No Points of Order 11

Winston Stucki

December 2018

1 Introduction

This paper will present the proof that there exist no rational torsion points of order 11 on any elliptic curve over $\mathbb{Q}$, which was proven in 1940 by Billing and Mahler. The first half of this proof will be presented thoroughly and rigorously, with an emphasis on detail so as to explain every step to the reader coherently. Alas, the second half will not be as rigorous and will not justify everything as a result of my currently limited understanding of algebraic number theory, although the steps will be outlined as will the relevance to the overall proof. I used Ian Kiming's notes [1] as a basis for my proof

Theorem 1. (Billing-Mahler): An elliptic curve defined over $\mathbb{Q}$ does not have a rational torsion point of order 11.

We begin by assuming that we have some elliptic curve with a rational point $\widetilde{P}$ with order 11. We will first propose a few definitions which are vital to the proof:

$$\widetilde{P}_i := i\widetilde{P} = \widetilde{P} + \cdots + \widetilde{P} \quad (i \text{ times}),$$

and, because $\widetilde{P}_{11} = 0$,

$$\widetilde{P}_i = \widetilde{P}_j \iff i \equiv j \quad (11).$$

Additionally,

$$(*) \qquad \widetilde{P}_i, \widetilde{P}_j, \widetilde{P}_k \text{ lie on a line} \iff \widetilde{P}_i + \widetilde{P}_k + \widetilde{P}_k = 0 \iff i + j + k \equiv 0 \quad (11).$$

The connection between the second and third statement of $(*)$ is clear, and their connection to the first statement is due to the following: If $\widetilde{P}_i + \widetilde{P}_k + \widetilde{P}_k = 0$, then $\widetilde{P}_k = -(\widetilde{P}_i + \widetilde{P}_j) = (\widetilde{P}_i * \widetilde{P}_j)$, which is colinear with $\widetilde{P}_i$ and $\widetilde{P}_j$.

We will also use the following lemma frequently, which we will not bother to prove as it follows from some linear algebra:

Lemma: Let k be a field and let (a, b, c) and (α, β, γ) be two distinct points on $\mathbb{P}^2(k)$. There is a unique line through these points and it is given by:

$$\begin{vmatrix} x & y & z \\ a & b & c \\ \alpha & \beta & \gamma \end{vmatrix} = 0.$$

Two lines given by equations $ux + vy + wz = 0$ and $u'x + v'y + w'z = 0$ coincide iff the points (u, v, w) and (u', v', w') coincide as points in $\mathbb{P}^2(k)$.

Two distinct lines in $\mathbb{P}^2(k)$ intersect at exactly one point.

2 Implications of a Point of Order 11

Consider the 3 points $\widetilde{P}_0 = (0, 1, 0), \widetilde{P}_1 = (a, b, c)$, and $\widetilde{P}_2 = (\alpha, \beta, \gamma)$. $0 + 1 + 2 = 3$ so by $(*)$ we know these points do not lie on a line. The second statement of the above lemma then implies that the vectors $(0, 1, 0), (a, b, c)$ and (α, β, γ) are linearly independent. Hence there is a linear map ϕ of $\mathbb{Q}^3$ which maps the points $\widetilde{P}_0, \widetilde{P}_1, \text{and} \widetilde{P}_2$ to the points

$$P'_0 := (0, 1, 0), \quad P'_1 := (1, 0, 0), \text{ and } \quad P'_2 := (0, 0, 1) \text{ respectively.}$$

That is, we can consider ϕ to be a bijective map on $\mathbb{P}^2(Q)$ to itself that preserves lines, and that torsion points are preserved as well, so P_1' has order 11, so we may denote $P_i' = \phi(\widetilde{P}_i)$. Then it follows from $(*)$ that

$$i + j + k \equiv 0 \iff \widetilde{P}_i, \widetilde{P}_j, \widetilde{P}_k \text{ lie on a line.} \iff P_i', P_j', P_k' \text{ lie on a line.}$$

Namely, $(*)$ holds for P_i' in place of the $\widetilde{P}_i$.

Consider the point $P_3' = (u, v, w)$. By $(*)$ we know that P_3' is not on the line through P_0' and P_1'. Since the line through these two points is given by the equation $z = 0$ (by the lemma), this implies that $w \neq 0$. Similarly it is not on the line through P_0' and P_2' or the line through P_1' and P_2', so we find that $u \neq 0$ and $v \neq 0$.

Hence we may consider another invertible linear map ψ of $\mathbb{Q}^3$ which is given by $x \mapsto x/u, y \mapsto y/v, z \mapsto z/w$. ϕ is a bijective map which maps lines to lines in $\mathbb{P}^2(\mathbb{Q})$. This map fixes the points $P_0', P_1',$ and P_2', as they are elements of $\mathbb{P}^2(\mathbb{Q})$, which are equivalent under scalar multiplication by elements of $\mathbb{Q}$.

We now denote

$$P_i := \psi(P_i') = \phi(\psi(\widetilde{P}_i)) \qquad \text{for } i \in \mathbb{Z}$$

Thus we know:

$$P_0 = (0, 1, 0), P_1 = (1, 0, 0), P_2 = (0, 0, 1), P_3 = (1, 1, 1),$$

$$P_i = P_j \iff i \equiv j \pmod{11},$$

and as a result of preservation of lines by ψ:

$$P_i, P_j, P_k \text{ lie on a line} \iff i + j + k \equiv 0 \pmod{11}.$$

Let us put:

$$P_4 = (x_1, x_2, x_3).$$

Proposition 1. Given the above,

$$P_{-3} = (1, 0, 1),$$

and the coordinates x_1, x_2, x_3 satisfy the equation

$$x_1^2 x_2 - x_1^2 x_3 + x_1 x_3^2 - x_2^2 x_3 = 0.$$

Proof. For $i \neq j \pmod{11}$ there is a unique line through the points P_i and P_j, we will call it $L_{i,j}$. Our lemma tells us how to find an equation for $L_{i,j}$ if we know the coordinates of P_i and P_j.

Also, if we have integers k, i, j, m, n such that $k + i + j \equiv k + m + n \equiv 0 \pmod{11}$, which indicates that P_k, P_i, P_j are colinear, as are P_k, P_m, P_n. Thus P_k is in the intersection $L_{i,j} \cap L_{m,n}$, which will be one point if the two lines are distinct.

By use of the lemma we can get the equations for the following lines:

$$L_{0,1} : z = 0,$$

$$L_{0,2} : x = 0,$$

$$L_{0,3} : x - z = 0,$$

$$L_{1,2} : y = 0,$$

$$L_{1,4} : x_3 y - x_2 z = 0,$$

$$L_{2,3} : x - y = 0.$$

P_{-3} is the unique point of intersection of the lines $L_{0,3}$ and $L_{1,2}$, because $-3+0+3 \equiv -3+1+2 \equiv 0 \pmod{11}$, and the lines are clearly distinct. By combining these equations we find that

$$P_{-3} = (1, 0, 1).$$

Which proves the first statement of this proposition.

We may now find an equation for $L_{-3,4}$:

$$L_{-3,4} : -x_2 x + (x_1 - x_3)y + x_2 z = 0.$$

The point P_{-1} is the unique point of intersection between $L_{0,1}$ and $L_{-3,4}$, so by combining their respective equations we find that:

$$P_{-1} = (x_1 - x_3, x_2, 0).$$

We may now find an equation for $L_{-1,3}$:

$$L_{-1,3} : x_2 x - (x_1 - x_3)y + (x_1 - x_2 - x_3)z = 0.$$

The point P_{-2} is the unique point of intersection between $L_{0,2}$ and $L_{-1,3}$, so by combining their equations we find that:

$$P_{-2} = (0, x_1 - x_2 - x_3, x_1 - x_3).$$

We may now find an equation for $L_{-2,-3}$:

$$L_{2,3} : (x_1 - x_2 - x_3)x + (x_1 - x_3)y - (x_1 - x_2 - x_3)z = 0.$$

The point P_{-5} is the unique point of intersection between $L_{1,4}$ and $L_{2,3}$, so by combining their equations we find that:

$$P_{-5} = (x_2, x_2, x_3).$$

We may now find an equation for $L_{0,5}$:

$$L_{0,-5} : x_3 x - x_2 z = 0.$$

The point P_5 is the unique point of intersection between $L_{0,-5}$ and $L_{-2.-3}$, so by combining their equations we find that:

$$P_5 = ((x_1 - x_3)x_2, -x_1 x_2 + x_1 x_3 + x_2^2 - x_3^2, (x_1 - x_3)x_3).$$

Note that $x_1 - x_3 \neq 0$ as otherwise this would imply $P_{-2} = P_0$, which is a contradiction; also, $x_2 \neq 0$ as otherwise this would imply that $P_{-5} = P_2$ which is a contradiction. Thus P_5 is a point in $\mathbb{P}^2(Q)$ as the x and z components are both nonzero, and its coordinates satisfy the equations for the lines $L_{0,-5}$ and $L_{-2,-3}$.

Now, since $2 + 4 + 5 \equiv 0 \pmod{11}$, we know that the points P_2, P_4, and P_5 lie on a line. If we combine the lemma with the coordinates of P_2, P_4, and P_5, we know that:

$$\begin{vmatrix} 0 & 0 & 1 \\ x_1 & x_2 & x_3 \\ (x_1 - x_3)x_2 & -x_1 x_2 + x_1 x_3 + x_2^2 - x_3^2 & (x_1 - x_3)x_3 \end{vmatrix} = 0,$$

which is equivalent to the following statement:

$$x_1^2 x_2 - x_1^2 x_3 + x_1 x_3^2 - x_2^2 x_3 = 0. \qquad \square$$

Corollary 1. If there exists an elliptic curve defined over $\mathbb{Q}$ that has a rational point of order 11, then the cubic curve C given by the equation:

$$u^2 v - u^2 w + uw^2 - v^2 w$$

has more than 5 rational points.

Proof. The curve C clearly has the following 5 rational points:

$$P_0 = (0,1,0), P_1 = (1,0,0), P_2 = (0,0,1), P_3 = (1,1,1), P_{-3} = (1,0,1).$$

In addition, if we assume the existence of a rational point of order 11 on some elliptic curve over $\mathbb{Q}$, proposition 1 revealed the existence of a sixth rational point P_4 on C, which is different from all the points P_0, P_1, P_2, P_3, and P_{-3}.

3 The Cubic Curve C

If we prove the following proposition, it creates a contradiction with Corollary 1, which indicates that our initial assumption that there exists a point of order 11 on any elliptic curve over $\mathbb{Q}$ is false, which then implies theorem 1.

Proposition 2. The cubic curve C given by the equation:

$$u^2v - u^2w + uw^2 - v^2w = 0$$

has exactly 5 rational points (namely the 5 points (0,1,0), (1,0,0), (0,0,1), (1,1,1), and (1,0,1)).

We can apply a birational transformation to C which will give us an elliptic curve E which is in Weierstrass form, such that rational points on C will be mapped to rational points on E.

Proposition 3. Consider the cubic curve C given by the equation:

$$u^2v - u^2w + uw^2 - v^2w = 0,$$

as well as the elliptic curve E given by the Weierstrass equation:

$$y^2z = x^3 - 4x^2z + 16z^3.$$

The map f defined by:

$$f(u, v, w) := (4uv, 8v^2 - 4uw, uw)$$

maps points (u,v,w) on C with $uv \neq 0$ to points (x, y, z) on E with $x(y + 4z) \neq 0$.

conversely, the map g defined by:

$$g(x, y, z) := (2x^2, x(y + 4z), 4z(y + 4z))$$

maps points (x,y,z) on E with $x(y + 4z) \neq 0$ to points (u, v, w) on C with $uv \neq 0$, and we have:

$$(f \circ g)(x, y, z) = (x, y, z) \text{ whenever } x(y + 4z) \neq 0.$$

$$(g \circ f)(u, v, w) = (u, v, w) \text{ whenever } uv \neq 0.$$

Proof. Take some point (u, v, w) on C with $uv \neq 0$, which clearly forces $w \neq 0$.

We now denote:

$$V := \frac{v}{u}, \quad W := \frac{w}{u}, \quad t := \frac{V}{W}.$$

As we are in projective space we can freely multiply by scalar constants, so by dividing the equation for C by u^3 we have:

$$\frac{v^2w}{u^3} - \frac{w^2}{u^2} + \frac{w}{u} - \frac{v}{u} = t^2W^2 - W + (1 - t) = 0.$$

If we apply the quadratic formula on $t^2W^2 - W + (1 - t) = 0$ as a degree 2 polynomial of W, we find that

$$\pm\sqrt{R} = wt^2W - 1 = 2 \cdot \frac{v^2}{uw} - 1$$

where

$$R := 1 - 4t^2(1 - t) = 4t^3 - 4t^2 + 1.$$

Hence if we put

$$x := 4t = 4 \cdot \frac{v}{w}, \quad y := \pm\sqrt{R} = 8 \cdot \frac{v^2}{uw} - 4$$

then

$$y^2 = 4^2R = 4^3t^3 - 4 \cdot 4^2t^2 + 16 = x^3 - 4x^2 + 16$$

so

$$(x, y, 1) = (4uv, 8v^2 - 4uw, uw)$$

is a point on the elliptic curve E.

Conversely, if (x, y, z) is a point on E with $x(y + 4z) \neq 0$, then

$$(u, v, w) := (2x^2, x(y + 4z), 4z(y + 4z))$$

is a point in the projective plane, and it is on C because:

$$
\begin{aligned}
u^2(v-w)+uw^2-v^2w &= 4x^2(y+4z)(x^2(x-4z)+8(y+4z)z^2-(y+4z)^2z) \\
&= 4x^2(y+4z)(x^3-4x^2z+16z^3-y^2z) \\
&= 0.
\end{aligned}
$$

The last two claims of proposition 3 can be easily checked. □

Corollary 2. The cubic curve C has exactly 5 rational points if and only if the elliptic curve:

$$E : y^2z = x^3 - 4x^2z + 16z^3$$

has exactly 5 rational points.

Proof. The maps f and g from proposition 3 clearly map rational points on C to rational points on E and vice versa, respectively. From proposition 3 we know that there is a bijection between the sets

$$A := (u, v, w) \in C(\mathbb{Q}) | uv \neq 0$$

and

$$B := \{(x, y, z) \in E(\mathbb{Q}) | x(y + 4z) \neq 0\}.$$

The rational points (u, v, w) on C which aren't elements of A, i.e. where $uv = 0$, are clearly the following 4 points:

$$(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 0, 1).$$

And likewise, the rational points (x, y, z) on E which are not in B, i.e. $x(y + 4z) = 0$ are found to be the 4 points:

$$(0, 1, 0), (0, \pm 4, 1), (4, -4, 1).$$

Thus:

$$\#C(\mathbb{Q}) = 5 \iff \#A = 1 \iff \#B = 1 \iff \#E(\mathbb{Q}) = 5.$$

4 The Elliptic Curve E

By Corollary 2 the following proposition implies proposition 2 which proves theorem 1.

Proposition 4. The elliptic curve:

$$E : x^3 - 4x^2 + 16$$

has exactly 5 rational points.

Proof. We can use Nagell-Lutz to determine that $E(\mathbb{Q})_{tors}$ has order 5 (and is generated by the point $(0, 4)$).

The group $E(\mathbb{Q})$ is isomorphic to $E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$ where r is the rank. Thus the claim reduces to the claim that $E(\mathbb{Q})$ has rank 0, i.e. that it has finitely many elements.

Note that some of the following claims, particularly those related to algebraic number theory, will not be sufficiently justified, and will rather be accepted as a "black box" of sorts.

The polynomial $f(x) := x^3 - 4x^2 + 16$ is irreducible with discriminant:

$$Disc(f) = -2^8 \cdot 11.$$

Because the discriminant is negative, there must be one real solution and two complex solutions which are conjugates of each other. Let $\theta = \theta_1, \theta_2, \theta_3$ denote the roots of f, where θ is the real root.

Now, we consider the cubic number field:

$$K := \mathbb{Q}(\theta).$$

Through the use of a calculator, one can compute the following information about K:

The discriminant of K is:

$$Disc(K) = -44 = -2^2,$$

the ring of integers of K (which is the ring of elements of K which act as integers) is:

$$O_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta^2,$$

the unit rank of K is 1, and a fundamental unit is:

$$\eta := 1 - \frac{1}{2}\theta$$

so that the units of O_K are:

$$O_K^\times = \langle -1 \rangle \times \langle \eta \rangle.$$

The class number of K is:

$$h_K = 1.$$

Also, we have a homomorphism that is utilized in the proof of the irreducible case of Mordell's theorem:

$$\mu : E(\mathbb{Q}) \to K^\times/(K^\times)^2$$

which is defined by:

$$\mu(O) = 1, \quad \mu(x, y) := (x - \theta) \mod (K^\times)^2.$$

The homomorphism μ has kernel $2E(\mathbb{Q})$ (I will not prove this)

We know that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$, so we have

$$E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r$$

where the rank r of $E(\mathbb{Q})$ is a nonnegative integer. It follows that:

$$\text{Im}(\mu) \cong E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

Thus, proving that $r = 0$ reduces to proving that μ has trivial image.

Suppose that μ doesn't have a trivial image, so there is a rational point (x, y) on E such that $\mu(x, y)$ is nontrivial, namely that $x - \theta$ is not a square in K.

We know that x and y can be expressed as:

$$x = \frac{r}{t^2}, y = \frac{s}{t^3}$$

where $r, s, t \in \mathbb{Z}$ and $\gcd(r, t) = gcd(s, t) = 1$. Thus we get that:

$$\mu(x, y) = (x - \theta) \mod (K^\times)^2 = (r - t^2\theta) \mod (K^\times)^2$$

so we know

$$r - t^2\theta \notin (K^\times)^2.$$

We now consider the integral ideal $(r - t^2\theta)$ of O_K. Due to another part of the proof to the irreducible case of Mordell's theorem, we have that:

$$(\triangle) \qquad (r - t^2\theta) = \left(\prod_i \mathfrak{p}_i^{a_i} \right) \cdot \mathfrak{A}^2$$

where $\mathfrak{A}$ is some integral ideal, $a_i \in \{0, 1\}$, and the $\mathfrak{p}_i$ are distinct prime ideals of O_K such that each $\mathfrak{p}_i$ divides the discriminant:

$$\prod_{j \neq k} (\theta_j - \theta_k)^2 = \text{Disc}(f) = -2^8 \cdot 11,$$

which due to some algebraic number theory, each $\mathfrak{p}_i$ divides the discriminant, so they each divide either 2 or 11.

We claim that all exponents a_i in the product $\prod_i \mathfrak{p}_i^{a_i}$ are 0. To arrive at this result we accept that the prime decompositions of 2 and 11 in K are the following:

$$(2) = \mathfrak{p}^3, \quad (11) = \mathfrak{q}^2 \cdot \mathfrak{q}' \text{ with } \mathfrak{q} \neq \mathfrak{q}'$$

and that we have:

$$N_{K/\mathbb{Q}}(\mathfrak{p}) = 2, \quad N_{K/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(\mathfrak{q}') = 11.$$

The product $\prod_i \mathfrak{p}_i^{a_i}$ can be written to be:

$$\prod_i \mathfrak{p}_i^{a_i} = \mathfrak{p}^{a_1}\mathfrak{q}^{a_2}(\mathfrak{q}')^{a_3}$$

Where $a_1, a_2, a_3 \in 0, 1$, and

$$\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{a_i} = 2^{a_1} \cdot 11^{a_2+a_3}.$$

On the other hand, we have that

$$\begin{aligned}\prod_i N_{K/\mathbb{Q}}(\mathfrak{p})^{a_i} \cdot N_{K/\mathbb{Q}}(\mathfrak{A})^2 \quad &= \quad N_{K/\mathbb{Q}}(r - t^2\theta) \\ &= \quad ((r - t^2\theta_1)(r - t^2\theta_2)(r - t^2\theta_3)) \\ &= \quad (t^6(x - \theta_1)(x - \theta_2)(x - \theta_3)) \\ &= \quad (t^6y^2) = (s)^2\end{aligned}$$

so $\prod_i N_{K/\mathbb{Q}}(\mathfrak{p}_i)^{a_i}$ is a square.

Thus the only possible cases are where $a_1 = 0$ and $a_2 = a_3 = 0$ or $a_2 = a_3 = 1$.

Consider the case in which $a_2 = a_3 = 1$. then $(\triangle)$ informs us that $\mathfrak{q}\mathfrak{q}'|(r - t^2\theta)$. Because $11 = \mathfrak{q}^2\mathfrak{q}'$ we can conclude that:

$$11|\mathfrak{q}^2(\mathfrak{q}')^2|(r - t^2\theta)^2 = r^2 - 2rt^2\theta + t^4\theta^2$$

where the number

$$\frac{r^2 - 2rt^2\theta + t^4\theta^2}{11}$$

is in the ring of integers $O_K = \mathbb{Z} + \mathbb{Z} \cdot \frac{1}{2}\theta + \mathbb{Z} \cdot \frac{1}{4}\theta^2$, as 11 divides the top half. Thus 11 is forced to divide both r and t which is a contradiction as $\gcd(r, t) = 1$.

Thus the only remaining possibility is where $a_1 = a_2 = a_3 = 0$, and $(\triangle)$ tells us that $(r - t^2\theta = \mathfrak{A}^2$ for some integral ideal $\mathfrak{A}$. Since K has class number 1, it follows that $\mathfrak{A} = (\alpha)$ for some $\alpha \in O_K$. Thus:

$$r - t^2\theta = u \cdot a^2$$

where u is a unit that is not a square in K, because $r - t^2\theta$ is not a square in K. We may assume that $u \in \{-1, \eta, -\eta\}$, where $\eta := 1 - \frac{1}{2}\theta$, such that we choose appropriate α. Now,

$$N_{K/\mathbb{Q}}(u) \cdots N_{K/\mathbb{Q}} = N_{K/\mathbb{Q}}(r - t^2\theta) = s^2$$

where $N_{K/\mathbb{Q}}(u) > 0$ as the right hand side is a square. Once we consider that $N_{K/\mathbb{Q}}(-1) = -1$ and that $N_{K/\mathbb{Q}}(\eta) = 1$ (which I believe implies that $N_{K/\mathbb{Q}}(-\eta) = -1$), we are restricted to the case

$$r - t^2\theta = \eta \cdot \alpha^2$$

for some $\alpha \in O_K$. Let $\beta := \eta\alpha$ and say $\beta = a + b \cdot \frac{1}{2}\theta + c \cdot \frac{1}{4}\theta$, where $a, b, c \in \mathbb{Z}$. We find that a, b, c satisfy the following equation, which is the above equation with both sides multiplied by η:

$$\eta \cdot (r - t^2\theta) = (1 - \frac{1}{2}\theta)(r - t^2\theta) = \beta^2 = (a + b \cdot \frac{1}{2}\theta + c \cdot \frac{1}{4}\theta^2)^2$$

Upon using the fact that $\theta^3 = 4\theta^2 - 16, \theta^4 = 4\theta^3 - 16\theta = 16\theta^2 - 16\theta - 64$, we can calculate that the above equation is equivalent to:

$$r - (\frac{r}{2} + t^2)\theta + \frac{t^2}{2}\theta^2 = (a^2 - 4c^2 - 4bc) + (ab - c^2)\theta + (\frac{b^2}{4} + \frac{ac}{2} + bc + c^2)\theta^2.$$

As these are two polynomials of θ with degree 2 it follows that their coefficients must be equal. Namely:

$$(i) \qquad r = a^2{-}4c^2{-}4bc,$$

$$(ii) \qquad -r - 2t^2 = 2ab - 2c^2,$$

$$(iii) \qquad 2t^2 = b^2{+}2ac{+}4bc{+}4c^2.$$

Then, *(iii)* implies that b is even, and *(ii)* implies that r is even, which subsequently implies that a is even. Since a and b are both even, then the right hand side of *(iii)* is divisible by 4, which directly implies that t is now even, so $\gcd(r, t) \geq 2$ which contradicts $\gcd(r, t) = 1$.

Thus, the map μ is trivial, which implies that the rank of $E(\mathbb{Q})$ is 1, so $\#E(Q) = \#E_{\text{tors}}(Q) = 5$ (proving proposition 4), and hence by corollary 2, C has exactly 5 rational points (proposition 2) which contradicts corollary 1, which of course implies that our initial assumption that there is a point of order 11 on some elliptic curve is false, which directly implies theorem 1. □

References

[1] Ian Kiming et al. There are no points of order 11 on elliptic curves over q.