Enriques surfaces with a dense set of rational points, appendix to the paper by J.-L. Colliot-Thélène

Alexei Skorobogatov

The aim of this note is to deduce from the results of Bender and Swinnerton-Dyer [BS], as refined by Colliot-Thélène [CT], that rational points are Zariski dense on certain Enriques surfaces defined over a number field k, conditionally on the Schinzel Hypothesis (H) and the finiteness of Tate–Shafarevich groups of elliptic curves over k. It was shown by Bogomolov and Tschinkel [BT] that for any Enriques surface Y defined over a number field k there exists a finite extension K/k such that K-points are Zariski dense on Y ("potential density" of rational points). We intend to show that the results of [BS] and [CT] can be used to construct explicit families of Enriques surfaces over any number field k with the property that already k-points are Zariski dense. Although the general construction is conditional on the above mentioned conjectures, once an equation is written it is often possible to give a direct (and unconditional) proof of the Zariski density of rational points. We check this for the explicit example in the end of this note using an idea from [BT]. It is not known whether or not there exists an Enriques or $K3$-surface X over a number field k such that $X(k)$ is not empty but not Zariski dense in X.

Proposition 1. *Let k be a field of characteristic zero. Let $c, d \in k[t]$ be polynomials, $deg(c) = 2$, $deg(d) = 4$, $deg(c^2 - d) = 4$, such that $td(c^2 - d)$ is separable. Then there exists a regular minimal model Y of the affine surface*

$$y_1^2 = t(x - c(t)), \; y_2^2 = t(x^2 - d(t)) \tag{1}$$

which is an Enriques surface (hence Y is unique). Any $K3$ double covering of Y is given by $t = mu^2$, for some $m \in k^*$.

Proof. A standard argument (cf. [CSS97], Section 4) shows that for any discrete valuation $v : k(Y)^* \to \mathbf{Z}$, which is trivial on k, the valuation $v(t)$ is even. Indeed, if $v(t) > 0$, then $v(d) = v(c^2 - d) = 0$ by our assumption. If $v(x) \neq 0$, then from the second equation (1) we see that $v(t)$ is also even. The case $v(x) = 0$, $v(x - c) > 0$, $v(x^2 - d) > 0$ leads to $v(c^2 - d) > 0$, which is a contradiction. Hence either $v(x - c) = 0$ or $v(x^2 - d) = 0$, implying that $v(t)$ is even. Now if $v(t) = -l < 0$, then $v(c) = -2l$, $v(d) = -4l$, $v(c^2 - d) = -4l$. It is clear from the second equation (1) that if $v(x) \neq -2l$, then $v(t)$ is even. Suppose $v(x) = -2l$. In the case when $v(x^2 - d) > -4l$ and $v(x - c) > -2l$, we have $v(c^2 - d) > -4l$, which is a contradiction. Hence at least one of $x^2 - d$ and $x - c$ has even valuation, implying that $v(t)$ is even in all cases.

It follows that the divisor (t) on any regular model of (1), in particular, on Y, is a double, that is, $(t) = 2D$ for some $D \in Div(Y)$. Hence the double covering $X(m) \to Y$ given by $t = mu^2$, $m \in k^*$, is unramified. Let $y_1 = uw_1$, $y_2 = uw_2$, then $X(m)$ is given by the affine equations

$$w_1^2 = m(x - c(mu^2)), \; w_2^2 = m(x^2 - d(mu^2)) \tag{2}$$

The affine surface (2) is isomorphic to

$$w_2^2 = m^{-1}w_1^4 + 2c(mu^2)w_1^2 + m(c(mu^2)^2 - d(mu^2)) \tag{3}$$

Note that 0 is not a root of $d(t)$ and $c(t)^2 - d(t)$, hence $c(mu^2)$ and $c(mu^2)^2 - d(mu^2))$ are separable. Then it is easy to check that the affine surface (3) is regular. The projection to the coordinate u gives rise to a proper morphism $\pi : X(m) \to \mathbf{P}^1_k$. It is an easy local calculation (cf. [CT], Lemma 1.3.2, as we are exactly in the situation of that paper) that the conditions imposed on c and d ensure that

1) each fibre of π at a root of $d(mu^2) = 0$ is a rational curve with one node (fibre of type I_1);

2) each fibre at a root of $c(mu^2)^2 - d(mu^2) = 0$ is the union of two rational curves tranversally intersecting each other in two points (fibre of type I_2);

3) all other fibres of π, including the fibre at infinity, are smooth.

We shall write $X = X(m)$, $\overline{X} = X \times_k \overline{k}$, where $\overline{k}$ is an algebraic closure of k. The topological Euler characteristic $e(\overline{X})$ equals $8 \times 2 + 8 = 24$ (see, e.g. [BPV], Prop. 11.4, p. 97). The canonical class K_X can be written as $\pi^*(nP)$, where P is a k-point on $\mathbf{P}^1_k$, $n = \chi(\mathcal{O}_X) - 2$, and $\chi(\mathcal{O}_X)$ is the Euler characteristic of the structure sheaf on X ([BPV], Cor. 12.3, p. 162). In any case $(K_X)^2 = 0$, and hence the formula $(K_X)^2 + e(\overline{X}) = 12\chi(\mathcal{O}_X)$ implies that $\chi(\mathcal{O}_X) = 2$. Now the above formula for the canonical class gives $K_X = 0$. This implies $H^2(X, \mathcal{O}_X) = 1$, hence $H^1(X, \mathcal{O}_X) = 0$. This proves that $X = X(m)$ is a $K3$-surface. It is one of the equivalent definitions of Enriques surfaces that these are the surfaces with a $K3$ unramified double covering. In particular, Y is an Enriques surface. QED

Proposition 2. *Suppose that $m \in k^* \setminus k^{*2}$, and that $d(mu^2)$ and $c(mu^2)^2 - d(mu^2)$ are irreducible polynomials, such that the fields $K_1 = k[u]/(d(mu^2))$ and $K_2 = k[u]/(c(mu^2)^2 - d(mu^2))$ do not contain quadratic extensions of k. Then the elliptic $K3$-surface $X(m)$ satisfies the assumptions (1), (2), (3.a) and (3.b) of Theorem A of* [CT]. *If $m(c(mr^2)^2 - d(mr^2)) \in k^{*2}$ for some $r \in k$, then $X(m)$ has a k-point.*

Proof. Assumptions (1) and (2) clearly hold since m is a non-square constant. Assumption (3.a) says that the natural map $k^*/k^{*2} \to K_1^*/K_1^{*2}$ is injective. Non-trivial elements of its kernel correspond to quadratic extensions of k contained in K_1, and we assumed that there are none. For the same reason $k^*/k^{*2} \to K_2^*/K_2^{*2}$ is injective. Assumption (3.b) which asserts the injectivity of $k^*/\langle k^{*2}, m\rangle \to K_2^*/\langle K_2^{*2}, m\rangle$, is then obviously satisfied. If $r, s \in k$ are such that $m(c(mr^2)^2 - d(mr^2)) = s^2$, then $w_1 = 0$, $w_2 = s$, $u = r$, $x = c(mr^2)$ is a solution of (2). Since (2) defines a smooth affine surface, this point gives rise to a k-point on $X(m)$. QED

Lemma. *Let $f(t)$ be an irreducible polynomial of even degree n with Galois group $G \subset S_n$. Then $k_f = k[t]/(f(t))$ contains a quadratic extension of k if and only if $G \cap S_{n-1}$ is contained in a subgroup of G of index 2.*

Proof. Call K the splitting field of $f(t)$, then we have $Gal(K/k) = G$. Let $H = G \cap S_{n-1}$, then the field k_f is recovered as the field of invariants $k_f \simeq K^H$. If $k \subset L \subset k_f \subset K$, where $[L : k] = 2$, then the corresponding sequence of subgroups of G reads as $G \supset F \supset H \supset 1$, for some index 2 subgroup $F \subset G$. QED

Corollary. *Assume the Schinzel Hypothesis (H) and the finiteness of the Tate–Shafarevich groups of elliptic curves over $\mathbf{Q}$. Suppose that $c(t), d(t) \in \mathbf{Q}[t]$ satisfy the following conditions:*

(a) $deg(c(t)) = 2$, $deg(d(t)) = 4$, $deg(c(t)^2 - d(t)) = 4$, and $td(t)(c(t)^2 - d(t))$ is separable;

(b) $d(t)$ and $c(t)^2 - d(t)$ are irreducible with Galois group isomorphic to S_4;

(c) $d(-u^2)$ and $c(-u^2)^2 - d(-u^2)$ are irreducible with Galois group isomorphic to the semi-direct product of $(\mathbf{Z}/2)^4$ and S_4, where S_4 acts on $(\mathbf{Z}/2)^4$ by permutations of factors;

(d) $d(0) - c(0)^2 \in \mathbf{Q}^{*2}$.

Then $\mathbf{Q}$-rational points are Zariski dense on the Enriques surface Y defined by (1).

Proof. Set $m = -1$. In the notation of the previous proof G is the semi-direct product of $(\mathbf{Z}/2)^4$ and S_4, where S_4 acts on $(\mathbf{Z}/2)^4$ by permutations of factors. Hence H is the semi-direct product of $(\mathbf{Z}/2)^3$ and S_3. It is clear that H is not contained in a subgroup of G of index 2: such a subgroup is normal, but the conjugates of H generate G. Proposition 2 now shows that all the conditions of Theorem A of [CT] are satisfied for $X(-1)$. Our condition (d) implies that $X(-1)$ has a $\mathbf{Q}$-point with $u = 0$. Hence Theorem A of [CT] implies that $\mathbf{Q}$-points are Zariski dense on $X(-1)$, and hence also on Y. QED

Conditions (a), (b) and (c) are satisfied for "generic" coefficients of $d(t)$ and $c(t)$. If one takes

$$d(t) = t^4 + t^2 + t + 5, \quad c(t) = 2(t^2 + 1),$$

then (a) and (d) hold. On the other hand, the Galois groups of $d(t)$ and $c(t)^2 - d(t)$ are of order 24, hence isomorphic to S_4. That of $d(-u^2)$ and $c(-u^2)^2 - d(-u^2)$ are of order $384 = 24 \times 16$ (computed using MAGMA package). The Galois group of any polynomial $f(u^2)$, where $deg(f) = 4$, is contained in the semi-direct product of $(\mathbf{Z}/2)^4$ and S_4. Hence the Galois groups of $d(-u^2)$ and $c(-u^2)^2 - d(-u^2)$ are equal to this semi-direct product. Thus (b) and (c) also hold. Condition (d) is obviously satisfied. We conclude that the Enriques surface given by

$$y^2 = tx^4 + 4t^2(t^2 + 1)x^2 + t^3(3t^4 + 7t^2 - t - 1) \tag{4}$$

should have a Zariski dense set of $\mathbf{Q}$-rational points. In fact, this can be rigourously proved.

Proposition 3. *The surface (4) has a Zariski dense set of rational points.*

Proof. It will be easier to work with the $K3$-covering of (4) given by $t = -u^2$. This surface $X = X(-1)$ is given by

$$w_2^2 = -w_1^4 + 4(u^4 + 1)w_1^2 - (3u^8 + 7u^4 + u^2 - 1) \tag{5}$$

The surface (5) contains the curve C of genus one given by $w_1 = u^2$. Its equation is

$$w_2^2 = -3u^4 - u^2 + 1 \tag{6}$$

Let us prove that $C(\mathbf{Q})$ is infinite. This curve contains the points $P = (1/2, 3/4)$ and $Q = (0, 1)$. Let us show that $P - Q$ has infinite order in the Jacobian of C. It is easier to work with the isogeneous curve $C_1 : \; z^2 = t(-3t^2 - t + 1)$, where the unramified covering of degree 2 is $f : C \to C_1$ is $t = u^2$, $z = uw_2$ (f will become an isogeny after an appropriate choice of base points). The standard procedure yields the coordinate change

$t = -3^{-3}(x+3)$, $z = 3^{-4}y$, and the equation of C_1 takes the standard form $y^2 = x^3+Ax+B$ with $A = -270$, $B = -27 \times 29$. Then $M = f(P)$ has coordinates $(x_M, y_M) = (33, 6 \times 27)$, and $f(Q)$ is a point of order 2 (when the origin of the group law on C_1 is the point at infinity). Since $y_M \neq 0$ and y_M^2 (which is even) does not divide $4A^3 + 27B^2$ (which is odd), we conclude that $M = f(P)$ has infinite order in C_1. Thus the same is true for $f(P) - f(Q)$, and hence $P - Q$ has infinite order in the Jacobian of C.

Consider the double covering $\phi : C \to \mathbf{P}^1_{\mathbf{Q}}$ given by projection to the coordinate u; this is just the restriction of $\pi : X \to \mathbf{P}^1_{\mathbf{Q}}$ to C. Let $\tau : C \to C$ be the corresponding involution, $\tau(u, w_2) = (u, -w_2)$. We note that $C(\mathbf{R})$ is connected, and since $C(\mathbf{Q})$ is infinite, $C(\mathbf{Q})$ is dense in $C(\mathbf{R})$ in the real topology. Let R be one of two real points of C with coordinate $w_2 = 0$ (ramification points of ϕ). There is a sequence $P_n \in C(\mathbf{Q})$ converging to R in the real topology. We observe that the fibre of π through R is a smooth curve of genus one, as $-3u^4 - u^2 + 1$ is coprime with the irreducible polynomials $d(-u^2)$ and $c(-u^2)^2 - d(-u^2)$. Then $\tau(P_n) - P_n$ has infinite order in the Jacobian of the fibre of π through P_n, provided $n > N$ for some positive N. Indeed, by Mazur's theorem the torsion of elliptic curves over $\mathbf{Q}$ is bounded. On the other hand, $\tau(P_n) - P_n$ tends to zero, hence cannot be torsion for $n > N$. (The key idea that when a ramification point lies on a smooth fibre, rational points are Zariski dense, is taken from [BT].)

We have found infinitely many $\mathbf{Q}$-fibres of $\pi : X \to \mathbf{P}^1_{\mathbf{Q}}$, each with infinitely many $\mathbf{Q}$-rational points. This implies the density of $\mathbf{Q}$-rational points of X in the Zariski topology. QED

Remarks. 1. We used Mazur's theorem to simplify the argument, without any doubt one can find a proof not based on this theorem.

2. It should be possible to construct similar examples for Enriques surfaces given by

$$y_1^2 = f(t)(x^2 - c(t)),\ y_2^2 = f(t)(x^2 - d(t))$$

where f, c, d, $c - d$ are all of degree 2 such that $fcd(c - d)$ is a separable polynomial (cf. [CSS97], Example 4.1.2 and Remark 5.3.1). In this case the conditional result pointing to the Zariski density of rational points is proved in [CSS98].

3. The morphism $Y \to \mathbf{P}^1_k$ has two double fibres. It is proved in ([CSS97], Cor. 2.4) that if a pencil of curves of genus one defined over a number field k has at least 5 (geometric) double fibres, then all k-points are contained in finitely many k-fibres, and hence are not Zariski dense.

I would like to thank Sir Peter Swinnerton-Dyer for showing me the curve (6), and Jean-Louis Colliot-Thélène for useful discussions.

References

[BPV] W. Barth, C. Peters, A. Van de Ven. *Compact complex surfaces.* Springer–Verlag, 1984.

[BS] A.O. Bender and Sir Peter Swinnerton-Dyer. *Solubility of certain pencils of curves of genus 1, and of the intersection of two quadrics in* $\mathbf{P}^4$. Proc. London Math. Soc., to appear.

[BT] F.A. Bogomolov and Yu. Tschinkel. *Density of rational points on Enriques surfaces.* Math. Res. Lett. **5** (1998) 623–628.

[CT] J.-L. Colliot-Thélène. *Hasse principle for pencils of curves of genus one whose Jacobians have a rational 2-division point*, this volume.

[CSS97] J.-L. Colliot-Thélène, A.N. Skorobogatov and Sir Peter Swinnerton-Dyer. *Double fibres and double covers: paucity of rational points.* Acta Arithm. **79** (1997) 113–135.

[CSS98] J.-L. Colliot-Thélène, A.N. Skorobogatov and Sir Peter Swinnerton-Dyer. *Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points.* Inv. Math. **134** (1998), 579–650.

Department of Mathematics
Imperial College
180 Queen's Gate
London SW7 2BZ
U.K.