ACTA ARITHMETICA
140.4 (2009)

Elementary 3-descent with a 3-isogeny

by

Henri Cohen (Talence) and Fabien Pazuki (Paris)

1. Introduction. The aim of this work is to give a very explicit way to estimate the rank of an elliptic curve over $\mathbb{Q}$ using 3-descent. We will suppose that the elliptic curve has a rational 3-torsion subgroup. This allows us to pick an affine model of the form $y^2 = x^3 + D(ax+b)^2$. After introducing the descent maps, we explain in Section 2 how to use 3-descent. Then we show how to compute principal homogeneous spaces in the case $D = 1$ in Section 3. We do the same in Section 4 for the case $D \neq 1$, which is a bit more technical. Sections 5 and 6 include all the results needed for local solubility. For the sake of brevity we do not include all the details of the calculations, they are of course available upon request. In Section 7, one finds several examples of families where we find the $\mathbb{Q}$-rank, and we also give some applications, such as prime values of certain cubic forms.

The main strategy here is improving on [2, Section 8.4], where this explicit way of doing descent is explained for 2-descent. The 3-Selmer group has also been studied in [17] and [5]. See for example [3, 4, 10] and their references for a more general treatment. For some other articles on the subject one could refer to [1, 6, 13, 15, 11].

1.1. *The geometric setting.* We recall a few facts about descent on elliptic curves. Let E/k be an elliptic curve over a number field k and let $n \geq 2$ be an integer. First, using Galois cohomology, we have the short exact sequences:

$$\begin{tikzcd}
0 \arrow[r] & E(k)/nE(k) \arrow[r, "\delta"] \arrow[d] & H^1(k, E[n]) \arrow[r] \arrow[d, "\prod_v \mathrm{res}_v"] \arrow[dr, "\varphi"] & H^1(k, E)[n] \arrow[r] \arrow[d, "\prod_v \mathrm{res}_v"] & 0 \\
0 \arrow[r] & \prod_v E(k_v)/nE(k_v) \arrow[r, "\prod_v \delta_v"] & \prod_v H^1(k_v, E[n]) \arrow[r] & \prod_v H^1(k_v, E)[n] \arrow[r] & 0
\end{tikzcd}$$

2010 *Mathematics Subject Classification*: 11G05, 14G05, 14H52, 14K02.
Key words and phrases: elliptic curves, 3-descent.

DOI: 10.4064/aa140-4-6

We recall the definition of the *n-Selmer group*:

$$\mathrm{Sel}^{(n)}(k,E) := \mathrm{Ker}\Big(\varphi : H^1(k,E[n]) \to \prod_v H^1(k_v,E)[n]\Big).$$

We also recall the definition of the *Tate–Shafarevich group*:

$$Ш(k,E) := \mathrm{Ker}\Big(H^1(k,E) \to \prod_v H^1(k_v,E)\Big).$$

This leads to the following short exact sequence:

$$0 \to E(k)/nE(k) \to \mathrm{Sel}^{(n)}(k,E) \to Ш(k,E)[n] \to 0,$$

where one can show that every term is a finite group, so that

$$|\mathrm{Sel}^{(n)}(k,E)| = |E(k)/nE(k)|\,|Ш(k,E)[n]|,$$

which gives

$$n^{\mathrm{rk}(E/k)} = \frac{|\mathrm{Sel}^{(n)}(k,E)|}{|E(k)_{\mathrm{tors}}/nE(k)_{\mathrm{tors}}|\,|Ш(k,E)[n]|}.$$

Thus, to get the exact value of the rank $\mathrm{rk}(E/k)$, we must compute the n-Selmer group and the n-torsion part of the Tate–Shafarevich group.

Recall that a *twist* of an object X defined over k is an object Y defined over k that is isomorphic to X over $\bar{k}$.

Since $\mathrm{Sel}^{(n)}(k,E) \subset H^1(k,E[n])$, if we find a geometric object X such that $\mathrm{Aut}_{\bar{k}}(X) \cong E[n]$, we can interpret the elements of the n-Selmer group as twists of the object X. This idea gives rise to different interpretations of the elements of the n-Selmer group, as is clearly explained in [3, 4]. In the present paper we are going to describe explicitly the geometrical interpretation of those elements that we now recall. First, if O denotes the identity element of E, the complete linear system given by $|n.O|$ induces a morphism $E \to \mathbb{P}^{n-1}$.

Definition 1.1. A *diagram* $[C \to S]$ is a morphism from a torsor C under E to a variety S. We will say that two diagrams $[C_1 \to S_1]$ and $[C_2 \to S_2]$ are *isomorphic* if the following diagram is commutative:

$$\begin{tikzcd} C_1 \arrow[r] \arrow[d, "\cong"] & S_1 \arrow[d, "\cong"] \\ C_2 \arrow[r] & S_2 \end{tikzcd}$$

We will define a *Brauer–Severi diagram* $[C \to S]$ to be a twist of the diagram $X = [E \to \mathbb{P}^{n-1}]$. In particular, S is a twist of $\mathbb{P}^{n-1}$, called a *Brauer–Severi variety*.

Following [4], we interpret an element of the n-Selmer group of E as a Brauer–Severi diagram $[C \to S]$ such that the curve C has points everywhere locally, hence one can take $S = \mathbb{P}^{n-1}$.

We now specialize to the case $n = 3$. In this particular case, the Brauer–Severi diagrams we are looking for are of the type $[C \to \mathbb{P}^2]$, the curve C being a plane cubic with points everywhere locally, given with an action of $E[3]$ on it by linear automorphisms.

1.2. *The arithmetic setting.* For the proofs of all the results given in this section, we refer to [2, Section 8.4], although there are other pointers in the literature. The 3-Selmer group in this particular case has also been studied in [17] and [5].

Let E be an elliptic curve defined over $\mathbb{Q}$ and having a rational 3-torsion subgroup that we denote $\{O, T, -T\}$. Let us stress here that the point T does not need to be rational itself. It is easy to see that E can be given by an affine equation of the type

$$y^2 = x^3 + D(ax + b)^2$$

with a, b, and D in $\mathbb{Q}$, and the discriminant of E is $16b^3D^2(4Da^3 - 27b)$, so we must have b and D nonzero and $4Da^3 - 27b \neq 0$. The 3-torsion point T is equal to $(0, b\sqrt{D})$, so is rational if and only if $D \in \mathbb{Q}^{*2}$.

Lemma 1.2. *There exists a unique equation of E of the form $y^2 = x^3 + D(ax + b)^2$, where a, b, and D are in $\mathbb{Z}$, D is a fundamental discriminant* (*including* 1), $b > 0$, *and if we write $b = b_1b_3^3$ with b_1 cubefree then* $(a, b_3) = 1$.

Proof. We can write uniquely $D = D_0f^2$, where D_0 is a fundamental discriminant and $f \in \mathbb{Q}^*$, so our initial equation can be written $y^2 = x^3 + D_0(a'x + b')^2$ with $a' = fa$ and $b' = fb$. Changing (x, y) into $(x/u^2, y/u^3)$ changes (a', b') into (ua', u^3b'), so it is clear that we may assume that a and b are in $\mathbb{Z}$, and if $b = b_1b_3^3$ and $g = (b_3, a)$, changing (x, y) into (xg^2, yg^3) changes (a, b) into $(a/g, b/g^3)$, hence (a, b_3) into $(a/g, b_3/g)$, so ensures that $(a, b_3) = 1$. Finally, changing (a, b) into $(-a, -b)$ ensures that $b > 0$. Uniqueness is immediate and left to the reader. ∎

From now on, we will always assume that the equation of our curve is given and satisfies the conditions of the above lemma (although we will mainly use the fact that D is a fundamental discriminant), and we will denote by K the field $K = \mathbb{Q}(\sqrt{D})$ of discriminant D, which will be equal to $\mathbb{Q}$ if $D = 1$ and to a quadratic field otherwise.

Given such a curve E, our aim is to give an estimate for the rank of E, and if possible the rank itself, using 3-descent. We first recall the definition and main properties of the 3-descent maps.

Definition 1.3. Let E be an elliptic curve defined over $\mathbb{Q}$, choose an affine model given by an equation $y^2 = x^3 + D(ax + b)^2$ with D a fundamental discriminant, and let $T = (0, b\sqrt{D})$ be a 3-torsion point.

(1) The 3-*descent map* α is a map from $E(\mathbb{Q})$ to the subgroup G_3 of classes of elements of K^*/K^{*3} whose norm is a cube (or $G_3 = \mathbb{Q}^*/\mathbb{Q}^{*3}$ if $D = 1$) defined by $\alpha(O) = 1$, $\alpha((0,b)) = 1/(2b)$ when $D = 1$, and in general by $\alpha((x,y)) = y - (ax+b)\sqrt{D}$.

(2) The curve $\widehat{E}$ is defined by a similar equation $y^2 = x^3 + \widehat{D}(\widehat{a}x + \widehat{b})^2$, where $\widehat{D} = -3D$, $\widehat{a} = a$, and $\widehat{b} = (27b - 4a^3D)/9$, and the corresponding 3-descent map is denoted $\widehat{\alpha}$. Moreover, we have $\widehat{T} = (0, \widehat{b}\sqrt{\widehat{D}}) = (0, (27b - 4a^3D)\sqrt{-3D}/9)$.

(3) The map ϕ from E to $\widehat{E}$ is defined by

$$\phi(P) = \left(\frac{x^3 + 4D((a^2/3)x^2 + abx + b^2)}{x^2}, \frac{y(x^3 - 4Db(ax+2b))}{x^3}\right)$$

for $P \neq O$ and $P \neq \pm T$, and $\phi(P) = \widehat{O}$ if $P = O$ or $P = \pm T$, and the map $\widehat{\phi}$ from $\widehat{E}$ to E is defined in the same way, replacing the coefficients of E by those of $\widehat{E}$, except that the x-coordinate must be divided by 9 and the y-coordinate by 27.

Proposition 1.4.

(1) *ϕ and $\widehat{\phi}$ are dual 3-isogenies (in particular group homomorphisms) between E and $\widehat{E}$, so that $\widehat{\phi} \circ \phi$ and $\phi \circ \widehat{\phi}$ are the multiplication-by-3 maps on E and $\widehat{E}$ respectively. The kernel of ϕ (over $\overline{\mathbb{Q}}$) is $\{O, \pm T\}$, and that of $\widehat{\phi}$ is $\{\widehat{O}, \pm\widehat{T}\}$.*

(2) *The map α is a group homomorphism from $E(\mathbb{Q})$ to G_3, and* $\mathrm{Ker}(\alpha) = \widehat{\phi}(\widehat{E}(\mathbb{Q}))$.

2. 3-Descent with a rational 3-isogeny. We now explain how the use of the 3-descent maps α and $\widehat{\alpha}$ gives a precise estimate on the rank of E (and of the isogenous curve $\widehat{E}$, which has the same rank). Before proving the main result (Proposition 2.2 below), we need the following precise description of the rational 3-torsion points of an elliptic curve (evidently, if an elliptic curve does not have a rational 3-torsion subgroup, in other words if it does not have an equation of the form $y^2 = x^3 + D(ax+b)^2$, the only rational 3-torsion point is O).

Lemma 2.1. *Let $y^2 = x^3 + D(ax+b)^2$ be the equation of an elliptic curve E with rational 3-torsion subgroup, and assume as usual that this equation is written so that D is a fundamental discriminant. The rational 3-torsion points of E are the following:*

(1) *If $D = 1$: the points O and $(0, \pm b)$.*

(2) *If $D = -3$ and $2(9b + 4a^3) = t^3$ is the cube of a rational number*

$t \neq 0$: *the point* O *and the points* P *such that*

$$x(P) = \frac{t^2}{3} + \frac{3}{t^2}\left(4ab + \frac{16}{9}\,a^4\right) + \frac{4a^2}{3}.$$

(3) *Otherwise*, *only the point* O.

Proof. Let $Q=(x,y)$ be a 3-torsion point. Then $x([2]Q)=x(-Q)=x(Q)$, which gives, using the formulas on p. 59 of [16] for the duplication law on the elliptic curve E,

$$x(3x^3 + 4Da^2x^2 + 12Dabx + 12Db^2) = 0.$$

Let $P(x) = 3x^3 + 4Da^2x^2 + 12Dabx + 12Db^2$. Note that $\mathrm{Disc}(P) = -48D^2(-27b + 4Da^3)^2b^2$. So either $x = 0$, and then $y^2 = Db^2$, or $P(x) = 0$ and after an easy calculation we obtain

$$y^2 = -\frac{D}{3}\,(ax + 3b)^2.$$

It is then straightforward to find the rational solutions, keeping in mind that D is a fundamental discriminant. ∎

We can now give the following exact analogue of Proposition 8.2.8 of [2], whose proof we follow verbatim.

Proposition 2.2. *Let* E *be the elliptic curve* $y^2 = x^3 + D(ax + b)^2$ *and* $\widehat{E}$ *the* 3*-isogenous curve with equation* $y^2 = x^3 - 3D(ax + (27b - 4a^3D)/9)^2$ *as above*, *and let* α *and* $\widehat{\alpha}$ *be the corresponding* 3*-descent maps. Then*

$$|\mathrm{Im}(\alpha)|\,|\mathrm{Im}(\widehat{\alpha})| = 3^{r+\delta},$$

where r *is the rank of* E (*and of* $\widehat{E}$), $\delta = 1$ *if* $D = 1$ *or* $D = -3$, *and* $\delta = 0$ *otherwise.*

Proof. If E_t denotes the torsion subgroup of E we have

$$E(\mathbb{Q})/3E(\mathbb{Q}) \simeq E_t(\mathbb{Q})/3E_t(\mathbb{Q}) \oplus (\mathbb{Z}/3\mathbb{Z})^r.$$

Set $G = E_t(\mathbb{Q})$. We know that if G is a finite abelian group then $G/3G$ is noncanonically isomorphic to $G[3]$, in other words to the group of 3-torsion points of G. Thus by Lemma 2.1, $E_t(\mathbb{Q})/3E_t(\mathbb{Q})$ is trivial unless either $D = 1$, or $D = -3$ and $2(9b + 4a^3)$ is a cube. Write $\delta_{D,n}$ for the usual Kronecker δ-symbol, and $\gamma(a, b)$ for the truth value of the condition that $2(9b + 4a^3)$ is a cube. With this notation we can thus write

$$|E(\mathbb{Q})/3E(\mathbb{Q})| = 3^{r+\delta_{D,1}+\delta_{D,-3}\gamma(a,b)}.$$

On the other hand, let us consider our 3-isogenies ϕ and $\widehat{\phi}$. Since $\widehat{\phi}\circ\phi$ is the multiplication-by-3 map, we evidently have

$$|E(\mathbb{Q})/3E(\mathbb{Q})| = [E(\mathbb{Q}) : \widehat{\phi}(\widehat{E}(\mathbb{Q}))][\widehat{\phi}(\widehat{E}(\mathbb{Q})) : \widehat{\phi}(\phi(E(\mathbb{Q})))].$$

Now for any group homomorphism $\widehat{\phi}$ and subgroup B of finite index in an abelian group A we evidently have

$$\frac{\widehat{\phi}(A)}{\widehat{\phi}(B)} \simeq \frac{A}{B+\operatorname{Ker}(\widehat{\phi})} \simeq \frac{A/B}{(B+\operatorname{Ker}(\widehat{\phi}))/B} \simeq \frac{A/B}{\operatorname{Ker}(\widehat{\phi})/(\operatorname{Ker}(\widehat{\phi})\cap B)}.$$

Thus

$$[\widehat{\phi}(A):\widehat{\phi}(B)] = \frac{[A:B]}{[\operatorname{Ker}(\widehat{\phi}):\operatorname{Ker}(\widehat{\phi})\cap B]}.$$

We are going to use this formula with $A = \widehat{E}(\mathbb{Q})$ and $B = \phi(E(\mathbb{Q}))$. We know that $\operatorname{Ker}(\widehat{\phi})$ (over $\overline{\mathbb{Q}}$) has three elements $\widehat{O}$ and $\pm\widehat{T}$, and $\widehat{T} \in \phi(E(\mathbb{Q}))$ if and only if $D = -3$, so (once again over $\overline{\mathbb{Q}}$), $\operatorname{Ker}(\widehat{\phi}) = \{O, \pm\widehat{T}\}$ if $D = -3$, and is trivial otherwise. Thus, if $D \neq -3$ we have $[\operatorname{Ker}(\widehat{\phi}):\operatorname{Ker}(\widehat{\phi})\cap B] = 1$. Assume now that $D = -3$, so that the equation of E is $y^2 = x^3 - 3(ax+b)^2$, and that of $\widehat{E}$ can be taken to be $y^2 = x^3 + (3ax + (9b + 4a^3))^2$. Then $[\operatorname{Ker}(\widehat{\phi}):\operatorname{Ker}(\widehat{\phi})\cap B] = 1$ if $\widehat{T} \in \phi(E(\mathbb{Q}))$, and is equal to 3 otherwise. We know (see for instance [2, Proposition 8.4.4]) that $\widehat{T} \in \phi(E(\mathbb{Q}))$ if and only if $2(9b + 4a^3)$ is a cube, in other words with the notation introduced above, if and only if $\gamma(a, b) = 1$. Thus,

$$[\widehat{\phi}(\widehat{E}(\mathbb{Q})):\widehat{\phi}(\phi(E(\mathbb{Q})))] = \frac{[\widehat{E}(\mathbb{Q}):\phi(E(\mathbb{Q}))]}{3^{\delta_{D,-3}(1-\gamma(a,b))}}.$$

Putting everything together we obtain

$$\begin{aligned}&3^{r+\delta_{D,1}+\delta_{D,-3}\gamma(a,b)}\\ &\quad= |E(\mathbb{Q})/3E(\mathbb{Q})| = [E(\mathbb{Q}):\widehat{\phi}(\widehat{E}(\mathbb{Q}))][\widehat{\phi}(\widehat{E}(\mathbb{Q})):\widehat{\phi}(\phi(E(\mathbb{Q})))]\\ &\quad= [E(\mathbb{Q}):\widehat{\phi}(\widehat{E}(\mathbb{Q}))][\widehat{E}(\mathbb{Q}):\phi(E(\mathbb{Q}))]3^{\delta_{D,-3}(\gamma(a,b)-1)}.\end{aligned}$$

On the other hand, the 3-descent map α on $E(\mathbb{Q})$ has kernel $\widehat{\phi}(\widehat{E}(\mathbb{Q}))$, so $[E(\mathbb{Q}):\widehat{\phi}(\widehat{E}(\mathbb{Q}))] = |\operatorname{Im}(\alpha)|$, and similarly $[\widehat{E}(\mathbb{Q}):\phi(E(\mathbb{Q}))] = |\operatorname{Im}(\widehat{\alpha})|$, so finally we obtain

$$|\operatorname{Im}(\alpha)|\,|\operatorname{Im}(\widehat{\alpha})| = 3^{r+\delta_{D,1}+\delta_{D,-3}},$$

proving the proposition. ∎

It follows from this proposition that to compute the rank it is sufficient to compute the cardinality of $\operatorname{Im}(\alpha)$ and of $\operatorname{Im}(\widehat{\alpha})$, which we do separately. As in the case of 2-descent, we cannot give an algorithm for this, since there is an obstruction embodied in the 3-part of the Tate–Shafarevich group of E, but the method works in many cases. The goal of the next sections is thus to compute $|\operatorname{Im}(\alpha)|$.

3. The case $D = 1$. We first treat the case $D = 1$. We choose the equation of our elliptic curve as $y^2 = x^3 + (ax + b)^2$ with a and b as in

Lemma 1.2, and we recall that the fundamental 3-descent map α from $E(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*3}$ is defined by $\alpha(O) = 1$, $\alpha((0,b)) = 1/(2b)$, and $\alpha((x,y)) = y - (ax+b)$ for all other points of $E(\mathbb{Q})$.

Note: For brevity, when we speak of a solution to a homogeneous equation we always mean a *nontrivial* solution, where the variables are not all equal to 0. Similarly, when we speak of a solution to a homogeneous congruence modulo p^k for some prime p, we always mean a solution where all the variables are p-integral, and at least one of them has p-adic valuation equal to 0, typically $\min(v_p(X), v_p(Y), v_p(Z)) = 0$.

Theorem 3.1. *Keep the above notation.*

(1) *An element $\overline{u} \in \mathbb{Q}^*/\mathbb{Q}^{*3}$ belongs to the image of α if and only if for some* (*or any*) *representative $u \in \mathbb{Q}^*$ the homogeneous cubic equation*

$$uX^3 + (1/u)Y^3 + 2bZ^3 - 2aXYZ = 0$$

has an integer (*or rational*) *solution.*

(2) *More precisely, for $u = 1$ it has the solution $(X,Y,Z) = (1,-1,0)$, for $u = 1/(2b)$ it has the solution $(X,Y,Z) = (0,1,-1)$, and if $y - (ax+b) = uz^3$ for some $z \in \mathbb{Q}^*$ it has the solution $(X,Y,Z) = (z^2, -x, z)$. Conversely, if (X,Y,Z) is a solution of the equation with $Z \neq 0$ then $(x,y) = (-XY/Z^2, (uX^3 - (1/u)Y^3)/(2Z^3))$ is a preimage of u in $E(\mathbb{Q})$, and $z = X/Z$.*

(3) *If the above equation has a rational solution and if u is the unique positive integer cubefree representative of $\overline{u}$, then $u_1u_2 \mid (2b)$, where $u = u_1^2u_2$ with the u_i squarefree and coprime, and the solubility of the equation is equivalent to that of*

$$u_1X^3 + u_2Y^3 + (2b/(u_1u_2))Z^3 - 2aXYZ = 0.$$

Proof. (1) and (2). The cases $u = 1$ and $u = 1/(2b)$ (corresponding to the points O and $T = (0,b)$ respectively) being clear, we assume that we are not in these cases. Then by definition if $\overline{u}$ belongs to the image of α there exist $(x,y) \in E(\mathbb{Q})$ and $z \in \mathbb{Q}^*$ such that $uz^3 = y - (ax+b)$, and if we set $X = z^2$, $Y = -x$, and $Z = z$ then

$$\begin{aligned}uX^3 + (1/u)Y^3 + 2bZ^3 - 2aXYZ &= \frac{1}{u}\,(u^2z^6 + 2uz^3(ax+b) - x^3)\\ &= \frac{1}{u}\,((uz^3 + ax + b)^2 - x^3 - (ax+b)^2)\\ &= \frac{1}{u}\,(y^2 - (x^3 + (ax+b)^2)) = 0,\end{aligned}$$

as claimed. Note that since $z \in \mathbb{Q}^*$ we have $Z \neq 0$. Conversely, let (X,Y,Z) be a solution to our equation with $Z \neq 0$. If we set $x = -XY/Z^2$ and $y = (uX^3 - (1/u)Y^3)/(2Z^3)$, we have $x^3 + (ax+b)^2 =$

$(-X^3Y^3 + Z^2(bZ^2 - aXY)^2)/Z^6$, and since by the cubic equation we have $-2Z(bZ^2 - aXY) = uX^3 + (1/u)Y^3$, it follows that

$$\begin{aligned} x^3 + (ax+b)^2 &= ((uX^3 + (1/u)Y^3)^2 - 4X^3Y^3)/(4Z^6) \\ &= (uX^3 - (1/u)Y^3)/(4Z^6) = y^2, \end{aligned}$$

so $(x, y) \in E(\mathbb{Q})$. Furthermore,

$$\begin{aligned} \alpha((x,y)) = y - (ax+b) &= (uX^3 - (1/u)Y^3)/(2Z^3) - (bZ^2 - aXY)/Z^2 \\ &= (1/(2Z^3))(uX^3 - (1/u)Y^3 - 2Z(bZ^2 - aXY)) \\ &= (1/(2Z^3))(2uX^3) = u(X/Z)^3, \end{aligned}$$

so is equal to u up to cubes, hence (x, y) is indeed a preimage of u, as claimed.

For (3), let u be the (unique) positive integer cubefree representative of $\overline{u}$, and write $u = u_1^2u_2$ with the u_i squarefree and coprime. Replacing Y by u_1u_2Y in the cubic equation we obtain the equivalent equation

$$u_1^2u_2X^3 + u_1u_2^2Y^3 + 2bZ^3 - 2au_1u_2XYZ = 0.$$

It is clear that this homogeneous cubic equation has a rational solution if and only if it has an integer solution, and we may in addition assume that $\gcd(X, Y, Z) = 1$. Assume by contradiction that $u_1u_2 \nmid 2b$. Since u_1u_2 is squarefree, this means that there exists a prime p such that $p \mid u_1u_2$ and $p \nmid 2b$. Since exchanging X and Y in the above equation is equivalent to the exchange of u_1 and u_2, we may assume that $p \mid u_1$, hence $p \nmid u_2$. Since p divides the first, second and fourth terms of the equation it divides the third, and since $p \nmid 2b$, we deduce that $p \mid Z$. Thus p^2 divides the first, third and fourth terms, so it divides the second, and since u_1 is squarefree and $p \nmid u_2$, we deduce that $p \mid Y$. Thus, p^3 divides the second, third and fourth terms, so it divides the first, and again since u_1 is squarefree and $p \nmid u_2$, we deduce that $p \mid X$, contradicting the assumption $\gcd(X, Y, Z) = 1$. We can thus divide by u_1u_2 to obtain the final equation given in (3). ■

Geometric interpretation. The plane cubic equation in (1) of Theorem 3.1 is the equation of a twist C of the elliptic curve $\widehat{E}$. We can recover a linear action by linear automorphisms by doing the following: we pick $s \in \mathbb{Q}^*$ and consider the action

$$(X : Y : Z) \mapsto (sX : (1/s)Y : Z).$$

This action gives a curve isomorphic to C with u replaced by us^3. This is what was predicted in the geometrical interpretation of [3, 4] recalled in the introduction.

4. The case $D \neq 1$.

We now assume specifically that $D \neq 1$, so that $K = \mathbb{Q}(\sqrt{D})$ is a genuine quadratic field. Note that to use 3-descent with a rational 3-torsion subgroup, we must compute the image of the 3-descent map both for the curve E and for a 3-isogenous curve $\widehat{E}$ whose $\widehat{D}$ is such that $\widehat{D} = -3D$. Thus, we always need to consider curves with $D \neq 1$. We will denote by τ the nontrivial element of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, so that $\tau(\sqrt{D}) = -\sqrt{D}$ and $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$ the norm from K to $\mathbb{Q}$, both for elements and for ideals. If $u \in K^*$ we denote by $[u]$ the class of u in K^*/K^{*3}.

4.1. *Description of the image of* α. The equation of our curve is $y^2 = x^3+D(ax+b)^2$, and the 3-descent map is a map α from $E(\mathbb{Q})$ to the subgroup G_3 of K^*/K^{*3} of classes $[u]$ of elements u such that $u\tau(u) = \mathrm{N}_{K/\mathbb{Q}}(u) \in \mathbb{Q}^{*3}$, defined by $\alpha(O) = 1$ and $\alpha((x,y)) = y - (ax+b)\sqrt{D}$ for all other points of $E(\mathbb{Q})$ (note that $T = (0, b\sqrt{D}) \notin E(\mathbb{Q})$). The image of α can be described as follows.

Theorem 4.1. *Keep the above notation.*

(1) *An element* $[u] \in G_3 \subset K^*/K^{*3}$ *belongs to the image of* α *if and only if for some* (*or any*) *representative* $u \in K^*$ *of the form* $u = v^2\tau(v)$ *the homogeneous cubic equation*

$$2v_2X^3 + 2Dv_1Y^3 + \frac{2b}{v_1^2 - Dv_2^2}Z^3 + 6v_1X^2Y + 6v_2DXY^2 + 2a(X^2Z - DY^2Z) = 0$$

has an integer (*or a rational*) *solution*, *where we write* $v = v_1 + v_2\sqrt{D}$.

(2) *More precisely*, *for* $u = 1$ *it has the solution* $(X,Y,Z) = (1,0,0)$, *and if* $y - (ax+b)\sqrt{D} = v^2\tau(v)z^3$ *for some* $z \in \mathbb{Q}^*$ *it has the solution* $(X,Y,Z) = (z_1, z_2, 1)$, *where* $z = z_1+z_2\sqrt{D}$. *Conversely*, *if* (X,Y,Z) *is a solution of the equation with* $Z \neq 0$ *then*

$$(x,y) = \left(v\tau(v)\,\frac{X^2 - DY^2}{Z^2}, v\tau(v)\,\frac{\Re(v(X+Y\sqrt{D})^3)}{Z^3}\right)$$

is a preimage of u *in* $E(\mathbb{Q})$ *with* $z = (X+Y\sqrt{D})/Z$, *where by abuse of notation we write* $\Re(\alpha) = (\alpha + \tau(\alpha))/2$.

Proof. If we set $a' = a\sqrt{D}$ and $b' = b\sqrt{D}$, and ignore for the moment all rationality questions, the equation of our curve is $y^2 = x^3 + (a'x+b')^2$, so if $y-(a'x+b') = y-(ax+b)\sqrt{D} = uz^3$ then $(X,Y,Z) = (z^2, -x, z)$ is a solution to the modified cubic equation $uX^3 + (1/u)Y^3 + 2b\sqrt{D}Z^3 - 2a\sqrt{D}XYZ = 0$, and conversely if (X,Y,Z) is such a solution then $(x,y) = (-XY/Z^2, (uX^3 - (1/u)Y^3)/(2Z^3))$ is a point on the curve. So formally there is no problem. We must now add the condition that not only $(x,y) \in E(K)$, but $(x,y) \in E(\mathbb{Q})$.

We first choose suitable representatives u. Let for the moment u be any representative of $[u]$, so that $u\tau(u)=\mu^3$ for some $\mu\in\mathbb{Q}$. This implies that $(u^2/\mu^3)\tau(u^2/\mu^3)=1$, hence by a weak form of Hilbert's Theorem 90, we have $u^2=\mu^3v/\tau(v)$ for some $v\in K$, hence $u=(u/\mu)^3\tau(v)/v=(u/(\mu v))^3v^2\tau(v)$. Since u is defined up to cubes, we may therefore assume that $u=v^2\tau(v)$ for some $v\in K^*$. Thus $u\tau(u)=\mu^3$ with $\mu=v\tau(v)$. Multiplying v by a suitable rational number we can assume that $v\in\mathbb{Z}_K$.

Now the condition $x\in\mathbb{Q}$ means that $XY/Z^2\in\mathbb{Q}$, so that $Y/Z=\lambda\tau(X/Z)$ for some $\lambda\in\mathbb{Q}^*$. The condition $y\in\mathbb{Q}$ is thus that $u\alpha^3-(\lambda^3/u)\tau(\alpha)^3\in\mathbb{Q}$, where $\alpha=X/Z$. Replacing u by $v^2\tau(v)$ and dividing by the rational number $v\tau(v)$ gives the condition $v\alpha^3-(\lambda^3/(v^3\tau(v)^2))\tau(\alpha)^3\in\mathbb{Q}$. Setting $\beta=v\alpha^3$ and $r=(\lambda/(v\tau(v)))^3\in\mathbb{Q}^*$ gives $\beta-r\tau(\beta)\in\mathbb{Q}$, so if $\beta=s+t\sqrt{D}$, we have $\beta-r\tau(\beta)=s+t\sqrt{D}-r(s-t\sqrt{D})$, hence the condition is $t(r+1)=0$, in other words either $r=-1$, so $\lambda=-\mu$, or $t=0$.

If $t=0$ then $\beta=v\alpha^3\in\mathbb{Q}$, hence $u=v^2\tau(v)=(\beta/(\alpha^2\tau(\alpha)))^3$, so $[u]$ is trivial. It follows that the case $t=0$ corresponds to the unit element of G_3, which we now exclude.

Thus we may assume that $\lambda=-\mu$. The cubic equation is thus $u\alpha^3-\tau(u\alpha^3)+2a\sqrt{D}\,\mu\alpha\tau(\alpha)+2b\sqrt{D}=0$, and since $\mu=v\tau(v)$ this gives $(v\alpha^3-\tau(v\alpha^3))/(2\sqrt{D})+a\alpha\tau(\alpha)+b/(v\tau(v))=0$. Recall that v is given, so write $v=v_1+v_2\sqrt{D}$ and $\alpha=x_1+x_2\sqrt{D}$. The above equation is thus

$$2v_2x_1^3+2Dv_1x_2^3+6v_1x_1^2x_2+6v_2Dx_1x_2^2+2a(x_1^2-Dx_2^2)+2b/(v_1^2-Dv_2^2)=0,$$

so setting $x_1=X/Z$, $x_2=Y/Z$ with X, Y, Z in $\mathbb{Z}$ we obtain finally

$$\begin{aligned}2v_2X^3+2Dv_1Y^3&+(2b/(v_1^2-Dv_2^2))Z^3\\&+6v_1X^2Y+6v_2DXY^2+2a(X^2Z-DY^2Z)=0.\end{aligned}$$

The formulas for (X,Y,Z) knowing x and y and vice versa are immediately obtained by replacing the corresponding quantities in the formula given for the case $D=1$. ■

Remarks.

(1) The cubic equation in (1) of Theorem 4.1 can be written as

$$\begin{aligned}(v(X+Y\sqrt{D})^3&-\tau(v)(X-Y\sqrt{D})^3)/\sqrt{D}\\&+2aZ(X+Y\sqrt{D})(X-Y\sqrt{D})+2b/(v\tau(v))Z^3=0.\end{aligned}$$

(2) By the theorem, the solubility of the equation depends only on the class $[u]$ of u, hence we can change v into $v\gamma^3$ for any $\gamma\in K^*$, or v into vr for any $r\in\mathbb{Q}^*$ without changing the solubility of the equation. This is of course clear directly.

(3) Since the image $\mathrm{Im}(\alpha)$ of α is a *group*, $[u]\in\mathrm{Im}(\alpha)$ if and only if $[1/u]\in\mathrm{Im}(\alpha)$, so the solubility for v is equivalent to that for v^{-1}.

Furthermore, since $\tau(u) = u^{-1}(v\tau(v))^3$, we have $[\tau(u)] \in \mathrm{Im}(\alpha)$, so the solubility for v is equivalent to that for $\tau(v)$.

(4) *Geometric interpretation.* The plane cubic equation in (1) of Theorem 4.1 is the equation of a twist C of the elliptic curve $\widehat{E}$. We get a linear action by linear automorphisms by doing the following: we pick $s \in \mathbb{Q}^*$ and consider the action

$$(X : Y : Z) \mapsto (sX : sY : (1/s^2)Z).$$

This action gives a curve isomorphic to C with u replaced by us^9.

The reader will notice that we have not given an analogous result to (3) of Theorem 3.1, which is essential since it is necessary to check only a finite number of elements of G_3. We do this in the next subsection.

4.2. *Reduction of elements of G_3.* We begin with the following lemma.

LEMMA 4.2. *Assume that x and y are rational numbers such that $y^2 = x^3 + D(ax+b)^2$, and write $x = m/d^2$ and $y = n/d^3$ with* $\gcd(m,d) = \gcd(n,d) = 1$ *and $d > 0$. Finally, set*

$$\mathfrak{f} = \gcd(n - d(am+bd^2)\sqrt{D}, n + d(am+bd^2)\sqrt{D}),$$

where the GCD is understood in the sense of ideals.

(1) *There exist integers f and g such that g is a squarefree integer dividing D, and $\mathfrak{f} = fg\mathfrak{d}$, where $\mathfrak{d}$ is the unique ideal such that $\mathfrak{d}^2 = g\mathbb{Z}_K$ (when $D = 1$ we have of course $g = 1$ and $\mathfrak{d} = \mathbb{Z}$).*

(2) *If we write $f = f_1q^3$ with f_1 cubefree then $gf_1q^2 \mid 2b$, and in particular $g \mid$* $\gcd(D, 2b)$.

(3) *If $p \mid f_1$ then p is split in $K/\mathbb{Q}$, and in particular g and f_1 are coprime.*

Proof. The case $D = 1$, which we do not need, is left to the reader, so assume that $D \neq 1$, so that K is a quadratic field. We can write uniquely $\mathfrak{f} = F\mathfrak{d}$, where $F \in \mathbb{Z}$ and $\mathfrak{d}$ is an integral ideal of K which is *primitive*, in other words not divisible by any element of $\mathbb{Z}$ other than ± 1. Evidently $\mathfrak{d}$ cannot be divisible by inert primes; since $\mathfrak{f}$ is the GCD of two conjugate elements it is stable by conjugation, hence $\mathfrak{d}$ cannot be divisible by an ideal $\mathfrak{p}$ above a split prime p, otherwise it would also be divisible by $\tau(\mathfrak{p})$, hence by $p = \mathfrak{p}\tau(\mathfrak{p})$. Finally, since $\mathfrak{p}^2 = p\mathbb{Z}_K$ for a ramified prime p, $\mathfrak{d}$ cannot be divisible by a ramified prime to a power higher than the first, so $\mathfrak{d}$ is equal to a product of distinct ramified primes. Thus $\mathfrak{d} = \prod_{\mathfrak{p} \in S_0} \mathfrak{p}$ for some set S_0 of ramified primes $\mathfrak{p}$, and if $g = \prod_{\mathfrak{p} \in S_0} p$, where p is the prime number below $\mathfrak{p}$, we thus have $\mathfrak{f} = F \prod_{p \mid g} \mathfrak{p}$ and $g \mid D$, hence also $\mathfrak{f}^2 = F^2 g$.

Let us now use our equation. Replacing x and y by m/d^2 and n/d^3 we obtain the equation

$$(n-d(am+bd^2)\sqrt{D})(n+d(am+bd^2)\sqrt{D}) = n^2 - Dd^2(am+bd^2)^2 = m^3.$$

It follows that $F^2g \mid m^3$. Let $p \mid g$ and $\mathfrak{p}$ be the prime ideal above p. Since the two factors are conjugate, if $v \geq 1$ is the $\mathfrak{p}$-adic valuation of the first factor, it is also that of the second. This implies that both $v = v_{\mathfrak{p}}(\mathfrak{f})$ and $3v_{\mathfrak{p}}(m) = 2v_{\mathfrak{p}}(\mathfrak{f})$, in other words

$$3v_p(m) = v_{\mathfrak{p}}(\mathfrak{f}) = v = v_{\mathfrak{p}}(\mathfrak{f}^2)/2 = v_{\mathfrak{p}}(F^2g)/2 = v_p(F^2g) = 1 + 2v_p(F)$$

since $p \mid g$ and g is squarefree. We deduce that $v_p(F) \equiv 1 \pmod 3$, and in particular $v_p(F) \geq 1$, so $p \mid F$, proving that $g \mid F$. Thus, $F = fg$ for some $f \in \mathbb{Z}$. The same reasoning shows that if p is *any* inert or ramified prime (dividing $\mathfrak{f}$ or not) then $3v_p(m) = v_{\mathfrak{p}}(\mathfrak{f})$, so $3 \mid v_{\mathfrak{p}}(\mathfrak{f})$.

Since $f^2g^3 \mid m^3$ we have $g \mid m$ and $f^2 \mid (m/g)^3$. Write $f = f_1q^3$ with f_1 cubefree. For all primes p we have $v_p(m/g) \geq v_p(q) + \lceil 2v_p(f_1)/3 \rceil$. Since $0 \leq v_p(f_1) \leq 2$ we have $\lceil 2v_p(f_1)/3 \rceil = v_p(f_1)$, so $f_1q^2 \mid m/g$. Note that $\mathfrak{f}^2 = f^2g^3 = f_1^2g^3q^6$, so since for any inert or ramified prime we have $3 \mid v_{\mathfrak{p}}(\mathfrak{f})$, for such a prime we have $v_p(f_1) = 0$, so f_1 is only divisible by split primes. In particular, it is coprime to D, hence to g.

Since $(n - d(am + bd^2)\sqrt{D})/(fg)$ is an algebraic integer and D is a fundamental discriminant, it follows that $fg \mid 2\gcd(n, d(am + bd^2))$, hence $fg = gf_1q^3 \mid 2\gcd(n, d(am+bd^2))$. Since $2bd^3 = 2d(am+bd^2) - 2adm$ and $gf_1q^2 \mid m$ we deduce that $2bd^3 \equiv 0 \pmod{gf_1q^2}$. Since d and n are coprime there exist integers u and v such that $un+vd^3 = 1$, hence $2b = 2bvd^3+2bun$, and since $gf_1q^2 \mid 2bd^3$ and $gf_1q^2 \mid 2n$, we have $gf_1q^2 \mid 2b$, as claimed. ∎

Corollary 4.3. *Keep the above notation, and let* $[u] \in \mathrm{Im}(\alpha) \subset G_3$. *There exists an integral ideal* $\mathfrak{v}$ *of* K *such that* $u\mathbb{Z}_K = \mathfrak{v}^2\tau(\mathfrak{v})\mathfrak{q}^3$ *for some ideal* $\mathfrak{q}$ *of* K, $\gcd(\mathfrak{v}, \tau(\mathfrak{v})) = 1$ *and* $f_1 = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{v})$ *is a cubefree divisor of* $2b$ *divisible only by primes which are split in* $K/\mathbb{Q}$.

Proof. The above lemma states that if we set

$$\mathfrak{f} = \gcd(n - d(am+bd^2)\sqrt{D}, n + d(am+bd^2)\sqrt{D})$$

there exist integers f_1, g, and q in $\mathbb{Z}$ and an ideal $\mathfrak{d} \in K$ such that $\mathfrak{f} = f_1q^3g\mathfrak{d}$ with f_1 cubefree divisible only by split primes, $g \mid \gcd(D, 2b)$, $g\mathbb{Z}_K = \mathfrak{d}^2$, and $gf_1q^2 \mid 2b$. Thus $\mathfrak{f} = f_1(q\mathfrak{d})^3$. Set $\mathfrak{a}_- = (n - d(am+bd^2)\sqrt{D})/\mathfrak{f}$ and $\mathfrak{a}_+ = (n + d(am+bd^2)\sqrt{D})/\mathfrak{f}$, so that $\gcd(\mathfrak{a}_-, \mathfrak{a}_+) = 1$ and our equation implies $\mathfrak{a}_-\mathfrak{a}_+ = m^3/\mathfrak{f}^2$ (since we work with ideals, we lose some unit information here). Since f_1 is cubefree and divisible only by split primes, it is also cubefree as an ideal, and the condition $\mathfrak{f}^2 \mid m^3$ implies as above that $f_1(q\mathfrak{d})^2 \mid m$, hence $gf_1q^2 \mid m$ (this time in $\mathbb{Z}$), so the equation now reads

$$\mathfrak{a}_-\mathfrak{a}_+ = f_1(m/(gf_1q^2))^3\mathbb{Z}_K.$$

Since $\mathfrak{f}$ is stable by conjugation, it is clear that $\mathfrak{a}_+ = \tau(\mathfrak{a}_-)$, so this equation gives the norm of $\mathfrak{a}_\pm$. In any case, write $\mathfrak{a}_- = \mathfrak{f}_-\mathfrak{q}_-^3$, $\mathfrak{a}_+ = \mathfrak{f}_+\mathfrak{q}_+^3$ with $\mathfrak{f}_\pm$ cubefree, so that in particular $\gcd(f_-, f_+) = 1$, and also $\mathfrak{f}_+ = \tau(\mathfrak{f}_-)$ and $\mathfrak{q}_+ = \tau(\mathfrak{q}_-)$. At the level of ideals our equation is thus $\mathfrak{f}_-\mathfrak{f}_+(\mathfrak{q}_-\mathfrak{q}_+)^3 = f_1(m/(gf_1q^2))^3\mathbb{Z}_K$. As we already mentioned, f_1 is also cubefree in K, and since $\mathfrak{f}_-$ and $\mathfrak{f}_+$ are coprime and cubefree, by uniqueness of the decomposition into the product of a cubefree ideal and a cube it follows that $\mathfrak{q}_-\mathfrak{q}_+ = m/(gf_1q^2)\mathbb{Z}_K$ and $\mathfrak{f}_-\mathfrak{f}_+ = f_1\mathbb{Z}_K$. In particular, $\mathfrak{f}_- \mid f_1$.

Now recall that the 3-descent map α is defined on an affine point as the class modulo cubes of $y - (ax+b)\sqrt{D} = (n - d(am+bd^2)\sqrt{D})/d^3$. Thus

$$\alpha((x,y))\mathbb{Z}_K = \mathfrak{f}\mathfrak{a}_- = f_1(q\mathfrak{d})^3\mathfrak{f}_-\mathfrak{q}_-^3 = f_1\mathfrak{f}_-(q\mathfrak{d}\mathfrak{q}_-)^3 = \mathfrak{v}^2\tau(\mathfrak{v})\mathfrak{q}_1^3$$

for some ideal $\mathfrak{q}_1$, with $\mathfrak{v} = \mathfrak{f}_-$, as claimed. ∎

Remark. It is clear that the condition $\gcd(\mathfrak{v}, \tau(\mathfrak{v})) = 1$ implies that $\mathfrak{v}$ is primitive, in other words the only elements of $\mathbb{Z}$ which divide it are ± 1. Furthermore, since $\mathfrak{v}^2\tau(\mathfrak{v}) = u\mathfrak{q}^{-3}$, the ideal class of $\mathfrak{v}$ in $Cl(K)$ belongs in fact to $(Cl(K)/Cl(K)^3)[\tau+2]$, where for any group G and map ϕ from G to G, $G[\phi]$ denotes the elements of G killed by ϕ, in other words the kernel of ϕ.

Now recall the definition of a 3-*virtual unit* (or *virtual cube*) and 3-*Selmer group*: an element $u \in K^*$ is a virtual cube if $u\mathbb{Z}_K = \mathfrak{q}^3$ is the cube of an ideal. The group of virtual cubes modulo cubes of elements is called the 3-Selmer group of K and denoted $S_3(K)$. It is clear that $S_3(K) \subset G_3$, and it is well-known and easy that we have a natural exact sequence

$$1 \to U(K)/U(K)^3 \to S_3(K) \to Cl(K)[3] \to 1.$$

Let as usual $I(K)$ denote the group of (nonzero) fractional ideals of K, and let $G_3^{\mathfrak{c}}$ be the subgroup of $I(K)/I(K)^3$ of classes of ideals whose norm is a cube.

Lemma 4.4. *We have a natural exact sequence*

$$1 \to S_3(K) \to G_3 \to G_3^{\mathfrak{c}} \to Cl(K)/Cl(K)^3 \to 1.$$

Proof. Consider first the map i from G_3 to $G_3^{\mathfrak{c}}$ which sends a class $[u]$ to the class of $u\mathbb{Z}_K$. It is clear that it does send G_3 to $G_3^{\mathfrak{c}}$. If $[u]$ is sent to the unit element of $G_3^{\mathfrak{c}}$ this means that $u\mathbb{Z}_K = \mathfrak{q}^3$ for some ideal $\mathfrak{q}$, in other words $[u] \in S_3(K)$, giving the kernel. Consider now the map sending the class of an ideal modulo cubes to its ideal class. It defines a map π from $G_3^{\mathfrak{c}}$ to $Cl(K)/Cl(K)^3$. If some ideal $\mathfrak{a}$ is sent to the unit element of $Cl(K)/Cl(K)^3$ this means that there exist an ideal $\mathfrak{q}$ and an element $\gamma \in K^*$ such that $\mathfrak{a} = \gamma\mathfrak{q}^3$. Thus, the class of $\mathfrak{a}$ modulo cubes of ideals is equal to that of $\gamma\mathbb{Z}_K$. Furthermore, the norm of $\mathfrak{a}$ is a cube, so that of γ also (since -1 is a cube), hence γ does come from G_3, proving exactness at $G_3^{\mathfrak{c}}$. Finally, let us show that the map π is surjective. Let $\mathfrak{a}$ be an ideal, representative of an element of $Cl(K)/Cl(K)^3$. Then since $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = a \in \mathbb{Q}^*$, $\mathfrak{a}\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ is in the same ideal class as $\mathfrak{a}$, and its norm is evidently equal to $(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}))^3$, so the class of $\mathfrak{a}$ is the image of the class of $\mathfrak{a}\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ in G_3^c, proving surjectivity and the lemma. ■

Corollary 4.5. *Denote by $\alpha^i = i \circ \alpha$ the* 3*-descent map from E to G_3^c. Then*

$$|\mathrm{Im}(\alpha)| = |\mathrm{Im}(\alpha^i)|\,|S_3(K) \cap \mathrm{Im}(\alpha)|.$$

In particular, if $D < 0$, $D \neq -3$, and $3 \nmid h(K)$ then $|\mathrm{Im}(\alpha)| = |\mathrm{Im}(\alpha^i)|$.

Proof. By the above lemma the map i induces an injection from $G_3/S_3(K)$ to G_3^c. Thus, for any subgroup H of G_3 the map i induces a bijection from $H/(S_3(K) \cap H)$ to $i(H)$. Applying this to the finite subgroup $\mathrm{Im}(\alpha)$ gives the formula of the corollary, and the special case corresponds to $S_3(K) = 1$. ■

Note that if γ is a 3-virtual unit then $\mathrm{N}(\gamma) = \gamma\tau(\gamma)$ is a cube. More generally, if γ is such that $\mathrm{N}(\gamma) = n^3$ is a cube we can write $\gamma = v^2\tau(v)q^3$ with $v = \gamma$ and $q = 1/n$. Thus, using Corollaries 4.3 and 4.5 and Theorem 4.1 we can compute $|\mathrm{Im}(\alpha)|$. Note however that it will be completely algorithmic and easy to prove everywhere local solubility of our homogeneous cubic equations, so that we will compute the 3-Selmer group of E. On the other hand, for global solubility, either we find a solution with a reasonable search bound, or we are led to believe that no such solution exists, coming from a nontrivial element of the 3-part of the Tate–Shafarevich group. Thus, it is reasonable to give an algorithm which computes both the rank of the 3-Selmer group and a lower bound for the rank of the curve, so which gives the exact rank when they coincide.

(1) For each class $[\gamma] \in S_3(K)$ choose a representative $\gamma \in K^*$, and check that the equation of Theorem 4.1 has a solution for $v = \gamma$ (more on this later); let T_S be the group of $[\gamma]$ for which it is everywhere locally soluble (ELS), and T_G the subgroup generated by the elements for which we find that it has a global solution. Thus $T_G \subset T \subset T_S \subset S_3(K)$, where $T = S_3(K) \cap \mathrm{Im}(\alpha)$. This will allow us to compute T exactly if $T_S = T_G$, and otherwise if the search bound is sufficiently large, we suspect (but cannot prove without further work) that in fact $T = T_G$ and that the elements of T_S/T_G correspond to nontrivial elements of the 3-part of the Tate–Shafarevich group. Note that using the fact that T_G and T_S are groups, it is not necessary to test all classes $[\gamma]$, but in fact using the fact that they are even $\mathbb{F}_3$-vector spaces it is sufficient to work on bases of these spaces and use linear algebra. Finally, choose a set R_S of representatives of $S_3(K)/T_S$ and a set R_G of representatives of T_S/T_G.

(2) Let f be the largest positive integer cubefree divisor of $2b$ divisible only by split primes, and write $f = \prod_{1\le i\le s} p_i^{v_i}$ with $1 \le v_i \le 2$. For each p_i, let $\mathfrak{p}_i$ be one of the two prime ideals above p_i, fixed once and for all. Find all ideals $\mathfrak{v}$ of the form $\mathfrak{v} = \prod_{1\le i\le s} \mathfrak{p}_i^{x_i v_i}$ with $-1 \le x_i \le 1$ whose ideal class is a cube (although this seems to be 3^s principal ideal tests, it is easy to reduce to only s such tests using linear algebra, but in practice $Cl(K)$ will be small).

(3) For each ideal $\mathfrak{v}$ that we have found write $\mathfrak{v} = u\mathfrak{q}^3$ for some ideal $\mathfrak{q}$ and some element $u \in K^*$, where clearly the class $[u]$ of u in G_3 is determined uniquely modulo multiplication by an element of $S_3(K)$. For the moment, we choose any u as above.

(4) For each $[\gamma_S] \in R_S$, where R_S is the system of representatives of $S_3(K)/T_S$ computed in (1), and any representative $\gamma_S \in K^*$, check whether the equation of Theorem 4.1 is everywhere locally soluble (ELS) for $v = u\gamma_S$ (more on this later). If this is the case for some $[\gamma_S] \in R_S$, there will be only one such class, and then $\mathfrak{v} \in \mathrm{Sel}(\alpha^i)$, with evident notation, otherwise $\mathfrak{v} \notin \mathrm{Sel}(\alpha^i)$. In the latter case, we do nothing more, otherwise for each $[\gamma_G] \in R_G$, where R_G is the system of representatives of T_S/T_G computed in (1), and any representative $\gamma_G \in K^*$, check whether the equation of Theorem 4.1 has a global solution up to a reasonable search bound for $v = u\gamma_S\gamma_R$. If this is the case, once again there will be only one such class, and then $\mathfrak{v} \in \mathrm{Im}(\alpha^i)$, otherwise we suspect (but cannot be sure) that $\mathfrak{v} \notin \mathrm{Im}(\alpha^i)$. We let I_G be the group generated by the $\mathfrak{v}$ for which we are sure, so that I_G is a subgroup of $\mathrm{Im}(\alpha^i)$, probably equal to it.

(5) At the end of this process we have computed the Selmer group cardinality $|\mathrm{Sel}(\alpha)| = |\mathrm{Sel}(\alpha^i)|\,|T_S|$, and the groups $|I_G|$ and T_G probably equal to $\mathrm{Im}(\alpha^i)$ and T respectively, but in any case satisfying $T_G \subset T \subset T_S$ and $I_G \subset \mathrm{Im}(\alpha^i) \subset \mathrm{Sel}(\alpha^i)$, and so $|I_G|\,|T_G| \mid |\mathrm{Im}(\alpha)| \mid |\mathrm{Sel}(\alpha)|$, the unknown quantity being $|\mathrm{Im}(\alpha)|$. If $|I_G|\,|T_G| = |\mathrm{Sel}(\alpha)|$ then of course these quantities are equal to $|\mathrm{Im}(\alpha)|$. Otherwise, we output both quantities, and a message saying that we expect $|\mathrm{Im}(\alpha)|$ to be equal to $|I_G|\,|T_G|$ and that the elements of $\mathrm{Sel}(\alpha)/I_GT_G$ correspond to nontrivial elements of the 3-part of the Tate–Shafarevich group.

5. Local solubility of $u_1X^3+u_2Y^3+u_3Z^3-cXYZ=0$. It remains to decide whether or not the cubic equations of Theorems 3.1 and 4.1 have a rational solution. It is unfortunately well-known that there is no algorithm for doing this. We thus proceed as follows: we first check whether the equation is everywhere locally soluble (which we will abbreviate to ELS). If not, there are no rational solutions. Otherwise, either there is an obstruction in the 3-part of the Tate–Shafarevich group, or there does exist a rational solution which we can find using a more or less efficient search. If we do find one, we are done, otherwise we give up and can only give bounds on $|\mathrm{Im}(\alpha)|$, not its precise value.

Testing ELS is an algorithmic process, but is not completely trivial. In this section we give such an algorithm. Since the degree is odd there is no need to look at local solubility in $\mathbb{R}$. We treat the following slightly more general problem: decide solubility in $\mathbb{Q}_p$ of the equation

$$F(X,Y,Z)=u_1X^3+u_2Y^3+u_3Z^3-cXYZ=0.$$

For $D=1$, in other words, for the equation of Theorem 3.1, we apply the results that we obtain with $u_3=2b/(u_1u_2)$ and $c=2a$.

5.1. *Reduction of the cubic equation and bad primes.* By multiplying X, Y, and Z by suitable powers of p it is clear that without loss of generality we may assume that u_1, u_2, u_3 and c are p-integral. Dividing by a suitable power of p we assume that

$$\min(v_p(u_1),v_p(u_2),v_p(u_3),v_p(c))=0.$$

We need further reductions, as follows.

LEMMA 5.1. *Assume as above that* $\min(v_p(u_1),v_p(u_2),v_p(u_3),v_p(c))=0$.

(1) *If* $\min(v_p(u_1),v_p(u_2),v_p(u_3))>0$ *the equation is soluble in* $\mathbb{Q}_p$.

(2) *Assume that* $v_p(c)>0$, *so that* $\min(v_p(u_1),v_p(u_2),v_p(u_3))=0$. *The equation is equivalent to one where either* $v_p(c)=0$ *or*

$$\max(v_p(u_1),v_p(u_2),v_p(u_3))\le 2.$$

(3) *Assume that* $v_p(c)>0$ *and that* $\max(v_p(u_1),v_p(u_2),v_p(u_3))\le 2$ (*which can be achieved by* (2)), *and without loss of generality order the variables so that* $0=v_p(u_1)\le v_p(u_2)\le v_p(u_3)\le 2$, *and let* $\mathbf{v}=(v_p(u_2),v_p(u_3))$. *Then*:

   (a) *If* $\mathbf{v}=(1,2)$ *the equation is not soluble in* $\mathbb{Q}_p$.

   (b) *Otherwise the equation is equivalent to one such that either* $v_p(c)=0$ *or* $v_p(u_1u_2u_3)\le 2$ (*and* $\min(v_p(u_1),v_p(u_2),v_p(u_3))=0$ *if* $v_p(c)>0$).

Thus, given a completely general cubic equation of the form $u_1X^3+u_2Y^3+u_3Z^3-cXYZ=0$, we use the following procedure, where we distinguish the cases $c\ne 0$ and $c=0$.

Assume first that $c\ne 0$.

(1) Let $g=\gcd(u_1,u_2,u_3,c)$, and replace (u_1,u_2,u_3,c) by $(u_1/g,u_2/g,u_3/g,c/g)$, so that we may now assume that $\gcd(u_1,u_2,u_3,c)=1$.

(2) For each prime $p\mid c$, do the following.

(a) By dividing u_1, u_2, u_3, and c by suitable powers of p as explained in the lemma, we reduce to an equation with either $v_p(c) = 0$ or $\max(v_p(u_1), v_p(u_2), v_p(u_3)) \leq 2$.

(b) If now $v_p(c) = 0$ or $\min(v_p(u_1), v_p(u_2), v_p(u_3)) > 0$ we do nothing more for the prime p. Otherwise, reorder the variables u_i so that $0 = v_p(u_1) \leq v_p(u_2) \leq v_p(u_3) \leq 2$.

(c) If $v_p(u_2) = 1$ and $v_p(u_3) = 2$, the equation has no solution.

(d) Otherwise, if necessary by changing (u_1, u_2, u_3, c) into
$$(u_2/p^2, u_3/p^2, pu_1, c/p),$$
we may assume that also $v_p(u_1u_2u_3) \leq 2$.

Assume now that $c = 0$.

(1) Let $g = \gcd(u_1, u_2, u_3)$, and replace (u_1, u_2, u_3) by $(u_1/g, u_2/g, u_3/g)$, so that we may now assume that $\gcd(u_1, u_2, u_3) = 1$.

(2) Replace u_1, u_2, and u_3 by their cubefree part, so that $\max(v_p(u_1), v_p(u_2), v_p(u_3)) \leq 2$.

(3) For each prime $p \mid u_1u_2u_3$, do the following.

(a) Reorder the variables u_i so that $0 = v_p(u_1) \leq v_p(u_2) \leq v_p(u_3) \leq 2$.

(b) If $v_p(u_2) = 1$ and $v_p(u_3) = 2$, the equation has no solution.

(c) Otherwise, if necessary by changing (u_1, u_2, u_3) into
$$(u_2/p^2, u_3/p^2, pu_1),$$
we may assume that also $v_p(u_1u_2u_3) \leq 2$.

This leads to the following definition:

Definition 5.2. We will say that a cubic equation is *p-reduced* if
$$\min(v_p(u_1), v_p(u_2), v_p(u_3)) = 0$$
and $v_p(u_1u_2u_3) \leq 2$ for all primes p dividing c (all primes if $c = 0$).

Thanks to the above lemma, we can therefore always assume that our cubic equation is p-reduced, since if $\min(v_p(u_1), v_p(u_2), v_p(u_3)) > 0$ the equation has a p-adic solution.

Lemma 5.3. *Let p be a prime and let $u_1X^3 + u_2Y^3 + u_3Z^3 - cXYZ = 0$ be a cubic equation with p-integral coefficients, not necessarily p-reduced. If $p \neq 3$, $v_p(u_1) = v_p(u_2) = v_p(u_3) = 0$, and $v_p(27u_1u_2u_3 - c^3) = 0$, the equation is soluble in $\mathbb{Q}_p$.*

Proof. Let us look at the singular points of the cubic over $\mathbb{F}_p$. First, a point with $Z = 0$ is singular if $u_1X^3 + u_2Y^3 = 0$, $3u_1X^2 = 0$, and $3u_2Y^2 = 0$, and since we assume $p \neq 3$ and $v_p(u_i) = 0$, this implies $X = Y = 0$, which is not possible. Thus, any singular point has $Z \neq 0$, so we may assume that $Z = 1$. Since $p \neq 3$, the equation has a singular point in $\mathbb{F}_p$ for $Z = 1$ if and only if $3u_1X^2 - cY = 0$, $3u_2Y^2 - cX = 0$, and $3u_3 - cXY = 0$. If there is such a singular point we cannot have $c = 0$, otherwise $u_3 = 0$, in other words $v_p(u_3) \geq 1$, a contradiction. Thus $Y = 3u_1X^2/c$, $X = 3u_2Y^2/c = 27u_1^2u_2X^4/c^3$, hence either $X = 0$, which is not possible since otherwise $X = Y = 0$ hence $u_3 = 0$, or $X^3 = c^3/(27u_1^2u_2)$, so that $3u_3 = cXY = 3u_1X^3 = c^3/(9u_1u_2)$, in other words $27u_1u_2u_3 - c^3 = 0$, which is also excluded. Thus the cubic is nonsingular over $\mathbb{F}_p$. Since it is a curve of genus 1 and $3 - 2\sqrt{2} > 0$, it follows from the Weil bounds that for every prime p it has a nontrivial point in $\mathbb{F}_p$. If p is not in the excluded list, this point is necessarily nonsingular, and since we assume $p \neq 3$ we can perform a Hensel lift to $\mathbb{Z}_p$ as soon as we know that there is a solution modulo p, proving the lemma. ∎

5.2. *Local solubility for $p \mid u_1u_2u_3$, $p \neq 3$.* Thanks to Lemma 5.1, we may assume that our cubic equation is p-reduced, and thanks to Lemma 5.3, it is enough to consider the primes p such that $v_p(u_1u_2u_3) > 0$, $v_p(27u_1u_2u_3 - c^3) > 0$, or $p = 3$. We begin by primes $p \neq 3$ such that $v_p(u_1u_2u_3) > 0$. For such primes, by symmetry we may assume that $v_p(u_1) > 0$, and since the equation is p-reduced we have $\min(v_p(u_2), v_p(u_3)) = 0$, so again by symmetry we may assume that $0 \leq v_p(u_1) \leq v_p(u_2) \leq v_p(u_3)$.

Lemma 5.4. *Let p be a prime and assume that our cubic equation is p-reduced, $p \neq 3$ and $v_p(u_1u_2u_3) > 0$, with $0 \leq v_p(u_1) \leq v_p(u_2) \leq v_p(u_3)$. The equation is soluble in $\mathbb{Q}_p$ if and only if one of the following conditions is satisfied.*

(1) $v_p(c) = 0$.
(2) $v_p(c) > 0$, $v_p(u_1) = v_p(u_2) = 0$, *and the class of u_1/u_2 modulo p is a cube in $\mathbb{F}_p^*$.*
(3) $v_p(c) > 0$, $v_p(u_1) = 0$, $v_p(u_2) = v_p(u_3) = 1$, *and the class of u_2/u_3 modulo p is a cube in $\mathbb{F}_p^*$.*

Remarks.

(1) Note that since the cubic equation is p-reduced, the above lemma covers all possible cases for which $p \neq 3$ and $v_p(u_1u_2u_3) > 0$: indeed, if $v_p(c) > 0$ we have necessarily $v_p(u_1u_2u_3) \leq 2$, so up to ordering either $v_p(u_1) = v_p(u_2) = 0$ (and $v_p(u_3) \leq 2$), or $v_p(u_1) = 0$ and $v_p(u_2) = v_p(u_3) = 1$.
(2) It follows from the proof that the equation is also soluble in case (1) when $p = 3$, in other words if $v_3(u_1u_2u_3) > 0$ and $v_3(c) = 0$, but the assumption $p \neq 3$ is necessary in cases (2) and (3).

5.3. *Local solubility for $p \mid (27u_1u_2u_3 - c^3)$, $p \neq 3$.* In this section, we assume that p is a prime different from 3 such that $p \mid (27u_1u_2u_3 - c^3)$. We may also assume that $p \nmid u_1u_2u_3$ since these primes have already been taken care of in the preceding subsection.

Lemma 5.5. *Let p be a prime, assume that our cubic equation is p-reduced, and assume that $p \neq 3$, $v_p(u_1u_2u_3) = 0$, and $v_p(27u_1u_2u_3 - c^3) > 0$. The equation is soluble in $\mathbb{Q}_p$ if and only if u_2/u_1 is a cube in $\mathbb{F}_p^*$.*

5.4. *Local solubility for $p = 3$.* Finally, we consider local solubility at the prime $p = 3$. By the remarks made above, when $v_3(c) = 0$ we have seen that the cubic equation is locally soluble at 3 if $v_3(u_1u_2u_3) > 0$. We may therefore assume that either $v_3(c) > 0$, or $v_3(c) = v_3(u_1u_2u_3) = 0$. In the latter case the result is immediate:

Lemma 5.6. *If $v_3(c) = 0$ the cubic equation has a solution in $\mathbb{Q}_3$.*

The final case to be treated is $v_3(c) > 0$. In this case, we need a small strengthening of Hensel's lemma, which we give in a slightly more general form that we will need below.

Lemma 5.7. *Set $P_0 = (X_0, Y_0, Z_0)$, and let $k \geq 1$. Assume that $v_3(F(P_0)) \geq 2k$ and $\min(v_3(F'_X(P_0)), v_3(F'_Y(P_0)), v_3(F'_Z(P_0))) = k$. Assume that all second and third partial derivatives of F are divisible by 3 at the point P_0, the condition on the third derivatives being required only if $k = 1$. Then there exists a 3-adic point $P = (X, Y, Z)$ such that $F(P) = 0$ with $P \equiv P_0 \pmod{3^k}$.*

Now for $F(P) = u_1X^3 + u_2Y^3 + u_3Z^3 - cXYZ$ we have for instance $F'_X(P) = 3u_1X^2 - cYZ$, and since $v_3(c) > 0$ all the partial derivatives are divisible by 3 at any point, so to apply the lemma it is enough to find a point such that $F(P_0) \equiv 0 \pmod{3^{2k}}$ and

$$\min(v_3(F'_X(P_0)), v_3(F'_Y(P_0)), v_3(F'_Z(P_0))) = k.$$

We will mainly use this lemma with $k = 1$, but we will need it also with $k = 2$.

In fact, we need a variation of the above lemma for $k = 2$.

Lemma 5.8. *Let $P_0 = (X_0, Y_0, Z_0)$ be such that*

$$v_3(F(P_0)) \geq 3 \quad \text{and} \quad \min(v_3(F'_X(P_0)), v_3(F'_Y(P_0)), v_3(F'_Z(P_0))) = 2,$$

and assume that all second, third, and fourth partial derivatives of F are divisible by 3 at P_0. Assume in addition that for all $P_1 \equiv P_0 \pmod 3$ such that $v_3(F(P_1)) \geq 3$ we also have $\min(v_3(F'_X(P_1)), v_3(F'_Y(P_1)), v_3(F'_Z(P_1))) = 2$. Then there exists a 3-adic point $P = (X, Y, Z)$ such that $F(P) = 0$ with $P \equiv P_0 \pmod 3$.

Of course for our cubics the fourth partial derivatives vanish.

Recall that a solution (X, Y, Z) of a congruence modulo some power of 3 is always such that $\min(v_3(X), v_3(Y), v_3(Z)) = 0$.

Lemma 5.9. *Let $p = 3$, assume the cubic equation is 3-reduced, and $v_3(c) > 0$, so that $v_3(u_1u_2u_3) \le 2$. Reorder the variables so that $0 = v_3(u_1) \le v_3(u_2) \le v_3(u_3)$.*

(1) *If $v_3(c) \ge 2$ and $v_3(u_1u_2u_3) = 0$ the equation has a solution in $\mathbb{Q}_3$ if and only if $u_i \equiv \pm u_j \pmod 9$ for some $i \ne j$.*
(2) *If $v_3(c) \ge 2$ and exactly one of the u_i is divisible by 3 (in other words $v_3(u_2) = 0$ and $v_3(u_3) > 0$), the equation has a solution in $\mathbb{Q}_3$ if and only if either $u_1 \equiv \pm u_2 \pmod 9$, or if $v_3(u_3) = 1$.*
(3) *If $v_3(c) \ge 2$, and two of the u_i are divisible by 3 (in other words $v_3(u_2) = v_3(u_3) = 1$ since the equation is 3-reduced), the equation has a solution in $\mathbb{Q}_3$ if and only if $u_2/3 \equiv \pm u_3/3 \pmod 9$.*
(4) *If $v_3(c) = 1$ and exactly one of the u_i is divisible by 3 (i.e., $v_3(u_2) = 0$ and $v_3(u_3) > 0$), the equation has a solution in $\mathbb{Q}_3$ if and only if either $u_1 \equiv \pm u_2 \pmod 9$, or there exist s_1 and s_2 in $\{-1, 1\}$ such that $c \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod 9$.*
(5) *If $v_3(c) = 1$ and two of the u_i are divisible by 3 (i.e., $v_3(u_2) = v_3(u_3) = 1$), the equation has a solution in $\mathbb{Q}_3$.*

Note that this lemma does not cover the case where $v_3(c) = 1$ and none of the u_i is divisible by 3, or equivalently $v_3(u_1u_2u_3) = 0$, which will be covered by Lemma 5.10 below.

Lemma 5.10. *Let $p = 3$ and assume that $v_3(c) > 0$ and $v_3(u_1u_2u_3) = 0$.*

(1) *If $u_i \equiv \pm u_j \pmod 9$ for some $i \ne j$, the cubic equation has a solution in $\mathbb{Q}_3$.*
(2) *If $u_i \not\equiv \pm u_j \pmod 9$ for $i \ne j$ (which implies that $u_1u_2u_3 \equiv \pm 1 \pmod 9$), the equation has a solution in $\mathbb{Q}_3$ if and only if there exist signs $s_1 = \pm 1$ and $s_2 = \pm 1$ such that $c \equiv s_1u_1 + s_2u_2 + s_1s_2u_3 \pmod{27}$.*

Remarks.

(1) We only assume that $v_3(c) > 0$ and not $v_3(c) = 1$, although the case $v_3(c) \ge 2$ is covered by Lemma 5.9: indeed, it is easy to see that case (2) of the above lemma cannot occur when $v_3(c) \ge 2$.
(2) It follows from the proof that case (1) occurs if and only if there exists a solution (X, Y, Z) with $\min(v_3(X), v_3(Y), v_3(Z)) = 0$ but one of the variables is divisible by 3.
(3) In case (2), there is no need to search among the four possibilities for the signs s_i: since $3 \mid c$ it is easy to see that we must take $s_1 \equiv u_2u_3 \pmod 3$ and $s_2 \equiv u_1u_3 \pmod 3$.

We have thus proved the local solubility of the general cubic equation

$$F(X, Y, Z) = u_1X^3 + u_2Y^3 + u_3Z^3 - cXYZ = 0,$$

hence in particular of the equation

$$u_1X^3 + u_2Y^3 + (2b/(u_1u_2))Z^3 - 2aXYZ = 0$$

of Theorem 3.1.

6. Local solubility: the case $D \neq 1$

6.1. *Reduction of the cubic equation, bad primes, and split primes.* We now consider local solubility when $D \neq 1$. Although we will do the same type of computations as in the case $D = 1$, there are evidently some added complications.

It is essential to begin by a reduction of the cubic equation of Theorem 4.1. Recall that in the case $D = 1$ we could reduce to an equation where $u = u_1^2u_2$ with the u_i squarefree and coprime. We have seen in Section 4.2 that the analogous statement for $D \neq 1$ involves ideals, so we cannot immediately reproduce what we have done.

Recall that the cubic equation of Theorem 4.1 can be written as $F(X,Y,Z) = 0$, where if $v = v_1 + v_2\sqrt{D}$ we have

$$\begin{aligned}F(X,Y,Z) &= 2v_2X^3 + 2Dv_1Y^3 + (2b/(v_1^2 - Dv_2^2))Z^3\\&\quad + 6v_1X^2Y + 6v_2DXY^2 + 2a(X^2Z - DY^2Z)\\&= (v(X+Y\sqrt{D})^3 - \tau(v)(X-Y\sqrt{D})^3)/\sqrt{D}\\&\quad + 2aZ(X+Y\sqrt{D})(X-Y\sqrt{D}) + (2b/(v\tau(v)))Z^3,\end{aligned}$$

and we will use both forms interchangeably.

Lemma 6.1. *If $p \neq 3$, $v_p(v\tau(v)) = 0$, $v_p(2b) = 0$, and $v_p(27b-4a^3D) = 0$ the above cubic equation is soluble in $\mathbb{Q}_p$.*

Recall that, analogously to ideals, an algebraic integer v is said to be *primitive* if $v/n \in \mathbb{Z}_K$ with $n \in \mathbb{Z}$ if and only if $n = \pm 1$.

Lemma 6.2. *Let $[u] \in \mathrm{Im}(\alpha)$. In the above cubic equation, we may assume that $[u] = [v^2\tau(v)]$ where v is a primitive algebraic integer such that $v\tau(v)$ is divisible only by split primes. In particular, v and $\tau(v)$ generate coprime ideals. Furthermore, if $D \equiv 0 \pmod 4$ we may also assume that $v = v_1 + v_2\sqrt{D}$ with $v_2 \in \mathbb{Z}$.*

Note that, in contrast to the case $D = 1$, we cannot deduce from this lemma that $v\tau(v) \mid 2b$. It is easy to show using Corollary 4.3 that if $3 \nmid h(K)$, we may assume that $v\tau(v) \mid (2b)^{h(K)}$, and in particular all prime numbers dividing $v\tau(v)$ (which are necessarily split) divide $2b$, but this may not be true if $3 \mid h(K)$.

Since v is now an algebraic integer, we have $2v_1 \in \mathbb{Z}$ and $2v_2 \in \mathbb{Z}$, so all the coefficients of the equation are integers, except perhaps for $2b/(v\tau(v))$.

Corollary 6.3. *Assume as above that $v = v_1 + v_2\sqrt{D}$ is a primitive algebraic integer such that $v\tau(v)$ is divisible only by split primes, and let p be any split prime. There exists $d_p \in \mathbb{Q}_p$ such that $d_p^2 = D$. The cubic equation of Theorem* 4.1 *has a solution in $\mathbb{Q}_p$ if and only if the equation $u_1X^3+u_2Y^3+u_3Z^3-cXYZ=0$ does, where $u_1 = v_1+v_2d_p$, $u_2 = v_1-v_2d_p$, $u_3 = (2b/v\tau(v))d_p$, and $c = 2ad_p$.*

Since we have given a complete algorithm to determine the solubility in $\mathbb{Q}_p$ of an equation of the type $u_1X^3+u_2Y^3+u_3Z^3-cXYZ=0$, this solves the problem for $D \neq 1$ in the case where p is a split prime. Thus we are left with the study of ramified and inert primes, so thanks to Lemma 6.2, we may assume that $v_p(v\tau(v)) = 0$, so in particular $v_p(2b/(v\tau(v))) \geq 0$.

Thus we assume that p is a ramified or inert prime, and $v_p(v\tau(v)) = 0$, and recall that our equation is $F(X,Y,Z) = 0$ with

$$F(X,Y,Z) = (v(X+Y\sqrt{D})^3 - \tau(v)(X-Y\sqrt{D})^3)/\sqrt{D} + u_3Z^3 \\ + 2aZ(X+Y\sqrt{D})(X-Y\sqrt{D}),$$

with $u_3 = 2b/(v\tau(v))$, hence $v_p(u_3) \geq 0$. We begin with inert primes.

6.2. *The case of inert primes.* If p is an inert prime, consider the field $K_p = \mathbb{Q}_p(\sqrt{D})$, which up to isomorphism is the unique unramified extension of degree 2 of $\mathbb{Q}_p$, and whose residue field is $\mathbb{F}_{p^2}$, so that we can also consider the class of $\sqrt{D}$ in $\mathbb{F}_{p^2}^*$, and τ is defined on $\mathbb{F}_{p^2}$ as in characteristic 0. By abuse of notation, if α and β are elements of $K = \mathbb{Q}(\sqrt{D})$ or of K_p, we will write $\alpha \equiv \beta \pmod{p}$ to mean that the class of α and β in the residue field is the same. Note that we work in K_p or K for practicality, but that the cubic equation has coefficients in $\mathbb{Q}$, and we also look for solutions in $\mathbb{Q}$.

Before studying the bad primes, we need an auxiliary lemma.

Lemma 6.4. *Let $p \neq 3$ be an inert prime. The following conditions are equivalent*:

(1) *There exist X and Y such that $\tau(v)/v \equiv ((X+Y\sqrt{D})/(X-Y\sqrt{D}))^3 \pmod{p}$ in the above sense.*

(2) *The class of $\tau(v)/v$ is a cube in $\mathbb{F}_{p^2}^*$.*

(3) *Either $p \equiv 1 \pmod{3}$, or $p \equiv 2 \pmod{3}$ and $v^{(p^2-1)/3} \equiv 1 \pmod{p}$.*

Lemma 6.5. *Let $D \neq 1$, and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2. *Let p be an inert prime number such that $v_p(2b) > 0$, $v_p(v\tau(v)) = 0$ and $p \neq 3$, and if $p = 2$, assume that $v_p(2b) \leq 2$. The cubic equation of Theorem* 4.1 *is locally soluble at p if and only if one of the following conditions is satisfied.*

(1) *$v_p(2a) = 0$.*

(2) *$v_p(2a) > 0$ and the class of $\tau(v)/v$ modulo p is a cube in $\mathbb{F}_{p^2}^*$.*

We now consider the prime $p = 2$, assumed to be inert, when $v_2(2b) \geq 3$. Since the equation is 2-reduced, note that either $v_2(a) > 0$, in which case $v_2(b) \leq 2$ hence $v_2(2b) = 3$, or $v_2(a) = 0$. Furthermore, we can write $v = v_1 + v_2\sqrt{D} = (w_1 + w_2\sqrt{D})/2$ with w_1 and w_2 in $\mathbb{Z}$ such that $w_1 \equiv w_2 \pmod{2}$, and since v is primitive, either $w_1 \equiv w_2 \equiv 1 \pmod{2}$, or w_1 and w_2 are even with $w_1 \not\equiv w_2 \pmod{4}$.

LEMMA 6.6. *Let $D \neq 1$, and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2. *Assume that $p = 2$ is an inert prime, in other words $D \equiv 5 \pmod{8}$, and that $v_2(2b) \geq 3$, and write $w_1 = 2v_1$ and $w_2 = 2v_2$.*

(1) *If $w_1 \equiv 2 \pmod{4}$ and $w_2 \equiv 0 \pmod{4}$ or $w_1 \equiv 0 \pmod{4}$ and $w_2 \equiv 2 \pmod{4}$ the equation has a solution in $\mathbb{Q}_2$.*
(2) *If $w_1 \equiv w_2 \equiv 1 \pmod{2}$, the equation has a solution in $\mathbb{Q}_2$ if and only if either $v_2(2b) \geq 4$ or $v_2(a) > 0$.*

LEMMA 6.7. *Let $D \neq 1$, and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2. *Let p be an inert prime number such that $v_p(2b) = v_p(v\tau(v)) = 0$, $v_p(27b - 4Da^3) > 0$, and $p \neq 3$. The equation of Theorem* 4.1 *is locally soluble at p if and only if $\tau(v)/v$ is a cube in $\mathbb{F}_{p^2}^*$.*

Recall that $v_p(v\tau(v)) = 0$ since we assume that p is not split.

LEMMA 6.8. *Let $D \neq 1$ and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2, *and that $p = 3$ is an inert prime, i.e., $D \equiv 2 \pmod{3}$. Set $u_1 = 2v_2$, $u_2 = 2v_1D$, and $u_3 = 2b/(v\tau(v))$.*

(1) *If $v_3(2a) = 0$ the equation has a solution in $\mathbb{Q}_3$.*
(2) *If $v_3(2a) \geq 2$ the equation has a solution in $\mathbb{Q}_3$ if and only if either $v_3(u_1) \geq 2$, $v_3(u_2) \geq 2$, $u_i \equiv \pm u_j \pmod{9}$ for some $i \neq j$ and a suitable sign, or $u_3 \equiv 2(\pm u_1 \pm u_2) \pmod{9}$ for suitable signs.*
(3) *If $v_3(2a) = 1$, $v_3(2b) > 0$, and $v_3(u_1u_2) \geq 1$, the equation has a solution in $\mathbb{Q}_3$ if and only if either $v_3(u_1) \geq 2$ and $v_3(u_2) \geq 2$, or $v_3(2a + 2b) = 1$.*
(4) *If $v_3(2a) = 1$, $v_3(2b) > 0$, and $v_3(u_1u_2) = 0$, the equation has a solution in $\mathbb{Q}_3$ if and only if either $u_1 \equiv \pm u_2 \pmod{9}$, or $2a + b \equiv \pm u_1 \pm u_2 \pmod{9}$ for suitable signs.*

LEMMA 6.9. *Let $D \neq 1$ and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2, *and that $p = 3$ is an inert prime, i.e., $D \equiv 2 \pmod{3}$. Set $u_1 = 2v_2$, $u_2 = 2v_1D$, and $u_3 = 2b/(v\tau(v))$. Assume that $v_3(2a) = 1$ and $v_3(u_1) = v_3(u_2) = v_3(2b) = 0$, and set $u_4 = u_3 + 2a$, so that also $v_3(u_4) = 0$.*

(1) *If* $u_i \equiv \pm u_j \pmod 9$ *for some* $i \neq j$ *with* $i, j = 1$, 2, *or* 4, *the equation has a solution in* $\mathbb{Q}_3$.

(2) *Otherwise*, *the equation has a solution in* $\mathbb{Q}_3$ *if and only if* $2a+u_4 = 4a+u_3 \equiv \pm 3D \pmod{27}$ *for a suitable sign.*

Similar remarks to those given after Lemma 5.10 apply here.

This concludes the study of local solubility in the case of inert primes.

6.3. *The case of ramified primes*

Lemma 6.10. *Let* $D \neq 1$ *and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2. *If* p *is a ramified prime such that* $p \neq 3$, *the equation is soluble in* $\mathbb{Q}_p$.

Lemma 6.11. *Let* $D \neq 1$ *and assume that the elliptic curve is given by an equation satisfying the conditions of Lemmas* 1.2 *and* 6.2. *Assume* $p = 3$ *is ramified*, *in other words* $3 \mid D$, *and to simplify notation*, *set* $u_3 = 2b/(v\tau(v))$.

(1) *If* $v_3(2a) = 0$, *the equation has a solution if and only if one of the following conditions is satisfied*:

(a) $v_3(2v_2) > 0$.

(b) $v_3(2v_2) = v_3(2a + u_3) = 0$.

(2) *If* $v_3(2a) \geq 2$, *the equation has a solution if and only if one of the following conditions is satisfied*:

(a) $D \equiv 3 \pmod 9$ *and* $v_3(u_3) = 0$.

(b) $D \equiv 3 \pmod 9$, $v_3(u_3) > 0$, *and* $v_3(2v_2) > 0$.

(c) $D \equiv 6 \pmod 9$ *and* $v_3(2v_2) \geq 2$.

(d) $D \equiv 6 \pmod 9$ *and* $v_3(2v_2) = v_3(u_3) = 1$.

(e) $D \equiv 6 \pmod 9$, $v_3(2v_2) = 0$, *and* $u_3 \equiv \pm 2v_2 \pmod 9$.

(f) $u_3 \equiv \pm 2v_1 D \pmod{27}$.

We will treat the case where $v_3(2a) = 1$ below.

Lemma 6.12. *Keep the notation and assumptions of the preceding lemma*, *assume that* $v_3(2a) = 1$, *and set* $u_4 = u_3 + 2a$. *The cubic equation has a solution if and only if one of the following conditions is satisfied*:

(a) $D \equiv 3 \pmod 9$ *and* $v_3(u_4) = 0$.

(b) $D \equiv 3 \pmod 9$, $v_3(u_4) > 0$, *and* $v_3(2v_2) > 0$.

(c) $D \equiv 6 \pmod 9$ *and* $v_3(2v_2) \geq 2$.

(d) $D \equiv 6 \pmod 9$ *and* $v_3(2v_2) = v_3(u_4) = 1$.

(e) $D \equiv 6 \pmod 9$, $v_3(2v_2) = 0$, *and* $u_4 \equiv \pm 2v_2 \pmod 9$.

(f) $v_3(u_3) = 1$ *and there exists* $s = \pm 1$ *such that* $2v_1(D/3) \equiv s(u_3/3 - 2a(D/3)) \pmod 9$ *and* $2v_1 s \not\equiv 2a/3 \pmod 3$.

(g) $v_3(u_3) = 1$ *and there exists* $s = \pm 1$ *such that* $2v_1(D/3) \equiv s(u_3/3 - 2a(D/3)) \pmod 9$, $2v_1 s \equiv 2a/3 \pmod 3$, $v_3(2v_2) = 0$, *and* $D \equiv 3 \pmod 9$.

(h) $v_3(u_3) = 1$ *and there exists* $s = \pm 1$ *such that* $2v_1(D/3) \equiv s(u_3/3 - 2a(D/3)) \pmod{27}$, $2v_1 s \equiv 2a/3 \pmod 3$, $v_3(2v_2) = 0$, *and* $D \equiv 6 \pmod 9$.

(i) $v_3(u_3) = 1$ *and there exists* $s = \pm 1$ *such that* $2v_1 s \equiv 2a/3 \pmod 3$, $v_3(2v_2) > 0$, *and there exists* $t \in \{-1, 0, 1\}$ *and* $r \in \{-1, 0, 1\}$ *such that*

$$2v_1(D/3) \equiv s(u_3/3 - 2a(D/3)) - 6v_2(D+3)t - 9(2v_1 s - 2a/3)st^2 \\ - 3r(D(2v_1 + a/3) + 6rDv_1 + 6at^2) \pmod{81}.$$

This finishes the study of local solubility.

7. Examples

7.1. *The curves* $y^2 = x^3 + (kp)^2$ *for* $k = 1$, 2, *or* 4. In this section we consider the family of curves E_{kp} with equation $y^2 = x^3 + (kp)^2$, where p is a prime and $k = 1$, 2, or 4. The restriction on k is made so that no other prime apart from 2 divides it. Note that it is not necessary to consider higher powers of 2 since the curve $y^2 = x^3 + (8kp)^2$ is trivially isomorphic to $y^2 = x^3 + (kp)^2$. Furthermore, the primes $p = 2$ and 3 give rise to a finite number of curves which can be treated individually (specifically, for $p = 2$ the rank is equal to 0, for $(k, p) = (1, 3)$ and $(2, 3)$ the rank is 1, Mordell–Weil generators being $(-2, 1)$ and $(-3, 3)$ respectively, and for $(k, p) = (4, 3)$ the rank is again 0, and the torsion is always of order 3 generated by $T = (0, kp)$, except for $(k, p) = (4, 2)$, for which it has order 6 generated by $(8, 24)$). We therefore assume that $p \geq 5$, so that in particular all of these curves have rational 3-torsion generated by $T = (0, kp)$ equal to their full rational torsion subgroup.

We first compute the image of α. For this, we consider the cubic equations of Theorem 3.1(3), in other words $u_1X^3 + u_2Y^3 + u_3Z^3 = 0$, where $u_1u_2 \mid 2kp$ and $u_3 = 2kp/(u_1u_2)$, where we recall that u_1u_2 is squarefree. Up to exchange of u_1 and u_2, it is easy to check that the only possibilities are $(1, 1, 2kp)$, $(1, 2, kp)$, $(1, p, 2k)$, $(1, 2p, k)$, and $(2, p, k)$. The first one (corresponding to $u = 1$) gives an evidently soluble equation, corresponding to the unit element of the elliptic curve.

- When $k = 1$, the fourth one (corresponding to $u = 2p$ and $u = 4p^2$) is also soluble, and it corresponds to the two nontrivial rational 3-torsion points on the curve, and the other three (corresponding to $u = 2$, 4, p, p^2, $4p$, and $2p^2$) are equivalent.

- When $k = 2$, the fifth one (corresponding to $u = 4p$ and $u = 2p^2$) is also soluble, and it again corresponds to the two nontrivial rational 3-torsion points on the curve, the second and fourth (corresponding to $u = 2$, 4, $2p$, and $4p^2$) are equivalent, and the third corresponds to $u = p$ and p^2. Since the set (of classes) of u for which the equation is soluble forms a group and since $4p$ and $2p^2$ belong to this group, it follows that $[p]$ and $[p^2]$ will be in the group if and only if 4 and 2 are, so in fact the three equations are equivalent, although slightly less trivially.
- Finally, when $k = 4$ the third equation (corresponding to p and p^2) is clearly soluble (since $2k = 8$ is a cube), and this again corresponds to the two rational 3-torsion points. The other equations correspond respectively to $u = 2$ and 4, $u = 2p$ and $4p^2$, and $u = 4p$ and $2p^2$, and once again because of the group structure all the equations are in fact equivalent.

We see that in each case it is sufficient to consider the equation with $u_1 = 1$, $u_2 = 2$, hence $u_3 = kp$. The result is as follows:

Lemma 7.1. *Keep the above assumptions. The equation $X^3 + 2Y^3 + kpZ^3 = 0$ is ELS if and only if $k \neq 4$, either $p \equiv 2 \pmod 3$ or $2^{(p-1)/3} \equiv 1 \pmod 3$, and $kp \not\equiv \pm 4 \pmod 9$.*

Proof. This of course immediately follows from the above study. More precisely, if $k = 4$ the 2-adic valuations of the coefficients are $(0, 1, 2)$, so the equation has no 2-adic solutions by Lemma 5.1. On the other hand, if $k = 1$ or $k = 2$, the 2-adic valuations are $(0, 0, 1)$ and $(0, 1, 1)$ respectively, and since all elements of $\mathbb{F}_2^*$ are cubes, we conclude by Lemma 5.4 that the equation has a solution in $\mathbb{Q}_2$. For p-adic solubility we also use this lemma, since the p-adic valuations are $(0, 0, 1)$, and we conclude that the equation has a p-adic solution if and only if 2 is a cube in $\mathbb{F}_p^*$, leading to the given condition. Finally, since the 3-adic valuations are $(0, 0, 0)$ we use Lemma 5.9(1), which tells us that the equation has a 3-adic solution if and only if $u_i \equiv \pm u_j \pmod 9$ for some $i \neq j$, which gives $kp \equiv \pm 1$ or $\pm 2 \pmod 9$, in other words $kp \not\equiv \pm 4 \pmod 9$ since $3 \nmid kp$. ∎

Corollary 7.2. *Let $p \geq 5$ be prime, let $k = 1$, 2, or 4, and let E be the elliptic curve $y^2 = x^3 + (kp)^2$.*

(1) *For $k = 1$, if either $p \equiv \pm 4 \pmod 9$, or $p \equiv 1$ or $7 \pmod 9$ and $2^{(p-1)/3} \not\equiv 1 \pmod p$, then $\mathrm{Im}(\alpha) = \{1, 2p, 4p^2\}$, and in particular $|\mathrm{Im}(\alpha)| = 3$.*

(2) *For $k = 1$ and $p \equiv 2 \pmod 9$ we have $|\mathrm{Im}(\alpha)| = 9$.*

(3) *For $k = 2$, if either $p \equiv \pm 2 \pmod 9$, or $p \equiv 1$ or $4 \pmod 9$ and $2^{(p-1)/3} \not\equiv 1 \pmod p$, then $\mathrm{Im}(\alpha) = \{1, 4p, 2p^2\}$, and in particular $|\mathrm{Im}(\alpha)| = 3$.*

(4) *For* $k = 4$ *we always have* $\mathrm{Im}(\alpha) = \{1, p, p^2\}$, *and in particular* $|\mathrm{Im}(\alpha)| = 3$.

(5) *In all other cases*, $|\mathrm{Im}(\alpha)| = 3$ *or* 9. *More precisely*, *the cubic equation* $X^3 + 2Y^3 + kpZ^3 = 0$ *is ELS*, *and* $|\mathrm{Im}(\alpha)| = 9$ *if and only if it is globally soluble.*

Proof. (1), (3), (4), and (5) are clear from the lemma by inspection. For (2), we use Proposition 3.3, p. 438 of Satgé [14]. ∎

Remark. In [12], Rodríguez Villegas and Zagier have characterized the primes which are sums of two cubes. If their method could be extended to primes which are of the form $x^3 + 2y^3$, and also of the form $x^3 + 4y^3$, it would determine $\mathrm{Im}(\alpha)$ in all cases.

We now compute the image on the dual curve $\widehat{E}$, whose equation is $y^2 = x^3 - 27(kp)^2$, so that $D = -3$ and $b = 3kp$. We first determine local solubility of the equation corresponding to $\rho = (-1 + \sqrt{-3})/2$, and for the moment we do not necessarily assume that $k \mid 4$.

Lemma 7.3.

(1) *Let* k *be such that* $8 \nmid k$. *The equation corresponding to* ρ *is locally soluble at the primes* 2, 3, *and* p *if and only if* $p \equiv \pm 1 \pmod 9$, $k \equiv \pm 4 \pmod 9$, *and* $4 \mid k$.

(2) *In particular*, *if* $k = 1$, 2, *or* 4, *the equation corresponding to* ρ *is ELS if and only if* $k = 4$ *and* $p \equiv \pm 1 \pmod 9$.

Proof. We have $2v_1 = -1$, $2v_2 = 1$, and $2b = 6kp$, so $u_3 = 2b/(v\tau(v)) = 6kp$. The prime 2 being inert, by Lemma 6.5, if $4 \nmid k$ the equation is locally soluble at 2 if and only if ρ is a cube in $\mathbb{F}_4^*$, which is not the case since the only cube is 1. On the other hand, if $4 \mid k$ Lemma 6.6 tells us that the equation is locally soluble at 2. Let us now look at the prime p. If $p \equiv 1 \pmod 3$ then p is split, so by Corollary 6.3 the equation is locally soluble at p if and only if $(v_1 + v_2 d_p)X^3 + (v_1 - v_2 d_p)Y^3 + 6kpZ^3 = 0$ is, and since the p-adic valuations are $(0, 0, \geq 1)$, by Lemma 5.4 this is true if and only if $(v_1 + v_2 d_p)/(v_1 - v_2 d_p) \equiv \rho^2/\rho = \rho \pmod p$ is a cube in $\mathbb{F}_p^*$, hence if and only if $\rho^{(p-1)/3} \equiv 1 \pmod p$, which is the case if and only if $p \equiv 1 \pmod 9$. If $p \equiv 2 \pmod 3$ then p is inert, so by Lemma 6.5 the equation is locally soluble at p if and only if ρ is a cube in $\mathbb{F}_{p^2}^*$, hence if and only if $p^2 \equiv 1 \pmod 9$, in other words $p \equiv -1 \pmod 9$ since we assume $p \equiv 2 \pmod 3$. It follows that the local condition at p is $p \equiv \pm 1 \pmod 9$. Finally, let us look at the prime 3. Since $2a = 0$ we use Lemma 6.11(2), which tells us that the equation is locally soluble at 3 if and only if $6kp \equiv \pm 3 \pmod{27}$, or equivalently $kp \equiv \pm 4 \pmod 9$, proving (1) since $p \equiv \pm 1 \pmod 9$, and (2) follows immediately. ∎

Next, we assume that $p \equiv 1 \pmod 3$. In this case we can write $p = \pi\tau(\pi)$ with $\pi = (w_1 + w_2\sqrt{-3})/2$ in 12 different ways, and it is well-known and easy that up to sign and exchange of π and $\tau(\pi)$ there is exactly one such decomposition with $3 \mid w_2$.

Lemma 7.4. *Let $p \equiv 1 \pmod 3$, let $\pi = (w_1 + w_2\sqrt{-3})/2$ be such that $\pi\tau(\pi) = p$, and let k be such that $8 \nmid k$, $3 \nmid k$, and $p \nmid k$. The equation corresponding to π is locally soluble at the primes 2, 3, and p if and only if* (a) *either $4 \mid k$ or $4 \nmid k$ and $2 \mid w_2 \in \mathbb{Z}$, and* (b) $(w_1/(2k))^{(p-1)/3} \equiv 1 \pmod p$, *and* (c) *either $3 \mid w_2$, or $3 \nmid w_2$ and $p \equiv k^2 + 3 \pmod 9$.*

Proof. We have $2v_1 = w_1$, $2v_2 = w_2$, and $u_3 = 2b/(v\tau(v)) = 6k$. The prime 2 being inert, as above Lemmas 6.5 and 6.6 tell us that the equation is locally soluble at 2 if and only if either $4 \mid k$, or $4 \nmid k$ and $(w_1+w_2\sqrt{-3})/2 = 1$ in $\mathbb{F}_4^*$, which is equivalent to $2 \mid w_2$. By Corollary 6.3 the equation is locally soluble at p if and only if $(v_1 + v_2d_p)X^3 + (v_1 - v_2d_p)Y^3 + 6kd_pZ^3 = 0$ is. Since $v_1^2 - v_2^2d_p^2 = p$, we may assume for instance that d_p is chosen so that $v_p(v_1 - v_2d_p) = 1$, so in particular $v_2d_p \equiv v_1 \pmod p$. The p-adic valuations of the coefficients are thus $(0, 1, 0)$, so by Lemma 5.4 local solubility is equivalent to $(v_1 + v_2d_p)/(6kd_p)$ being a cube in $\mathbb{F}_p^*$, and since $v_1 \equiv v_2d_p \pmod p$, this means that $v_1/(3kd_p) = w_1/(6kd_p)$ is a cube in $\mathbb{F}_p^*$. This is equivalent to $(w_1/(6kd_p))^2 = -w_1^2/(108k^2)$ being a cube, hence to $(w_1/(2k))^2$ being a cube, hence to $w_1/(2k)$ being a cube, leading to the given condition. Finally, let us look at the prime 3. Since $2a = 0$ we use Lemma 6.11(2), which tells us (since $3 \nmid k$, so that $v_3(u_3) = 1$) that the equation is locally soluble at 3 if and only if either $3 \mid w_2$, or $6k \equiv \pm 3w_1 \pmod{27}$, in other words $2k \equiv \pm w_1 \pmod 9$. However, since $w_1^2 + 3w_2^2 = 4p$, if $3 \nmid w_2$ we have $w_1^2 \equiv 4p - 3 \pmod 9$, and since the condition $2k \equiv \pm w_1 \pmod 9$ is equivalent to $w_1^2 \equiv 4k^2 \pmod 9$ (since $3 \nmid w_1$), we obtain the equivalent condition $4p \equiv 4k^2 + 3 \pmod 9$, or equivalently $p \equiv k^2 + 3 \pmod 9$, finishing the proof of the lemma. ∎

Corollary 7.5. *Let $p \geq 5$ be prime, let $k = 1$, 2, or 4, and let $\widehat{E}$ be the elliptic curve $y^2 = x^3 - 27(kp)^2$.*

(1) *For $k = 1$ or $k = 2$, if either $p \equiv 2 \pmod 3$, or $p \equiv 1 \pmod 3$ and $p \not\equiv k^2 + 3 \pmod 9$, and $2^{(p-1)/3} \not\equiv 1 \pmod p$, then $\operatorname{Im}(\widehat{\alpha})$ is trivial.*
(2) *For $k = 4$, if $p \equiv 2$ or $5 \pmod 9$ then $\operatorname{Im}(\widehat{\alpha})$ is trivial.*
(3) *Otherwise, $|\operatorname{Im}(\widehat{\alpha})| = 1$ or 3 when $k = 1$, $k = 2$, or $k = 4$ and $p \equiv 8 \pmod 9$, and $|\operatorname{Im}(\widehat{\alpha})| = 1$, 3, or 9 when $k = 4$ and $p \equiv 1 \pmod 3$.*

Proof. Since $2b = 6kp$, 2 is inert, and 3 is ramified, with the notation of Section 4.2, we must have $f_1 = 1$ if $p \equiv 2 \pmod 3$ and $f_1 = 1$ or p if $p \equiv 1 \pmod 3$. In the first case, the only possible v are 1, ρ, and ρ^2, while in the second case we have in addition the three possible π (up to sign and conjugation) such that $\pi\tau(\pi) = p$. It follows that:

- If $\rho \notin \mathrm{Im}(\widehat{\alpha})$ and none of the three possible π is in $\mathrm{Im}(\widehat{\alpha})$ then $\mathrm{Im}(\widehat{\alpha}) = \{1\}$, so $|\mathrm{Im}(\widehat{\alpha})| = 1$.
- If $\rho \notin \mathrm{Im}(\widehat{\alpha})$ and one of the three possible π (so necessarily exactly one) is in $\mathrm{Im}(\widehat{\alpha})$ then $\mathrm{Im}(\widehat{\alpha}) = \{1, \pi, \tau(\pi)\}$, hence $|\mathrm{Im}(\widehat{\alpha})| = 3$.
- If $\rho \in \mathrm{Im}(\widehat{\alpha})$ and none of the three possible π (in this case they are equivalent) is in $\mathrm{Im}(\widehat{\alpha})$ then $\mathrm{Im}(\widehat{\alpha}) = \{1, \rho, \rho^2\}$, hence $|\mathrm{Im}(\widehat{\alpha})| = 3$.
- If $\rho \in \mathrm{Im}(\widehat{\alpha})$ and one of the three possible π is in $\mathrm{Im}(\widehat{\alpha})$ (hence all are) then $\mathrm{Im}(\widehat{\alpha}) = \{\rho^j, \rho^j\pi, \rho^j\tau(\pi) : 0 \le j \le 2\}$, hence $|\mathrm{Im}(\widehat{\alpha})| = 9$.

Since in the two preceding lemmas we have studied local solubility of the equation in all these cases, we conclude by inspection. ■

We can say a little more:

Proposition 7.6.

(1) *Assume that* $k = 1$ *and* $p \equiv 4 \pmod 9$, *or that* $k = 2$ *and* $p \equiv 7 \pmod 9$, *and write* $p = m^2 + 3n^2$, *where* m *and* n *are integers which are unique up to sign. The equation corresponding to* $\pi = m + n\sqrt{-3}$ (*i.e., with* $v_1 = m$ *and* $v_2 = n$) *is ELS*, *and* $|\mathrm{Im}(\widehat{\alpha})| = 3$ *if and only if it is globally soluble.*

(2) *Assume that* $k = 4$ *and* $p \equiv 8 \pmod 9$. *The equation corresponding to* ρ *is ELS*, *and* $|\mathrm{Im}(\widehat{\alpha})| = 3$ *if and only if it is globally soluble.*

(3) *Assume that* $k = 4$ *and* $p \equiv 4$ *or* $7 \pmod 9$, *and write* $4p = m^2 + 27n^2$, *where* m *and* n *are unique up to sign. The equation corresponding to* $\pi = (m + 3n\sqrt{-3})/2$ (*i.e., with* $v_1 = m/2$ *and* $v_2 = 3n/2$) *is ELS*, *and* $|\mathrm{Im}(\widehat{\alpha})| = 3$ *if and only if it is globally soluble.*

Proof. Apply the same method as above. ■

We will see below that it follows from BSD that these equations (of Proposition 7.6) should in fact always be globally soluble.

Corollary 7.7.

(1) *If* $p \equiv 5 \pmod 9$, *or* $p \equiv 1$ *or* $7 \pmod 9$ *and* $2^{(p-1)/3} \not\equiv 1 \pmod p$, *the elliptic curve* E_p *with equation* $y^2 = x^3 + p^2$ *has rank* 0. *If* $p \equiv 2 \pmod 9$, *it has rank* 1. *Otherwise*, *if* $p \equiv 4$ *or* $8 \pmod 9$ *it has rank* 0 *or* 1, *and if* $p \equiv 1$ *or* $7 \pmod 9$ *it has rank* 0, 1, *or* 2.

(2) *If* $p \equiv 2 \pmod 9$, *or* $p \equiv 1$ *or* $4 \pmod 9$ *and* $2^{(p-1)/3} \not\equiv 1 \pmod p$, *the elliptic curve* E_{2p} *with equation* $y^2 = x^3 + 4p^2$ *has rank* 0. *Otherwise*, *if* $p \equiv 5$, 7, *or* $8 \pmod 9$ *it has rank* 0 *or* 1, *and if* $p \equiv 1$ *or* $4 \pmod 9$ *it has rank* 0, 1, *or* 2.

(3) *If* $p \equiv 2$ *or* $5 \pmod 9$ *the elliptic curve* E_{4p} *with equation* $y^2 = x^3 + 16p^2$ *has rank* 0. *Otherwise*, *if* $p \equiv 4$, 7, *or* $8 \pmod 9$ *it has rank* 0 *or* 1, *and if* $p \equiv 1 \pmod 9$ *it has rank* 0, 1, *or* 2.

Proof. Clear, since $|\mathrm{Im}(\alpha)|\,|\mathrm{Im}(\widehat{\alpha})| = 3^{r+1}$. (No need of BSD here.) ∎

This corollary allows us to determine the rank exactly for instance with $k = 1$ for $p = 61$, 79, 113, 131, 149, 151, 163, 293, etc., with $k = 2$ for $p = 29$, 83, 137, 139, 173, 181, 199, etc., and with $k = 4$ for $p = 41$, 59, 101, 131, 137, etc. for which `mwrank`, at least in its basic version, is not able to determine the rank using 2-descent.

Remarks.

(1) We can use the "parity conjecture" in this context (see for example [7] and [8]), in other words the analytic rank has the same parity as the algebraic rank, so whenever in the above the rank is known to be equal to 0 or 1 then it is always 1, while when the rank is known to be equal to 0, 1, or 2 then it is always 0 or 2, and both cases occur. This has been proved in certain cases: as already mentioned, by Satgé for $k = 1$ and $p \equiv 2 \pmod 9$, and in an unpublished work Elkies has shown that for $k = 4$ and $p \equiv 4$ or $7 \pmod 9$ the rank is indeed 1.

(2) The case $k = 4$ corresponds to primes which are sums of two cubes, so by [12] one knows that when $p \equiv 1 \pmod 9$ the rank is equal to 0 or 2, and exactly for which primes it is equal to 2. It is possible that either their method or Elkies' can be extended to the cases $k = 1$ and $k = 2$.

(3) The result for $k = 4$ can also be proved, less naturally, using 2-descent; see Theorem 6.4.17 of [2].

When the cubics are ELS, we may of course try to look for a global solution by search. A very efficient way of looking for rational points on a homogeneous cubic has been described by N. Elkies in [9], see also an unpublished preprint of J. Cremona on the subject. It has been implemented by several people. Using a slightly modified implementation due to M. Watkins, we can for instance find that a generator $P = (x, y)$ of the Mordell–Weil group of $y^2 = x^3 + p^2$ for $p = 1759$, which has rank 1, is given by

$$x = -\frac{2424795595146084331000753504998742221113923535}{306355106217656287860679698739497360246768 4},$$

$$y = \frac{864324039631860519772461964704651578477928121938887651420903789485 7}{536213427492815950218651184732885026614027411803532116695694824 8}.$$

This generator is not found by `mwrank` even at a high search limit. On the other hand, it could certainly be found using the Heegner point method.

For a more complicated example, for $p = 9511$ the curve $y^2 = x^3 + p^2$ has analytic rank 2, so the Heegner point method is not applicable, and `mwrank` even at a high search limit finds only the one-dimensional subspace of the (free part of the) Mordell–Weil group generated by $P_1 = (-210, 9011)$.

Using our implementation, we find that the full free part has basis (P_1, P_2) with $P_2 = (x, y)$, where

$$x = \frac{327019845171864486214422948249508747878830128281}{456289760665179363242981599270033206574137600},$$

$$y = \frac{92890043770264171014255964610503972850176417273682124237369198272789821}{9746778232027925565271633950191532413151456450450966045051557376000}.$$

In the following tables, we summarize what is proved (either using 3-descent as above, by Satgé, in Elkies' unpublished work, or in Rodríguez Villegas Zagier's work), what is a consequence of BSD, and what remains to be done. The tables are coded as follows. In the first column we indicate the residue of p modulo 9, and if relevant, in the second column we indicate the cubic character $\left(\frac{2}{p}\right)_3$ of 2 modulo p, 1 meaning that $2^{(p-1)/3} \equiv 1 \pmod{p}$, and ρ, ρ^2 meaning of course $2^{(p-1)/3} \not\equiv 1 \pmod{p}$. In the third, fourth, and fifth columns we give $|\mathrm{Im}(\alpha)|$, $|\mathrm{Im}(\widehat{\alpha})|$, and the rank of the curve respectively, and when two values are given, both occur. In the last column, we give a pair of symbols (A, B), corresponding to $(|\mathrm{Im}(\alpha)|, |\mathrm{Im}(\widehat{\alpha})|)$, where P means proved, BSD means proved under BSD, S means Satgé, ELK means Elkies, RVZ means Rodríguez Villegas–Zagier, and U means unknown.

Curves $y^2 = x^3 + p^2$, $p \geq 5$

p mod 9	$(\frac{2}{p})_3$	$\|\mathrm{Im}(\alpha)\|$	$\|\mathrm{Im}(\widehat{\alpha})\|$	rank	proved
1	1	9 or 3	3 or 1	2 or 0	(U, U)
1	ρ, ρ^2	3	1	0	(P, P)
2	–	9	1	1	(S, P)
4	–	3	3	1	$(\mathrm{P}, \mathrm{BSD})$
5	–	3	1	0	(P, P)
7	1	9 or 3	3 or 1	2 or 0	(U, U)
7	ρ, ρ^2	3	1	0	(P, P)
8	–	9	1	1	$(\mathrm{BSD}, \mathrm{P})$

Curves $y^2 = x^3 + 4p^2$, $p \geq 5$

p mod 9	$(\frac{2}{p})_3$	$\|\mathrm{Im}(\alpha)\|$	$\|\mathrm{Im}(\widehat{\alpha})\|$	rank	proved
1	1	9 or 3	3 or 1	2 or 0	(U, U)
1	ρ, ρ^2	3	1	0	(P, P)
2	–	3	1	0	(P, P)
4	1	9 or 3	3 or 1	2 or 0	(U, U)
4	ρ, ρ^2	3	1	0	(P, P)
5	–	9	1	1	$(\mathrm{BSD}, \mathrm{P})$
7	–	3	3	1	$(\mathrm{P}, \mathrm{BSD})$
8	–	9	1	1	$(\mathrm{BSD}, \mathrm{P})$

Curves $y^2 = x^3 + 16p^2$, $p \geq 5$

p mod 9	$(\frac{2}{p})_3$	$\lvert\mathrm{Im}(\alpha)\rvert$	$\lvert\mathrm{Im}(\widehat{\alpha})\rvert$	rank	proved
1	–	3	9 or 1	2 or 0	(P, RVZ)
2	–	3	1	0	(P, P)
4	–	3	3	1	(P, ELK)
5	–	3	1	0	(P, P)
7	–	3	3	1	(P, ELK)
8	–	3	3	1	(P, BSD)

An immediate corollary of the above tables and of Corollary 7.2 and Proposition 7.6 is the following:

Corollary 7.8.

(1) *Assume BSD. If* $p \equiv 2$ *or* $8 \pmod 9$ *there exist* x *and* y *in* $\mathbb{Q}$ *such that* $p = x^3 + 2y^3$, *and if* $p \equiv 5$ *or* $8 \pmod 9$ *there exist* x *and* y *in* $\mathbb{Q}$ *such that* $p = x^3 + 4y^3$.

(2) *Assume that either* $k = 1$ *and* $p \equiv 4 \pmod 9$, *or* $k = 2$ *and* $p \equiv 7 \pmod 9$, *and write* $p = m^2 + 3n^2$. *If BSD is true the equation*

$$nX^3 - 3mY^3 + 3kZ^3 + 3mX^2Y - 9nXY^2 = 0$$

is globally soluble.

(3) *Assume that* $p \equiv 8 \pmod 9$. *If BSD is true the equation*

$$X^3 + 3Y^3 + 24pZ^3 - 3X^2Y - 9XY^2 = 0$$

is globally soluble.

(4) *Assume that* $p \equiv 4$ *or* $7 \pmod 9$, *and write* $4p = m^2 + 27n^2$. *Without any assumption the equation*

$$nX^3 - mY^3 + 8Z^3 + mX^2Y - 9nXY^2 = 0$$

is globally soluble.

Proof. Clear, since these correspond respectively to $\lvert\mathrm{Im}(\alpha)\rvert = 9$ under BSD, to $\lvert\mathrm{Im}(\widehat{\alpha})\rvert = 3$ under BSD for (2) and (3), and to $\lvert\mathrm{Im}(\widehat{\alpha})\rvert = 3$ by Elkies' result. ∎

7.2. *The curves* $y^2 = x^3 + (kp)^2$ *for* $k = 3$ *or* 9. Once again the restriction on k is made so that no other prime apart from 3 divides it, and it is not necessary to consider higher powers of 3. Furthermore, the primes $p = 2$ and $p = 3$ give rise to a finite number of curves which can be treated individually (specifically, the rank is zero unless $(k, p) = (3, 2)$, in which case it has rank 1, a Mordell–Weil generator being $(-3, 3)$, and the torsion is of order 3 generated by $T = (0, kp)$, unless $(k, p) = (9, 3)$, in which case it has order 6 generated by $(18, 81)$). We therefore assume that $p \geq 5$.

As before, we first compute the image of α. For this, we consider the cubic equations of Theorem 3.1(3), in other words $u_1X^3+u_2Y^3+u_3Z^3=0$, where $u_1u_2 \mid 2kp$ and $u_3=2kp/(u_1u_2)$, where we recall that u_1u_2 is squarefree. Up to exchange of u_1 and u_2, it is easy to check that the only possibilities are $(1,1,2kp)$, $(1,2,kp)$, $(1,3,2kp/3)$, $(1,6,kp/3)$, $(1,p,2k)$, $(1,2p,k)$, $(1,3p,2k/3)$, $(1,6p,k/3)$, $(2,3,kp/3)$, $(2,p,k)$, $(2,3p,k/3)$, $(3,p,2k/3)$, $(3,2p,k/3)$, and $(6,p,k/3)$. The first one (corresponding to $u=1$) gives an evidently soluble equation, corresponding to the unit element of the elliptic curve.

Consider first $k=3$. We obtain the equations $(1,2,3p)$, $(1,3,2p)$, $(1,6,p)$, $(1,p,6)$, $(1,2p,3)$, $(1,3p,2)$, $(1,6p,1)$, $(2,3,p)$, $(2,p,3)$, $(2,3p,1)$, $(3,p,2)$, $(3,2p,1)$, and $(6,p,1)$. The equation $(1,6p,1)$ (corresponding to $u=6p$ and $u=(6p)^2$) corresponds to the two 3-torsion points of the curve. Apart from that, up to permutation of the u_i we have to study solubility for $(1,2,3p)$ (corresponding to $u=2$, 4, $3p$, $9p^2$, $12p$, and $18p^2$), $(1,3,2p)$ (corresponding to $u=3$, 9, $2p$, $4p^2$, $18p$, and $12p^2$), $(1,6,p)$ (corresponding to $u=6$, 36, p, p^2, $36p$, and $6p^2$), $(2,3,p)$ (corresponding to $u=12$, 18, $4p$, $2p^2$, $9p$, and $3p^2$).

Lemma 7.9. *We have two cases*:

(1) *If* $p \equiv 2 \pmod 3$ *all the above cubic equations are ELS*, *giving a total of* 27 *ELS equations.*
(2) *If* $p \equiv 1 \pmod 3$, *then either both* 2 *and* 3 *are cubes in* $\mathbb{F}_p^*$, *in which case once again all the above equations are ELS for a total of* 27, *or either* 2 *or* 3 *or both are non cubes*, *in which case only nine equations are ELS.*

Proof. Using the lemmas that we have proved it is immediate to show that all the equations are soluble at 2 and 3. The only problem is at p, and by Lemma 5.4 the equations are also soluble at p if and only if the classes of 2, 3, 6, and 3/2 respectively are cubes in $\mathbb{F}_p^*$, and if $p \equiv 2 \pmod 3$ this is trivially true.

Assume now that $p \equiv 1 \pmod 3$. We consider four cases, according to the cubic residue character of 2 and 3 modulo p.

(1) If 2 and 3 are not cubes in $\mathbb{F}_p^*$, then either their product or their quotient is a cube, so we deduce that either $(1,6,p)$ or $(2,3,p)$ is locally soluble (but not both), giving a total of $6+3=9$ possible values of u.
(2) If 2 or 3 is a cube in $\mathbb{F}_p^*$ but not both, then 6 and 3/2 cannot be cubes, so we deduce that either $(1,2,3p)$ or $(1,3,2p)$ is locally soluble, giving again 9 possible values of u.

(3) If both 2 and 3 are cubes in $\mathbb{F}_p^*$ then all the equations are locally soluble, giving a total of $24+3=27$ possible values of u, proving the lemma. ∎

Corollary 7.10.

(1) *If* $p\equiv 2 \pmod 3$ *then* $|\mathrm{Im}(\alpha)|=3$, 9, *or* 27 *and assuming BSD we have* $|\mathrm{Im}(\alpha)|=3$ *or* 27 *and the following are equivalent*:

(a) $|\mathrm{Im}(\alpha)|=27$.
(b) $\mathrm{rk}(E)=2$.
(c) *There exist* x *and* y *in* $\mathbb{Q}$ *such that* $p=x^3+6y^3$.
(d) *There exist* x *and* y *in* $\mathbb{Q}$ *such that* $p=2x^3+3y^3$.
(e) *There exist* x *and* y *in* $\mathbb{Q}$ *such that* $p=4x^3+12y^3$.
(f) *There exist* x *and* y *in* $\mathbb{Q}$ *such that* $p=9x^3+18y^3$.

(2) *If* $p\equiv 1 \pmod 3$ *and* 2 *and* 3 *are not both cubes in* $\mathbb{F}_p^*$ *then* $|\mathrm{Im}(\alpha)|=3$ *or* 9, *and assuming BSD we have* $|\mathrm{Im}(\alpha)|=9$ *and* $\mathrm{rk}(E)=1$, *and furthermore for* $(a,b)=(1,6)$, $(2,3)$, $(4,12)$, *or* $(9,18)$, *there exist* x *and* y *in* $\mathbb{Q}$ *such that* $p=ax^3+by^3$ *if and only if* b/a *is a cube in* $\mathbb{F}_p^*$.

(3) *If* $p\equiv 1 \pmod 3$ *and* 2 *and* 3 *are both cubes in* $\mathbb{F}_p^*$ *then either* C_{π_0} *is globally soluble*, *in which case the six conditions of* (1) *are again equivalent except that the second must be replaced by* $\mathrm{rk}(E)=3$, *or* C_{π_0} *is not globally soluble*, *in which case* $|\mathrm{Im}(\alpha)|=9$ *and* $\mathrm{rk}(E)=1$, *and exactly one of the equations* $p=x^3+6y^3$, $p=2x^3+3y^3$, $p=4x^3+12y^3$, *or* $p=9x^3+18y^3$ *has a solution with* x *and* y *in* $\mathbb{Q}$.

Proof. The assertions independent of BSD follow immediately from the above lemma. On the other hand, if either $p\equiv 2 \pmod 3$ or $p\equiv 1 \pmod 3$ and 2 and 3 are not both cubes in $\mathbb{F}_p^*$, we have $|\mathrm{Im}(\widehat{\alpha})|=1$, so that $3^{\mathrm{rk}(E)+1}=|\mathrm{Im}(\alpha)|$. If $p\equiv 2 \pmod 3$ the root number of E is equal to $+1$, so assuming BSD the rank of E is even, hence $|\mathrm{Im}(\alpha)|=3$ or 27, and the result clearly follows in this case. If $p\equiv 1 \pmod 3$ the root number of E is equal to -1, so assuming BSD the rank of E is odd, hence $|\mathrm{Im}(\alpha)|=9$ when 2 and 3 are not both cubes, and the result also follows. Finally, if $p\equiv 1 \pmod 3$ and 2 and 3 are both cubes, then $|\mathrm{Im}(\widehat{\alpha})|=1$ or 3, and it is equal to 3 if and only if C_{π_0} (which is ELS) is globally soluble. Assuming BSD the rank of E is again odd, so we have two cases:

- If C_{π_0} is not globally soluble we again have $|\mathrm{Im}(\widehat{\alpha})|=1$, so $|\mathrm{Im}(\alpha)|=9$ and $\mathrm{rk}(E)=1$.
- If C_{π_0} is globally soluble we have $|\mathrm{Im}(\widehat{\alpha})|=3$, so either $|\mathrm{Im}(\alpha)|=3$ and $\mathrm{rk}(E)=1$, or $|\mathrm{Im}(\alpha)|=27$ and $\mathrm{rk}(E)=3$. ∎

Note that although C_{π_0} is ELS, it is not always globally soluble: the smallest p for which it is not is $p=3889$, for which the 2-rank based `mwrank` program of Cremona tells us that the rank is equal to 1, and on the other hand $(X, Y, Z) = (91, -211, 19)$ is a solution of the $(2, 3, p)$ cubic so $|\mathrm{Im}(\alpha)| \geq 9$, hence by the above if C_{π_0} were globally soluble we would have $\mathrm{rk}(E) = 3$, which is not the case.

Consider now $k = 9$. We obtain the equations $(1, 2, 9p)$, $(1, 3, 6p)$, $(1, 6, 3p)$, $(1, p, 18)$, $(1, 2p, 9)$, $(1, 3p, 6)$, $(1, 6p, 3)$, $(2, 3, 3p)$, $(2, p, 9)$, $(2, 3p, 3)$, $(3, p, 6)$, $(3, 2p, 3)$, and $(6, p, 3)$. The equation $(3, 2p, 3)$ (corresponding to $u = 18p$ and $u = 12p^2$) corresponds to the two 3-torsion points of the curve. Apart from that, up to permutation of the u_i we have to study solubility for $(1, 2, 9p)$ (corresponding to $u = 2$ and 4), $(1, 3, 6p)$ (corresponding to $u = 3$, 9, $6p$, and $36p^2$), $(1, 6, 3p)$ (corresponding to $u = 6$, 36, $3p$, $9p^2$), $(1, 9, 2p)$ (corresponding to $u = 2p$ and $4p^2$), $(1, 18, p)$ (corresponding to $u = p$ and p^2), $(2, 3, 3p)$ (corresponding to $u = 12$, 18, $12p$, and $18p^2$), $(2, 9, p)$ (corresponding to $u = 4p$ and $2p^2$), and $(3, 6, p)$ (corresponding to $u = 9p$, $3p^2$, $36p$, and $6p^2$).

Once again, the equations are all locally soluble at 2. However, they are not all locally soluble at 3 (in fact, $(3, 6, p)$ is never locally soluble at 3), and using once again the local solubility results that we have proved, we obtain the following lemma:

Lemma 7.11.

(1) *If* $p \equiv 2 \pmod 3$, *exactly two of the above seven equations are ELS, giving always a total of nine values of* u.

(2) *If* $p \equiv 1 \pmod 3$ *and* $3/2$, 3, *or* 6 *are cubes respectively for* $p \equiv 1$, 4, *or* $7 \pmod 9$, *once again exactly two of the above seven equations are ELS, giving always a total of nine values of* u. *Otherwise, none are ELS, giving a total of three values of* u (*corresponding to the* 3-*torsion points*).

Proof. The seventh equation is not locally soluble at 3, and the six others are ELS if and only if $p \equiv \pm 4 \pmod 9$ and 3 is a cube for $(1, 3, 6p)$ and $(1, 9, 2p)$, $p \equiv \pm 2 \pmod 9$ and 6 is a cube for $(1, 6, 3p)$ and $(2, 9, p)$, or $p \equiv \pm 1 \pmod 9$ and $3/2$ is a cube for $(1, 18, p)$ and $(2, 3, 3p)$, and the result follows. ∎

Acknowledgements. We would like to thank J. Cremona and T. Fisher for their interest and the anonymous referee for his advice.

References

[1] J. W. S. Cassels, *Arithmetic on curves of genus 1. I. On a conjecture of Selmer*, J. Reine Angew. Math. 202 (1959), 52–99.

[2] H. Cohen, *Number Theory. Vol. I. Tools and Diophantine Equations*, Grad. Texts in Math. 239, Springer, New York, 2007.

[3] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. 615 (2008), 121–155.

[4] —, —, —, —, —, *Explicit n-descent on elliptic curves. II. Geometry*, ibid. 632 (2009), 63–84.

[5] M. DeLong, *A formula for the Selmer group of a rational three-isogeny*, Acta Arith. 105 (2002), 119–131.

[6] Z. Djabri, E. F. Schaefer and N. P. Smart, *Computing the p-Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. 352 (2000), 5583–5597.

[7] T. Dokchitser and V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory 128 (2008), 662–679.

[8] —, —, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math., to appear.

[9] N. D. Elkies, *Rational points near curves and small nonzero* $|x^3 - y^2|$ *via lattice reduction*, in: Algorithmic Number Theory (Leiden), Lecture Notes in Comput. Sci. 1838, Springer, 2000, 33–63.

[10] T. Fisher, *Finding rational points on elliptic curves using 6-descent and 12-descent*, J. Algebra 320 (2008), 853–884.

[11] —, *The Cassels–Tate pairing and the Platonic solids*, J. Number Theory 98 (2003), 105–155.

[12] F. Rodríguez Villegas and D. Zagier, *Which primes are sums of two cubes?*, in: Number Theory (Halifax, NS, 1994), CMS Conf. Proc. 15, Amer. Math. Soc., 1994, 295–306.

[13] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory 23 (1986), 294–317.

[14] —, *Un analogue du calcul de Heegner*, Invent. Math. 87 (1987), 425–439.

[15] E. F. Schaefer and M. Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. 356 (2004), 1209–1231.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1992.

[17] J. Top, *Descent by 3-isogeny and 3-rank of quadratic fields*, in: Advances in Number Theory (Kingston, ON, 1991), Oxford Univ. Press, 1993, 303–317.

IMB Université Bordeaux I
351 Cours de la Libération
33405 Talence, France
E-mail: cohen@math.u-bordeaux1.fr
http://www.math.u-bordeaux.fr/~cohen/

IMJ Université Paris 7
site Chevaleret
2, place Jussieu
75251 Paris Cedex 05, France
E-mail: pazuki@math.jussieu.fr
http://www.math.jussieu.fr/~pazuki

Received on 28.3.2009
and in revised form on 27.4.2009 (5985)