb{P}^2 .

First, observe that the points on the line [w:x:y:z] = [s:-t:-s:t] which are integral with respect to w = 0 are exactly those for which [1: -t/s: -1: t/s] has integer

coordinates, i.e. [s:t] = [1:n] where n is an integer. The corresponding points in \mathbb{P}^2 have coordinates [n+1:1:n] with $n \in \mathbb{Z}$.

The idea is to select a conic of the pencil trough P_1 , P_2 , P_3 , P_4 which passes trough an integral point of the above line. If condition on the discriminant is satisfied, then, since the blown-up conic has one integer point, we can apply Theorem 3.2 to show that it has infinitely many. Repeating the argument for all the integer points of the line we obtain the sought Zariski dense set of integer points. It remains to check condition (2) of Theorem 3.2.

The linear system of conics through P_1, P_2, P_3, P_4 has equation

(4)
$$C_{[a:b]}: a(-rs+rt) + b(r^2 - rs + s^2 - st + t^2) = 0$$

so that the conic C_n through [n+1:1:n] is given by

 $[a:b] = [2n^2 + 1:1 - n^2].$

After some calculations we find that the discriminant of the quadratic equation for the points at infinity is

(5)
$$\Delta = \frac{-36u^3 - 54u + 9}{(2u+1)^3}$$

where u = b/a. The solution for $\Delta > 0$ is

$$-\frac{1}{2} < u < 0.1637399876771411...$$

In particular for

(6)
$$u = \frac{1 - n^2}{2n^2 + 1}$$

the condition is satisfied for all $n \neq 0$. We have to check when Δ is non-square. Substituting (6) in (5) we find

$$\Delta = 12n^6 - 3$$

The diophantine equation

$$m^2 = 12n^6 - 3$$

has only finitely many integer solutions, since it represents an hyperelliptic curve of genus 2. Then for all sufficiently large integer n we have that the strict transform C_n of the conic C_n passing through the integral point [n + 1 : 1 : n] satisfies the hypotheses of Theorem 3.2 and so it has infinitely many integer points. Via this geometric construction we have proved

Theorem 4.1. The integer points $F(\mathbb{Z})$ are Zariski dense in the Fermat cubic surface.

This result is not new, since it is implicit in the paper [17] of Lehmer. He proved that the curves in F of equation⁴

$$\begin{cases} 1+z = -3m^2(x+y) \\ x^3+y^3+z^3+1 = 0 \end{cases}$$

with $m \in \mathbb{Z}$, have infinitely many integer points, from which it follows the Zariski density. This method is not different from ours, since Lehmer's curves are strict transforms of conics passing through P_1, P_2, P_5, P_6 .

Unfortunately the integer points of the union of the curves C_n for n = 1, 2, ... are not sufficient for the IHP over \mathbb{Z} , since they form a thin set. In fact, we can consider the surface

$$Y = \{ (p,q) \in F \times L_{5,6} \, | \, q \in \mathcal{C}_{\lambda(p)} \cap L_{5,6} \}$$

where $L_{5,6}$ is the line passing through P_5 and P_6 . Then Y is endowed with the natural projection $\rho: Y \to F$ over the first coordinate. This is a degree two morphism, ramified over the curve C_l tangent to $L_{5,6}$ and it clearly lifts all the integral points we produced.

12

⁴Here we have changed the sign of the variables with respect to the formulas in the introduction, since these referred to $x^3 + y^3 + z^3 = 1$, while we are studying $x^3 + y^3 + z^3 + 1 = 0$.

However this method is much more powerful. In fact we have produced an infinite number of curves C_n with infinitely many integral points, and we still dispose of two other families of conics, the ones through P_1, P_2, P_5, P_6 and the ones through P_3, P_4, P_5, P_6 . Then we can repeat the above construction for both families using *every* curve C_n in place of the line [s: -t: -s: t]. Of course we have to study when the hypotheses of Theorem 3.2 are satisfied for the other two pencils. We then provide a detailed analysis of these pencils of conics.

Let us begin with the conics through P_1, P_2, P_5, P_6 . They are expressed by the equations

$$D_{[a:b]}: a(s-t)(r-s-t) + b(t^2 - tr + r^2)$$

where $[a:b] \in \mathbb{P}^1$. The line through the points at infinity is

$$ar + (b + 2a)s - (b + a)t = 0$$

and the discriminant at infinity is given by

$$\Delta = -3u^4 - 12u^3 - 18u^2 + 9$$

where u = b/a. Solving the inequality $\Delta > 0$ we find

$$-1 < u < 0.587401055408971...$$

In particular, it is sufficient that u lies in

$$-1 < u < \frac{1}{2}$$

From the definition of u we have that

$$u = \frac{(t-s)(r-s-t)}{t^2 - tr + r^2}$$

for any $[r:s:t] \in D_{[a:b]}$, so that, if there exists an integer point in $\mathcal{C}_n(\mathbb{Z})$ such that its blown-down point [r:s:t] satisfies

$$-1 < \frac{(t-s)(r-s-t)}{t^2 - tr + r^2} < \frac{1}{2}$$

then the strict transform $\mathcal{D}_{[a:b]}$ of the conic $D_{[a:b]}$ through this point will have positive discriminant at infinity and so, if Δ is non-square, by Theorem 3.2 it will have infinitely many integral points. Let us then study the above inequalities.

First, let us observe that $t^2 - tr + t^2$ is always positive, so that the inequality is equivalent to

$$-t^{2} + tr - r^{2}$$

The left-hand one is

$$r^2 - rs + s^2 > 0$$

which is always true. The right-hand one is

$$3t^2 - 3tr + r^2 + 2sr - 2s^2 > 0$$

which in the affine plane $(s \neq 0)$ becomes

$$3t^2 - 3tr + r^2 + 2r - 2 > 0$$

This defines the outer part of an ellipse, while from 4 the equation defining C_n in the affine plane $s \neq 0$ is

$$n^{2}(-r^{2}+2rt-r-t^{2}+t-1)+r^{2}+rt-2r+t^{2}-t+1=0$$

and for n sufficiently large it is an hyperbola lying in the area outside the ellipse. Thus we have proved that for almost all n, the curves of the family \mathcal{D} passing through an integral point of \mathcal{C}_n have positive discriminant at infinity.

We now repeat the same argument for the conics through P_3, P_4, P_5, P_6 . They are expressed by the equations

$$E_{[a:b]}: ar(t+s-r) + b(4r^2 - 2rt - 2rs + t^2 - ts + s^2)$$

where $[a:b] \in \mathbb{P}^1$. The line through the points at infinity is

$$as + b(r - s - t) = 0$$

and the discriminant at infinity is given by

$$\Delta = u^4 - 18u^2 + 36u - 27$$

where u = a/b. Then we can solve the inequality $\Delta > 0$ to find

$$u \in]-\infty, -5.107243650047037...[\cup]3, +\infty[$$

In particular it is sufficient that u lies in

$$u\in \left]-\infty,-6\right[\ \cup\ \left]3,+\infty\right|$$

From the definition of u we have that

$$u = \frac{4r^2 - 2rt - 2rs + t^2 - ts + s^2}{r(r - s - t)}$$

for any $[r:s:t] \in E_{[a:b]}$. As above we have reduced to study inequalities. Let us first consider the second one

$$\frac{4r^2 - 2rt - 2rs + t^2 - ts + s^2}{r(r - s - t)} > 3$$

We work in the affine plane $(s \neq 0)$, i.e. we normalize with respect to s. After some manipulations we get

$$\frac{r^2 + rt + t^2 + r - t + 1}{r(r - 1 - t)} > 0$$

The numerator is always positive since

$$r^{2} + rt + t^{2} + r - t + 1 = \left(\frac{r}{\sqrt{2}} + \frac{t}{\sqrt{2}}\right)^{2} + \left(\frac{r}{\sqrt{2}} + \frac{1}{\sqrt{2}}\right)^{2} + \left(\frac{t}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right)^{2} > 0$$

so that the above inequality is really

$$r(r-1-t) > 0$$

The other inequality is

$$\frac{4r^2-2rt-2r+t^2-t+1}{r(r-1-t)}<-6$$

Now suppose r(r-1-t) < 0 so that multiplying we get $4r^2 - 2rt - 2r + t^2 - t + 1 > -6r(r-1-t)$

which is

$$10r^2 - 8rt - 8r + t^2 - t + 1 > 0$$

One easily see that for almost all n, C_n lies in the union of

$$(r(r-1-t) > 0) \cup ((r(r-1-t) < 0) \cap (10r^2 - 8rt - 8r + t^2 - t + 1 > 0))$$

so that the condition on the discriminant is satisfied.

Before finishing the proof, we are going to show the relation between our method and Lehmer's construction of families of integer solutions. He starts with the solutions

(7)
$$x = -9m^4, \quad y = 9m^4 - 3m, \quad z = 9m^3 - 1$$

where m is an integer. This parametrizes the curve

$$\begin{cases} (x+y)^4 + 9x = 0\\ x^3 + y^3 + z^3 + 1 = 0 \end{cases}$$

giving an isomorphism with \mathbb{A}^1 with inverse

$$(x,y,z)\mapsto -rac{x+y}{3}$$

The curve has only one point at infinity, namely [0:1:-1:0]. If we blow down the curve, we find that its image is the conic

$$-2r^2 + r(s+t) + st = 0$$

It passes through the two blown-up points P_1 and P_2 and, having only [0:1:-1:0] at infinity, it has one more intersection point with the cubic in [0:0:1], with tangency multiplicity 4. For a given m, Lehmer produces an infinite number of parametric solutions on the curve

$$1 + z = -3m^2(x + y)$$

starting from the solution (7) and using the theory of Pell's equations. If we blow-down this curve, we find

$$3m^2(r^2 - rs + s^2) - (r^2 - rt + t^2) = 0$$

which is exactly the conic $D_{[a:b]}$ with $[a:b] = [-3m^2:3m^2-1]$. Then

$$u = \frac{b}{a} = \frac{3m^2 - 1}{-3m^2} = \frac{1}{3m^2} - 1$$

satisfies the condition on the positivity of the discriminant

$$-1 < \frac{1}{3m^2} - 1 < \frac{1}{2}$$

so that our method applies to these curves.

We now come to the proof of Theorem 1.15. We consider the morphism $\lambda \colon F \to \mathbb{P}^1$ given by the composition of the blow-down map and the rational map to \mathbb{P}^1 associated with the linear system. Geometrically we map a point $Q \in F$ to the projective point [a:b]defining the conic $D_{[a:b]}$ through $\pi(Q)$ and P_1, P_2, P_5, P_6 . A priori λ is a rational map, since it could not be defined over the exceptional divisors E_1, E_2, E_5, E_6 . However for a given point of, say, E_1 , there passes exactly one strict transform of a conic of the linear system, so we can map this point to the projective point associated with that conic. Thus λ can be extended to a morphism $\lambda \colon F \to \mathbb{P}^1$ with fiber $\mathcal{D}_{[a:b]}$ over [a:b]. Analogously, we call $\mu \colon F \to \mathbb{P}^1$ the map with fibers $\mathcal{E}_{[a:b]}$.

We now prove that $\lambda(\{p \in F(\mathbb{Z}) | \exists n \in \mathbb{N} \ p \in C_n\}) = \lambda(\bigcup_n C_n(\mathbb{Z}))$ is not thin in \mathbb{P}^1 . In other words, the set of points in \mathbb{P}^1 parametrizing the curves of \mathcal{D} passing through an integer point of C_n for some n is not thin. Moreover the curves of \mathcal{D} whose discriminant is a square are parametrized by a thin set, since they are given by the image of the projection from the curve

$$-3u^4 - 12u^3 - 18u^2 + 9 = m^2$$

to \mathbb{P}^1 mapping (u, m) to [1 : u] = [a : b]. The same of course is true for μ , and so we have produced two independent fibrations with a non-thin set of fibers (i.e. parametrized by a non-thin set) with infinitely many integer points. We can then apply the same proof of Theorem 1.14 to deduce Theorem 1.15.

Suppose by contradiction that $T = \lambda(\bigcup_n C_n(\mathbb{Z}))$ is thin. Then it is contained in a finite union of sets $\phi_i(Z_i(\mathbb{Q}))$, where Z_i is an absolutely irreducible curve and $\phi_i \colon Z_i \to \mathbb{P}^1$ is a finite map of degree > 1, ramified over a finite subset of \mathbb{P}^1 . We write \mathcal{R} for the union of those branch points. The analogue of Lemma 3.12 is:

Lemma 4.2. Let $C_t := C_{[1:t]}$ be the pencil defined by the equation (4). For C_t smooth, the restriction of λ to C_t is a degree two map with two ramification points. The value of λ at any of these points is a non-constant algebraic function of t.

Analogously, the λ -images of the two points at infinity of \mathcal{C}_n are given by non-constant functions of n. As a consequence we have that the set of branch points of λ restricted to \mathcal{C}_n and the set of values of λ at the points at infinity can intersect \mathcal{R} only for finitely many n. Let n be one integer for which this does not happen. Let $\phi: Z \to \mathbb{P}^1$ be one of the morphisms above. The fiber product $W \to \mathbb{P}^1$ of $\lambda: \mathcal{C}_n \to \mathbb{P}^1$ and $\phi: Z \to \mathbb{P}^1$ has the property that the image of $W(\mathbb{Q})$ is $\phi(Z(\mathbb{Q})) \cap \lambda(\mathcal{C}_n(\mathbb{Q}))$. The map ϕ , having degree > 1, must ramify over at least two points which are not branch points for λ , nor images of the two points at infinity. Hence the restriction to any irreducible component $V \subset W$ of the map $\pi: W \to \mathcal{C}_n$ must ramify somewhere and not above the points at infinity Qand Q'. Let $D = \pi^{-1}(Q + Q')$ be the divisor of V given by the pullback of the divisor at infinity of \mathcal{C}_n . Then there is a set of places S, containing the place at infinity, such that the integral points of \mathcal{C}_n which lift to rational points of V, actually lift to $V(\mathbb{Z}_S)$. In symbols, this means $\pi^{-1}(\mathcal{C}_n(\mathbb{Z})) \cap V(\mathbb{Q}) \subset V(\mathbb{Z}_S)$. However using Proposition 2.4 we have that $V(\mathbb{Z}_S)$ is finite so, repeating the argument for all irreducible component of W, we conclude that only finitely many points of $\mathcal{C}_n(\mathbb{Z})$ lift to rational points of W.

This proves that $\lambda(\mathcal{C}_n(\mathbb{Z})) \cap \phi(Z(k))$ is finite for each morphism ϕ , hence $\lambda(\mathcal{C}_n(\mathbb{Z})) \cap T$ is finite. However this is absurd since $\lambda(\mathcal{C}_n(\mathbb{Z})) \subset T$ and $\mathcal{C}_n(\mathbb{Z})$ is infinite.

As stated above, this concludes the proof of the theorem, since we have obtained two independent fibrations with a non thin set of fibers with infinitely many integer points, and the same proof of Theorem 1.14 applies.

Remark 4.3. Our method for the construction of the non-thin set of S-integral points has a geometrical interpretation. Indeed, one chooses

- (1) a point P on the line,
- (2) a point Q on the curve of C passing trough P,
- (3) a point R on the curve of \mathcal{D} passing trough Q.

Then there are three parameters all varying in \mathbb{P}^1 , since the lines and conics can be identified with \mathbb{P}_1 . Geometrically, we get a rational map $\mathbb{P}^3_1 \dashrightarrow F$ where $\mathbb{P}^3_1 \coloneqq \mathbb{P}_1 \times \mathbb{P}_1 \times \mathbb{P}_1$, which sends the three parameters to the point on the curve of \mathcal{D} identified by the above construction. We then have two maps $\mathbb{P}^3_1 \dashrightarrow F$, one for \mathcal{D} and one for \mathcal{E} . This delineates a difference with the method of Theorem 1.14, where we considered the integral points on a line and then the conics trough these points, so that we had two rational maps $\mathbb{P}^2_1 \dashrightarrow F$. This is also the case for the proof of Theorem 1.5 of Corvaja and Zannier, where they use two parameters for the construction of the non-thin set of rational points.

5. The WIHP for the complement of the smooth plane cubic

In [2], Beukers proved the following.

Theorem 5.1. Let $D \subset \mathbb{P}^2$ be a curve of degree ≤ 3 with at most normal crossing singularities, defined over a number field k, and let $X = \mathbb{P}^2 \setminus D$. Then there exists a finite extension of k and a finite set of places S such that $X(\mathcal{O}_S)$ is Zariski-dense in X.

Clearly, it suffices to study the complements of maximal degree deg D = 3, since Zariski density is easier to accomplish with a smaller D. The four cases are:

- (1) three lines in general position,
- (2) a smooth conic and a non tangent line,
- (3) a singular irreducible cubic,
- (4) a smooth cubic.

In all these cases, the strategy of the proof relies on constructing an infinite family of rational curves with two points at infinity (i.e. intersecting D, the divisor at infinity) and with infinitely many S-integral points. This gives the Zariski-density of $X(\mathcal{O}_S)$.

Once obtained the Zariski-density, one could try to see if these surfaces provide a positive instance of Problem 1.11.

Theorem 5.2. The complements of the curves above have the WIHP.

The first three cases reduce to the WIHP for \mathbb{G}_m^2 . This is already established and there are much more general results regarding algebraic groups (see [4, 6, 12, 25]). The most difficult case is the one of the smooth cubic. In fact one cannot prove the WIHP for this surface using the conics with infinitely many S-integral points found by Beukers. The obstruction is that they form a thin set covered by a map with ramification divisor not contained in the smooth cubic D. In other words, the WIHP for X cannot be proved using only the S-integral points coming from Beukers' conics. With our method we provide a different proof of the potential Zariski density and we are able to prove the WIHP as a corollary of Theorem 1.14.

In fact, suppose that D is defined in \mathbb{P}^2 by the equation D = (G(x, y, z) = 0). Then the smooth cubic surface $\widetilde{F} \subset \mathbb{P}^3$ of equation $S = (w^3 = G(x, y, z))$ is naturally endowed with the projection morphism $\pi : \widetilde{F} \to \mathbb{P}^2$ sending [x : y : z : w] to [x : y : z]. The pre-image of D is given by $H = (w = 0) \cap F$, hence it is a smooth hyperlane section of \widetilde{F} . This map

16

is (totally) ramified only above D, so $F = F \setminus H$ defines a cyclic étale covering of degree 3 of X, and since F is simply connected, it is the universal cover of X. We can apply Theorem 1.14 to show that for an extension $k \subset K$ and a set of places S, the surface Fhas the IHP. Since π is dominant, we can apply Corollary 2.2 to show that there exists an enlargement of S (which we still denote by S) such that $\pi(F(\mathcal{O}_S)) \subset X(\mathcal{O}_S)$. It follows $X(\mathcal{O}_S)$ is Zariski-dense.

The WIHP is a consequence of the IHP for F. In fact, suppose we are given finitely many finite maps $\pi_i: Y_i \to X$ lifting all the S-integral points of X, ramified outside D. We consider the fiber product $F \times_X Y_i$, which fits in the following diagram

$$F \times_X Y_i \xrightarrow{p_{i,2}} Y_i$$
$$\downarrow^{p_{i,1}} \qquad \downarrow^{\pi_i}$$
$$F \xrightarrow{\pi} X$$

We assert that all S-integral points of F lift to the covers $p_{i,1}$. Indeed, let us consider an S-integral point $q \in F(\mathcal{O}_S)$. By hypotheses the image $\pi(q)$ is S-integral in X. Then there is a cover π_i and a rational point $y \in Y_i(k)$ such that $\pi_i(y) = \pi(q)$. Therefore the point (q, y) lies in $F \times_X Y_i$ and $p_{i,1}(q, y) = q$. Moreover the covers $p_{i,1}$ are not trivial, since $\pi^{-1}(D) = H$ and π_i is ramified outside D, and this contradicts the IHP for F.

References

- F. Beukers, Integral points on cubic surfaces, Number theory (Ottawa, ON, 1996), 25?33, CRM Proc. Lecture Notes, 19, AMS, Providence, RI, (1999).
- [2] F. Beukers, Ternary Form Equations, J. Numb. Theory 54 (1995), 113-133.
- [3] E. Bombieri, W. Gubler, Heights in Diophantine Geometry, Cambridge Univ. Press, 2006.
- [4] J. L. Colliot-Thélène, J. J. Sansuc, Principal Homogeneous Spaces under Flasque Tori: Applications, J. Algebra 106 (1987), 148-205.
- [5] P. Corvaja, Integral Points on Algebraic Varieties. An introduction to Diophantine Geometry, Institute of Mathematical Sciences Lecture Notes, Hindustan Book Agency, New Delhi (2016).
- [6] P. Corvaja, Rational fixed points for linear group actions, Annali Scuola Normale Superiore Cl. Sci. (5) Vol. VI, Fasc. 4 (2007), 1-37.
- [7] P. Corvaja, U. Zannier, Applications of Diophantine Approximation to Integral Points and Transcendence (Cambridge Tracts in Mathematics), Cambridge Univ. Press, 2018.
- [8] P. Corvaja, U. Zannier, Integral points, divisibility between values of polynomials and entire curves on surfaces, Adv. Math., 225 (2010), 1095-1118.
- [9] P. Corvaja, U. Zannier, On the Hilbert property and the fundamental group of algebraic varieties, Math. Z., 284 (2017).
- [10] J. L. Demeio, Non-rational varieties with the Hilbert Property, https://arxiv.org/abs/1801.10413
- [11] N. Elkies, http://www.math.harvard.edu/ elkies/4cubes.html.
- [12] A. Ferretti, U. Zannier, Equations in the Hadamard ring of rational functions, Annali Scuola Normale Superiore Cl. Sci. (5) Vol. VI Fasc. 3 (2007), 457-475.
- [13] M. Fried, M. Jarden, Field Arithmetic, III Ed., Springer Verlag.
- [14] G. H. Hardy, E. M. Wright; D. R. Heath-Brown, J. H. Silverman, eds., An introduction to the theory of numbers (Sixth ed.), Oxford University Press, (2008) [1938].
- [15] B. Hassett, Yu. Tschinkel, Density of integral points on algebraic varieties, in: Rational Points on Algebraic Varieties, in: Progr. Math., vol. 199, Birkäuser, 2001, pp. 169-197.
- [16] S. Lang, Fundamentals of Diophantine Geometry, Addison Wesley, 1981.
- [17] D.H.Lehmer, On the diophantine equation $x^3 + y^3 + z^3 = 1$, Journal London Math. Soc. 31 (1956), 275-280.
- [18] J. C. P. Miller, M. F. C. Woollett, Solution of the diophantine equation $x^3 + y^3 + z^3 = k$, Journal London Math. Soc. 30 (1955), 101-110.
- [19] L. J. Mordell, On an infinity of integer solutions of $ax^3 + ay^3 + bz^3 = bc^3$, Journal London Math. Soc 30 (1955), 111-113.
- [20] L. J. Mordell, On the integer solutions of the equation $x^2 + y^2 + z^2 + 2xyz = n$, Journal London Math. Soc. 28 (1953), 500-510.
- [21] J-P. Serre, Lectures on the Mordell-Weil Theorem, Vieweg, 1982.

SIMONE COCCIA

- [22] J-P. Serre, Revêtements ramifiés du plan projectif, Séminaire Bourbaki, Tome 5 (1958-1960), Exposé no. 204, p. 483-489.
- [23] J-P. Serre, Topics in Galois Theory, Jones and Bartlett, Boston 1992.
- [24] H. Völklein, Groups as Galois Groups, Cambridge Univ. Press, 1996.
- [25] U. Zannier, Hilbert Irreducibility above algebraic groups, Duke Math. J., 153 (2010), 397-425.

Simone Coccia Scuola Superiore dell'Universitá di Udine Palazzo Garzolini di Toppo Wassermann Via Gemona 92 33100 Udine - ITALY coccia.simone@spes.uniud.it