The Topology of Rational Points

Barry Mazur

CONTENTS

Introduction
1. Comparison of Density Conditions
2. Curves
3. Conic Bundles over $\mathbf{P}^1$
4. Smooth Cubic Hypersurfaces
5. Smooth Complete Intersections of Two Quadrics in $\mathbf{P}^N$
6. Elliptic Surfaces
7. Some Abelian Varieties
8. Some Kummer Surfaces
9. Some Other K3 Surface Examples
References

The aim of this article is to provoke a discussion concerning the general nature of the topological closure of the set of rational solutions of systems of polynomial equations with rational coefficients.

INTRODUCTION

In the voluminous literature concerning rational points, has the nature of the topological closure (with respect to the usual real topology) of the set of rational points of an algebraic variety in its real locus ever been discussed head-on in any general context?

I suspect not. For various reasons—one of which will be given shortly—I think it might be useful to have such a discussion, even though the state of our knowledge concerning these matters is, at present, primitive.

By a *variety* we will mean a reduced scheme of finite type over a field (usually $\mathbf{Q}$).

Conjecture 1. *Let V be a smooth variety over $\mathbf{Q}$ such that $V(\mathbf{Q})$ is Zariski-dense in V. Then the topological closure of $V(\mathbf{Q})$ in $V(\mathbf{R})$ consists of a (finite) union of connected components of $V(\mathbf{R})$.*

I view this conjecture somewhat in the way a debating society, for example, might view a resolution, "Resolved that...", as a proposal on the table to be argued for or against. As will be clear in this paper, I also took the conjecture as a fruitful pretext for writing to a number of friends. In particular, I am very much indebted to J.-L. Colliot-Thélène, D. Rohrlich, J.-P. Serre, J. Silverman, and M. Waldschmidt for their bountiful help, and for their corrections and suggestions regarding preliminary versions of this manuscript.

Remark. Conjecture 1 is equivalent to asking that the topological closure of $V(\mathbf{Q})$ in $V(\mathbf{R})$ be open, or that (under the hypotheses of the conjecture) if a

1058-6458/92 $0.50 per page

topological component contains *one* rational point, the set of rational points is topologically dense in that component. In other words, in the context of the conjecture, rational points are "contagious" in topological components.

If W is any variety over $\mathbf{Q}$, let the *nucleus* of W mean the subvariety V that is the Zariski-closure in the smooth locus of W of the set of smooth $\mathbf{Q}$-rational points of W. Conjecture 1 then makes an assertion about the nucleus of any variety over $\mathbf{Q}$.

What types of varieties can have the property that their rational points are Zariski-dense? The widespread feeling about this, supported by precise conjectures due to Lang, Bombieri and Vojta, is that the Zariski-density of rational points in a projective variety V cannot occur unless, to put it vaguely, "$K \leq 0$", where K is the canonical line bundle of V. The arithmetic of some classes of varieties with $K \leq 0$ has been closely studied for a long time (e.g., abelian varieties, pencils of conics). There have also been some recent, quite precise, studies of the arithmetic of other classes of varieties with $K \leq 0$. For example, see [Manin 1990; 1991] and, in particular, Manin's linear growth conjecture for *Fano varieties*, that is, projective varieties where $-K$ is ample. (This is a particularly well-suited case for study, because one expects lots of rational points in this situation, and one has a very natural height function with respect to which these rational points can be "counted," namely, the height function attached to $-K$.) Also, see [Silverman 1991a; 1991b] for a recent detailed study of the arithmetic of certain K3 surfaces.

Since the real locus of a projective variety Y over $\mathbf{R}$ is, in fact, (finitely) triangulable, and since, if Z is a given closed subvariety of Y, a triangulation T of Y can be chosen so that a subcomplex of T provides a triangulation of the real locus of Z [Lojasiewicz 1964; Hironaka 1975], Conjecture 1 has the following consequence.

Conjecture 2. *The topological closure of the set of rational points of any variety over* $\mathbf{Q}$ *in its real locus is homeomorphic to the complement of a finite subcomplex in a finite complex.*

This conjecture implies that the topological closure of the set of rational points of any variety over $\mathbf{Q}$ in its real locus has the homotopy type of a finite complex and, in particular, it has the following consequence.

Conjecture 3. *The topological closure of the set of rational points of any variety over* $\mathbf{Q}$ *has at most a finite number of connected components.*

I was led to consider the preceding conjectures while studying the work of Matijasevic [Davis et al. 1976], who proved, about twenty years ago, that any listable (or, synonymously, recursively enumerable) subset $S \subset \mathbf{Z}$ is *Diophantinely definable*, in the sense that there is a single polynomial

$$P_S(t, x_1, \dots, x_n)$$

in $\mathbf{Z}[t, x_1, \dots, x_n]$ with the property that an integer t_0 is in S if and only if the polynomial

$$P_S(t_0, x_1, \dots, x_n)$$

in $\mathbf{Z}[x_1, \dots, x_n]$ possesses an integral zero (in the x_i's). The celebrated effect of this result is to provide a negative answer to Hilbert's Tenth Problem. More specifically, by considering a listable set $S \subset \mathbf{Z}$ whose complement is not listable, one sees that there is no machine algorithm whose input is a general integer t_0 and whose output is an answer to the question of whether or not $P_S(t_0, x_1, \dots, x_n)$ possesses an integral solution.

The analogue of Hilbert's Tenth Problem for *rational* rather than *integral* solutions is still open.

It has been suggested that one could obtain a negative answer to Hilbert's Tenth Problem for rational solutions (and more specifically, Matijasevic's proof could be directly transported to this case) if "the set of integers $\mathbf{Z}$ were Diophantinely definable in $\mathbf{Q}$", that is, if one could produce a polynomial

$$P_{\mathbf{Z}}(t, x_1, \dots, x_n)$$

in $\mathbf{Q}[t, x_1, \dots, x_n]$ with the property that a rational number t_0 is a rational integer if and only if the polynomial

$$P_{\mathbf{Z}}(t_0, x_1, \dots, x_n)$$

in $\mathbf{Q}[x_1, \dots, x_n]$ possesses a rational zero (in the x_i's). (For an expository discussion of these matters, and of Julia Robinson's theorem concerning the definability of the integers in the rationals, see [Flath and Wagon 1991].)

However, Conjecture 3 is in conflict with this. The truth of Conjecture 3 would imply that $\mathbf{Z}$ is not Diophantinely definable in $\mathbf{Q}$. For, if a polynomial of the sort $P_{\mathbf{Z}}(t, x_1, \dots, x_n)$ existed, we could take the hypersurface W defined by its zeroes in affine space $\mathbf{A}^{n+1}$ (coordinatized by $t, x_1, \dots, x_n$), and consider the projection $\pi : W \to \mathbf{A}^1$ given by $\pi(t, x_1, \dots, x_n) = t$. Then, directly from the definition of $P_{\mathbf{Z}}$, we would have

$$\pi(W(\mathbf{Q})) = \mathbf{Z} \subset \mathbf{Q} = \mathbf{A}^1(\mathbf{Q}).$$

Denoting by $\overline{W}$ the topological closure of $W(\mathbf{Q})$ in $W(\mathbf{R})$, we would then have $\pi(\overline{W}) = \mathbf{Z}$ as well, since $\mathbf{Z}$ is discrete in $\mathbf{R}$. It would follow that $\overline{W}$ has an infinite number of connected components, contradicting the assertion of Conjecture 3.

1. COMPARISON OF DENSITY CONDITIONS

It is natural to compare the question of openness of the closure of the set of rational points in the real locus with other "adelic" conditions of "openness" and of density. I am very thankful to Colliot-Thélène for his detailed letter to me, in which he explained what is known in various cases about these conditions, and from which I will be extensively quoting in subsequent paragraphs.

There are three other conditions of density amply discussed in the literature:

A. **Weak approximation.** We say that a smooth variety X over a global field k has the *weak approximation property* (over k) if the diagonal imbedding $X(k) \hookrightarrow \prod X(k_v)$ is dense, where v runs through all places of the global field k, and k_v is the completion of k at v.

B. **The condition that the Brauer–Manin obstruction is the only obstruction to weak approximation.** Let $\mathbf{A}_k$ denote the adele ring of a global field k. Let X be a smooth projective variety over k. Let $\mathrm{Br}(X)$ denote the Brauer group of the scheme $X_{/k}$. Local class field theory enables one to define a natural (continuous) right-linear pairing

$$\gamma : X(\mathbf{A}_k) \times \mathrm{Br}(X) \to \mathbf{Q}/\mathbf{Z}$$

[Colliot-Thélène and Sansuc 1987]; by global class field theory, the restriction of the pairing γ to $X(k) \times \mathrm{Br}(X)$ is trivial. Let $X(\mathbf{A}_k)^{\mathrm{Br}}$ denote the "left kernel" of γ, given the topology it inherits as a subspace of $X(\mathbf{A}_k)$. That is, $X(\mathbf{A}_k)^{\mathrm{Br}}$ equals

$$\{x \in X(\mathbf{A}_k) \mid \gamma(x, b) = 0 \text{ for all } b \in \mathrm{Br}(X)\}.$$

The image of the natural injection

$$X(k) \hookrightarrow X(\mathbf{A}_k)$$

is then in $X(\mathbf{A}_k)^{\mathrm{Br}}$. If the image of the mapping $X(k) \hookrightarrow X(\mathbf{A}_k)^{\mathrm{Br}}$ is dense in $X(\mathbf{A}_k)^{\mathrm{Br}}$, one says that *the Brauer–Manin obstruction is the only obstruction to weak approximation for X over k*.

C. **Weak-weak approximation (over k).** Here one requires merely that there be a finite set of places T of k such that for all *finite* sets of places S of k, disjoint from T, the diagonal imbedding

$$X(k) \hookrightarrow \prod_{v \in S} X(k_v)$$

is dense.

Let's compare these conditions with

D. **The S-openness condition.** For a fixed nonempty finite set S of places of k, the topological closure of the image of the diagonal imbedding

$$X(k) \hookrightarrow \prod_{v \in S} X(k_v)$$

is open in $\prod_{v \in S} X(k_v)$.

Visibly, A implies C, which, in turn, implies D for any finite nonempty set of places S disjoint from T. If X is smooth and projective, A implies B.

Since the pairing γ is continuous and the range $\mathbf{Q}/\mathbf{Z}$ of γ is discrete, one sees that B implies D if S is any finite nonempty set of archimedean places of k; in particular, if $k = \mathbf{Q}$, condition B implies that the closure of the set of $\mathbf{Q}$-rational points of X is open in the real locus of X, and therefore that Conjecture 1 is valid for X.

In this regard, it should be remarked that one cannot replace R by $\mathbf{Q}_p$ in Conjecture 1. It is not the case that if X is a smooth variety over $\mathbf{Q}$, the Zariski-density of $X(\mathbf{Q})$ in X guarantees that the topological closure of $X(\mathbf{Q})$ in $X(\mathbf{Q}_p)$ is open. For an explicit example, taken from [Gordon and Grant 1991], see the remark following Conjecture 5 in Section 7.

In the remainder of this paper, we will briefly sample the implications of Conjecture 1 for some varieties and produce a few not entirely trivial examples where the conjecture has been or can be verified either "unconditionally" or at least conditionally upon some more standard conjectures than Conjecture 1 (curves, some conic bundles over $\mathbf{P}^1$, smooth cubic hypersurfaces in $\mathbf{P}^N$, smooth intersections of two quadrics in $\mathbf{P}^N$, some elliptic surfaces, some abelian varieties, some K3 surfaces).

2. CURVES

Conjecture 1 is true for curves. Without loss of generality, one can restrict to smooth proper connected curves V; by Mordell's conjecture, proved by Faltings, V is of genus ≤ 1 if it satisfies the hypotheses of the conjecture. Both cases, genus 0 and genus 1, are easily resolved (the latter because the topological closure of an infinite subgroup in a one-dimensional Lie group is open).

3. CONIC BUNDLES OVER $\mathbf{P}^1$

In [Colliot-Thélène and Sansuc 1982] there is a careful discussion of much of what is known (either unconditionally or dependent upon *Schinzel's hypothesis*) concerning general varieties of the form

$$Q_i(x_{i,1}, \ldots, x_{i,n_i}) = P_i(\lambda_1, \ldots, \lambda_n),$$

for $i = 1, \ldots, r$, where the Q_i's are quadratic forms in the independent variables $x_{i,h}$, each of rank ≥ 2, and the P_i's are polynomials in the λ's with rational coefficients. Among these varieties and, more specially, among the family of conic bundles over $\mathbf{P}^1$, there is a collection of interesting cases supporting Conjecture 1.

First consider this somewhat older example due to Swinnerton-Dyer [1962]: the bundle of conics over $\mathbf{P}^1$ (parametrized by the variable λ) an affine piece of which is given by

$$x^2 + y^2 = (4\lambda - 7)(\lambda^2 - 2). \tag{1}$$

Swinnerton-Dyer shows that, of the two connected components in its real locus, one possesses no rational points, and the other has a dense set of them.

More generally, as Colliot-Thélène has explained to me, the following results have been proved.

Theorem. 1. *Condition B of Section* 1 (*over a number field k*) *holds for any conic bundle X over $\mathbf{P}^1_{/k}$ with no more than four geometric degenerate fibers.*

2. *Condition B* (*over a number field k*) *holds for any conic bundle X over $\mathbf{P}^1_{/k}$ with five geometric degenerate fibers; it holds for any smooth cubic surface possessing a line rational over k; and it holds for a smooth intersection of two quadrics in $\mathbf{P}^4$ with a k-rational point.*

For a proof of part 1, see [Colliot-Thélène et al. 1987] for the special case of Châtelet surfaces and [Colliot-Thélène 1990, Theorem 2] for all other cases. Compare also the discussion of this in [Colliot-Thélène 1986] and [Colliot-Thélène and Skorobogatov 1987].

For a proof of part 2, see [Salberger and Skorobogatov 1991].

It follows from this theorem that Conjecture 1 is true for these varieties; but one can establish Conjecture 1 for some of them by a simpler route. Specifically, for a discussion of Conjecture 1 in the case of smooth cubic surfaces, see Section 4.

As for conic bundles over $\mathbf{P}^1$ with more than five degenerate fibers, I am also thankful to Lan Wang, who has communicated to me the following explicit example: The real locus of the conic bundle

$$x^2 + y^2 = (4\lambda - 7)(\lambda^2 - 2)(2\lambda^2 - 3)$$

has three connected components, and its set of rational points is contained and is dense in exactly one of them.

4. SMOOTH CUBIC HYPERSURFACES

Here is an idea of Swinnerton-Dyer (going back, at least, to 1977: see [Colliot-Thélène 1977]) that was explained to me by Colliot-Thélène. It is a strategy to show that, for certain smooth $\mathbf{Q}$-unirational varieties $X_{/\mathbf{Q}}$, the topological closure of the set of $\mathbf{Q}$-rational points of X is open in the real locus of X. You first establish the existence of *some* open set V in the real locus in which rational points are dense, and then, for any connected component C of $X(\mathbf{R})$ containing one $\mathbf{Q}$-rational point, you "propagate" the rational points of V over C by applying enough birational $\mathbf{Q}$-automorphisms to V.

This works, for example, in the case of smooth cubic hypersurfaces:

Theorem (Swinnerton-Dyer). *Suppose that $X_{/\mathbf{Q}}$ is a smooth cubic hypersurface in $\mathbf{P}^N$, for $N \geq 3$. Then the closure of the set of $\mathbf{Q}$-rational points of X is* *open in the real locus of X. (In particular, Conjecture 1 holds for X, and in fact X satisfies condition D of Section 1—the S-openness condition—for any finite set of places of $\mathbf{Q}$.)*

Proof: For a proof, phrased only for smooth cubic surfaces in $\mathbf{P}^3$ but valid, *mutatis mutandis*, for smooth cubic hypersurfaces of dimension at least two, see [Colliot-Thélène 1977]. Here is a sketch of it.

One may first assume that $X(\mathbf{Q})$ is nonempty, because otherwise we would be done. It then follows from a result of Segre [Manin 1986, Chap. IV, §§7.8 and 8.1] that X is $\mathbf{Q}$-unirational, and consequently there is a mapping $\varphi : \mathbf{P}^{N-1} \to X$ defined over $\mathbf{Q}$, étale on some open nonempty set of $\mathbf{P}^{N-1}(\mathbf{R})$. Since $\mathbf{P}^{N-1}(\mathbf{Q})$ is dense in $\mathbf{P}^{N-1}(\mathbf{R})$, we see that there is, indeed, a nonempty open subset $V \subset X(\mathbf{R})$ such that $X(\mathbf{Q}) \cap V$ is dense in V. Fix such a V. For a point P in $X(\mathbf{R})$, define the *V-opposite set* $V(P)$ as the set of points $Q \in X(\mathbf{R})$ such that

1. $P \neq Q$, and the line $PQ \subset \mathbf{P}^N$ is neither contained in nor tangent to $X(\mathbf{R})$, and
2. the point of $PQ \cap X(\mathbf{R})$ distinct from P and Q (there is exactly one such point, by the previous condition) lies in V.

Since X is smooth, one can show that $V(P)$ is open and nonempty for any $P \in X(\mathbf{R})$. Note that conditions 1 and 2 are symmetrical in P and Q, and therefore we have the *symmetry property* $Q \in V(P)$ if and only if $P \in V(Q)$.

Lemma 1. *For $P \in X(\mathbf{R})$, there is an open neighborhood $N(P) \subset X(\mathbf{R})$ of P such that $V(P) \cap V(P') \neq \emptyset$ if $P' \in N(P)$.*

Proof: Fix a point $Q \in V(P)$ and take $N(P) = V(Q)$. Then, by the symmetry property, $N(P)$ contains P and hence is an open neighborhood of P. Again by the symmetry property, $P' \in N(P)$ implies $Q \in V(P')$ and therefore $V(P) \cap V(P')$ contains Q. □

Lemma 2. *If $P \in X(\mathbf{Q})$, the set of $\mathbf{Q}$-rational points in $V(P)$ is dense in $V(P)$.*

Proof: This follows from the fact that the set of $\mathbf{Q}$-rational points in V is dense in V, and that if we are given a line in $\mathbf{P}^N$ whose intersection with X consists of exactly three points, two of which are $\mathbf{Q}$-rational, the third is also $\mathbf{Q}$-rational. □

Now let P be in the topological closure of the set of $\mathbf{Q}$-rational points of X. We conclude the proof of the theorem by showing that there is an open neighborhood U of P in which the $\mathbf{Q}$-rational points are dense. Let $N(P)$ be as in Lemma 1, and let P' be a $\mathbf{Q}$-rational point in $N(P)$. By Lemma 2, the $\mathbf{Q}$-rational points are dense in $V(P')$, and by Lemma 1, $V(P) \cap V(P')$ is nonempty (and open). Take Q as a $\mathbf{Q}$-rational point of $V(P) \cap V(P')$ and put $U = V(Q)$. By the symmetry property, U contains P (and is therefore an open neighborhood of P). By Lemma 2, the $\mathbf{Q}$-rational points are dense in U. □

Colliot-Thélène has remarked that, despite the preceding result, we have little further information about the "density properties" of k-rational points of smooth cubic hypersurfaces, even of high dimension. For example, do smooth cubic hypersurfaces of sufficiently high dimension satisfy condition C of Section 1, weak-weak approximation? Our ignorance here contrasts with what is known about smooth complete intersections of two quadrics, as shown in the next section.

5. SMOOTH COMPLETE INTERSECTIONS OF TWO QUADRICS IN $\mathbf{P}^N$

Theorem. [Colliot-Thélène et al. 1987; Colliot-Thélène and Skorobogatov 1992] *Let $X_{/k}$ be a smooth complete intersection of two quadrics in $\mathbf{P}^N$, for $N \geq 5$. If $X(k)$ is not empty, X satisfies condition A of Section 1, "weak approximation" over k. The same result holds if X is the smooth part of a singular complete intersection of two quadrics in $\mathbf{P}^N$ and is not a cone.*

6. ELLIPTIC SURFACES

For simplicity, we concentrate here on the case of pencils over $\mathbf{Q}$ of (generically smooth) curves of genus one possessing (at least one) $\mathbf{Q}$-rational section. Fixing such a $\mathbf{Q}$-rational section as the zero-section, we can say that, for all but a finite number of points $r \in \mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$, the member of this family obtained by specializing to r is an elliptic curve, which we will denote by E_r.

Conjecture 4. *Suppose $\{E_r\}_r$ is a family of elliptic curves as above. Then either*

(a) *the (specialized) elliptic curve E_r has Mordell–Weil rank equal to zero for all but a finite number of elements $r \in \mathbf{Q}$, or*
(b) *the Mordell–Weil rank of E_r is positive for a dense set of rational numbers r.*

The only example I know of (a) is the banal case of a constant family, where the constant fiber elliptic curve has Mordell–Weil rank zero.

Proposition. *Conjecture* 1 *implies Conjecture* 4.

Proof: Let S denote the minimal regular model of our elliptic surface, and let $\pi : S \to \mathbf{P}^1$ denote the projection. If (a) does not hold, the set of $\mathbf{Q}$-rational points is Zariski-dense in S. The connected component Σ of $S(\mathbf{R})$ that contains the real locus of the zero section then contains one $\mathbf{Q}$-rational point (in fact, Σ contains at least a projective line of them). By Conjecture 1, the $\mathbf{Q}$-rational points of Σ are then dense in Σ.

Now suppose that (b) does not hold. This implies that there is a nonempty open subset $U \subset \mathbf{P}^1(\mathbf{R})$ such that U contains none of the singular members of our family and the Mordell–Weil group of E_r is finite for $r \in U \cap \mathbf{Q}$. Now consider $\Sigma_0 = \Sigma \cap \pi^{-1}(U)$, which is an open subset in Σ; Σ_0 is the union of the connected components containing the identity in $E_r(\mathbf{R})$ for all $r \in U$. Since the Mordell–Weil groups of E_r are finite, there is a uniform bound B $(= 16)$ for their order (by [Mazur 1976]), and consequently the $\mathbf{Q}$-rational points are *not* topologically dense in Σ_0. This contradicts the conclusion of the preceding paragraph; therefore (b) holds. □

To get some perspective on Conjecture 4, consider again equation (1) of Section 3, but this time consider it as a family of elliptic curves E_x (in the variables y and λ) parametrized by the variable x. One sees directly that for a certain interval of values of x, the elliptic curve E_x has two real components, and by the result of Swinnerton-Dyer already quoted, there are no rational points on the far components of the real locus of the elliptic curves E_x for these values of x, whereas the set of rational points on the connected component of the elliptic surface containing the identity section (at ∞) is dense in that component.

A particularly simple, but not entirely trivial, type of elliptic pencil to consider is that of a twisted constant family E_t, given by

$$D(t) \cdot y^2 = g_3(x),$$

where $g_3(x) \in \mathbf{Q}[x]$ is a monic cubic polynomial with distinct roots, for $D(t) \in \mathbf{Q}(t)$. Here one can try to analyze the situation by making use of the implications of the Birch–Swinnerton-Dyer conjecture concerning change of the parity of the rank of Mordell–Weil of different members of the family. For this, the reader should consult David Rohrlich's recent preprint [Rohrlich 1992] concerning the variation of the "root number" in families of elliptic curves, and Rohrlich's Theorems 1–4, which bear directly on Conjecture 4. We quote his Theorems 2 and 3 below. Let $T^{\pm}$ denote the set of $t \in \mathbf{Q}$ such that E_t is smooth and has root number ± 1. The Birch–Swinnerton-Dyer conjecture would imply that if $t \in T^+$ or $t \in T^-$, the parity of the rank of the Mordell–Weil group of E_t is even or odd, respectively.

Theorem. [Rohrlich 1992, Theorem 2] *One of the two mutually exclusive alternatives holds:*

(a) *T^+ and T^- are both dense in $\mathbf{R}$.*
(b) *One of the sets $T^{\pm}$ is $\{t \in \mathbf{Q} \mid D(t) > 0\}$, and the other is $\{t \in \mathbf{Q} \mid D(t) > 0\}$.*

Furthermore, if E is given, there exists a $D(t)$ such that (b) *holds and such that the number of sign changes of f on $\mathbf{R}$ exceeds any preassigned value. On the other hand, there exists $D(t)$ such that* (a) *holds if and only if E does not acquire everywhere good reduction over any abelian extension of $\mathbf{Q}$.*

By elementary arguments (and dependent upon no conjecture), Rohrlich proves the following theorem.

Theorem. [Rohrlich 1992, Theorem 3] *With notation as above, suppose that $D(t)$ is quadratic. If there exists $t \in \mathbf{Q}$ for which $D(t) \neq 0$, and the Mordell–Weil group of E_t has positive rank, then the set of all t such that the Mordell–Weil group of E_t has positive rank is dense in $\mathbf{R}$.*

It follows then that Conjecture 4 holds if $D(t)$ is of degree ≤ 2. Can elementary arguments be used to settle the case where $D(t)$ is of degree 3?

7. SOME ABELIAN VARIETIES

Conjecture 1 implies the following conjecture for simple abelian varieties over $\mathbf{Q}$.

Conjecture 5. *Let A be a simple abelian variety over $\mathbf{Q}$ whose Mordell–Weil rank is positive. Then the topological closure of $A(\mathbf{Q})$ in $A(\mathbf{R})$ is open (equivalently, it contains $A(\mathbf{R})^0$, the connected component of the identity).*

Conjecture 5 can be restated in terms of the relationship between the real periods of the abelian variety and the "Log" of $\mathbf{Q}$-rational points ("Log" being the multivalued inverse mapping to the exponential mapping $\mathrm{Exp} : T(\mathbf{R}) \to A(\mathbf{R})$, where T is the tangent space to A). Consider, for example, the case where the rank of $A(\mathbf{Q})$ is 1. Let Ω be the kernel of $\mathrm{Exp} : T(\mathbf{R}) \to A(\mathbf{R})$, let $\omega_1, \dots, \omega_g$ be a basis for Ω, and let $w \in T(\mathbf{R})$ be such that $\mathrm{Exp}(w)$ is a $\mathbf{Q}$-rational point of infinite order. Write w as a linear combination of the ω_i's with real coefficients,

$$w = r_1\omega_1 + r_2\omega_2 + \cdots + r_g\omega_g,$$

for $r_i \in \mathbf{R}$. Then (in the case where A is simple and $A(\mathbf{Q})$ is of rank 1) Conjecture 5 is equivalent to saying that the real numbers $1, r_1, \dots, r_g$ are $\mathbf{Q}$-linearly independent.

I asked Michel Waldschmidt what was known, or could be proved, in the direction of Conjecture 5. He replied that such a conjecture is indeed reasonable from the point of view of the theory of transcendental numbers, adding that Conjecture 5 is reminiscent of the famous Four Exponentials Conjecture (concerning usual logarithms of nonzero algebraic numbers), which reads

$$\log\alpha_1 \log\alpha_4 \neq \log\alpha_2 \log\alpha_3$$

if $\log\alpha_1/\log\alpha_2$ and $\log\alpha_1/\log\alpha_3$ are irrational. In this exponential case, only a weaker result is known, namely the Six Exponentials Theorem: If $\alpha_1, \dots, \alpha_6$ are algebraic numbers, and

$$\log\alpha_1/\log\alpha_2 = \log\alpha_3/\log\alpha_4 = \log\alpha_5/\log\alpha_6$$

is irrational, the three numbers $\log\alpha_1$, $\log\alpha_3$ and $\log\alpha_5$ are $\mathbf{Q}$-linearly dependent.

Toward Conjecture 5, Waldschmidt has proved the following theorem.

Theorem. [Waldschmidt 1991] *Let A be a simple abelian variety over $\mathbf{Q}$ of dimension d whose Mordell–Weil rank is at least $d^2 - d + 1$. Then Conjecture 5 holds for A, that is, the topological closure of $A(\mathbf{Q})$ in $A(\mathbf{R})$ is open.*

Moreover, by using arguments of D. Roy, Waldschmidt can prove that if the rank of $A(\mathbf{Q})$ is at least d^2, there is a single rational point $P \in A(\mathbf{Q}) \cap A(\mathbf{R})^0$ with the property that the subgroup generated by P is dense in $A(\mathbf{R})^0$ [Waldschmidt 1991].

Remark. The p-adic analogue of Conjecture 5 (and hence also of Conjecture 1) is false, since given any simple abelian surface A over $\mathbf{Q}$ whose Mordell–Weil rank is equal to 1, the topological closure of $A(\mathbf{Q})$ in $A(\mathbf{Q}_p)$ is a p-adic Lie group on one parameter and therefore is not open in $A(\mathbf{Q}_p)$. Here is a nice explicit example of this, taken from [Gordon and Grant 1991, §4]—in fact, the only example currently known to me. Let C be the curve

$$y^2 = x(x-1)(x-2)(x-5)(x-6),$$

and let $A_{/\mathbf{Q}}$ denote its jacobian. Then, by [Gordon and Grant 1991, Theorem 2], $A(\mathbf{Q})$ is isomorphic to $\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^4$.

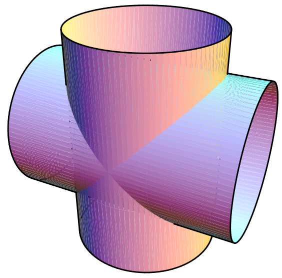
(The method of Gordon and Grant involves a computer search where 65536 separated cases are examined. It would be useful to develop a more conceptual descent argument to cover this and perhaps a number of other abelian varieties; it would also be interesting to buttress the descent argument with a check that the L function of A has a simple zero at $s = 1$, in accord with the Birch–Swinnerton-Dyer conjecture.)

The abelian variety A is simple over $\mathbf{Q}$. This is because (i) all of its 2-torsion is $\mathbf{Q}$-rational, and (ii) the order of $A(\mathbf{F}_{11})$ is 176 [Gordon and Grant 1991]. Since A has good reduction at 11, if $A_{/\mathbf{F}_{11}}$ were isogenous to a product of elliptic curves over $\mathbf{F}_{11}$, (i) would mean that each of the factor elliptic curves would have some nontrivial 2-torsion that is $\mathbf{F}_{11}$-rational, and (ii) would mean that one of these factors would have an $\mathbf{F}_{11}$-rational point of order 11. This factor then would have at least 22 $\mathbf{F}_{11}$-rational points, more than $1 + 11 + 2\sqrt{11}$, which is a contradiction.

8. SOME KUMMER SURFACES

We begin with a brief description of the basic geometry underlying Kummer surfaces. Let $A_{/\mathbf{Q}}$ be an abelian surface, and let $W = W_A$ be its associated Kummer surface, that is, if $\overline{W}$ is the quotient of A under the action of the involution $\alpha \mapsto -\alpha$, then W is obtained from $\overline{W}$ by blowing up (once) the image in $\overline{W}$ of each of the sixteen 2-torsion points of A. The variety W is proper and smooth and defined over $\mathbf{Q}$. If χ is any quadratic Dirichlet character, and $A_\chi/\mathbf{Q}$ is the abelian variety A twisted via the character χ, we have a canonical identification $W_A = W_{A_\chi}$. For any two quadratic characters χ_1 and χ_2 of the same sign (that is, satisfying $\chi_1(-1) = \chi_2(-1)$), we may identify the real loci $A_{\chi_1}(\mathbf{R}) = A_{\chi_2}(\mathbf{R})$. In particular, if χ is a quadratic character such that $\chi(-1) = 1$, then $A_\chi(\mathbf{R}) = A(\mathbf{R})$; we shall also use the abusive notation of $A(i\mathbf{R})$ for the locus of points $A(\mathbf{R})$ where χ is any choice of quadratic character with $\chi(-1) = -1$. $A(\mathbf{R})$ and $A(i\mathbf{R})$ have the same number of connected components, namely, either 1, 2, or 4 (one-quarter of the number of real 2-torsion points in A).

If we define $A^*(\mathbf{R})$ as the complement in $A(\mathbf{R})$ of the 2-torsion points, and likewise $A^*(i\mathbf{R})$, the topological closure in $W_A(\mathbf{R})$ of the image of each connected component of $A^*(\mathbf{R})$ or of $A^*(i\mathbf{R})$ consists, topologically, of the complement in a two-sphere of the union of the interiors of four disjoint closed discs, a space that I like to think of as a plumbers' cross, or four-way pipe join:



We call each of these crosses, viewed as a closed submanifold (with boundary) in $W_A(\mathbf{R})$, a *compartment* of $W_A(\mathbf{R})$. An *even compartment* is the image of a connected component of $A^*(\mathbf{R})$, and an *odd compartment* is the image of a component of $A^*(i\mathbf{R})$. The compact closed two-manifold $W_A(\mathbf{R})$ is connected and is a union of ν compartments (whose interiors are mutually disjoint, even compartments being joined to odd compartments), for $\nu = 2$, 4 or 8, that is, one-half the number of real 2-torsion points in A. The *neutral compartments* are the (two) compartments containing the blowup of the image of the identity element in A.

Multiplication by $n \in \mathbf{Z}$ in A induces a rational mapping $\varphi_n : W_A \to W_A$ on the Kummer surface (defined over $\mathbf{Q}$), since it commutes with multiplication by -1. The rational mapping φ_n is regular on the complement of $2n$-torsion points. If n is odd, the restriction of φ_n to $W_A(\mathbf{R})$ preserves compartments (that is, if $\mathcal{K}$ is a compartment, and $\mathcal{K}' \subset \mathcal{K}$ is the subspace on which φ_n is defined, then $\varphi_n(\mathcal{K}') \subset \mathcal{K}$); if n is even, φ_n brings all of $W_A(\mathbf{R})$ to the two neutral compartments.

An elementary engine for the production of lots of rational points on the Kummer surface W is the following:

(a) Find some curve X of (geometric) genus 0 in W that is the image of $\mathbf{P}^1_{/\mathbf{Q}}$ and that isn't one of the exceptional curves obtained by the blowing-up process;
(b) apply to X the rational mappings φ_n, for $n \in \mathbf{Z}$, to obtain a family X_n, for $n \in \mathbf{Z}$, of rational images of $\mathbf{P}^1_{/\mathbf{Q}}$.

Definition. *For X as in* (a)*, let $\mathcal{X} \in \mathcal{W}(\mathbf{R})$ denote the topological closure in $W(\mathbf{R})$ of the union of rational points $\bigcup_{n\in\mathbf{Z}} X_n(\mathbf{Q})$ in $W(\mathbf{Q})$.*

Since $X_n(\mathbf{Q})$ is dense in $X_n(\mathbf{R})$, it follows that $\mathcal{X}$ is also the topological closure of $\bigcup_{n\in\mathbf{Z}} X_n(\mathbf{R})$ in $W(\mathbf{R})$.

Lemma. *For any rational curve X as in step* (a) *above, either*

(i) *the inverse image of X in A is an elliptic curve, or*
(ii) *the subspace $\mathcal{X} \subset \mathcal{W}(\mathbf{R})$ is a union of compartments.*

Proof: In particular, we will show the equivalent statement that if any of the real curves $X_n(\mathbf{R})$ meets the interior of any compartment $\mathcal{K} \subset \mathcal{W}(\mathbf{R})$, then $\mathcal{K} \subset \mathcal{X}$. We suppose, with no loss of generality, that $n = 1$ and that $\mathcal{K}$ is an even compartment. Let $Y \subset A$ be the inverse image of X. Since $X(\mathbf{R})$ meets the interior of an even compartment, it follows that $Y(\mathbf{R})$ meets some component of $A^*(\mathbf{R})$. In particular, $Y(\mathbf{R})$ is nonempty. Let Y_n, for $n \in \mathbf{Z}$, denote the image of the curve Y under the endomorphism of the abelian variety A given by multiplication by n. Then, for any $n \in \mathbf{Z}$, Y_n is a (possibly reducible) curve, defined over $\mathbf{Q}$, imbedded in A in such a manner that it is stabilized by the involution given by multiplication by -1 in the abelian variety A, and such that its projection to W identifies its quotient (under this involution) with X_n. To prove our lemma, it suffices to prove that the topological closure U of $\bigcup_{n\in\mathbf{Z}} Y_n(\mathbf{R})$ in $A(\mathbf{R})$ is open. To prepare for this, the reader might be amused to first prove that if G is a compact, two-dimensional, commutative Lie group and $U \subset G$ is topologically closed and closed under multiplication by $n \in \mathbf{Z}$, then U is a finite union of closed subgroups in G. Then, returning to our U (the topological closure of $\bigcup_{n\in\mathbf{Z}} Y_n(\mathbf{R})$ in $A(\mathbf{R})$), there are two possibilities: either U is open in $A(\mathbf{R})$, in which case we are done; or U is contained in a finite union of Lie groups of dimension one. In the latter case, $Y(\mathbf{R})$ has infinite intersection with infinitely many distinct translates of itself, which can happen only if Y is an elliptic curve. □

Now suppose we have a smooth curve C of genus two defined over $\mathbf{Q}$. Let $u : C \to C$ denote the hyperelliptic involution. Let $A_{/\mathbf{Q}}$ denote the jacobian of C, and $W = W_A$ its associated Kummer surface. The action of u on C induces an involution on S^2C, the symmetric square of the curve C; if we denote by S^2C/u the quotient surface under the involution of S^2C that sends (a, b) to $(u(a), u(b))$, then S^2C/u is defined over $\mathbf{Q}$. We have a natural mapping $\eta : C \times C \to S^2C/u$, and a birational map (over $\mathbf{Q}$) $\beta : S^2C/u \to W$ whose composition with η sends $(a, b) \in C\times C$ to the image in W of the linear equivalence class of the divisor $(a) - (b)$ on C, which has degree zero. The birational map β comes from an actual morphism from S^2C/u to $\overline{W}$, the quotient of A under the action of multiplication by -1. This latter morphism can be seen to be regular off the diagonal curve in S^2C/u, and it sends that diagonal curve to the image of $0 \in A$ in $\overline{W}$. We also have an involution σ of S^2C/u (defined over $\mathbf{Q}$) induced from the involution $(a, b) \mapsto (a, ub)$ on $C \times C$. The quotient of S^2C/u by the action of this involution σ is easily seen to be isomorphic to the symmetric square of the genus-zero curve C/u, and hence to be isomorphic (at least over $\mathbf{C}$) to a rational surface. Conjugating the involution σ by the birational map β yields a rational map $\tau : W \to W$ of order two, defined over $\mathbf{Q}$ ("rational" in the sense that it is not everywhere defined as a morphism). This exhibits the map W, at least birationally, as a double cover of a surface that, over $\mathbf{C}$, is birationally isomorphic to $\mathbf{P}^2$.

We now turn to some applications of the lemma just proved. First consider the morphism $C \to W$ given, on a suitable affine open set, by the composition

$$C \xrightarrow{\iota} C\times C \to S^2C/u \xrightarrow{\beta} W,$$

where ι is the inclusion $C \to C \times C$ given by the formula $\iota(a) = (a, ua)$. Denote by X the image of C in W under this composition. Then X is isomorphic to the quotient curve C/u. The curve C/u is isomorphic over $\mathbf{Q}$ to $\mathbf{P}^1$, an isomorphism being induced by the rational function $f = \omega_1/\omega_2$ on C, where ω_1, ω_2 are two linearly independent differentials of the first kind on C, each defined over $\mathbf{Q}$. Hence the curve X is isomorphic over $\mathbf{Q}$ to $\mathbf{P}^1$. We may therefore apply the lemma to $X \subset W$; in particular, it is alternative (ii) that holds, giving us that the $\mathbf{Q}$-rational points of W lying in the compartments whose interiors meet $X(\mathbf{R})$ are dense in those compartments.

Now suppose that $c_0 \in C$ is a $\mathbf{Q}$-rational Weierstrass point, and consider the morphism which, on an affine open, is given by the composition

$$C \xrightarrow{j} C\times C \to S^2C/u \xrightarrow{\beta} W,$$

where the morphism j is given by $j(a) = (a, c_0)$. Denoting by X_{c_0} the image of C under the above composition, we are again in a position to apply our lemma, the conclusion being that the $\mathbf{Q}$-rational points of W lying in compartments whose interiors meet $X_{c_0}(\mathbf{R})$ are dense in those compartments.

If ν is the number of fixed points of the involution u on C that are defined over $\mathbf{R}$ (that is, $\nu =$ 0, 2, 4 or 6, the number of real Weierstrass points of C), one can compute in a straightforward manner the following quantities: the order α of the group of real 2-torsion in A; the number κ of distinct compartments $\mathcal{K}$ of $W(\mathbf{R})$; and (if $\nu > 0$) the number γ of compartments of $W(\mathbf{R})$ whose interiors meet $X_{c_0}(\mathbf{R})$, for c_0 any real Weierstrass point. The results are:

ν	0	2	4	6
α	4	4	8	16
κ	2	2	4	8
γ	–	2	4	6

As a sample of what can be obtained from the preceding discussion, consider the following corollary.

Corollary. *Let $g_5(x) \in \mathbf{Q}[x]$ be a monic quintic polynomial with rational coefficients and distinct roots, and with the further property that not all of its roots are real. Let C denote the smooth projective model attached to the affine plane curve $y^2 = g_5(x)$, and let $W_{/\mathbf{Q}}$ be its associated Kummer surface. Then the $\mathbf{Q}$-rational points of W are dense in the real locus of W.*

Proof: Having written our genus-two curve C as above, we have insured that the unique point at ∞ is a $\mathbf{Q}$-rational Weierstrass point, and therefore that $\nu = 2$ or 4. Taking $c_0 = \infty$, we see from the preceding table that X_{c_0} meets the interior of every compartment of $W(\mathbf{R})$, and therefore, by the lemma, the $\mathbf{Q}$-rational points of W are dense in $W(\mathbf{R})$. □

One case that eludes this kind of analysis is when all the roots of $g_5(x)$ are real and none are in $\mathbf{Q}$. In this case, we have shown by the preceding discussion that there are eight compartments, six of which are densely filled with rational points. What about the other two compartments? (This case would seem to yield a clean test case of Conjecture 1.)

9. SOME OTHER K3 SURFACE EXAMPLES

Given a K3 surface V or, for that matter, any variety possessing an infinite group of automorphisms $\mathcal{A}$ acting on it (defined over $\mathbf{Q}$), it is natural to consider the structure of orbits of rational points under the action of $\mathcal{A}$. This would suggest that one try to obtain, beforehand, some understanding of the action of $\mathcal{A}$ on the real locus. An elegant special case in which it is tempting to do this is for the 18-dimensional family of K3 surfaces, originally considered in [Wehler 1988], and taken up again by Silverman [1991a], who studies $\mathbf{Q}$-rational points on such K3 surfaces. Silverman develops an arithmetic theory surprisingly analogous in format to the arithmetic of abelian varieties.

A *Wehler K3 surface* is a smooth surface S contained in $\mathbf{P}^2 \times \mathbf{P}^2$ given by the intersection of two effective divisors, one of bidegree $(1,1)$, and the other of bidegree $(2,2)$. The projections of S to each of the two factors $\mathbf{P}^2$ are each of degree 2, and therefore each projection determines an involution of S. Let $\mathcal{G}$ denote a subgroup of automorphisms of S generated by these two involutions. The group $\mathcal{G}$ is shown to be the free product of the two cyclic groups of order 2 generated by the two involutions [Wehler 1988]. Silverman has begun some numerical studies of the dynamics of the action of this group $\mathcal{G}$ on the two-manifold of real points of S.

As a specific numerical example, Silverman takes for S the locus of common zeroes of the form

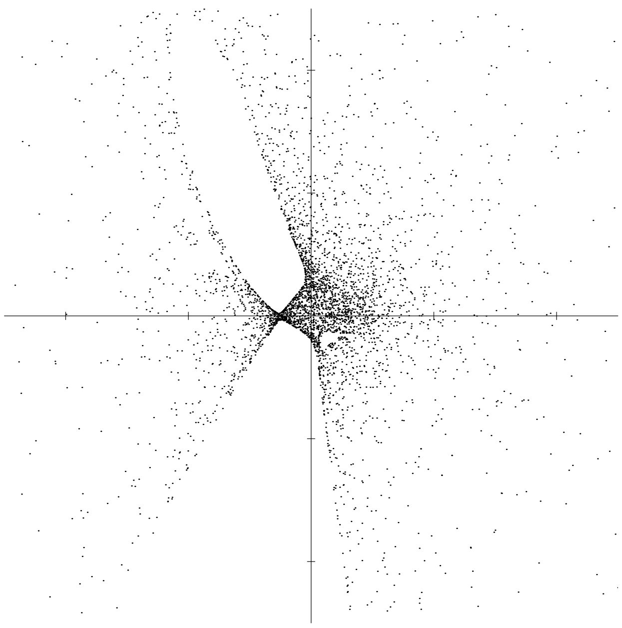
$$L(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2 + x_1y_1$$

on $\mathbf{P}^2 \times \mathbf{P}^2$ of bidegree $(1,1)$, and of the "randomly chosen" form Q of bidegree $(2,2)$ explicitly given in [Silverman 1991a, §5].

Starting with the $\mathbf{Q}$-rational point

$$P = ([12, 1, -20].[2, -4, 1])$$

Silverman plotted two-dimensional projections of the orbit of P under the action of $\mathcal{G}$. The picture reproduced below, courtesy of Curt McMullen, is of this same orbit, taken to 5000 iterations and projected onto the (x_1, x_2)-plane (the range shown is $-5 \le x_1, x_2 \le 5$). The two empty regions are those not in the image of the real locus.



Silverman also suggested doing numerical studies of the dynamics in K3's where the automorphism group is even richer; for example, consider a smooth surface S given by a form of tridegree $(2,2,2)$ in $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$. The surface S is a K3 and projects as a double cover to each of the three $\mathbf{P}^1 \times \mathbf{P}^1$'s as a result of deleting a factor in $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$. This gives three involutions on S, which generate a free product of three cyclic groups of order 2.

REFERENCES

[Colliot-Thélène 1977] J.-L. Colliot-Thélène, "Points rationnels sur les surfaces cubiques et composantes réelles (d'après H. P. F. Swinnerton-Dyer)" (unpublished typescript), 1977.

[Colliot-Thélène 1986] J.-L. Colliot-Thélène, "Arithmétique des variétés rationnelles et problèmes birationnels", pp. 641–653, *Proc. Int. Cong. Math.*, Berkeley, CA, 1986.

[Colliot-Thélène 1990] J.-L. Colliot-Thélène, "Surfaces rationnelles fibrées en coniques de degré 4", pp. 43–55, *Sém. Théor. Nombres Paris 1988–1989*, Birkhäuser, Boston, 1990.

[Colliot-Thélène and Sansuc 1982] J.-L. Colliot-Thélène and J.-J. Sansuc, "Sur le principe de Hasse et l'approximation faible, et sur une hypothèse de Schinzel", *Acta Arith.* **41** (1982), 33–53.

[Colliot-Thélène and Sansuc 1987] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles II", *Duke Math. J.* **54** (1987), 375–492.

[Colliot-Thélène et al. 1987] J.-L. Colliot-Thélène, J.-J. Sansuc, and H. P. F. Swinnerton-Dyer, "Intersections of two quadrics and Châtelet surfaces", *J. Reine Angew. Math.* **373** (1987), 37–107 (part I) and **374** (1987), (part II), 72–168.

[Colliot-Thélène and Skorobogatov 1987] J.-L. Colliot-Thélène and A. N. Skorobogatov, "R- equivalence on conic bundles of degree 4", *Duke Math. J.* **54** (1987), 671–677.

[Davis et al. 1976] M. Davis, Y. Matijasevic and J. Robinson, "Diophantine equations: Positive aspects of a negative solution", *Proc. Symp. Pure Math.* **28**, 323–378.

[Flath and Wagon 1991] D. Flath and S. Wagon, "How to pick out the integers in the rationals: An application of number theory to logic", *Amer. Math. Monthly* **98** (1991), 812–823.

[Gordon and Grant 1991] D. Gordon and D. Grant, "Computing the Mordell–Weil rank of Jacobians of curves of genus two" (preprint), University of Colorado, Boulder, 1991.

[Hironaka 1975] H. Hironaka, "Triangulations of algebraic sets", pp. 165–185, *Proc. Sympos. Pure Math.* **29**, Amer. Math. Soc., Providence, RI, 1975.

[Lojasiewicz 1964] S. Lojasiewicz, "Triangulation of semi-analytic sets", *Ann. Scuola Norm. Sup. Pisa* **18** (1964), 449–474.

[Manin 1986] Yu. Manin, *Cubic Forms, Algebra, Geometry, Arithmetic* (2nd ed.), North-Holland, Amsterdam, 1986.

[Manin 1990] Yu. Manin, *Algebraic Varieties With Many Rational Points*, Lecture Notes, MIT, Cambridge, MA, 1990.

[Manin 1991] Yu. Manin, "Notes on the arithmetic of Fano threefolds" (preprint no. 656), University of Utrecht, Utrecht, April 1991.

[Rohrlich 1992] D. Rohrlich, "Variation of the root number in families of elliptic curves" (preprint), Boston University, Boston, 1992.

[Salberger and Skorobogatov 1991] P. Salberger and A. N. Skorobogatov, "Weak approximation for surfaces defined by two quadratic forms", *Duke Math. J.* **63** (1991), 517–536.

[Silverman 1991a] J. Silverman, "Rational points on K3 surfaces: A new canonical height", *Invent. Math.* **105** (1991), 347–373.

[Silverman 1991b] J. Silverman, "Counting integer and rational points on varieties" (preprint), Brown University, Providence, RI, Dec. 1991.

[Swinnerton-Dyer 1962] P. Swinnerton-Dyer, "Two special cubic surfaces", *Mathematika* **9** (1962), 54–56.

[Waldschmidt 1991] M. Waldschmidt, "Transcendental numbers and functions of several variables" (preprint), Queen's University, Kingston, Ont., August 20, 1991.

[Wehler 1988] J. Wehler, "K3 surfaces with Picard number 2", *Arch. Math.* (*Basel*) **50** (1988), 73–82.

Barry Mazur, Department of Mathematics, Harvard University, Cambridge, MA 02138
(mazur@math.harvard.edu)

Received December 17, 1991; revised January 14, 1992