# DIAGONAL CUBIC EQUATIONS IN FOUR VARIABLES WITH PRIME COEFFICIENTS

Carmen Laura Basile*

*Department of Mathematics,*
*Imperial College of Science, Technology and Medicine, London*
(laura.basile@ic.ac.uk)

Thomas Anthony Fisher

*Department of Pure Mathematics and Mathematical Statistics,*
*Sidney Sussex College, Cambridge*
(T.A.Fisher@dpmms.cam.ac.uk)

November 2000

**Abstract**

The aim of this paper is to give an alternative proof of a theorem of R. Heath-Brown [3] regarding the existence of non-zero integral solutions of the equation $p_1X_1^3 + p_2X_2^3 + p_3X_3^3 + p_4X_4^3 = 0$ , where the $p_j$ are prime integers $\equiv 2 \pmod 3$.

We start by presenting the main result of this paper. This result has been proved by Roger Heath-Brown [3] under the conjecture that the difference $s(A) - r(A)$ between the Selmer rank and the arithmetic rank of the elliptic curve $X^3 + Y^3 = AZ^3$ is even. In this note we will show that we do not need this assumption and give a detailed proof of this result.

**Theorem 1** *Let $p_1, p_2, p_3, p_4$ be prime integers such that $p_i \equiv 2 \pmod 3$ $(1 \leq i \leq 4)$. Then the equation*

$$p_1X_1^3 + p_2X_2^3 + p_3X_3^3 + p_4X_4^3 = 0$$

*has non-zero integral solutions, assuming the conjecture that the Tate-Shafarevich group of the elliptic curve $X^3 + Y^3 = AZ^3$ over $\mathbb{Q}$ is finite.*

A much stronger result has been recently proved by Sir Peter Swinnerton-Dyer [7].

Note that in order to prove the above theorem, it is sufficient to prove that the equations

$$p_1X_1^3 + p_2X_2^3 = p$$
$$p_3X_3^3 + p_4X_4^3 = -p$$

*Supported by INdAM (Istituto Nazionale di Alta Matematica "F.Severi"), Italy.

have non-zero rational solutions for some prime integer $p$. So it suffices to prove that the equation $p_1X^3 + p_2Y^3 = p$ has non-zero solutions in $\mathbb{Q}$ or, equivalently, in a quadratic extension of $\mathbb{Q}$.

**Notation** *Let $\omega$ be a primitive cube root of unity and let $k = \mathbb{Q}(\omega)$.*
*Let $A \in \mathbb{Z} \setminus \{-1, 0, 1\}$ be a cube-free integer. We denote by $E_A$ the elliptic curve*

$$E_A\colon\ X^3 + Y^3 = AZ^3.$$

*For any $\alpha \in k^*$, let $C_{A,\alpha}$ be the smooth projective curve given by the equation*

$$C_{A,\alpha}\colon\ \alpha X^3 + \alpha^{-1}Y^3 = AZ^3.$$

For $\alpha \in k^*$, the curves $C_{A,\alpha}$ are principal homogeneous spaces over $E_A$. Moreover, it is clear that if $\alpha$ and $\beta$ belong to the same class modulo $(k^*)^3$ then the curves $C_{A,\alpha}$ and $C_{A,\beta}$ are isomorphic.

Let us consider the *multiplication-by-*$\sqrt{-3}$ endomorphism on $E_A$ (see [1]), given by

$$\begin{array}{rccl} \sqrt{-3}: & E_A & \longrightarrow & E_A \\ & (X,Y,Z) & \longmapsto & (\omega^2X^3 + \omega Y^3 - AZ^3,\ \omega X^3 + \omega^2 Y^3 - AZ^3,\ -3XYZ), \end{array}$$

and the following diagram with exact row

$$\begin{array}{ccccccc} 0 \longrightarrow E_A(k)/\sqrt{-3}E_A(k) & \longrightarrow & H^1(k, E_A\left[\sqrt{-3}\right]) & \longrightarrow & WC(E_A/k)\left[\sqrt{-3}\right] & \longrightarrow 0 \\ & & & \searrow & \downarrow & \\ & & & & \prod_v WC(E_A/k_v)\left[\sqrt{-3}\right] & \end{array}$$

where $WC(E_A/k)$ is the Weil-Châtelet group of $E_A/k$ and $v$ runs over all the places of $k$. It is readily verified that the group $E_A(\bar{k})\left[\sqrt{-3}\right]$ is isomorphic to the group $\mu_3(\bar{k})$ of cube roots of unity, as a $\mathrm{Gal}(\bar{k}/k)$-module. It follows from Kummer theory that $H^1(k, E_A\left[\sqrt{-3}\right])$ is isomorphic to $k^*/(k^*)^3$ and so we get the exact sequence

$$\begin{array}{ccccccc} 0 \longrightarrow E_A(k)/\sqrt{-3}E_A(k) & \longrightarrow & k^*/(k^*)^3 & \xrightarrow{f} & WC(E_A/k)\left[\sqrt{-3}\right] & \longrightarrow 0 \\ & & & {\scriptstyle g}\searrow & \downarrow & \\ & & & & \prod_v WC(E_A/k_v)\left[\sqrt{-3}\right] & \end{array}$$

where the map $f$ sends an element $\alpha(k^*)^3$ to the curve $C_{A,\alpha}$. We denote by $S(A)$ the Selmer group $S^{(\sqrt{-3})}(E_A/k)$ (which is defined to be the kernel of the map $g$ in the diagram above) and by $C(A)$ the kernel of the map $f$. Obviously $C(A)$ is a subgroup of $S(A)$; we can write them explicitly

$$\begin{aligned} S(A) &= \{\alpha(k^*)^3 :\ C_{A,\alpha} \text{ has } k_\pi\text{−points for any prime } \pi \in k,\ \alpha \in k^*\}, \\ C(A) &= \{\alpha(k^*)^3 :\ C_{A,\alpha} \text{ has } k\text{−points},\ \alpha \in k^*\}. \end{aligned}$$

Observe also that $C(A)$ is isomorphic to $E_A(k)/\sqrt{-3}E_A(k)$ (this follows immediately from the diagram above).

In the following two lemmas we will determine the structure of $S(A)$ when $A$ satisfies certain conditions.

**Lemma 2** *Let $\rho \in k$ be a prime above 3, and let $a, b, c \in k$ such that $a, b, c$ are congruent to 1 modulo $\rho^2$. If the projective curve*

$$E: \ aX^3 + b\omega Y^3 + c\omega^2 Z^3 = 0$$

*has a point over $k_\rho$, then $abc \equiv 1 \pmod{\rho^3}$.*

*Proof.* Let $(x, y, z)$ be a $k_\rho$-point of the curve $E$ and suppose that

$$\min\{\mathrm{val}_\rho(x), \mathrm{val}_\rho(y), \mathrm{val}_\rho(z)\} = 0.$$

Say

$$\begin{aligned} x &= x_0 + x_1\rho + x_2\rho^2 + \ldots, \\ y &= y_0 + y_1\rho + y_2\rho^2 + \ldots, \\ z &= z_0 + z_1\rho + z_2\rho^2 + \ldots \end{aligned}$$

with $(x_0, y_0, z_0) \neq (0, 0, 0)$.

From the condition $ax^3 + b\omega y^3 + c\omega^2 z^3 = 0$ it follows that $x_0^3 \equiv y_0^3 \equiv z_0^3 \pmod{\rho^2}$. Therefore we may assume $(x_0, y_0, z_0) = (1, 1, 1)$ and hence we get

$$(x^3, y^3, z^3) \equiv (1, 1, 1) \pmod{\rho^3}.$$

Let $a \equiv 1 + a_2\rho^2 \pmod{\rho^3}$, $b \equiv 1 + b_2\rho^2 \pmod{\rho^3}$ and $c \equiv 1 + c_2\rho^2 \pmod{\rho^3}$. Then from $a + b\omega + c\omega^2 \equiv 0 \pmod{\rho^3}$ it follows $a_2 + b_2 + c_2 \equiv 0 \pmod{\rho}$ and therefore $abc \equiv 1 + (a_2 + b_2 + c_2)\rho^2 \equiv 1 \pmod{\rho^3}$. □

**Lemma 3** *Let $A = p_1 p_2 N(\pi)$ where $p_1, p_2 \equiv 2 \pmod 3$ are integer primes, $\pi \equiv 1 \pmod 3$ is a prime in $\mathbb{Z}[\omega]$ such that $A \not\equiv 1 \pmod 9$ and $\left(\frac{\pi}{p_1}\right)_3 = \left(\frac{\pi}{p_2}\right)_3 \neq 1$. Then $S(A)$ is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$ as an abelian group.*

*Proof.* We will prove that $S(A)$ is generated by the elements $A(k^*)^3$ and $p_1 p_2^2 (k^*)^3$.

The curve $C_{A,A}$ has a $k$-point, namely $(1, 0, 1)$; hence $A(k^*)^3 \in S(A)$. Suppose now $\alpha \neq A$. Note that, in order to determine for which elements $\alpha$ the coset $\alpha(k^*)^3$ belongs to $S(A)$, it is sufficient to test the elements $\alpha$ where $\alpha$ is a cube-free integer in $\mathbb{Z}[\omega]$ such that

(i) $\alpha$ is composed of primes dividing $A$;

(ii) we can fix a prime in $\{p_1, p_2, \pi, \bar{\pi}\}$, say $\bar{\pi}$, such that $\bar{\pi}$ does not divide $\alpha$.

Indeed:

(i) suppose $\alpha$ contains a prime factor $\rho$ which does not divide $A$; it is then easy to verify that $C_{A,\alpha}$ contains no $k_\rho$-points. To get a contradiction, we suppose $C_{A,\alpha}$ contains a $k_\rho$-point $(X, Y, Z)$; so we have

$$\alpha^2 X^3 + Y^3 = \alpha A Z^3.$$

Considering the $\rho$-adic valuation of the right hand side and of the left hand side, and noting $\mathrm{val}_\rho(\alpha^2 X^3) \neq \mathrm{val}_\rho(Y^3)$, we get

$$\mathrm{val}_\rho\big(\alpha A Z^3\big) = \mathrm{val}_\rho\big(\alpha^2 X^3 + Y^3\big) = \min\{\mathrm{val}_\rho\big(\alpha^2 X^3\big)\,, \mathrm{val}_\rho\big(Y^3\big)\}.$$

But this is impossible since, on the one hand, $\mathrm{val}_\rho(\alpha A Z^3) = i + 3j$, where $i \in \{1, 2\}$ is defined to be the $\rho$-adic valuation of $\alpha$ and $j$ is an integer, and on the other hand

$$\min\{\mathrm{val}_\rho\big(\alpha^2 X^3\big)\,, \mathrm{val}_\rho\big(Y^3\big)\} = \min\{2i + 3h, 3l\}$$

with $h, l$ integers;

(ii) suppose $\bar{\pi}^j$ divides $\alpha$ (with $j = 1, 2$); then, since $S(A)$ is a group and $A(k^*)^3$ belongs to $S(A)$, instead of $\alpha$ we may consider the cube-free integer representative of the coset $(\alpha/A^j)\,(k^*)^3$.

As a result, we may assume $\alpha = \omega^m p_1^{n_1} p_2^{n_2} \pi^n$ where $m, n_1, n_2, n \in \{0, 1, 2\}$. In fact it is not difficult to prove that if $m \neq 0$ then $\alpha$ does not belong to $S(A)$. Indeed, to get a contradiction suppose that $m \neq 0$ and that $C_{A,\alpha}$ contains a $k_\rho$-point where $\rho \in k$ is a prime above 3. Then from Lemma 2 it follows that $A \equiv 1 \pmod{\rho^3}$ and hence $A \equiv 1 \pmod 9$ which contradicts our hypotheses. Therefore we may assume $m = 0$.

Let $\rho \in \mathbb{Z}[\omega]$ be a prime. If $\rho$ does not divide $3A$ then $C_{A,\alpha}$ contains points over $k_\rho$ for any $\alpha$. Indeed, a smooth curve of genus 1 always contains points over any finite field (see [2]); moreover if $\rho$ does not divide $3A$ then $C_{A,\alpha}$ is non-singular over $\mathbb{Z}[\omega]/\rho$ and therefore it contains a non-singular point over $\mathbb{Z}[\omega]/\rho$ which, by Hensel's lemma, can be lifted to a point over $k_\rho$.

Suppose now that $\rho$ divides $3A$; hence we have to consider the two cases $\rho \,|\, A$ and $\rho \,|\, 3$.

(1) Let $\rho$ divide $A$, so $\rho$ belongs to $\{p_1, p_2, \pi, \bar{\pi}\}$. We can consider three further subcases.

(1a) Let $\rho$ divide $\alpha$ exactly; then the projective curve

$$\alpha X^3 + \alpha^{-1} Y^3 = A Z^3$$

can also be written as

$$\frac{\alpha^2}{\rho^2}(\rho X)^3 + \rho Y^3 = \frac{\alpha A}{\rho^2}(\rho Z)^3.$$

Hence, considering the transformation $\rho X \to X$, $\rho Z \to Z$ and reducing modulo $\rho$, we get the curve

$$X^3 - \frac{A}{\alpha} Z^3 = 0$$

which contains a smooth point over $\mathbb{F}_\rho$ if and only if $\dfrac{A}{\alpha} \in (\mathbb{F}_\rho^*)^3$, i.e. if and only if $\left(\dfrac{A\alpha^{-1}}{\rho}\right)_3 = 1$. By Hensel's lemma, we can lift this smooth point over $\mathbb{F}_\rho$ to a point over $k_\rho$.

(1b) Suppose now $\rho^2$ divides exactly $\alpha$. Similarly, considering a suitable transformation and reducing modulo $\rho$, we get the curve

$$Y^3 - \frac{A\alpha}{\rho^3} Z^3 = 0$$

which contains a smooth point over $\mathbb{F}_\rho$ if and only if $\dfrac{A\alpha}{\rho^3} \in (\mathbb{F}_\rho^*)^3$, i.e. if and only if $\left(\dfrac{A\alpha\rho^{-3}}{\rho}\right)_3 = 1$.

(1c) Similarly, if $\rho$ does not divide $\alpha$, we get the curve

$$\alpha^2 X^3 + Y^3 = 0$$

which contains a smooth point over $\mathbb{F}_\rho$ if and only if $\alpha^2 \in (\mathbb{F}_\rho^*)^3$, i.e. $\left(\dfrac{\alpha}{\rho}\right)_3 = 1$.

Suppose $\rho = p_j$ with $j = 1, 2$.

If $p_j$ divides exactly $\alpha$, then by case (1a) we must have $\left(\dfrac{A\alpha^{-1}}{p_j}\right)_3 = 1$ and hence $\left(\dfrac{\alpha p_j^{-1}}{p_j}\right)_3 = 1$; indeed [†]

$$\left(\frac{A\alpha^{-1}}{p_j}\right)_3 = \left(\frac{p_h}{p_j}\right)_3 \left(\frac{p}{p_j}\right)_3 \left(\frac{\alpha^{-1}p_j}{p_j}\right)_3 = \left(\frac{\alpha p_j^{-1}}{p_j}\right)_3^{-1}$$

where $h \in \{1, 2\},\ h \neq j$ and $p = N(\pi)$.

If $p_j^2$ divides exactly $\alpha$, then by case (1b) we must have $\left(\dfrac{A\alpha p_j^{-3}}{p_j}\right)_3 = 1$ and therefore $\left(\dfrac{\alpha p_j^{-2}}{p_j}\right)_3 = 1$, since

$$\left(\frac{A\alpha p_j^{-3}}{p_j}\right)_3 = \left(\frac{p_h}{p_j}\right)_3 \left(\frac{p}{p_j}\right)_3 \left(\frac{\alpha p_j^{-2}}{p_j}\right)_3 = \left(\frac{\alpha p_j^{-2}}{p_j}\right)_3,$$

where again $h \in \{1, 2\}$ and $h \neq j$.

If $p_j$ does not divide $\alpha$, then by case (1c) we must have $\left(\dfrac{\alpha}{p_j}\right)_3 = 1$.

[†] If $q \neq 3$ is a prime integer with $\#\mathbb{F}_q^* \not\equiv 0 \pmod 3$ then $\left(\dfrac{n}{q}\right)_3 = 1$ for any $n \in \mathbb{Z}$ such that $(n, q) = 1$.

Finally, we obtain the two following conditions which must be satisfied in order to have $\alpha(k^*)^3 \in S(A)$:

$$\left(\frac{p_2^{n_2}\pi^n}{p_1}\right)_3 = 1 \quad \text{and} \quad \left(\frac{p_1^{n_1}\pi^n}{p_2}\right)_3 = 1.$$

Since

$$\left(\frac{p_2^{n_2}\pi^n}{p_1}\right)_3 = \left(\frac{p_2}{p_1}\right)_3^{n_2} \left(\frac{\pi}{p_1}\right)_3^{n} = \left(\frac{\pi}{p_1}\right)_3^{n}$$

and $\left(\frac{\pi}{p_1}\right)_3 \neq 1$ by hypothesis, the first condition is satisfied if and only if $n = 0$. It is easy to verify that for $n = 0$ the second condition is satisfied as well. Hence $\alpha = p_1^{n_1}p_2^{n_2}$. So, by case (1c), it follows that we must have $\left(\frac{\alpha}{\pi}\right)_3 = 1$; therefore, since by the Cubic Reciprocity Law $\left(\frac{p_1}{\pi}\right)_3 = \left(\frac{p_2}{\pi}\right)_3 \neq 1$, we get the condition $n_1 + n_2 \equiv 0 \pmod 3$. We may suppose $n_1 = 1$; then $\alpha = p_1p_2^2$ or, equivalently, $\alpha = p_1p_2^{-1}$.

(2) Suppose now that $\rho$ divides 3; in other words, since $3 = -\omega^2(1-\omega)^2$, suppose $\rho = 1 - \omega$ . Recall that now we have $A = p_1p_2p$ and $\alpha = p_1p_2^{-1}$; therefore the curve

$$\alpha X^3 + \alpha^{-1}Y^3 = AZ^3$$

is isomorphic to the curve

$$E\colon\ p_1X^3 + p_2Y^3 = pZ^3.$$

We have to prove that $E$ contains a point over $k_\rho$. Since $\mathbb{Q}_3$ is contained in $k_\rho$, it suffices to find a point over $\mathbb{Q}_3$.

By hypothesis $p \equiv 1 \pmod 3$ and $p_1, p_2 \equiv 2 \pmod 3$, so let

$$p \equiv 1 + 3b \pmod 9 \quad \text{and} \quad p_j \equiv -1 + 3a_j \pmod 9$$

for $j = 1, 2$; since $A \not\equiv 1 \pmod 9$ by hypothesis, we have $a_1 + a_2 - b \not\equiv 0 \pmod 3$. Thus the integers $a_1, a_2, -b$ cannot be all different modulo 3; wlog we may suppose $a_1 = a_2$. Therefore we have $p_1p_2^{-1} \equiv 1 \pmod 9$; in other words $p_1p_2^{-1}$ belongs to $1 + 9\mathbb{Z}_3$ which is contained in $(\mathbb{Z}_3^*)^3$. It follows that $E$ contains the point $(1, -y, 0)$ where $y \in \mathbb{Z}_3$ is a cube root of $p_1p_2^{-1}$. More precisely, if $p_1p_2^{-1} \equiv 1 + 9l \pmod{27}$, then we use Hensel's lemma to construct $y \in \mathbb{Z}_3$ such that $y \equiv 1 + 3l \pmod 9$ and $y^3 = p_1p_2^{-1}$.

Hence $E$ contains a $k_\rho$-point.

In conclusion, we have proved that $S(A)$ is generated by the two elements of order 3 $A(k^*)^3$ and $p_1p_2^2(k^*)^3$ and thus it is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$. □

The following two lemmas allow us to conclude that, under the hypotheses of Lemma 3, the two groups $C(A)$ and $S(A)$ coincide. This provides a local-to-global principle for the

curves $C_{A,\alpha}$ when $A$ is as in Lemma 3. As in the statement of Theorem 1, our work here is conditional on the finiteness of the Tate-Shafarevich group $Ш(E_A/\mathbb{Q})$.

To get a contradiction, let us suppose that $C(A)$ is strictly included in $S(A)$. Note that $C(A)$ cannot be the trivial group as $A(k^*)^3$ belongs to $C(A)$; then $C(A)$ has order 3. From the exactness of the sequence

$$0 \longrightarrow E_A(k)/\sqrt{-3}E_A(k) \longrightarrow \ k^*/(k^*)^3 \ \stackrel{f}{\longrightarrow} \ WC(E_A/k)\left[\sqrt{-3}\right] \ \longrightarrow 0,$$

it follows that $E_A(k)/\sqrt{-3}E_A(k)$ and $\mathbb{Z}/3$ are isomorphic as abelian groups (recall that $C(A)$ is the kernel of the map $f$). Hence from Lemma 3 and the exact sequence

$$0 \longrightarrow E_A(k)/\sqrt{-3}E_A(k) \longrightarrow S^{(\sqrt{-3})}(E_A/k) \longrightarrow Ш(E_A/k)\left[\sqrt{-3}\right] \longrightarrow 0$$

we deduce that $Ш(E_A/k)\left[\sqrt{-3}\right]$ is isomorphic to $\mathbb{Z}/3$ and this is impossible, as we will show in Lemma 5. But first we need one more result.

**Lemma 4** *Let $E/L$ be an elliptic curve over a number field $L$. Let $K$ be a Galois extension of $L$ of degree $n$. Let $m$ be a positive integer such that $(m,n)=1$. Then:*

$$Ш(E/L)[m] = Ш(E/K)[m]^{\mathrm{Gal}(K/L)}.$$

*In particular, assuming the finiteness of $Ш(E/L)$, the order of $Ш(E/K)[m]^{\mathrm{Gal}(K/L)}$ must be a square.*

*Proof.* Let us consider the following commutative diagram with exact rows and columns where the rows are obtained by the *multiplication-by-m* endomorphism and the columns are restriction-inflation sequences:

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & H^1(\mathrm{Gal}(K/L), E(K)[m]) & & H^1(\mathrm{Gal}(K/L), E(K))[m] & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(L)/mE(L) & \longrightarrow & H^1(L, E[m]) & \longrightarrow & H^1(L, E)[m] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(K, E[m]) & \longrightarrow & H^1(K, E)[m] & \longrightarrow & 0.
\end{array}$$

Since $\mathrm{Gal}(K/L)$ has order $n$, every element of $H^1(\mathrm{Gal}(K/L), E(K))$ has order dividing $n$ (this follows from properties of the restriction and corestriction maps; see [5]). Hence, as $m$ and $n$ are coprime, $H^1(\mathrm{Gal}(K/L), E(K))[m] = 0$. Thus from the diagram above it follows that $H^1(L,E)[m]$ injects into $H^1(K,E)[m]$.

From the exactness of the second row of the diagram we get the exact sequence

$$\begin{array}{c}
0 \longrightarrow E(K)/mE(K)^{\mathrm{Gal}(K/L)} \longrightarrow H^1(K, E[m])^{\mathrm{Gal}(K/L)} \longrightarrow \\
\longrightarrow H^1(K,E)[m]^{\mathrm{Gal}(K/L)} \longrightarrow H^1(\mathrm{Gal}(K/L), E(K)/mE(K)) = 0
\end{array}$$

where $H^1(\mathrm{Gal}(K/L), E(K)/mE(K))$ is the zero group because it is killed by $m$ and by $n$ which are coprime.

On the other hand, from the exact sequence of low degree terms of the Hochschild-Serre spectral sequence, we get the exact sequence

$$H^1(\mathrm{Gal}(K/L), E(K)[m]) \longrightarrow H^1(L, E[m]) \xrightarrow{\varphi} H^1(K, E[m])^{\mathrm{Gal}(K/L)} \longrightarrow \\ \longrightarrow H^2(\mathrm{Gal}(K/L), E(K)[m])$$

where the first and the last term are trivial because, again, they are killed by coprime integers. Hence the map $\varphi$ is an isomorphism. The following diagram of exact rows and columns summarizes the information we have obtained so far

$$\begin{array}{ccccc} 0 & & 0 & & \\ \downarrow & & \downarrow & & \\ H^1(L, E[m]) & \longrightarrow & H^1(L, E)[m] & \longrightarrow & 0 \\ \downarrow \varphi & & \downarrow \varphi' & & \\ H^1(K, E[m])^{\mathrm{Gal}(K/L)} & \xrightarrow{\varphi''} & H^1(K, E)[m]^{\mathrm{Gal}(K/L)} & \longrightarrow & 0 \\ \downarrow & & & & \\ 0. & & & & \end{array}$$

It is immediate to verify that the injective map $\varphi'$ is also surjective because of the surjectivity of the maps $\varphi''$ and $\varphi$. Therefore we obtain

$$H^1(L, E)[m] = H^1(K, E)[m]^{\mathrm{Gal}(K/L)}.$$

Let us consider now a place $v$ of $L$; since $K$ is a Galois extension of $L$, for any place $w$ of $K$ over $v$ the degrees of the local extensions $K_w/L_v$ divide $n$ and therefore they are coprime to $m$. Hence the reasoning above can be applied also to the extensions $K_w/L_v$ and thus we obtain

$$H^1(L_v, E)[m] = H^1(K_w, E)[m]^{\mathrm{Gal}(K_w/L_v)}.$$

Considering the corresponding Tate-Shafarevich groups, we get

$$Ш(E/L)[m] = Ш(E/K)[m]^{\mathrm{Gal}(K/L)}.$$

Furthermore, assuming the finiteness of $Ш(E/L)$, it follows from the existence of the Cassels alternating bilinear pairing on $Ш(E/L)$ that the order of $Ш(E/L)[m]$ is a perfect square and hence the order of $Ш(E/K)[m]^{\mathrm{Gal}(K/L)}$ is a square too. □

**Lemma 5** *If* $Ш(E_A/\mathbb{Q})$ *is finite, then* $Ш(E_A/k)\left[\sqrt{-3}\right]$ *cannot have order* 3.

*Proof.* To get a contradiction, assume that $Ш(E_A/k)\left[\sqrt{-3}\right]$ and $\mathbb{Z}/3$ are isomorphic as abelian groups.

Let $\tilde{E}_A$ be the quadratic twist of $E_A$ corresponding to the class of $-3$ in $H^1(\mathbb{Q}, \mathbb{Z}/2) = \mathbb{Q}^*/\mathbb{Q}^{*2}$; $\tilde{E}_A$ has equation

$$\tilde{E}_A\colon\ -3Y^2Z = X^3 - 432A^2Z^3$$

and is isomorphic to $E_A$ over $k$ through the map

$$\begin{array}{rccc} \psi: & E_A & \longrightarrow & \tilde{E}_A \\ & (X,Y,Z) & \longmapsto & (12AZ, \dfrac{36A}{\sqrt{-3}}(X-Y), X+Y). \end{array}$$

Let us consider the dual isogenies $\phi_1: E_A \longrightarrow \tilde{E}_A$ and $\phi_2: \tilde{E}_A \longrightarrow E_A$ given by the compositions $\phi_1 = \psi \circ \sqrt{-3}$ and $\phi_2 = -\sqrt{-3} \circ \psi^{-1}$; they are defined over $\mathbb{Q}$ and their composition $\phi_2 \circ \phi_1$ gives the *multiplication-by-*3 map on $E_A$.

To obtain a contradiction we have assumed that $Ш(E_A/k)\left[\sqrt{-3}\right]$ is isomorphic to $\mathbb{Z}/3$ as an abelian group; this is equivalent to the assumption that $Ш(E_A/k)[\phi_1]$ is isomorphic to $\mathbb{Z}/3$.

Let $\mathrm{Gal}(k/\mathbb{Q}) = \langle\sigma\rangle$. We have two possibilities: either $\sigma$ acts trivially on $Ш(E_A/k)[\phi_1]$ and therefore $Ш(E_A/k)[\phi]$ and $\mathbb{Z}/3$ are isomorphic as $\mathrm{Gal}(k/\mathbb{Q})$-modules; or $\sigma$ exchanges the two non-trivial elements of $Ш(E_A/k)[\phi_1]$ and so $Ш(E_A/k)[\phi_1]$ is isomorphic to $\mu_3$.

If $Ш(E_A/k)[\phi_1]$ is isomorphic to $\mathbb{Z}/3$ as a $\mathrm{Gal}(k/\mathbb{Q})$-module then $Ш(\tilde{E}_A/k)[\phi_2]$ is isomorphic to $\mu_3$ as a $\mathrm{Gal}(k/\mathbb{Q})$-module and vice versa. Indeed, if $Ш(E_A/k)[\phi_1]$ is composed of the cohomology classes $\xi_0, \xi_1, \xi_2$, then $Ш(\tilde{E}_A/k)[\phi_2]$ is composed of $\psi\xi_0, \psi\xi_1, \psi\xi_2$; moreover ${}^{\sigma}\psi = -\psi$. So, if $\sigma$ acts trivially on $Ш(E_A/k)[\phi_1]$ then it does not on $Ш(\tilde{E}_A/k)[\phi_2]$ and vice versa.

Suppose that $Ш(E_A/k)[\phi_1] \cong \mathbb{Z}/3$ as a $\mathrm{Gal}(k/\mathbb{Q})$-module and consider the exact sequence of $\mathrm{Gal}(k/\mathbb{Q})$-modules

$$0 \longrightarrow Ш(E_A/k)[\phi_1] \longrightarrow Ш(E_A/k)[3] \longrightarrow Ш(\tilde{E}_A/k)[\phi_2]$$

where the first map is the natural inclusion and the second one is induced by $\phi_1$. From this sequence we get the exact sequence

$$0 \longrightarrow Ш(E_A/k)[\phi_1]^{\mathrm{Gal}(k/\mathbb{Q})} \longrightarrow Ш(E_A/k)[3]^{\mathrm{Gal}(k/\mathbb{Q})} \longrightarrow Ш(\tilde{E}_A/k)[\phi_2]^{\mathrm{Gal}(k/\mathbb{Q})}$$

where $Ш(E_A/k)[\phi_1]^{\mathrm{Gal}(k/\mathbb{Q})} \cong \mathbb{Z}/3$ and $Ш(\tilde{E}_A/k)[\phi_2]^{\mathrm{Gal}(k/\mathbb{Q})} \cong 0$.
If $Ш(E_A/k)[\phi_1] \cong \mu_3$, it is sufficient to consider the sequence

$$0 \longrightarrow Ш(\tilde{E}_A/k)[\phi_2] \longrightarrow Ш(E_A/k)[3] \longrightarrow Ш(E_A/k)[\phi_1]$$

instead of that above.

In both cases, we can conclude that $Ш(E_A/k)[3]^{\mathrm{Gal}(k/\mathbb{Q})}$ is isomorphic to $\mathbb{Z}/3$. This contradicts Lemma 4 which claims that the order of $Ш(E_A/k)[3]^{\mathrm{Gal}(k/\mathbb{Q})}$ must be a square. As a result, $Ш(E_A/k)\left[\sqrt{-3}\right]$ cannot have order 3. □

In conclusion, we have proved that $C(A) = S(A)$ for $A = p_1p_2p$. Moreover, in the proof of Lemma 3 we have shown $p_1p_2^2(k^*)^3$ belongs to $S(A)$; it follows that the curve $p_1X^3 + p_2Y^3 = p$ has a $k_\rho-$point for any prime $\rho$ of $k$ and hence, by the local-to-global

principle, it has a point over the quadratic extension $k$ of $\mathbb{Q}$. Therefore it has a point over $\mathbb{Q}$.

In order to prove Theorem 1, it only remains to be shown that given the prime integers $p_1, p_2, p_3, p_4 \equiv 2 \pmod 3$ there exists a prime $\pi$ such that the hypotheses of Lemma 3 are satisfied for each of the triples $p_1, p_2, \pi$ and $p_3, p_4, \pi$.

**Lemma 6** *Let $p_1, p_2, p_3, p_4$ be prime integers congruent to 2 modulo 3. Then there exists a prime $\pi \in \mathbb{Z}[\omega]$ such that*

*(i)* $\pi \equiv 1 \pmod 3$*;*

*(ii)* $p_1p_2N(\pi)$ *and* $p_3p_4N(\pi)$ *are not congruent to 1 modulo 9;*

*(iii)* $\left(\frac{\pi}{p_1}\right)_3 = \left(\frac{\pi}{p_2}\right)_3 = \left(\frac{\pi}{p_3}\right)_3 = \left(\frac{\pi}{p_4}\right)_3 \neq 1.$

*Proof.* Let $B \in \{1, 4, 7\}$ such that

$$\begin{cases} p_1p_2B \not\equiv 1 \pmod 9 \\ p_3p_4B \not\equiv 1 \pmod 9. \end{cases}$$

Take a prime $\pi \in \mathbb{Z}[\omega]$ such that $N(\pi) \equiv B \pmod 9$. This condition can be satisfied by taking $\pi \equiv \beta \pmod 9$, where $\beta$ is an element of $\mathbb{Z}[\omega]$ congruent to $1, -2$ or $1+3\omega$ modulo 9 if $B = 1, 4$ or 7, respectively. Hence we have that $p_ip_jB \not\equiv 1 \pmod 9$ if and only if $p_ip_jN(\pi) \not\equiv 1 \pmod 9$. Therefore conditions (i) and (ii) are satisfied.

As far as condition (iii) is concerned, in order for $\pi$ to satisfy

$$\left(\frac{\pi}{p_1}\right)_3 = \left(\frac{\pi}{p_2}\right)_3 = \left(\frac{\pi}{p_3}\right)_3 = \left(\frac{\pi}{p_4}\right)_3 \neq 1$$

it is sufficient to take $\pi$ belonging to a suitable congruence class modulo $p_1p_2p_3p_4$. The Chinese Remainder Theorem allows us to determine a suitable residue class $\gamma$ modulo $9p_1p_2p_3p_3$ such that, if $\pi \equiv \gamma \pmod{9p_1p_2p_3p_3}$, then $\pi$ satisfies the required conditions. The existence of such a prime $\pi$ is assured by Dirichlet's Theorem. □

Hence Theorem 1 is proved.

We thank Alexei Skorobogatov for his help in the preparation of this note.

# 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] J.W.S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[3] R. Heath-Brown. *The solubility of diagonal cubic equations*. Proc. London Math. Soc. (3) 79 (1999), 241–259.

[4] J.-P. Serre. *A course in Arithmetic*. New York: Springer–Verlag, 1973.

[5] J.-P. Serre. *Galois cohomology*. Springer–Verlag Berlin Heidelberg, 1997.

[6] J.H. Silverman. *The Arithmetic of Elliptic Curves*. New York: Springer–Verlag, 1986.

[7] H.P.F. Swinnerton–Dyer. *The solubility of diagonal cubic surfaces*. Preprint (August 2000).