Chapter 3

Density results for Kummer surfaces

In the preprint [38], Sir Peter Swinnerton-Dyer has given two non-singular diagonal quartic surfaces over $\mathbb{Q}$ together with a proof that their rational points lie dense in the space of 2-adic points. A detailed proof of Swinnerton-Dyer's theorem was given in chapter 2. To the author's best knowledge, Swinnerton-Dyer's result provides the first proof of p-adic density of rational points on any K3 surface over $\mathbb{Q}$, for any prime number p. The goal of this chapter is to extend the results of Swinnerton-Dyer to all prime numbers p, giving for each p an infinite number of K3 surfaces over $\mathbb{Q}$ on which the rational points form a p-adically dense set.

The K3 surfaces for which we will obtain p-adic density results are Kummer surfaces. For an abelian variety B over a field of characteristic different from 2, let $\mathrm{Km}(B)$ denote the Kummer variety of B. It is the blow-up of the quotient $B/\langle -1\rangle$ in the image of the 2-torsion of B. When B is an abelian variety of dimension 2, the surface $\mathrm{Km}(B)$ is a K3 surface.

We will establish the following results.

Theorem 3.1. *Let p be a prime number. Then there exist infinitely many pairwise non-isomorphic Kummer surfaces X of the form $\mathrm{Km}(E \times E)$, with E an elliptic curve over $\mathbb{Q}$, such that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{R})$.*

Theorem 3.2. *Let p and q be distinct prime numbers not equal to 3. Then there exist infinitely many pairwise non-isomorphic Kummer surfaces X of the form $\mathrm{Km}(E \times E)$, with E an elliptic curve over $\mathbb{Q}$, such that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_q) \times X(\mathbb{R})$.*

Theorem 3.3. *There exists an elliptic curve E over $\mathbb{Q}$ and a set S of 331 prime numbers, such that, if X is the Kummer surface $\mathrm{Km}(E \times E)$, we have $X(\mathbb{Q})$ dense in $\prod_{p \in S} X(\mathbb{Q}_p)$.*

Theorem 3.4. *There exists an elliptic curve E over $\mathbb{Q}$ such that the set of rational points of $\mathrm{Km}(E \times E)$ lies dense in the space of p-adic points for all prime numbers p with $p \equiv 3 \pmod 4$ and $p > 7$.*

Theorem 3.5. *For an elliptic curve E over $\mathbb{Q}$ such that $\#E(\mathbb{Q})[2] = 2$, the set of rational points of $\mathrm{Km}(E \times E)$ lies dense in the space of p-adic points for infinitely many p.*

The proofs will be given in the present chapter. The proofs of Theorems 3.1 and 3.2 are given at the end of Section 3.4. Theorem 3.3 is proven in Section 3.5. Theorem 3.4 is proven in Section 3.6. Theorem 3.5 is proven in Section 3.7.

We will treat the archimedean completion $\mathbb{R}$ of $\mathbb{Q}$ as well as the non-archimedean completions $\mathbb{Q}_p$ for every prime p. Our terminology will be such that, for every number field k, we will take a prime of k to mean a place of k, i.e. an equivalence class of absolute values on $\mathbb{Q}$, two absolute values $|\cdot|_1$ and $|\cdot|_2$ being considered equivalent if and only if there exists a real number e such that $|x|_1 = |x|_2^e$ for all $x \in k$. We will take a prime to mean either a prime of $\mathbb{Q}$, in the sense defined above, or a prime number $p \in \mathbb{Z}_{\geq 0}$.

3.1 Birational invariance of density results

By a variety over a field k we shall mean a scheme that is separated and of finite type over k. For a number field k and a prime v of k, we denote by k_v the completion of k at v. If X is a variety over a number field k and S is a set of primes of k, we write $X(S) = \prod_{v \in S} X(k_v)$ to shorten notation. Unless stated otherwise, we will consider $X(k_v)$ as endowed with the analytic topology and $X(S)$ with the product topology.

Lemma 3.6. *Let X be a smooth geometrically integral variety over a number field k and let $Y \subset X$ be a non-empty Zariski open subset. If S is a finite set of primes of k and $U \subset X(S)$ is a non-empty open subset, then $U \cap Y(S)$ is non-empty.*

Proof. By definition of the product topology, the set U must contain a set $\prod_{v \in S} U_v$ with the $U_v \subset X(k_v)$ non-empty open sets. It is therefore enough

to show that if $U \subset X(k_v)$ is a non-empty open subset for some fixed v, then U cannot be contained in $Z(k_v)$, where we define Z as the complement of Y in X.

Suppose that $U \subset Z(k_v)$. We choose a point $z_0 \in U \cap Z(k_v)$. Let $t_1, \ldots, t_d$ denote a set of local parameters of X at z_0, where d is the dimension of X. By smoothness of X and the implicit function theorem, there exists a neighborhood U' of z_0 contained in U so that the map

$$\begin{aligned} \phi\colon U' &\to k_v^d \\ u &\mapsto (t_1(u), \ldots, t_d(u)) \end{aligned}$$

is a diffeomorphism onto its image. Since Z is a proper closed subset of X, there exists a function $g \in k(X)$ defined at z_0 that vanishes on Z. We view g as an element of the power series ring $k[[t_1, \ldots, t_d]]$ via the embedding of the local ring $\mathcal{O}_{X,z_0}$ into its completion $k[[t_1, \ldots, t_d]]$. We have that g converges on an open neighborhood of z_0 and by assumption, it must vanish on the non-empty open set $\phi(U')$ of k_v^d. But a power series that vanishes on an open neighborhood of $(0, \ldots, 0) \in k_v^d$ must be zero, which is a contradiction. □

If $f\colon Y \dashrightarrow X$ is a rational map between varieties over a number field k and $\Delta \subset Y(S)$ is some subset for some set S of primes of k, then we define the subset $f(\Delta)$ of $X(S)$ as

$$f(\Delta) = \{f(t) : \text{all } t \in \Delta \text{ for which } f(t) \text{ is defined}\}.$$

Proposition 3.7. *Let X and Y be geometrically integral varieties over a number field k and let S be a finite set of primes of k. Assume that $f\colon Y \dashrightarrow X$ is a birational map, and that $\Gamma \subset X(S)$ and $\Delta \subset Y(S)$ are subsets such that $f(\Delta) \subset \Gamma$ and $f^{-1}(\Gamma) \subset \Delta$. Then Γ is dense in $X(S)$ if and only if Δ is dense in $Y(S)$.*

Proof. The proof proceeds in four steps.

Step 0. By restricting the domain of f, we may assume that f is the inclusion of a non-empty Zariski open subset Y of X. The conditions $f(\Delta) \subset \Gamma$ and $f^{-1}(\Gamma) \subset \Delta$ now mean that f identifies Δ with a subset of Γ whose complement lies outside $f(Y(S))$.

Step 1. We claim that if $\Gamma \subset X(S)$ is dense, then $\Delta \subset Y(S)$ is dense. Since the v-adic topology is finer than the Zariski topology, the map $f\colon Y(S) \to X(S)$ is the inclusion of an open subset. Therefore if Γ is dense in $X(S)$, then $\Delta = \Gamma \cap Y(S)$ is dense in $Y(S)$.

Step 2. We claim that, under the assumption that X is smooth over k, the following is true: if $\Delta \subset Y(S)$ is dense, then $\Gamma \subset X(S)$ is dense. Let $U \subset X(S)$ be a non-empty open subset. We want to show that it contains the image of an element of Δ. By Lemma 3.6, the open subset $U \cap f(Y(S))$ of $f(Y(S))$ is non-empty, and by the assumption that $\Delta \subset Y(S)$ is dense it must contain the image of an element of Δ. This proves the claim.

Step 3. We claim that if $\Delta \subset Y(S)$ is dense, then $\Gamma \subset X(S)$ is dense, now without the smoothness assumption on X. For this step we combine the results of Step 1 and 2. By step 1, we may shrink Y if necessary; in particular, we may assume that Y is smooth over k. Now by resolution of singularities, there exists a smooth variety $\widetilde{X}$ over k, a morphism $\pi\colon \widetilde{X} \to X$, and an embedding $\widetilde{f}\colon Y \hookrightarrow \widetilde{X}$, such that the diagram

$$\begin{array}{ccc} Y & \xhookrightarrow{\widetilde{f}} & \widetilde{X} \\ \| & & \downarrow{\scriptstyle \pi} \\ Y & \xhookrightarrow{f} & X \end{array}$$

is commutative. So if $U \subset X(S)$ is a non-empty open subset, then $\pi^{-1}(U) \subset \widetilde{X}(S)$ is also a non-empty open subset. By the argument of the previous paragraph, the open subset $U \cap \widetilde{f}(Y(S))$ of $\widetilde{f}(Y(S))$ is then non-empty. It follows from the diagram that $U \cap f(Y(S))$ is also non-empty. Now arguing as in Step 2, we finish the proof. □

Corollary 3.8. *Let S be a set of primes and let X and Y be geometrically integral varieties over $\mathbb{Q}$ that are birational to each other. Then $X(\mathbb{Q})$ is dense in $\prod_{p\in S} X(\mathbb{Q}_p)$ if and only if $Y(\mathbb{Q})$ is dense in $\prod_{p\in S} Y(\mathbb{Q}_p)$.*

3.2 Procyclic and topologically cyclic groups

In this section, we recall the definitions of profinite and procyclic groups, and gather some facts about these. We will also introduce "topologically cyclic" groups (Definition 3.10). This term is non-standard, but will be very useful to us.

Definition 3.9. A topological group G is called profinite if it is an inverse limit

$$G = \varprojlim_{i\in I} G_i,$$

where the G_i are finite, and the topology on G is the coarsest topology such that the quotient maps $G \to G_i$ are continuous. A topological group G is called procyclic if it is an inverse limit

$$G = \varprojlim_{i \in I} C_i,$$

where the C_i are finite cyclic, and the topology on G is the coarsest topology such that the quotient maps $G \to C_i$ are continuous.

Definition 3.10. If G is a topological group, we call a set $V \subset G$ a generator set of G if the closure of $\langle V \rangle$ is equal to G. We will call $g \in G$ a topological generator of G if $\{g\}$ is a generator set of G. If G has a topological generator, then we call G topologically cyclic.

Lemma 3.11. *A profinite group is procyclic if and only if it is topologically cyclic.*

Proof. Let G be a profinite group. By Corollary 1.1.8(a) of [26], we may assume that G is the limit of an inverse system (G_i, t_{ji}) where the G_i are finite and the transition maps $t_{ji} \colon G_j \to G_i$ are surjective. The result now follows from Lemma 2.5.3 of [26]. □

In general, the topologically cyclic groups do not define the same class of topological groups as the procyclic groups. This is shown by the example of the circle $\mathbb{R}/\mathbb{Z}$, which is generated topologically by the class of any irrational real number. It does not have any non-trivial finite quotients, since it is divisible. Hence it is certainly not profinite.

It is very easy to give a complete classification of procyclic groups. We define a supernatural number to be a formal product

$$\prod_p p^{n(p)},$$

where the product is taken over all prime numbers p, and where $0 \leq n(p) \leq \infty$ for each p. The natural numbers (not counting zero) are those supernatural numbers $\prod_p p^{n(p)}$ with $n(p) < \infty$ for each p and $n(p) = 0$ for almost all p. Note that with this definition, there is an obvious division relation on the set of supernatural numbers that extends the ordinary one on the natural numbers. We may therefore take greatest common divisors and least common multiples of supernatural numbers, and it makes sense to describe two supernatural numbers as being coprime or not.

Definition 3.12. The order of a profinite group G is the least common multiple of the finite supernatural numbers $(G : H)$, where H runs through the open normal subgroups of G.

Note that if G_1 is profinite of order n_1 and G_2 is profinite of order n_2, then $G_1 \times G_2$ is profinite of order $n_1 n_2$. A procyclic group is determined up to isomorphism by its order.

Proposition 3.13. *The following statements are true.*

(i) For each integer $n \in \mathbb{Z}_{\geq 0}$, the discrete group $\mathbb{Z}/p^n\mathbb{Z}$ is the unique procyclic group of order p^n, and the group $\mathbb{Z}_p$ equipped with the p-adic topology is the unique procyclic group of order p^∞.

(ii) For any supernatural number $\sigma = \prod_p p^{n(p)}$, there is a unique procyclic group G of order σ. Moreover, the group G is the direct product $\prod_p G_p$, where the product is taken over all prime numbers p, and where G_p is the unique procyclic group of order $p^{n(p)}$.

Proof. This follows from Theorem 2.7.1 from [26] and the discussion following immediately afterwards. □

As a corollary, we note:

Corollary 3.14. *Let G_1 be procyclic of order n_1 and let G_2 be procyclic of order n_2. If n_1 and n_2 are coprime, then $G_1 \times G_2$ is again procyclic.*

Proof. We can write G_1 and G_2 as products of procyclic groups of order p^n. Since n_1 and n_2 are coprime, the set of primes appearing in the product for G_1 is disjoint from the set of primes appearing in the product for G_2 by Proposition 3.13(ii). Again by Proposition 3.13(ii), the product of G_1 and G_2 is procyclic. □

In the rest of the chapter, we will be mainly concerned with topologically cyclic groups. The following result complements Corollary 3.14.

Proposition 3.15. *The following statements are true.*

(i) Let G_1 be procyclic and let G_2 be $\mathbb{R}/\mathbb{Z}$. Then $G_1 \times G_2$ is topologically cyclic.

(ii) Let G_1 be procyclic of order coprime to 2, and let G_2 be $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $G_1 \times G_2$ is topologically cyclic.

Proof. For part (i), we let g_i be a topological generator of G_i for $i \in \{1, 2\}$. Write $G = G_1 \times G_2$ and $g = (g_1, g_2)$. We prove that if $U \subset G$ is an open subset, then some multiple of g lies in U. By shrinking U we may suppose it is of the form $U = U_1 \times U_2$ with $U_i \subset G_i$ open for $i \in \{1, 2\}$. Furthermore, U_1 contains a translate of some open subgroup $H \subset G_1$. Therefore, it is enough to see that the quotient map

$$G \to G_1/H \times G_2$$

has dense image, where the first factor is a group of finite order n carrying the discrete topology. Since g_1 is a topological generator of G_1, for every coset c in G_1/H there exists an $m \in \mathbb{Z}$ such that $(m + kn)g_1$ maps to c for all $k \in \mathbb{Z}$. But the set

$$\{(m + kn)g_2 : k \in \mathbb{Z}\}$$

lies dense in G_2. Hence the image of the set of multiples of g is a dense set in G.

Part (ii) follows from part (i) by taking $G_1' = G_1 \times \mathbb{Z}/2\mathbb{Z}$ and $G_2' = \mathbb{R}/\mathbb{Z}$. We have $G_1 \times G_2 = G_1' \times G_2'$, and G_1' is procyclic by Corollary 3.14. Now apply part (i) to G_1' and G_2'. □

3.3 Elliptic curves with good twists

3.3.1 Notation and definitions

For the rest of this chapter, we fix an elliptic curve E over $\mathbb{Q}$. Most of our results will therefore be of the form "Assume that E satisfies (some list of properties), then (some conclusion) holds." We assume that E is given by the affine equation $y^2 = f(x)$, with $f(x)$ a separable polynomial of degree 3. Let us denote the complement of $E[2]$ in E by E°. If $c \in k^*$, then by E^c we denote the quadratic twist of E by c, and we assume that it is given by the equation $cy^2 = f(x)$.

The inversion -1 on each twist E^c restricts to an involution of $(E^c)^\circ$, which we will also denote by -1. For c in a field $\ell \supset k$, we let A^c be the variety $(E^c)^\circ \times (E^c)^\circ$ over ℓ. We set $A = A^1$. The A^c are thus non-empty Zariski open subsets of the abelian surfaces $E^c \times E^c$. The quotient $A/\langle -1 \rangle$, where -1 acts diagonally, is a smooth subvariety Y of $X = \mathrm{Km}(E \times E)$. We will identify the variety Y with the subvariety of $\mathbb{A}^3_{\mathbb{Q}}$, with coordinates (x_1, x_2, z), given by

$$z^2 = f(x_1)f(x_2), \quad z \neq 0. \tag{3.1}$$

With this choice of model, the maps q_c defined by

$$q_c \colon A^c \to Y$$
$$((x_1, y_1), (x_2, y_2)) \mapsto (x_1, x_2, cy_1y_2)$$

are the quotient maps for the involution -1 on A_c. Note that $q_1 \colon A \to Y$ is obtained by restricting the quotient rational map $E \times E \dashrightarrow X$ to A.

3.3.2 Partition of the rational points of a Kummer surface

The role played by the varieties A^c, the morphisms q_c and the open subset $Y \subset X$ is explained by the following lemma. It is stated very generally, but we will only apply it for $k = \mathbb{Q}$ and ℓ equal either to $\mathbb{Q}_p$ for some prime number p or to $\mathbb{R}$.

Lemma 3.16. *Let k be a field containing $\mathbb{Q}$, and let $k \subset \ell$ be a field extension.*

(i) For every set $\Gamma(\ell)$ of coset representatives of ℓ^*/ℓ^{*2}, we have

$$Y(\ell) = \coprod_{c \in \Gamma(\ell)} q_c(A^c(\ell)).$$

Moreover, a point $(\xi_1, \xi_2, \zeta) \in Y(\ell)$ lies in $q_c(A^c(\ell))$ if and only if $c \in f(\xi_1)\ell^{*2}$.

(ii) The maps q_c induce a natural bijection

$$\coprod_{c \in \Gamma(\ell)} q_c : \coprod_{c \in \Gamma(\ell)} A^c(\ell)/\langle -1 \rangle \xrightarrow{\sim} Y(\ell).$$

Proof. The second assertion follows from the first, since

$$q_c \colon A^c \to Y$$

is the quotient map for the involution -1 on A^c. For the first assertion, it suffices to show the following: for every $P \in Y(\ell)$, there exists a $c \in \ell^*$ such that $P \in q_c(A^c(\ell))$, and moreover c is unique up to multiplication by a square in ℓ^*. Let $P = (\xi_1, \xi_2, \zeta)$ be an element of $Y(\ell)$. There is a unique element $c \in \Gamma(\ell)$ such that $f(\xi_1)/c = \alpha^2$ for some $\alpha \in \ell^*$. Then (ξ_1, α) and $(\xi_2, \alpha\zeta/f(\xi_1))$ are elements of $(E^c)^\circ(\ell)$; furthermore the point

$$((\xi_1, \alpha), (\xi_2, \alpha\zeta/f(\xi_1)) \in A^c(\ell)$$

maps to P under q_c. Now for the uniqueness of c up to squares: an element in $A^c(\ell)$ that maps to P by q_c is of the form $((\xi_1, \eta_1), (\xi_2, \eta_2))$, and from $(\xi_1, \eta_1) \in (E^c)^\circ(\ell)$ it follows that $c\eta_1^2 = f(\xi_1)$, so we have $c \in f(\xi_1)\ell^{*2}$. This ends the proof. □

Remark 3.17. Since A has a natural structure of $\mathbb{Z}/2\mathbb{Z}$-torsor over Y, part (i) of Lemma 3.16 is a special case of [33, eq. (2.12)].

3.3.3 Elliptic curves with good twists

We begin by stating the most important definition of this chapter.

Definition 3.18. Let S be a set of primes.

(i) For $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$ and $c \in \mathbb{Q}^*$, we call E^c a good twist of E with respect to (d_p) and S if for each $p \in S$ we have $c \in d_p\mathbb{Q}_p^{*2}$, and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

(ii) We say E has good twists if, for all $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$, there is $c \in \mathbb{Q}^*$ such that E^c is a good twist of E with respect to (d_p) and S.

If $S = \{p\}$ for some prime p, and if E has good twists with respect to (d_p) and S, we will also say that E has good twists with respect to d_p and p, and if E has good twists with respect to $S = \{p\}$, we will also say that E has good twists with respect to p.

Theorem 3.20 will show: if the elliptic curve E over $\mathbb{Q}$ has good twists with respect to S, and we have $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $\prod_{p\in S} X(\mathbb{Q}_p)$. For all primes p, we will give many examples of elliptic curves with good twists with respect to p.

Remark 3.19. The condition $c \in d_p\mathbb{Q}_p^{*2}$ appearing in Definition 3.18 is equivalent to the twists E^c and E^{d_p}, considered as elliptic curves over $\mathbb{Q}_p$, being isomorphic over $\mathbb{Q}_p$. We may thus rephrase the fact of E having good twists with respect to S as follows: for all collections of twists $\{E^{d_p}\}_{p\in S}$ of E over $\mathbb{Q}_p$, there exists a twist E^c of E over $\mathbb{Q}$ that is isomorphic over $\mathbb{Q}_p$ to E^{d_p} for each $p \in S$, for which $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

3.3.4 From good twists to density results

Theorem 3.20. *Let S be a set of primes and let E be an elliptic curve over $\mathbb{Q}$ that has good twists with respect to S. Let $X = \mathrm{Km}(E \times E)$. Then $X(\mathbb{Q})$ is dense in $\prod_{p\in S} X(\mathbb{Q}_p)$.*

Proof. Let $P = (P_p)_{p\in S}$ be a point of $\prod_{p\in S} Y(\mathbb{Q}_p)$. Since E has good twists with respect to S, there exists a $c \in \mathbb{Q}^*$ such that $c \in f(x_1(P_p))\mathbb{Q}_p^{*2}$ for each $p \in S$ and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$. By Lemma 3.16, we have that for each $p \in S$, the point P_p is in the image of the map

$$q_c \colon A^c(\mathbb{Q}_p) \to Y(\mathbb{Q}_p),$$

hence P is in the image of the map

$$q_{c,S} \colon \prod_{p\in S} A^c(\mathbb{Q}_p) \to \prod_{p\in S} Y(\mathbb{Q}_p).$$

Since $A^c(\mathbb{Q})$ lies dense in $\prod_{p\in S} A^c(\mathbb{Q}_p)$, the set $q_{c,S}(A^c(\mathbb{Q}))$ lies dense around P. □

3.3.5 A partial converse to Theorem 3.20

In this section, we provide a converse to Theorem 3.20 in the case where $S = \{p\}$ and $p > 2$ (see Proposition 3.23). We need a lemma first.

Lemma 3.21. *Let p be a prime and let $\mathscr{E}$ be an elliptic curve over $\mathbb{Q}_p$. Then $\mathscr{E}(\mathbb{Q}_p)$ can be generated topologically by three elements. If $p > 2$, then $\mathscr{E}(\mathbb{Q}_p)$ can be generated topologically by two elements.*

Proof. By Proposition 1.14(i), we have a topological isomorphism

$$\mathscr{E}(\mathbb{Q}_p) \cong \mathbb{Z}_p \times G$$

for some finite abelian group G. It follows from [32, Theorem VI.6.1] that, for every prime ℓ, the ℓ-torsion subgroup $G[\ell] = \mathscr{E}(\mathbb{Q}_p)[\ell]$ is generated by at most 2 elements. Hence by the structure theorem for finitely generated abelian groups we have $G \cong C_1 \times C_2$, with C_1 and C_2 cyclic groups for which the order of C_1 divides that of C_2. It is clear that the elements $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are topological generators of $\mathbb{Z}_p \times C_1 \times C_2$.

For the second part, note that $G[p] = \mathscr{E}(\mathbb{Q}_p)[p]$ cannot equal $\mathscr{E}(\overline{\mathbb{Q}}_p)[p]$, since $\mathbb{Q}_p(\mathscr{E}[p])$ contains a primitive p-th root of unity $\zeta_p \notin \mathbb{Q}_p$ by the existence of the Weil pairing. Therefore, the order of C_1 is coprime to p. Then if we define the elements P and Q in $\mathbb{Z}_p \times C_1 \times C_2$ to be $P = (1,1,0)$ and $Q = (0,0,1)$, the elements P and Q correspond to topological generators of $\mathscr{E}(\mathbb{Q}_p)$. □

Remark 3.22. We give an example showing that the second part of Lemma 3.21 fails for $p = 2$. Take the elliptic curve $\mathscr{E}$ over $\mathbb{Q}_2$ defined by $y^2 = x^3 - x$. It has CM over $\mathbb{Q}_2(\sqrt{-1})$, so has potentially good reduction. Since the reduction is bad, it must be additive. We have $\mathscr{E}_0(\mathbb{Q}_2) \cong \mathbb{Z}_2$ by Theorem 1.1, and clearly $\mathscr{E}(\mathbb{Q}_2)[2]$ is isomorphic to the Klein four-group. Hence by Proposition 1.14(ii) we have

$$\mathscr{E}(\mathbb{Q}_2) \cong \mathbb{Z}_2 \times C_1 \times C_2,$$

where C_1 and C_2 are cyclic groups of even order. Hence $\mathscr{E}(\mathbb{Q}_2)$ needs 3 elements to generate it topologically.

Proposition 3.23. *If $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$ for some prime p greater than 2, then E has good twists with respect to p.*

Proof. Let $d \in \mathbb{Q}_p^*$ be arbitrary, we will show that E has a good twist with respect to d and p. By Lemma 3.21, we may choose elements $P, Q \in E^d(\mathbb{Q}_p)$ such that $\langle P, Q\rangle$ is dense in $E^d(\mathbb{Q}_p)$. We may assume that P and Q are not contained in $E^d(\mathbb{Q}_p)[2]$. Let $R \in X(\mathbb{Q}_p)$ be the image of the point (P, Q) under the map

$$q_d \colon A^d \to Y.$$

If $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$, then by Corollary 3.8 there exists a sequence $\{R_i\}_{i=1}^{\infty} \subset Y(\mathbb{Q})$ converging to R. By Lemma 3.16 there are $c_i \in \mathbb{Q}^*$ and $(P_i, Q_i) \in A^{c_i}(\mathbb{Q})$ such that $R_i = q_{c_i}((P_i, Q_i))$. Again by Lemma 3.16, we have $c_i \in f(x_1(R_i))\mathbb{Q}_p^{*2}$ and $d \in f(x_1(R))\mathbb{Q}_p^{*2}$, so we have $c_i \equiv d \pmod{\mathbb{Q}_p^{*2}}$ for i sufficiently large. We claim that for these values of i, we have that $\langle P_i, Q_i\rangle$ is dense in $E^{c_i}(\mathbb{Q}_p)$, and therefore that $E^{c_i}(\mathbb{Q})$ is dense in $E^{c_i}(\mathbb{Q}_p)$. For these values of i, we fix isomorphisms over $\mathbb{Q}_p$

$$\phi_i \colon E^{c_i} \xrightarrow{\sim} E^d$$

The images of P_i and Q_i under $\pm\phi_i$ converge to $\pm P$ and $\pm Q$. Since P and Q are topological generators of $E^c(\mathbb{Q}_p)$, we have that P_i and Q_i are topological generators of $E^{c_i}(\mathbb{Q}_p)$. □

3.4 Density results for Kummer surfaces

In this section, we give sufficient conditions on E to have good twists with respect to a prime p, and we show that there are many cases in which these conditions are satisfied. Secondly, we give sufficient criteria for E and a set of primes S that imply that E has good twists with respect to S. At the end of this section, we will derive Theorems 3.1 and 3.2 from these results.

3.4.1 Topologically cyclic groups and density results

Recall that E is given by $y^2 = f(x)$, with f separable and of degree 3.

Lemma 3.24. *Assume that $f(x) = x^3 + ax + b$. Let p be a prime number.*

(i) Assume $p = 2$, $v_2(a) > 0$, and $v_2(b) = 1$. Then for all $d \in \mathbb{Q}_2^*$, the topological group $E^d(\mathbb{Q}_2)$ is procyclic of order 2^∞.

(ii) Assume $p = 3$, $v_3(a) = 1$, and $v_3(b) > 1$. Then for all $d \in \mathbb{Q}_3^*$, the topological group $E^d(\mathbb{Q}_3)$ is procyclic of order $2 \cdot 3^\infty$.

(iii) Assume $p > 3$, $v_p(a) > 0$, $v_p(b) = 1$. If $p = 5$, assume $a \not\equiv \pm 10 \pmod{25}$; if $p = 7$, assume $b \not\equiv \pm 14 \pmod{49}$. Then for all $d \in \mathbb{Q}_p^*$, the topological group $E^d(\mathbb{Q}_p)$ is procyclic of order p^∞ or $3 \cdot p^\infty$. Both orders occur for some d.

(iv) Assume $p > 3$, $v_p(a) = 1$, $v_p(b) > 1$. If $p = 5$, assume $a \not\equiv \pm 10 \pmod{25}$. Then for all $d \in \mathbb{Q}_p^*$, the topological group $E^d(\mathbb{Q}_p)$ is procyclic of order $2 \cdot p^\infty$.

(v) Assume $p > 3$, $v_p(a) > 1$, $v_p(b) = 2$. Then for all $d \in \mathbb{Q}_p^*$, the topological group $E^d(\mathbb{Q}_p)$ is procyclic of order p^∞ or $3 \cdot p^\infty$. Both orders occur for some d.

Proof. Without loss of generality, we assume that d satisfies $v_p(d) \in \{0, 1\}$. For the j-invariant $j(E)$ of E, we have

$$j(E) = 2^8 \cdot 3^3 \cdot \frac{a^3}{4a^3 + 27b^2}, \tag{3.2}$$

and the discriminant Δ_d of the model $\mathcal{E}^d$ of E^d over $\mathbb{Z}_p$ given by $y^2 = x^3 + ad^2x + bd^3$ is

$$\Delta_d = -16d^6(4a^3 + 27b^2).$$

In all cases, we have $v_p(j(E)) \geq 0$ and $v_p(\Delta_d) > 0$. This implies that the reduction type of E at p is potentially good, hence either good or additive; moreover, if $\mathcal{E}^d$ is a minimal model of E at p, then the reduction of E must be additive. In case (i), Tate's algorithm gives the following: firstly, $\mathcal{E}^d$ is a minimal model of E^d for all d; secondly, if $v_2(d) = 0$ then E^d has Kodaira type II, if $v_2(d) = 1$ and $v_2(a) = 1$ then E^d has Kodaira type III*, if $v_2(d) = 1$ and $v_2(a) > 1$ then E^d has Kodaira type II*. In cases (ii)-(v), we have that $v_p(\Delta_d)$ is strictly less than 12. Hence in each case, the Weierstrass curve $\mathcal{E}^d$ is a minimal model of E^d, so E^d has additive reduction in all cases.

Since E^d has additive reduction for all d, it follows from [32, Theorem C.15.1] that $\Phi = E^d(\mathbb{Q}_p)/E_0^d(\mathbb{Q}_p)$, the component group of the special fibre

of the Néron model, is a group of order at most 4. It follows from Theorem 1.1 that $E_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$ in each of the cases (i)-(v) and for all d. We have the tautological exact sequence

$$0 \to E_0^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to \Phi \to 0. \tag{3.3}$$

Applying Proposition 1.14(ii) to (3.3) gives that $E^d(\mathbb{Q}_p)$ is topologically isomorphic to a subgroup of $\mathbb{Z}_p \times \Phi'$ with Φ' a subgroup of Φ. To determine Φ', the following strategy may be followed: first one determines the Kodaira type of E^d at p to get an upper bound for Φ, leaving only a finite number of possibilities for Φ', and then one uses the division polynomials of E^d to identify the isomorphism type of Φ'.

We prove part (i). By the fact that the Kodaira type of E^d is II, III* or II*, the group Φ is of order at most 2. Hence we are done if we can show $E^d(\mathbb{Q}_2)[2] = 0$ for all d. We do this with the 2-division polynomial ψ_2 of E^d, which is $\psi_2 = x^3 + ad^2x + bd^3$, whose Newton polygon has vertices $(0, 1 + 3v_p(d))$, $(1, v_p(a) + 2v_p(d))$, and $(3, 0)$, which shows that its three roots in $\overline{\mathbb{Q}}_2$ have valuation $1/3 + v_p(d)$, so do not lie in $\mathbb{Q}_2$.

We prove part (ii). Tate's algorithm gives that the Kodaira type of E^d is III if $v_3(d) = 0$ and III* if $v_3(d) = 1$. Hence Φ is of order at most 2. We use the 2-division polynomial $\psi_2 = x^3 + ad^2x + bd^3$ of E^d to prove that $E^d(\mathbb{Q}_3)[2] \cong \mathbb{Z}/2\mathbb{Z}$ for all d. The Newton polygon of ψ_2 shows that two of its roots in $\overline{\mathbb{Q}}_3$ have valuation $1/2 + v_p(d)$, so do not lie in $\mathbb{Q}_3$. The third one is the unique one with valuation $v_p(b) + v_p(d) - 1$, so by Galois theory it must lie in $\mathbb{Q}_3$.

In parts (iii)-(v) we have $p > 3$. Since E^d has potentially good reduction, and p is different from 2 and 3, the table from [32, C.15] enables us to determine the Kodaira type of E^d at p, and hence an upper bound for Φ, just by knowing $v_p(\Delta_d)$.

In case (iii), we have to show that $E^d(\mathbb{Q}_p)[2] = 0$ for all d, while both $E^d(\mathbb{Q}_p)[3] = 0$ for some d and $E^d(\mathbb{Q}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$ for some d. We find from the table in [32, C.15] that the curve E^d has Kodaira type II if $v_p(d) = 0$ and Kodaira type IV* if $v_p(d) = 1$. In the first case, the component group is trivial, so $E^d(\mathbb{Q}_p) = E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ is procyclic of order p^∞ as claimed. In the second case, the group Φ has order 1 or 3, so $E^d(\mathbb{Q}_p)$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/3\mathbb{Z}$, so indeed procyclic of order p^∞ or $3 \cdot p^\infty$. We show that both possibilities occur. We therefore investigate the 3-division polynomial ψ_3^d of E^d. Its Newton polygon shows that ψ_3^d has a unique zero $x_d \in \overline{\mathbb{Q}}_2$ of valuation $2v_p(a) + v_p(d) - 1$, which is therefore defined over $\mathbb{Q}_p$, while the remaining three roots have valuation $1/3 + v_p(d)$, so lie outside of $\mathbb{Q}_p$. We

conclude: if $x_d^3 + ad^2x_d + bd^3$ is a square in $\mathbb{Q}_p^*$, we have $E^d(\mathbb{Q}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$; otherwise we have $E^d(\mathbb{Q}_p)[3] = 0$. Note that there indeed exists $d \in \mathbb{Q}_p^*$ such that we have $x_d^3 + ad^2x_d + bd^3 \in \mathbb{Q}_p^{*2}$, since we have

$$x_d^3 + ad^2x_d + bd^3 = d^3(x_1^3 + ax_1 + b),$$

where $x_1 \in \mathbb{Q}_p^*$ is the unique zero of ψ_3^1 in $\mathbb{Q}_p$.

In case (iv), the curve E^d has Kodaira type III if $v_p(d) = 0$ and Kodaira type III* if $v_p(d) = 1$. In both cases, we find from the table in [32, C.15] that Φ has order 1 or 2, and that therefore $E^d(\mathbb{Q}_p)$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/2\mathbb{Z}$. To show that only the latter possibility occurs, we use the 2-division polynomial $x^3 + ad^2x + bd^3$ of E^d. We find from the Newton polygon that there are two roots with valuation $1/2 + v_p(d)$, and one with valuation $v_p(b) + v_p(d) - 1$, which therefore lies in $\mathbb{Q}_p$.

In case (v), the curve E^d has Kodaira type IV if $v_p(d) = 0$ and Kodaira type II* if $v_p(d) = 1$. As in case (iii), we find from the table that Φ has order 1 or 2 if $v_p(d) = 0$, and order 1 if $v_p(d) = 1$, which implies that $E^d(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/3\mathbb{Z}$ if $v_p(d) = 0$ and to $\mathbb{Z}_p$ if $v_p(d) = 1$. As in case (iii), we use the Newton polygon of the 3-division polynomial of E^d to show that it has a unique zero $x_d \in \overline{\mathbb{Q}}_2$ of valuation $2v_p(a)+v_p(d)-1$, which is therefore defined over $\mathbb{Q}_p$, while the remaining three roots have valuation $1/3 + v_p(d)$, so lie outside of $\mathbb{Q}_p$. The same argument as the one given for case (iii) shows that both $E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ and $E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \mathbb{Z}/3\mathbb{Z}$ occur for suitable d. □

Lemma 3.25. *For all $d \in \mathbb{R}$, the group $E^d(\mathbb{R})$ is topologically isomorphic to $\mathbb{R}/\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^e$, where $e \in \{0, 1\}$. Furthermore, we have $e = 0$ if and only if f has only one real root.*

Proof. The first assertion is proven in [31, V.2.3.1]. The second one is standard. □

Lemma 3.26. *Let S be a finite set of primes and let $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$. For all $p \in S$, let (ξ_p, η_p) be in $E^{d_p}(\mathbb{Q}_p)$ and let γ_p and ϵ_p be real numbers. Then there exists a non-zero rational number c, such that for all $p \in S$ we have $v_p(c - d_p) > \gamma_p$, and such that there exists a point $(\xi, \eta) \in E^c(\mathbb{Q})$ satisfying $v_p(\xi - \xi_p) > \epsilon_p$ for all $p \in S$.*

Proof. We may assume that $\eta_p \neq 0$ for all $p \in S$. By the approximation theorem, there exist ξ and η with $\eta \neq 0$ in $\mathbb{Q}$ such that, for all $p \in S$, we have $v_p(\xi - \xi_p) > \epsilon_p$ and $v_p(\eta - \eta_p) > \epsilon_p$. Define $c = f(\xi)/\eta^2$. Since for all

$p \in S$ we have $f(\xi_p)/\eta_p^2 = d_p$, we may assume that c satisfies $v_p(c-d_p) > \gamma_p$ for all $p \in S$ by choosing both ξ closer to ξ_p and η closer to η_p if necessary. Now the twist E^c of E, given by the equation $(f(\xi)/\eta^2)y^2 = f(x)$, trivially contains the point (ξ, η), and both c and ξ satisfy the requirements. □

Proposition 3.27. *Let E be an elliptic curve over $\mathbb{Q}$ and let S be a finite set of primes. Assume that $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$ is topologically cyclic for all tuples $(d_p)_p \in \prod_{p\in S} \mathbb{Q}_p^*$. Then E has good twists with respect to S.*

Proof. It suffices to show that for all $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$, there exists $c \in \mathbb{Q}^*$, such that for each $p \in S$ we have $c \in d_p\mathbb{Q}_p^{*2}$, and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

We choose $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$. Let $P = ((\xi_p, \eta_p))_p$ be a topological generator of $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$. By the previous proposition, there exists a twist E^c of E, with c arbitrarily close to each of the d_p, such that there exists a point $(\xi, \eta) \in E^c(\mathbb{Q})$ with ξ arbitrarily close to each of the ξ_p. If c is sufficiently close to each of the d_p, we have $c \in d_p\mathbb{Q}_p^{*2}$; we may therefore assume that we can choose $\alpha_p \in \mathbb{Q}_p^{*2}$ such that $\alpha_p^2 = c/d_p$ for each p.

We now claim that, if ξ is sufficiently close to each of the ξ_p, then (ξ, η) is a topological generator of $\prod_{p\in S} E^c(\mathbb{Q}_p)$, and hence $E^c(\mathbb{Q})$ lies dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$. For each $p \in S$, there is an isomorphism defined over $\mathbb{Q}_p$

$$\begin{aligned} \psi_p \colon E^c &\to E^{d_p} \\ (x, y) &\mapsto (x, \alpha_p y) \end{aligned}$$

Hence the ψ_p combine to give an isomorphism of topological groups

$$\psi \colon \prod_{p\in S} E^c(\mathbb{Q}_p) \xrightarrow{\sim} \prod_{p\in S} E^{d_p}(\mathbb{Q}_p).$$

Under ψ, the point $((\xi, \eta))_p$ maps to a point $P' = ((\xi, \eta'_p))_p$, for certain $(\eta'_p) \in \prod_{p\in S} \mathbb{Q}_p$. If ξ is sufficiently close to the ξ_p, we can make P' as close as we want to the image of P under an automorphism of $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$ that acts on the η_p by multiplication by ± 1; hence for ξ sufficiently close to the ξ_p, the point P' is a topological generator of $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$, and so (ξ, η) is a topological generator of $\prod_{p\in S} E^c(\mathbb{Q}_p)$. □

3.4.2 Proof of Theorems 3.1–3.2

Lemma 3.28. *If E_1 and E_2 are elliptic curves over $\mathbb{Q}$ that do not admit complex multiplication over $\mathbb{Q}$, and for which $\mathrm{Km}(E_1 \times E_1)$ is $\overline{\mathbb{Q}}$-isomorphic to $\mathrm{Km}(E_2 \times E_2)$, then E_1 and E_2 are isogenous over $\overline{\mathbb{Q}}$.*

Proof. Let E_1 and E_2 be as in the statement of the lemma. By [34, eq. (10)], we have that $\mathrm{NS}(E_1 \times E_1)$ has rank 3, and is generated by the classes of $D_1 = E_1 \times \{0\}$, $D_2 = \{0\} \times E_1$, and D_3, which is the diagonal copy of E_1 inside $E_1 \times E_1$. The discriminant of $\mathrm{NS}(E_1 \times E_1)$ equals

$$\det \begin{pmatrix} D_1^2 & D_1D_2 & D_1D_3 \\ D_1D_2 & D_2^2 & D_2D_3 \\ D_1D_3 & D_2D_3 & D_3^2 \end{pmatrix} = \det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = 2.$$

Theorem 0.1 of [15] says that if B_1 and B_2 are abelian surfaces over $\overline{\mathbb{Q}}$ such that $\mathrm{NS}(B_1)$ has rank 3 and has square-free discriminant, and such that $\mathrm{Km}(B_1) \cong \mathrm{Km}(B_2)$, then B_2 is isomorphic to either B_1 or its dual. If we apply this result with B_i equal to $E_i \times E_i$ base-changed to $\overline{\mathbb{Q}}$ for $i \in \{1, 2\}$, and use that the $E_i \times E_i$ are their own duals, we find that $E_1 \times E_1$ is isomorphic to $E_2 \times E_2$ over $\overline{\mathbb{Q}}$. The Poincaré Complete Reducibility Theorem [23, p. 173] implies that E_1 is isogenous to E_2 over $\overline{\mathbb{Q}}$. □

Lemma 3.29. *Let E_1 be an elliptic curve over $\mathbb{Q}$ that does not admit complex multiplication over $\overline{\mathbb{Q}}$. Then there are only finitely many elliptic curves E_2 over $\mathbb{Q}$ up to $\overline{\mathbb{Q}}$-isomorphism such that E_1 and E_2 are isogenous over $\overline{\mathbb{Q}}$.*

Proof. Let E_1 be as in the statement of the lemma. The proof is an application of [32, Corollary IX.6.2], which says that there are only finitely many elliptic curves E_2 over $\mathbb{Q}$ up to $\mathbb{Q}$-isomorphism such that E_1 and E_2 are isogenous over $\mathbb{Q}$.

Let E_2 be an elliptic curve over $\mathbb{Q}$ and let $\phi\colon E_1 \to E_2$ be a $\overline{\mathbb{Q}}$-isogeny. By [32, Corollary IX.6.2], it suffices to show that there exists a quadratic twist E_2' of E_2 over $\mathbb{Q}$ such that E_1 and E_2' are isogenous over $\mathbb{Q}$. Let $\overline{\phi}\colon E_2 \to E_1$ be the dual isogeny to ϕ. Then there exists an integer n with $\phi \circ \overline{\phi} = [n]_{E_2}$, where $[n]_{E_i}$ is multiplication by n on E_i for $i \in \{1, 2\}$. We construct a cocycle

$$c\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$$

as follows: for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have that $c'_\sigma\colon E_2 \to E_2$ defined by $c'_\sigma = {}^\sigma\phi \circ \overline{\phi}$ is an endomorphism of degree n^2. Since E_1 does not admit complex multiplication over $\overline{\mathbb{Q}}$, the same holds for E_2, and we have $c'_\sigma = \pm[n]_{E_2}$. We define $c_\sigma \in \{\pm 1\}$ to be such that $c'_\sigma = c_\sigma[n]_{E_2}$. It is a trivial verification that c_σ is a cocycle.

By the theory of quadratic twists, there exists a quadratic twist E_2' of E_2 and a $\overline{\mathbb{Q}}$-isomorphism

$$\psi\colon E_2 \to E_2'$$

such that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have ${}^{\sigma}(\psi^{-1}) \circ \psi = c_\sigma$. Let $\chi\colon E_1 \to E_2'$ be the $\overline{\mathbb{Q}}$-isogeny $\psi \circ \phi$, and let $\overline{\chi} = \overline{\phi} \circ \psi^{-1}$. We have $\overline{\chi} \circ \chi = [n]_{E_1}$, so $\overline{\chi}$ is the dual isogeny to χ. For every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$ {}^{\sigma}\overline{\chi} \circ \chi = {}^{\sigma}\overline{\phi} \circ {}^{\sigma}\psi^{-1} \circ \psi \circ \phi = [n]_{E_1}. $$

Hence χ is defined over $\mathbb{Q}$. This concludes the proof. □

Corollary 3.30. *Let $\mathcal{C}$ be a collection of elliptic curves over $\mathbb{Q}$, representing infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. Then the collection of Kummer surfaces*

$$ \{\mathrm{Km}(E' \times E') : E' \in \mathcal{C}\} $$

contains infinitely many pairwise non-$\overline{\mathbb{Q}}$-isomorphic surfaces.

Proof. Since there are only a finite number of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ that admit complex multiplication over $\overline{\mathbb{Q}}$, we may assume that $\mathcal{C}$ does not contain any such elliptic curves. By Lemma 3.28, if the Kummer surfaces $\mathrm{Km}(E_1 \times E_1)$ and $\mathrm{Km}(E_2 \times E_2)$ are $\overline{\mathbb{Q}}$-isomorphic, then E_1 and E_2 are $\overline{\mathbb{Q}}$-isogenous. But by Lemma 3.29, for every $E_1 \in \mathcal{C}$, there are only finitely many $E_2 \in \mathcal{C}$ up to $\overline{\mathbb{Q}}$-isomorphism such that E_1 and E_2 are $\overline{\mathbb{Q}}$-isogenous. Since the elliptic curves in $\mathcal{C}$ represent infinitely many $\overline{\mathbb{Q}}$-isomorphism classes, we are done. □

We use the results obtained so far to give the proofs of Theorems 3.1 and 3.2.

Proof of Theorem 3.1. Assume that the elliptic curve E is given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$. We give conditions on a and b implying that, if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{R})$. We treat the case $p = 3$ separately.

First, assume $p = 3$. Assume that $a > 0$, $v_3(a) = 1$, and $v_3(b) > 1$. Then according to Lemma 3.24(ii), we have that $E^d(\mathbb{Q}_3)$ is a procyclic group of order $2 \cdot 3^\infty$ for all $d \in \mathbb{Q}_p^*$. Since $x^3 + ax + b$ has only one real root by the positivity of a, we have $E^d(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ for all $d \in \mathbb{R}$ by Lemma 3.25. Now Proposition 3.15 yields that $E^{d_3}(\mathbb{Q}_3) \times E^{d_\infty}(\mathbb{R})$ is topologically cyclic for all $d_3 \in \mathbb{Q}_3$ and $d_\infty \in \mathbb{R}$. Finally, Proposition 3.27 implies that E has good twists with respect to $\{3, \infty\}$, so $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_3) \times X(\mathbb{R})$ by Theorem 3.20.

Now assume $p \neq 3$. We assume that a and b in $\mathbb{Q}$ are such that $v_p(a) > 0$, and $v_p(b) = 1$; if $p = 2$ we require additionally that $a > 0$, if $p = 5$ we require

additionally that $a \not\equiv \pm 10 \pmod{25}$, and if $p = 7$, we require additionally that $b \not\equiv \pm 14 \pmod{49}$. Lemma 3.24(i)+(iii) gives that $E^{d_p}(\mathbb{Q}_p)$ is a procyclic group of order p^∞ or $3 \cdot p^\infty$ for all $d \in \mathbb{Q}_p^*$. Our assumptions on a and b together with Lemma 3.25 imply that, for all $d_\infty \in \mathbb{R}$, the group $E^{d_\infty}(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; moreover, if $p = 2$, then, for all $d_\infty \in \mathbb{R}$, the group $E^{d_\infty}(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$. Proposition 3.15 yields that $E^{d_p}(\mathbb{Q}_p) \times E^{d_\infty}(\mathbb{R})$ is topologically cyclic for all $d_p \in \mathbb{Q}_p$ and $d_\infty \in \mathbb{R}$. As in the previous case, we find that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{R})$.

Finally, it follows from equation (3.2) that the conditions on a and b given above correspond to infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. The theorem thus follows from Corollary 3.30. □

Proof of Theorem 3.2. Assume that the elliptic curve E is given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$. For p and q as in the theorem, we give conditions on a and b implying that, if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_q) \times X(\mathbb{R})$. We may assume that $p < q$.

We assume that a and b in $\mathbb{Q}^*$ are such that they satisfy the following conditions: $a > 0$, $v_p(a) = 1$, $v_p(b) > 1$, $v_q(a) > 0$, and $v_q(b) = 1$; if one of p and q equals 5, we require additionally that $a \not\equiv \pm 10 \pmod{25}$, and if $q = 7$, we require additionally that $b \not\equiv \pm 14 \pmod{49}$. According to parts (i), (iii) and (iv) of Lemma 3.24 and Corollary 3.14, the group $E^{d_p}(\mathbb{Q}_p) \times E^{d_q}(\mathbb{Q}_q)$ is procyclic for all $d_p \in \mathbb{Q}_p$ and $d_q \in \mathbb{Q}_q$. Observe that $E^d(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ for all $d \in \mathbb{R}$ by the fact that $a > 0$. Then by Proposition 3.15, we get that $E^{d_p}(\mathbb{Q}_p) \times E^{d_q}(\mathbb{Q}_q) \times E^{d_\infty}(\mathbb{R})$ is topologically cyclic for all choices of $d_p \in \mathbb{Q}_p$, $d_q \in \mathbb{Q}_q$, and $d_\infty \in \mathbb{R}$. By Proposition 3.27 and Theorem 3.20, we have that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_q) \times X(\mathbb{R})$.

As in the proof of Theorem 3.1, the conditions on a and b given above correspond to infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. Hence, again by Corollary 3.30, we are done. □

3.5 Large product topologies

Lemma 3.31. *Let $p > 3$ be a prime number and let $\mathscr{E}$ be an elliptic curve over $\mathbb{Q}_p$ with good reduction. Assume that the groups $\widetilde{\mathscr{E}}(\mathbb{F}_p)$ and $\widetilde{\mathscr{E}^t}(\mathbb{F}_p)$ are both cyclic of order coprime to p, where $\widetilde{\mathscr{E}}$ is the reduction modulo p of $\mathscr{E}$ and $\widetilde{\mathscr{E}^t}$ its unique non-trivial quadratic twist. Then $\mathscr{E}^d(\mathbb{Q}_p)$ is a procyclic*

group for all $d \in \mathbb{Q}_p^*$. Moreover, its order is equal to

$$\#\mathscr{E}^d(\mathbb{Q}_p) = \begin{cases} \#\widetilde{\mathscr{E}}(\mathbb{F}_p) \cdot p^\infty & \text{if } d \in \mathbb{Q}_p^{*2} \\ \#\widetilde{\mathscr{E}^t}(\mathbb{F}_p) \cdot p^\infty & \text{if } d \notin \mathbb{Q}_p^{*2} \text{ and } v_p(d) \text{ is even} \\ \#\widetilde{\mathscr{E}}(\mathbb{F}_p)[2] \cdot p^\infty & \text{if } v_p(d) \text{ is odd} \end{cases}$$

Proof. By changing to a $\mathbb{Q}_p$-isomorphic curve if necessary, it suffices to restrict to the case where $d \in \mathbb{Q}_p^*$ satisfies $v_p(d) = 0$ or $v_p(d) = 1$. First assume that we have $v_p(d) = 0$. Since p is a prime of good reduction for $\mathscr{E}^d$, by [32, VII.2.1] we have a short exact sequence

$$0 \to \mathscr{E}_1^d(\mathbb{Q}_p) \to \mathscr{E}^d(\mathbb{Q}_p) \to C \to 0 \tag{3.4}$$

where $\mathscr{E}_1^d(\mathbb{Q}_p)$ is the kernel of reduction of $\mathscr{E}^d$, which is topologically isomorphic to $\mathbb{Z}_p$ by [32, IV.6.4(b)], and C is $\widetilde{\mathscr{E}}(\mathbb{F}_p)$ if $d \in \mathbb{Z}_p^{*2}$ and $\widetilde{\mathscr{E}^t}(\mathbb{F}_p)$ otherwise. By assumption, the order of C is coprime to p. By Proposition 1.14(iv), then we must have

$$\mathscr{E}^d(\mathbb{Q}_p) \cong \mathscr{E}_1^d(\mathbb{Q}_p) \times C, \tag{3.5}$$

with C as above. Therefore, the group $\mathscr{E}^d(\mathbb{Q}_p)$ is a procyclic topological group by Corollary 3.14. Since $\mathscr{E}^d(\mathbb{Q}_p)$ is a direct product, its order is the product of the orders of $\mathscr{E}_1^d(\mathbb{Q}_p)$ and C. This proves the lemma in the case $v_p(d) = 0$.

Now we assume that $v_p(d) = 1$. The minimal discriminant of the twist $\mathscr{E}^d$ has valuation 6, and from the table in [32, C.15] we see that $\mathscr{E}^d$ is of reduction type I_0^*, and the component group of the special fibre of its Néron model is isomorphic to a subgroup of the Klein four-group. Hence $\mathscr{E}^d(\mathbb{Q}_p)$ sits in a short exact sequence of topological groups

$$0 \to \mathscr{E}_0^d(\mathbb{Q}_p) \to \mathscr{E}^d(\mathbb{Q}_p) \to \Phi \to 0, \tag{3.6}$$

where Φ is isomorphic to a subgroup of the Klein four-group. Since $\mathscr{E}^d$ can be given of an equation $y^2 = x^3 + ad^2x + bd^3$ with a and b in $\mathbb{Z}_p$, the group $\mathscr{E}_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$ by Theorem 1.1. We conclude that $\mathscr{E}^d(\mathbb{Q}_p)$ is an extension of a finite abelian 2-group by $\mathbb{Z}_p$, and hence must be isomorphic to the direct product by Proposition 1.14(iv). We have then that $\Phi = \Phi[2] = \mathscr{E}^d(\mathbb{Q}_p)[2]$, and this is isomorphic to $\mathscr{E}(\mathbb{Q}_p)[2]$ since the twisting does not affect the 2-torsion. We have $\mathscr{E}(\mathbb{Q}_p)[2] = \widetilde{\mathscr{E}}(\mathbb{F}_p)[2]$ by (3.6) and Proposition 1.14(iv). Since $\widetilde{\mathscr{E}}(\mathbb{F}_p)$ is cyclic, so is $\widetilde{\mathscr{E}}(\mathbb{F}_p)[2]$, and therefore $\mathscr{E}^d(\mathbb{Q}_p) \cong \mathscr{E}_0^d(\mathbb{Q}_p) \times \widetilde{\mathscr{E}}(\mathbb{F}_p)[2]$ is procyclic by Corollary 3.14. The assertion about the order follows as in the first part. □

The following corollary will be used to prove Theorem 3.3.

Corollary 3.32. *Let S be a set of prime numbers > 3 such that:*

(i) for all $p \in S$, the elliptic curve E has good reduction at p;

(ii) for all $p \in S$ and all $\delta \in \mathbb{F}_p^*$, the group $\widetilde{E}^\delta(\mathbb{F}_p)$ is cyclic, where $\widetilde{E}$ denotes the reduction of E modulo p;

(iii) for all $(\delta_p)_p \in \prod_{p\in S} \mathbb{F}_p^*$, the numbers $\#\widetilde{E}^{\delta_p}(\mathbb{F}_p)$ are pairwise coprime, and are coprime to $\log_2 \#E(\mathbb{R})[2]$ and the elements of S.

Then if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{R}) \times \prod_{p\in S} X(\mathbb{Q}_p)$.

Proof. Lemma 3.31 shows that, for all $p \in S$, the prime numbers dividing the orders of the groups $E^d(\mathbb{Q}_p)$, as d runs through $\mathbb{Q}_p^*$, are equal to p and the primes dividing $\#\widetilde{E}^\delta(\mathbb{F}_p)$, where δ runs through $\mathbb{F}_p^*$. Lemma 3.14 and assumptions (i)-(iii) then imply that, for all $(d_p)_p \in \prod_{p\in S} \mathbb{Q}_p^*$, the topological groups $E^{d_p}(\mathbb{Q}_p)$ are procyclic and pairwise of coprime order.

By Proposition 3.15 and the fact that the numbers $\#\widetilde{E}^{\delta_p}(\mathbb{F}_p)$ are coprime to $\log_2 \#E(\mathbb{R})[2]$ for all $p \in S$ and $\delta_p \in \mathbb{F}_p^*$, the groups $E^{d_\infty}(\mathbb{R}) \times \prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$ are topologically cyclic for all $(d_p)_p \in \prod_{p\in S} \mathbb{Q}_p^*$ and $d_\infty \in \mathbb{R}$. The result now follows from Proposition 3.27 and Theorem 3.20. □

Theorem 3.33. *Assume that E is given by $y^2 = x^3 + x + 1$. Let S be the following set of 331 primes:* $S = \{$467, 1033, 1289, 1823, 2081, 2221, 2591, 2887, 3163, 3229, 4691, 4751, 6047, 7103, 7883, 8069, 8663, 9221, 11909, 12149, 12211, 13451, 13567, 14207, 14419, 14557, 15299, 15959, 18089, 18233, 19889, 20201, 20857, 21379, 21803, 24509, 25031, 26711, 27091, 28477, 28607, 29333, 29723, 32309, 37139, 38791, 39359, 39953, 40519, 41957, 42179, 44867, 45233, 45757, 47501, 48767, 49711, 50581, 51563, 52379, 53699, 55487, 56951, 57089, 57413, 63659, 64153, 64217, 66347, 68927, 71597, 71987, 72139, 72869, 73061, 73583, 73613, 73849, 76679, 77377, 78179, 78889, 79531, 81197, 81953, 82883, 82997, 84299, 85061, 85259, 87407, 87641, 88741, 89909, 90373, 90499, 92699, 98519, 98801, 102533, 104831, 105563, 108161, 108877, 110237, 112403, 116131, 117659, 122051, 125399, 125899, 125941, 126397, 131321, 131507, 131797, 133769, 135851, 135887, 136531, 137239, 137867, 138869, 139921, 140269, 144299, 145139, 145829, 146801, 147083, 148157, 148663, 149533, 149731, 149921, 151637, 154849, 157019, 157901, 159899, 164581, 164617, 165713, 166949, 167879, 169859, 170953, 173501, 174413, 175361, 182687, 184187, 185599, 186583, 187373, 187787, 187931, 188171, 190409, 192233, 194891,

195103, 196709, 197441, 198959, 199313, 199603, 199783, 202031, 203531, 204557, 204973, 205129, 205441, 209123, 210907, 212081, 214507, 214559, 219251, 220771, 221261, 221411, 222109, 225371, 228601, 228913, 230389, 230999, 231109, 232607, 234989, 238181, 238213, 239119, 240319, 241727, 242083, 242453, 245753, 251171, 251879, 251969, 253109, 254369, 263489, 263849, 265091, 265711, 266089, 266129, 267749, 268253, 270329, 271619, 272549, 273281, 274831, 276323, 278819, 278917, 280061, 280963, 281893, 283837, 287003, 287501, 289343, 289607, 290767, 291371, 291559, 292133, 293071, 297191, 297589, 306781, 308003, 310087, 311237, 314407, 315461, 315527, 315899, 317459, 319031, 320611, 322079, 322583, 324983, 325229, 327517, 328589, 330439, 332851, 333791, 337327, 337907, 339517, 342389, 342527, 344429, 347993, 350159, 352309, 353401, 353963, 354337, 361789, 364853, 365929, 370067, 371737, 371873, 372397, 376039, 376577, 379913, 380189, 381209, 381527, 390703, 393299, 393539, 402419, 408461, 409391, 414077, 414893, 419599, 419789, 421703, 422407, 423221, 424601, 427169, 429887, 431521, 433859, 439661, 440983, 442333, 443759, 447257, 450847, 453569, 456553, 456679, 457381, 460099, 462311, 466061, 467651, 470279, 471923, 472057, 475793, 476137, 477409, 478679, 480463, 481097, 486449, 487717, 491149, 491327, 493291, 494699, 495449, 495947, 495973 }. *Then* $E(\mathbb{Q})$ *is dense in* $E(\mathbb{R}) \times \prod_{p\in S} E(\mathbb{Q}_p)$.

Proof. One proves this by taking the list S and verifying (for example with the help of `sage`) that E and S as in the theorem satisfy the hypotheses of Corollary 3.32.

The assertion about the cardinality of S is left to the reader. □

Proof of Theorem 3.3. Theorem 3.3 follows from Theorem 3.33. □

Remark 3.34. The list S in Theorem 3.33 was found by defining the following procedure in `sage` [35]. The prime numbers that are to be included in S are contained in the set `greedyList`; this set is only added to while the procedure runs. The set `primeList` keeps track of the prime numbers p whose inclusion in S still has to be decided; it is equal to the set of prime numbers between `min_p` and `max_p` at the start of the procedure, and every time a new prime number p is added to S, the prime divisors of $\#\widetilde{E}^{\delta}(\mathbb{F}_p)$ are removed from it, where δ runs over the elements of $\mathbb{F}_p^*$. The set `greedyBlacklist` contains the primes in `greedyList` as well as the set of prime divisors of $\widetilde{E}^{\delta}(\mathbb{F}_p)$, where p runs over the elements of `greedyList` and δ runs over the elements of $\mathbb{F}_p^*$. If $E(\mathbb{R})[2] = 4$, the initial value of `greedyBlacklist` is $\{2\}$, otherwise its initial value is $\emptyset$.

```
def findPrimes(E,min_p,max_p):
    Disc = E.discriminant()
    min_p = max(min_p,5)

    primeList = set([p for p in prime_range(min_p,max_p)])
    greedyList = set([])
    greedyBlacklist = set([])
    phi_2 = (E.division_polynomial(2)).change_ring(RR)
    if len(phi_2.roots()) == 3:
        greedyBlacklist.add(2)

    while primeList != set([]):
        p = primeList.pop()
        if (Disc % p) != 0 and p not in greedyBlacklist:
            Ep = E.base_extend(GF(p))
            A = Ep.abelian_group()
            B = Ep.quadratic_twist().abelian_group()
            if A.is_cyclic() == true:
                if B.is_cyclic() == true:
                    S = set(A.order().prime_divisors())
                    T = set(B.order().prime_divisors())
                    U = S.union(T)
                    greedyList.add(p)
                    for s in U:
                        if s == p or s in greedyBlacklist:
                            greedyList.remove(p)
                            break
            if p in greedyList:
                Up = U.union([p])
                greedyBlacklist = greedyBlacklist.union(Up)
                primeList = primeList.difference(U)
    return(greedyList);
```

One gets the list S in Theorem 3.33 by running the commands

```
E = EllipticCurve([1,1]); min_p = 5; max_p = 500000
findPrimes(E,min_p,max_p)
```

3.6 Proof of Theorem 3.4

We keep our notation and assumptions as explained in section 3.3.1.

Theorem 3.35. *Assume that $E/\mathbb{Q}$ is given by $y^2 = x^3 + x$. Then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$ for all p with $p \equiv 3 \pmod 4$ and $p > 7$.*

Proof. Let p be a prime congruent to 3 mod 4. For $d \in \mathbb{Q}_p^*$, the twist E^d of E is given by the equation $y^2 = x^3 + d^2x$. By Lemma 3.27 and Theorem 3.20, it suffices to show that $E^d(\mathbb{Q}_p)$ is procyclic for all $d \in \mathbb{Q}_p^*$. By changing to a $\mathbb{Q}_p$-isomorphic curve if necessary, it suffices to restrict to the case of $d \in \mathbb{Q}_p^*$ with $v_p(d)$ equal to 0 or 1.

First assume $v_p(d) = 0$. Let $\widetilde{E^d}$ be the reduction of E^d modulo p. Then $\#\widetilde{E^d}(\mathbb{F}_p) = p + 1$. This follows from the fact that $\widetilde{E^d}$ is supersingular [32, V.4.5] and the fact that $p > 3$. We claim that $\widetilde{E^d}(\mathbb{F}_p)$ is cyclic. Suppose that $(\mathbb{Z}/\ell\mathbb{Z})^2 \subset \widetilde{E^d}(\mathbb{F}_p)$ for some prime ℓ. Then p must split completely in $\mathbb{Q}(\zeta_\ell)$, giving $\ell \mid p-1$. On the other hand ℓ must certainly divide $\#\widetilde{E^d}(\mathbb{F}_p) = p+1$; therefore we must have $\ell = 2$. But since x^3+d^2x has a linear and a quadratic irreducible factor over $\mathbb{F}_p$, we must have $\#\widetilde{E^d}(\mathbb{F}_p)[2] = 2$. This gives a contradiction, proving the claim.

By [32, VII.2.1] and the fact that E^d has good reduction at p, we have a short exact sequence:

$$0 \to E_1^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to \widetilde{E^d}(\mathbb{F}_p) \to 0,$$

where the kernel of reduction $E_1^d(\mathbb{Q}_p)$ of E^d is isomorphic to $\mathbb{Z}_p$ by [32, IV.6.4(b)]. We conclude that $E^d(\mathbb{Q}_p)$ is topologically isomorphic to the direct product of $\mathbb{Z}_p$ and a cyclic group of order $p + 1$. By Proposition 1.14(iv), the group $E^d(\mathbb{Q}_p)$ is procyclic.

Now assume $v_p(d) = 1$. Then E^d has additive reduction with Kodaira type IV [32, C.15]. Hence we have a short exact sequence

$$0 \to E_0^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to G \to 0,$$

where $E_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$ by Theorem 1.1, and G is isomorphic to a subgroup of the Klein four-group. Again by Proposition 1.14(iv), the group $E^d(\mathbb{Q}_p)$ is topologically isomorphic to the direct product of $\mathbb{Z}_p$ and G. Hence G is isomorphic to $E^d(\mathbb{Q}_p)[2] = E(\mathbb{Q}_p)[2]$, which we already knew to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Hence by Corollary 3.14, the group $E^d(\mathbb{Q}_p)$ is procyclic. □

Proof of Theorem 3.4. Theorem 3.4 follows from Theorem 3.35. □

3.7 Proof of Theorem 3.5

In this section, we will now prove Theorem 3.5. The core of the proof of this theorem is a slight modification of the proof of Theorem 1 of [11] by Rajiv Gupta and M. Ram Murty. We will need the following lemma, which is reasonably standard.

Lemma 3.36. *Let p be a prime. Let E be an elliptic curve over $\mathbb{Q}$ and $\widetilde{E}$ its reduction modulo p. If $\widetilde{E}(\mathbb{F}_p)[\ell]$ is not cyclic for some prime ℓ, then $p \equiv 1 \pmod{\ell}$.*

Proof. If $\widetilde{E}(\mathbb{F}_p)[\ell]$ is not cyclic for some prime ℓ, the prime p must split completely in $\mathbb{Q}(E[\ell])$. By the existence of the Weil pairing, we have $\mathbb{Q}(\zeta_\ell) \subset \mathbb{Q}(E[\ell])$. Hence p splits completely in $\mathbb{Q}(\zeta_\ell)$. Now the theory of cyclotomic fields implies that $p \equiv 1 \pmod{\ell}$. □

Theorem 3.37. *For every elliptic curve E over $\mathbb{Q}$ such that $\#E(\mathbb{Q})[2] = 2$, the set of rational points of $\mathrm{Km}(E \times E)$ lies dense in the space of its p-adic points for infinitely many primes p.*

Proof. Take an elliptic curve E as in the statement of the theorem. Whenever we write $\widetilde{E}$, we will mean the reduction of E modulo the prime p under consideration and $\widetilde{E}^t$ for its non-trivial quadratic twist.

In this proof, we will call a prime p "good" for an elliptic curve E if the groups $\widetilde{E}(\mathbb{F}_p)$ and $\widetilde{E}^t(\mathbb{F}_p)$ are both cyclic, and "bad" otherwise. Applying Lemma 3.31, Proposition 3.27 and Theorem 3.20 in turn, one sees that it suffices to prove that there exist infinitely many primes p that are good for E. (Note that, since $\#E(\mathbb{Q})[2] = 2$, the condition in Lemma 3.31 that the order of both groups be different from p is automatically satisfied if p is not equal to 2 and is a prime of good reduction.)

We will restrict to a set of primes among which the primes that are good for E are easier to count. Following Gupta and Murty, we define the following set of primes for each pair of positive real numbers ϵ and x:

$$S_\epsilon(x) = \left\{ p \leq x \text{ prime } : \begin{array}{l} E \text{ has good reduction at } p, \text{ each odd prime} \\ \text{divisor of } p-1 \text{ is } \geq x^{1/4+\epsilon} \text{ and divides} \\ p-1 \text{ only once, and } p \text{ is non-split in } \mathbb{Q}(E[2]) \end{array} \right\}$$

In [11, Lemma 3], Gupta and Murty prove, using a result from sieve theory by Fouvry and Iwaniec [10], that there exists an $\epsilon > 0$ such that

$$\#S_\epsilon(x) \gg \frac{x}{\log^2 x}. \tag{3.7}$$

We choose an ϵ such that (3.7) holds, and we define $S(x) = S_\epsilon(x)$. For every integer a we let $S(a,x) \subset S(x)$ be the subset of primes p such that a_p is equal to a, where $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$ is the trace of the Frobenius of E at p. By the Hasse–Weil bound, we have

$$S(x) = \coprod_{|a| \leq 2x^{1/2}} S(a,x).$$

We claim that if $x \in \mathbb{R}$ is large enough, then for every integer a with $|a| \leq 2x^{1/2}$, there are primes ℓ_a and ℓ_a^t, both greater than or equal to $x^{1/4+\epsilon}$, such that, for all $p \in S(a,x)$, we have that $\widetilde{E}(\mathbb{F}_p)[\ell]$ is cyclic for all primes $\ell \neq \ell_a$ and $\widetilde{E}^t(\mathbb{F}_p)[\ell']$ is cyclic for all primes $\ell' \neq \ell_a^t$. Choose an integer a such that $|a| \leq 2x^{1/2}$. First, assume that $p \in S(a,x)$ and $\widetilde{E}(\mathbb{F}_p)[\ell]$ is not cyclic. Then ℓ must be odd, since p does not split in $\mathbb{Q}(E[2])$. Then we must have

$$\ell^2 \mid \#\widetilde{E}(\mathbb{F}_p) = p + 1 - a. \tag{3.8}$$

We also have

$$\ell \mid p - 1 \tag{3.9}$$

by Lemma 3.37. This last fact implies, by the definition of $S(x)$ and the fact that ℓ is odd, that we have

$$\ell \geq x^{1/4+\epsilon} \tag{3.10}$$

Together, (3.8) and (3.9) imply $\ell \mid a - 2$. If x is large enough, then the integer a, whose absolute value is less than $2x^{1/2}$, has at most one prime divisor that is greater than or equal to $x^{1/4+\epsilon}$. Hence, if there is such a prime divisor ℓ_a, we have $\ell = \ell_a$. If there is no such prime divisor, we may set ℓ_a equal to any prime we want. For the other part, we assume that $p \in S(a,x)$ and $\widetilde{E}^t(\mathbb{F}_p)[\ell']$ is not cyclic. Now we use that $\ell^2 \mid \#\widetilde{E}^t(\mathbb{F}_p) = p + 1 + a$. Reasoning as before, we find that ℓ' must be an odd prime divisor of $a + 2$ that is greater than or equal to $x^{1/4+\epsilon}$. Again, there is at most one such a prime divisor for x large enough: if there exists one we will call it ℓ_a^t, and then we must have $\ell' = \ell_a^t$; if not, we let ℓ_a^t be arbitrary. This proves the claim made at the start of the paragraph.

Assuming that x is large enough as in the previous paragraph, we can now give a lower bound in terms of x on the number of primes p in $S(a,x)$ such that p is good for E in the sense defined earlier. If $p \in S(a,x)$ is bad for E, then we must have either $\ell_a^2 \mid p + 1 - a$ or $(\ell_a^t)^2 \mid p + 1 + a$. Since

both ℓ_a and ℓ_a^t are greater than or equal to $x^{1/4+\epsilon}$, and we have $p \leq x$, the number of $p \in S(a,x)$ that are bad for E is bounded above by

$$\frac{x}{\ell_a^2} + \frac{x}{(\ell_a^t)^2} + O(1) \leq \frac{x}{x^{1/2+2\epsilon}} + \frac{x}{x^{1/2+2\epsilon}} + O(1) = 2x^{1/2-2\epsilon} + O(1).$$

Summing the above over all integers a with $|a| \leq 2x^{1/2}$, we find that the total number of p in $S(x)$ that is bad for E is at most

$$4x^{1/2} \cdot \left(2x^{1/2-2\epsilon} + O(1)\right) = 8x^{1-2\epsilon} + O(x^{1/2}).$$

Comparing this with (3.7), we see that, for x large enough, the number of good primes in $S(x)$ grows at least as fast asymptotically as $\frac{x}{\log^2 x}$ times a constant. □

Proof of Theorem 3.5. Theorem 3.5 coincides with Theorem 3.37. □