

An elliptic sequence is not a sampled linear recurrence sequence

F. Luca and T. Ward

ABSTRACT. Let E be an elliptic curve defined over the rationals and in minimal Weierstrass form, and let $P = (x_1/z_1^2, y_1/z_1^3)$ be a rational point of infinite order on E , where x_1, y_1, z_1 are coprime integers. We show that the integer sequence $(z_n)_{n \geq 1}$ defined by $nP = (x_n/z_n^2, y_n/z_n^3)$ for all $n \geq 1$ does not eventually coincide with $(u_{n^2})_{n \geq 1}$ for any choice of linear recurrence sequence $(u_n)_{n \geq 1}$ with integer values.

CONTENTS

1. Introduction	1319
2. A Diophantine proof of a special case of the main theorem	1321
3. A p -adic proof of the main theorem	1329
3.1. Orders of points on elliptic curves	1329
3.2. Proving Theorem 2	1331
Appendix	1333
Acknowledgements	1337
References	1337

1. Introduction

Let E be an elliptic curve defined over \mathbb{Q} , given by an equation of the form

$$(1) \quad y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ and with discriminant $\Delta_E = 4A^3 + 27B^2 \neq 0$, and write all affine points in the form $(x/z^2, y/z^3)$ with $\gcd(x, y, z) = 1$ and $z > 0$. Let $P = (x_1/z_1^2, y_1/z_1^3) \in E(\mathbb{Q})$ have infinite order and associate to P the integer sequence $(z_n)_{n \geq 1}$ where $nP = (x_n/z_n^2, y_n/z_n^3)$ for all $n \geq 1$. We will refer to such sequences as being elliptic divisibility sequences (there are several different definitions and we will only be cavalier about the distinction

Received February 18, 2015.

2010 *Mathematics Subject Classification.* 11B37; 11G05.

Key words and phrases. Elliptic divisibility sequence; nontorsion point; linear recurrence sequence.

where it does not matter). It is known that such a sequence has a characteristic quadratic-exponential growth rate, $\log z_n = (c + o(1))n^2$ as $n \rightarrow \infty$ (see [4, Sec. 10.4] for a discussion of the relation between sequences of this form and elliptic divisibility sequences defined via a bilinear recurrence or the sequence of division polynomials of the curve, and for references to some of the basic facts about linear and bilinear recurrence sequences including the growth rate). The constant c is the canonical height of the point P on the curve E .

On the other hand, an integer sequence $(u_n)_{n \geq 1}$ is said to be a linear recurrence sequence of order $k \geq 1$ if there are constants c_1, \dots, c_k with c_k nonzero satisfying

$$(2) \quad u_{n+k} = c_1 u_{n+k-1} + \dots + c_k u_n$$

for all $n \geq 1$, and k is minimal with this property. By Fatou's lemma [6, p. 369] we may assume that c_1, \dots, c_k are also integers. It is known that such a sequence (under a nondegeneracy hypothesis detailed later) has a characteristic linear-exponential growth rate: for any $\epsilon > 0$ there is some $N = N(\epsilon, (u_n))$ and constants $A, C > 0$ with $C^{(1-\epsilon)n} \leq |u_n| \leq AC^n n^k$ for all $n \geq N$ (see Evertse [5] or van der Poorten and Schlickewei [18]). The deep part of this statement is to control possible cancellation between dominant characteristic roots of equal size. We will not use this result here, but instead will deal directly with the possible multiplicity of dominant roots. Here the characteristic growth parameter C is the maximum of the set of absolute values of zeros of the associated characteristic polynomial.

It also makes sense to ask questions about arithmetic properties. For example:

- Does the sequence have a 'Zsigmondy bound', meaning that eventually each term of the sequence has a prime divisor that does not divide any earlier term? Silverman [15, Lemma 9] has shown that an elliptic divisibility sequence always has this property, and this will be used below. Some linear recurrence sequences do have this property (including, in particular, all Lucas and Lehmer sequences) and some do not.
- Does the sequence count periodic points for some map? Here it is known that some — but far from all — linear recurrence sequences do, while Silverman and Stephens [17] show that no elliptic divisibility sequence does.

In light of the growth rate observations particularly, it is natural to ask if an elliptic divisibility sequence is simply a linear recurrence sequence in disguise, obtained by sampling the linear recurrence sequence at the squares. Our purpose here is to show that this is not the case in the following robust sense. Let us say that sequences $(a_n)_{n \geq 1}$ and $(b_n)_{n \geq 1}$ are *eventually equal*, written $(a_n)_{n \geq 1} =_e (b_n)_{n \geq 1}$, if there is some $N = N((a_n), (b_n))$ with $a_n = b_n$ for all $n \geq N$.

Theorem 1. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over the rationals, let $P = (x_1/z_1^2, y_1/z_1^3) \in E(\mathbb{Q})$ be a point of infinite order, and let $(z_n)_{n \geq 1}$ be a sequence of integers satisfying $nP = (x_n/z_n^2, y_n/z_n^3)$ (the sign of z_n can be chosen arbitrarily). Then no integer linear recurrence sequence $(u_n)_{n \geq 1}$ has the property that*

$$(z_n)_{n \geq 1} =_e (u_{n^2})_{n \geq 1}.$$

For any such sequence $(z_n)_{n \geq 1}$ there is some $\ell \geq 1$ with the property that $(z_{\ell n})_{n \geq 1}$ is, up to signs, an elliptic divisibility sequence in the recurrence sense, meaning that it satisfies the nonlinear recurrence defined by specifying four initial integral values w_1, w_2, w_3, w_4 with $w_1 w_2 w_3 \neq 0$ and with $w_2 | w_4$, and satisfies

$$(3) \quad w_{2n+1} w_1^3 = w_{n+2} w_n^3 - w_{n+1}^3 w_{n-1}$$

for $n \geq 2$ and

$$(4) \quad w_{2n} w_2 w_1^2 = w_{n+2} w_n w_{n-1}^2 - w_n w_{n-2} w_{n+1}^2.$$

Since the property of being a linear recurrence sequence is preserved under the operation taking $(u_n)_{n \geq 1}$ to $(u_{\ell^2 n})_{n \geq 1}$, it is therefore enough to show that Theorem 1 holds for elliptic divisibility sequences defined either geometrically using a nontorsion point on an elliptic curve or using the nonlinear recurrence relation.

For a restricted class of linear recurrence sequences we can already deduce Theorem 1 from the work of Silverman and Stephens [17], by the following argument. Moss [8, Th. 2.2.2] has given a combinatorial proof that if $(u_n)_{n \geq 1}$ counts the periodic points for some map, then so does $(u_{n^k})_{n \geq 1}$ for any $k \geq 1$. It follows that (for example) sampling a Lehmer–Pierce sequence along the squares never produces an elliptic divisibility sequence.

We shall give two proofs of Theorem 1, a complex (Diophantine) one, which works only when the signs of z_n are chosen in a specific way, and a p -adic (arithmetic) one which works for any choice of signs.

2. A Diophantine proof of a special case of the main theorem

This particular proof works when $(z_n)_{n \geq 1}$ is an elliptic divisibility sequence. We make this assumption throughout this section. We start with a linear recurrence sequence $(u_n)_{n \geq 1}$ of some order $k \geq 1$, assume the relation

$$(5) \quad (z_n)_{n \geq 1} =_e (u_{n^2})_{n \geq 1},$$

deduce certain properties the linear recurrence sequence must have, and then argue that the hypothesis leads to a contradiction. If $k = 1$ then $(u_n)_{n \geq 1}$ is either constant or a geometric progression and so in particular the largest prime factor of u_n is bounded. On the other hand, as mentioned above, Silverman [15, Lemma 9] has shown that all but finitely many terms of $(z_n)_{n \geq 1}$ have a primitive prime divisor (that E is really an elliptic curve — it has

nonvanishing discriminant — is used here), and so the largest prime divisor of $(z_n)_{n \geq 1}$, and hence of $(u_n)_{n \geq 1}$, cannot be bounded. It follows that $k > 1$.

Assume therefore that $(u_n)_{n \geq 1}$ has order $k \geq 2$ and satisfies (2); write

$$\Psi(x) = x^k - c_1x^{k-1} - \dots - c_k = \prod_{i=1}^s (x - \alpha_i)^{\sigma_i}$$

where $\alpha_1, \dots, \alpha_s \in \mathbb{C}$ are distinct roots with multiplicity $\sigma_1, \dots, \sigma_s$ respectively. As usual we may then write the terms of the sequence as a generalized power sum

$$(6) \quad u_n = \sum_{i=1}^r P_i(n)\alpha_i^n,$$

for all $n \geq 1$, where the polynomials $P_i(X) \in \mathbb{Q}(\alpha_1, \dots, \alpha_s)[X]$ have degree $(\sigma_i - 1)$ for $i = 1, \dots, s$ (the claim on the degrees being a consequence of the assumed minimality of k ; taking the form of (6) in fact characterizes being a linear recurrence sequence of order no more than k , which implies useful consequences like $(u_{mn})_{n \geq 1}$ being a linear recurrence of order no more than k for any $m \geq 1$ if $(u_n)_{n \geq 1}$ is a linear recurrence of order k , for instance).

We next claim that — for the purposes of proving Theorem 1 — we may assume that $(u_n)_{n \geq 1}$ is nondegenerate. This is a standard reduction argument in the study of linear recurrence sequences, which we outline briefly. A linear recurrence sequence of order k written as (6) is said to be degenerate if for some pair $1 \leq i \neq j \leq s$ the quotient α_i/α_j is a root of unity, and nondegenerate if not. Since the group of roots of unity in $\mathbb{K} = \mathbb{Q}(\alpha_1, \dots, \alpha_s)$ is a finite cyclic group, there is some M with the property that if a product $\zeta = \alpha_1^{m_1} \dots \alpha_s^{m_s}$ is a root of unity, then $\zeta^M = 1$. Thus we may replace the sequence $(u_n)_{n \geq 1}$ with $(u_{M^2n})_{n \geq 1}$, which is clearly a linear recurrence sequence of order no more than k by (6), and the relation (5) implies that $(z_{Mn})_{n \geq 1} =_e (u_{M^2n})_{n \geq 1}$, which is the same relation but with the point P replaced with MP . Here we are taking advantage of the geometric description of the elliptic divisibility sequence. Thus it is sufficient to show Theorem 1 for nondegenerate linear recurrence sequences of order $k \geq 2$. By rescaling once again (which will not affect the nondegeneracy), we may also assume that the elliptic divisibility sequence satisfies the nonlinear recurrence (3)–(4).

Re-label the zeroes of Ψ so that

$$|\alpha_j| = \rho = \max\{|\alpha_i| \mid 1 \leq i \leq s\} > 1$$

for $j = 1, \dots, r$ and $|\alpha_j| \leq \rho^{1-\delta}$ for $j = r+1, \dots, s$ for some $\delta > 0$ (that $\rho > 1$ follows from (5) and the fact that the sequence $(z_n)_{n \geq 1}$ grows like c^{n^2} for some $c > 1$, since the canonical height of a nontorsion point is positive). So

we may write $\alpha_j = \rho e^{i\theta_j}$ with $\theta_j \in (-\pi, \pi]$ for $j = 1, \dots, r$, and

$$u_n = \sum_{i=1}^r P_i(n)\alpha_i^n + O\left(n^D \rho^{n(1-\delta)}\right),$$

where $D := \max\{\sigma_i : 1 \leq i \leq s\}$.

From (3) and (4) we have

$$z_{2n+1} = z_{n+2}z_n^3 - z_{n-1}z_{n+1}^3$$

for all $n \geq 1$. Using (5), we deduce that

$$\begin{aligned} (7) \quad & \sum_{i=1}^r P_i((2n+1)^2)\alpha_i^{(2n+1)^2} \\ &= \left(\sum_{i=1}^r P_i((n+2)^2)\alpha_i^{(n+2)^2}\right) \times \left(\sum_{i=1}^r P_i(n^2)\alpha_i^{n^2}\right)^3 \\ &\quad - \left(\sum_{i=1}^r P_i((n-1)^2)\alpha_i^{(n-1)^2}\right) \times \left(\sum_{i=1}^r P_i((n+1)^2)\alpha_i^{(n+1)^2}\right)^3 \\ &\quad + O\left(n^{8D} \rho^{4n^2+4n-\delta n^2}\right) \end{aligned}$$

for large $n \geq 1$. So, it makes sense to consider the expression

$$\begin{aligned} & F(X, Z_1, \dots, Z_r) \\ &:= \sum_{i=1}^r P_i((2X+1)^2)Z_i^{(2X+1)^2} \\ &\quad - \left(\sum_{i=1}^r P_i((X+2)^2)Z_i^{(X+2)^2}\right) \left(\sum_{i=1}^r P_i(X^2)Z_i^{X^2}\right)^3 \\ &\quad + \left(\sum_{i=1}^r P_i((X-1)^2)Z_i^{(X-1)^2}\right) \left(\sum_{i=1}^r P_i((X+1)^2)Z_i^{(X+1)^2}\right)^3 \\ &=: \sum_{j=1}^L Q_j(X)M_j(X, Z_1, \dots, Z_r), \end{aligned}$$

where the $Q_j(X)$ are polynomials in the variable X of degree at most $8D$, and for fixed positive integer X the expressions $M_j(X, Z_1, \dots, Z_r)$ are monomials in Z_1, \dots, Z_r of degree $4X^2+4X+1$ or $4X^2+4X+4$. Here, $L = r+2r^4$. Further, up to relabeling of the indices $j \in \{1, \dots, L\}$, we may assume that

$$(Q_i(X), M_i(X)) = (P_i((2X+1)^2), Z_i^{4X^2+4X+1})$$

for $1 \leq i \leq r$, and that

$$(Q_i(X), M_i(X)) = \left(P_i((X + 2)^2)P_i^3(X^2) - P_i((X - 1)^2)P_i^3((X + 1)^2), Z_i^{4X^2+4X+4} \right)$$

for $r + 1 \leq j \leq 2r$. Note that $M_j(X)$ involves at least two of the indeterminates Y_1, \dots, Y_r for $j > 2r$ and that $M_j(X)$ has total degree $4X^2 + 4X + 4$ for all $j > r$. Since we need to specialize the expression $F(X, Z_1, \dots, Z_r)$ to $X = n$ and $(Z_1, \dots, Z_r) = (\alpha_1, \dots, \alpha_r)$, where the components of this last r -dimensional vector are multiplicatively independent complex numbers with the same absolute value ρ , we find it convenient to make the change of variable $Z_i := Ze^{iY_i}$, and thus look at the expression

$$\begin{aligned} G(X, Z, Y_1, \dots, Y_r) &:= F(X, Ze^{iY_1}, \dots, Ze^{iY_r}) \\ &:= \sum_{i=1}^r P_i((2X + 1)^2)(Ze^{iY_i})^{(2X+1)^2} \\ &\quad - \left(\sum_{i=1}^r P_i((X + 2)^2)(Ze^{iY_i})^{(X+2)^2} \right) \left(\sum_{i=1}^r P_i(X^2)(Ze^{iY_i})^{X^2} \right)^3 \\ &\quad + \left(\sum_{i=1}^r P_i((X - 1)^2)(Ze^{iY_i})^{(X-1)^2} \right) \left(\sum_{i=1}^r P_i((X + 1)^2)(Ze^{iY_i})^{(X+1)^2} \right)^3 \\ &= Z^{4X^2+4X+1} \sum_{j=1}^{L_1} Q_j(X, Z)_{Y_1, \dots, Y_r} e^{f_j(Y_1, \dots, Y_r, X)}, \end{aligned}$$

where $L_1 := L - r$,

$$Q_j(X, Z)_{Y_1, \dots, Y_r} = \begin{cases} (Q_j(X) - (Ze^{iY_j})^3 Q_{j+r}(X))e^{iY_j}, & 1 \leq j \leq r; \\ Z^3 Q_{j+r}(X) M_{j+r}(0, e^{iY_1}, \dots, e^{iY_r}), & r + 1 \leq j \leq L_1, \end{cases}$$

and

$$e^{f_j(Y_1, \dots, Y_r, X)} = \begin{cases} e^{iY_j(4X^2+4X)}, & 1 \leq j \leq r; \\ \frac{M_{j+r}(X, e^{iY_1}, \dots, e^{iY_r})}{M_{j+r}(0, e^{iY_1}, \dots, e^{iY_r})}, & r + 1 \leq j \leq L_1. \end{cases}$$

Note that the expressions $f_j(Y_1, \dots, Y_r, X)$ are linear forms in iY_1, \dots, iY_r whose coefficients are quadratic polynomials in X . In fact,

$$f_i(Y_1, \dots, Y_r, X) = i \sum_{j \in I_i} m_{i,j}(X) Y_j,$$

where $I_i \in \{1, \dots, r\}$, $m_{i,j}(X)$ are quadratic polynomials in X with integer coefficients, $m_{i,j}(0) = 0$ for all $1 \leq i \leq L_1$ and $j \in I_i$, and

$$\sum_{j \in I_i} m_{i,j}(X) = 4X^2 + 4$$

for all $1 \leq i \leq L_1$. For $i = 1, \dots, r$, we have $I_i = \{i\}$, therefore

$$m_{i,i}(X) = 4X^2 + 4X,$$

while for $i > r$, I_i has at least two (and at most four) elements. Now that we have fixed some notation, we return to (7), put the dominant terms on the left-hand side, the expression inside O on the right-hand side, and divide both sides by ρ^{4n^2+4n+1} obtaining (in our notation)

$$(8) \quad \rho^{-4n^2-4n-1}G(n, \rho, \theta_1, \dots, \theta_r) = \sum_{i=1}^{L_1} x_i = O(\rho^{-\delta_1 n^2}),$$

where $\delta_1 := \delta/2$ and

$$x_i = x_i(n) = Q_i(n, \rho)_{\theta_1, \dots, \theta_r} e^{i f_i(n)}$$

for $1 \leq i \leq L_1$, with

$$f_i(n) := f_i(\theta_1, \dots, \theta_r, n)$$

for all $i \in \{1, \dots, L_1\}$. Let us take a closer look at

$$f_i(X) = \sum_{j \in I_i} m_j(X) \theta_j \in \mathbb{C}[x]$$

for $i \in \{1, \dots, L\}$. We claim that if two elements in $\{f_1, \dots, f_L\}$ are equivalent modulo the equivalence relation

$$f_{\ell_1}(X) \equiv_{\pi} f_{\ell_2}(X) \iff \frac{1}{\pi}(f_{\ell_1}(X) - f_{\ell_2}(X)) \in \mathbb{Q}[X]$$

then they are in fact equal. To see this, notice that $f_{\ell_1}(X) \equiv_{\pi} f_{\ell_2}(X)$ implies that

$$e^{i(f_{\ell_1}(n) - f_{\ell_2}(n))}$$

is a monomial in $\alpha_1/\rho, \dots, \alpha_r/\rho$ and is a root of unity. In particular, for some positive integer A we have

$$e^{Ai(f_{\ell_1}(n) - f_{\ell_2}(n))} = 1.$$

This leads to

$$\left(\prod_{j \in I_{\ell_1}} \left(\frac{\alpha_j}{\rho} \right)^{Am_{\ell_1,j}(n)} \right) \left(\prod_{j \in I_{\ell_2}} \frac{\alpha_j}{\rho} \right)^{-Am_{\ell_2,j}(n)} = 1.$$

Since $\sum_{j \in I_{\ell}} m_{\ell,j}(n)$ is equal to $4n^2 + 4n$, this gives

$$\prod_{j \in I_{\ell_1}} \alpha^{Am_{\ell_1,j}(n)} \prod_{j \in I_{\ell_2}} \alpha_j^{-Am_{\ell_2,j}(n)} = 1,$$

so $I_{\ell_1} = I_{\ell_2}$ and $m_{\ell_1,j}(n) = m_{\ell_2,j}(n)$ for $j \in I_{\ell_1}$ and for all n since $\alpha_1, \dots, \alpha_r$ are multiplicatively independent, and hence $f_{\ell_1}(n) = f_{\ell_2}(n)$ for all n . It follows that $f_{\ell_1}(X) = f_{\ell_2}(X)$. In particular, we deduce that $e^{i(f_{\ell_1}(n) - f_{\ell_2}(n))}$ is not a root of unity for large n if $f_{\ell_1}(X) \neq f_{\ell_2}(X)$.

The method of proof consists now in completing the following three steps:

- (a) For each $i \in \{1, \dots, L_1\}$ there is some $j \in \{1, \dots, L_1\}$, $j \neq i$, such that $f_j = f_i$.
- (b) If $i \in \{1, \dots, r\}$ and $f_j = f_i$ for some $j \neq i$, then $j \geq r + 1$.
- (c) The final contradiction.

Let us look at the left-hand side of (8). Assume first that it is not identically zero as a function of n . Then the expression on the right-hand side of (8) is not identically zero either, so $L \geq 1$. Moreover, the vector

$$(9) \quad \mathbf{x}(n) = (x_1(n), \dots, x_L(n))$$

satisfies

$$(10) \quad H(\mathbf{x}) \geq \rho^{\kappa n^2}$$

for some appropriate positive constant κ , where H denotes the naïve height. Indeed, this follows because

$$x_j(n) = Q_j(n, \rho)_{\theta_1, \dots, \theta_r} e^{f_j(n)},$$

$j = 1, \dots, r$, where $Q_j(n, \rho)_{\theta_1, \dots, \theta_r}$ as given by (17) is nonzero because $P_j(X)$ is nonzero by Lemma 5. Since from now on $X = n$ is the only variable, we omit the dependence on $\rho, \theta_1, \dots, \theta_r$ when we refer to the polynomials $Q_j(X, \rho)_{\theta_1, \dots, \theta_r}$. Indeed, if the degree of $P_j(X)$ is $d_j > 0$, then the degree of $Q_j(X, \rho)_{\theta_1, \dots, \theta_r}$ is $8d_j - 3 > 0$, otherwise $P_j(X)$ is a nonzero constant $P_j(0)$, and $Q_j(X)$ is the nonzero constant $P_j(0)$. If $r = 1$, then $Q_1(n, \rho)_{\theta_1} e^{f_1(n)}$ is the only term in the left-hand side of (8), so (8) is impossible. Thus, $r \geq 2$, so one of θ_1 and θ_2 is not in $\mathbb{Q}\pi$. Thus, one of $e^{i\theta_1}$ or $e^{i\theta_2}$ is not a root of unity, which implies the inequality (10) by considering just the first two coordinates of \mathbf{x} , namely $x_1(n)$ or $x_2(n)$. We assume that n is large, in particular that it is outside the finite set of zeros of all the nonzero polynomials $Q_1(X), \dots, Q_L(X)$. It is then an immediate consequence of Schmidt’s subspace theorem [12] that the solutions $\mathbf{x}(n)$ of the form (9) to the inequality

$$\sum_{i=1}^{L_1} x_i = O\left(H(\mathbf{x})^{-\delta_1/\kappa}\right),$$

which is implied by (8) via (10), live in finitely many subspaces of $\overline{\mathbb{Q}}^{\#\mathcal{D}}$. That is, there exist finitely many nonzero vectors $\mathbf{d} \in \{\mathbf{d}^{(1)}, \dots, \mathbf{d}^{(u)}\} \subset \overline{\mathbb{Q}}^{\#\mathcal{D}}$ with the property that on writing $\mathbf{d}^{(\ell)} = (d_i^{(\ell)})_{1 \leq i \leq L}$ we must have that there exists some $\ell \in \{1, \dots, u\}$ such that

$$(11) \quad \sum_{i=1}^{L_1} d_i^{(\ell)} x_i = 0.$$

All this was in the case when the left-hand side of (8) is nonzero. If it is zero, we get Equation (11) at once, with $d_i^{(\ell)} = 1$ for $1 \leq i \leq L_1$. So it remains to look at equations of the form (11). For each n satisfying (11) the left-hand side can be nondegenerate or degenerate. Here, nondegenerate means that

the sum over any proper subset of $\{1, \dots, L_1\}$ on the left-hand side of (11) does not sum to zero. In any case an equation of the form (11) may be thought of as a sum with a bounded number of terms of sums over disjoint subsets of $\{1, \dots, L_1\}$ each of which comprises a nondegenerate equation. That is, if (11) is degenerate, then we may write

$$\{1 \leq i \leq L_1 : d_i^{(\ell)} \neq 0\} = \bigcup_{j=1}^t \Gamma_j^{(\ell)},$$

where the right-hand side is a partition into $t \geq 2$ nonempty subsets $\Gamma_j^{(\ell)}$ of the set on the left, and such that

$$\sum_{i \in \Gamma_j^{(\ell)}} d_i^{(\ell)} x_i = 0$$

for $1 \leq j \leq t$, where each such equation is nondegenerate, meaning that no proper subsum on the left is zero. So we may assume without loss of generality that Equation (11) is nondegenerate. As in the proof of the finiteness of the number of nondegenerate solutions to S -unit equation (see Schlickewei [11] for example; technically, (11) is not an S -unit equation since in addition to the elements $e^{if_i(n)}$ which belong to the multiplicative subgroup of \mathbb{C}^* generated by $\{\alpha_1, \dots, \alpha_r, \rho\}$, the elements $x_i(n)$ also involve the polynomials $Q_i(n)$ in n , but their heights are of size $n^{O(1)} = e^{o(n)}$, an amount which is negligible, so the argument goes through), we are lead to the conclusion that for each $\ell \in \{1, \dots, u\}$ there exist $i_1^{(\ell)} \neq i_2^{(\ell)}$ and a finite set of complex numbers $\mathcal{D}_{i_1^{(\ell)}, i_2^{(\ell)}}^{(\ell)}$ such that for each such n , there is some $\ell \in \{1, \dots, u\}$ with

$$\frac{x_{i_1}^{(\ell)}(n)}{x_{i_2}^{(\ell)}(n)} \in \mathcal{D}_{i_1^{(\ell)}, j_1^{(\ell)}, i_2^{(\ell)}, j_2^{(\ell)}}^{(\ell)}.$$

We omit the dependence on ℓ for the rest of this argument Hence,

$$\frac{Q_{i_1}(n)}{Q_{i_2}(n)} e^{i(f_{j_1}(n) - f_{j_2}(n))} \in \mathcal{D}_{i_1, j_1, i_2, j_2}.$$

We thus get that

$$(12) \quad e^{i(f_{j_1}(n) - f_{j_2}(n))} \in \mathcal{D}_{i_1, j_1, i_2, j_2} \left(\frac{Q_{i_2}(n)}{Q_{i_1}(n)} \right).$$

If $f_{j_1}(X) \neq f_{j_2}(X)$ then, by previous arguments, for large n the number on the left-hand side of (12) above is not a root of unity so its height is at least $e^{\kappa_2 n}$ for some positive constant κ_2 , while the height of the number on the right-hand side of (12) is $n^{O(1)}$. Thus, (8) cannot hold for large n unless $f_{j_1} = f_{j_2}$. This almost proves step (a). To complete the argument, fix some $j_1 \in \{1, \dots, L_1\}$ and apply the argument above to derive an equation like (11). If it is nondegenerate and involves j_1 (so (11) holds for infinitely

many n with some ℓ such that $d_{j_1}^{(\ell)} \neq 0$), we are done. If not, we pick some j such that $d_j^{(\ell)} \neq 0$, express $x_j(n)$ linearly from (11) as

$$x_j(n) = - \sum_{j' \neq j} \left(d_{j'}^{(\ell)} / d_j^{(\ell)} \right) x_{j'}(n),$$

and insert this into the left-hand side of (7). Again we get a linear form in the variables $x_i(n)_{1 \leq i \leq L_1, i \neq j}$ (that is, in a smaller number of variables) which involves $x_{j_1}(n)$ and which is “smaller” to which we may apply the same argument. Eventually, after finitely many steps, we get to an equation like (11) involving our chosen j_1 and some other indices with infinitely many nondegenerate solutions in n , showing that $f_{j_1} = f_{j_2}$ for some $j_2 \neq j_1$, which proves step (a).

Step (b) is immediate. Indeed, we have $f_i = i\theta_i(4X^2 + 4X)$ for $i = 1, \dots, r$ and $\theta_i \neq \theta_j$ for $i \neq j$ in $\{1, \dots, r\}$ so $f_i(X) = f_j(X)$ is impossible with distinct indices i, j both in $\{1, \dots, r\}$.

For step (c), for each $i \in \{1, \dots, r\}$, let $j_i > r$ be such that $f_i = f_{j_i}$. Matching leading coefficients in $f_i(X) = f_{j_i}(X)$ (as polynomials in X) and dividing across by 4, we get

$$\theta_i = \sum_{j \in I_i} (d_{i,j}/4)\theta_j.$$

Here, $d_{i,j}$ is the leading coefficient of $m_{i,j}(X)$. As noted above, $d_{i,j} > 0$ and

$$\sum_{j \in I_i} d_{i,j} = 4,$$

so θ_i is in the interior of the convex hull of the set $\{\theta_j \mid j \in I_i\}$. If I_i has only two elements, one of which is i itself, we deduce, from $I_i = \{i, j\}$, that $(4 - d_{i,i})\theta_i = d_{i,j}\theta_j$, which is impossible since α_i/α_j is not a root of unity. Thus, either I_i does not contain i , or it does contain i and has at least 3 elements. So, each θ_i is in the convex hull of the remaining ones (and all these numbers are in the interval $(-\pi, \pi]$). Picking i to correspond to the smallest θ_i , we get a contradiction.

A different way of seeing this last step is to think of $(\theta_1, \dots, \theta_r)$ as a solution \mathbf{x} to the linear system of equations $\mathbf{A}\mathbf{x} = \mathbf{x}$, where \mathbf{A} is the $r \times r$ matrix with entry $d_{i,j}/4$ in position (i, j) if $i \in \{1, \dots, r\}$ and $j \in I_i$, and 0 otherwise. Then \mathbf{A} is a matrix whose entries are nonnegative, has row sums equal to 1 and each row contains at least two nonzero entries. It is straightforward to see that the eigenspace corresponding to the eigenvalue 1 of such a matrix is one dimensional, and is spanned by $(1, 1, \dots, 1)^T$. Hence, $\theta_i = \theta_j$ for $i = 1, \dots, r$, which is a contradiction.

This finishes the proof of step (c) and the first proof of the main theorem.

3. A p -adic proof of the main theorem

In this section we give a different proof of a slightly stronger statement than Theorem 1, by reducing both the elliptic and the linear recurrence sequence modulo carefully chosen primes, and finding incompatible behaviours. Two remarks are in order here. First, we will need to call on results elsewhere that guarantee a sufficient supply of primes with the required properties. Second, the arithmetic argument here is one approach and there may be others.

Theorem 2. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over the rationals, let $P = (x_1/z_1^2, y_1/z_1^3) \in E(\mathbb{Q})$ be a point of infinite order, let $(z_n)_{n \geq 1}$ be an integer sequence satisfying $nP = (x_n/z_n^2, y_n/z_n^3)$, and let $(u_n)_{n \geq 1}$ be a linear recurrence sequence. Then there is an infinite set of primes p with the property that a period of $(u_{n^2})_{n \geq 1}$ modulo p cannot be a period of $(z_n)_{n \geq 1}$ modulo p . In particular, no linear recurrence sequence $(u_n)_{n \geq 1}$ has the property that $(z_n)_{n \geq 1} =_e (u_{n^2})_{n \geq 1}$.*

This approach permits some arithmetic perturbation of the sequences without affecting the conclusion. Specifically, if $(z_n)_{n \geq 1}$ is replaced by any sequence $(z_n w_n)_{n \geq 1}$ where the set of primes dividing any term of $(w_n)_{n \geq 1}$ is finite, then the same conclusion holds. This allows us, in particular, to assume that the sign of z_n is arbitrarily chosen. This means once again that the proof gives the same result for elliptic divisibility sequences defined in terms of the bi-linear recurrences (3) and (4).

3.1. Orders of points on elliptic curves. For a prime p , let $E(\mathbb{F}_p)$ be the set of solutions modulo p of the equation (1) reduced modulo p , together with the point at infinity O . Write, in the usual notation,

$$\#E(\mathbb{F}_p) = p - a_p + 1$$

for the number of \mathbb{F}_p -points on E . Then $a_p \in (-2\sqrt{p}, 2\sqrt{p})$ by Hasse's theorem, and if $p \nmid \Delta_E$, then $E(\mathbb{F}_p)$ forms a group with the group law inherited from the Mordell–Weil group law on E reduced modulo p . When p divides Δ_E , we have $a_p \in \{0, \pm 1\}$ (we refer to Silverman [14, Ch. 5] for standard results on $E(\mathbb{F}_p)$). If $p \nmid \Delta_E z_1$, then $P = (x_1/z_1^2, y_1/z_1^3)$ can be thought of as a point on $E(\mathbb{F}_p)$ which is not the identity, and from now on we make the assumption that P is a nontorsion point on $E(\mathbb{Q})$ and that $p \nmid \Delta_E z_1$. We also claim that — for our purposes — we may safely assume that $x_1 y_1 \neq 0$. To see this, notice first that $y_1 \neq 0$ (since if $y_1 = 0$ then P is of order 2 in $E(\mathbb{Q})$). If $x_1 = 0$, then after replacing P by $2P$ (which is still of infinite order) we have $x_1 \neq 0$. Furthermore, the order of $2P$ modulo p either equals the order of P modulo p , or equals half of it (depending of whether the order of P modulo p is odd or even). Thus for any odd prime q the order of $2P$ modulo p is a multiple of q if and only if the order of P modulo p is a multiple of q . Hence, for the purpose of deciding

whether the order of P modulo p is a multiple of q or not, we may replace, if we wish, P by $2P$ and so assume that $x_1y_1 \neq 0$ below.

Now let q be a fixed large prime. We will ask what can be said about the set of primes p with the property that the order of $P \in E(\mathbb{F}_p)$ is divisible by q . In order to do this, we will make use of recent work of Meleleo and Pappalardi (which may be found in the thesis of Meleleo [7]; there is also a video presentation by Pappalardi [9] of some of the results; the density statement we need may also be found in a paper of David and Wu [3]). Before doing this, we need to recall some group-theoretic properties of $E(\mathbb{F}_p)$.

Let $E[q] = \{Q \mid qQ = O\}$ denote the subgroup of q -torsion points in the curve E . As an \mathbb{F}_q -vector space, $E[q]$ can be identified with \mathbb{F}_q^2 . Adjoining the coordinates of the points $Q \in E[q]$ to \mathbb{Q} gives a Galois extension of \mathbb{Q} with Galois group isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ (we will suppress this isomorphism and simply speak of the Galois groups arising as being given by matrix or affine groups). Serre's open image theorem [13] says that there exists a positive integer $\Delta_{1,E}$ depending on E with the property that if $q \nmid \Delta_{1,E}$, then this Galois group is all of $\mathrm{GL}_2(\mathbb{F}_q)$ (We assume that $\Delta_{1,E}$ is already divisible by all the prime factors of Δ_E).

Suppose now that we want to study the density of the set of primes p such that a_p and p have prescribed values modulo q , say a and b . Then one can identify the Frobenius action of such a prime p with the equivalence class of a 2×2 matrix in $\mathrm{GL}_2(\mathbb{F}_q)$ whose trace is a modulo q and whose determinant is b modulo q . That is, for given residue classes a and $b \neq 0$ modulo q , the density

$$\lim_{x \rightarrow \infty} \frac{\#\{p \leq x \mid a_p \equiv a \pmod{q} \text{ and } p \equiv b \pmod{q}\}}{\pi(x)} = \delta_{q;a,b},$$

exists and equals

$$(13) \quad \delta_{q;a,b} = \frac{\#\{J \in \mathrm{GL}_2(\mathbb{F}_q) \mid \mathrm{tr}(J) = a, \text{ and } \det(J) = b\}}{\#\mathrm{GL}_2(\mathbb{F}_q)}$$

where we write as usual π for the prime counting function. In particular, $\delta_{q;a,b}$ is always positive since the conditions in (13) define a positive proportion of $\mathrm{GL}_2(\mathbb{F}_q)$. Assume next that we want to add the point P to the picture and see what happens to its order in $E(\mathbb{F}_p)$ modulo q .

We claim that $E_P[q] = \{R \mid qR = P\}$ is a two-dimensional affine \mathbb{F}_q vector space. To see this, pick some $R_0 \in E_P[q]$ and notice that $R \in E_P[q]$ if and only if $R - R_0 \in E[q]$, itself identified with a two-dimensional \mathbb{F}_q vector space. We also adjoin the coordinates of the points of $E_P[q]$ to \mathbb{Q} , in addition to the coordinates of the points in $E[q]$. Then, by an analogue of Serre's open mapping theorem due to Bachmakov [1] (an accessible and thorough treatment of the results outlined there may be found in a paper of Ribet [10]), there exists a constant $\Delta_{2,E,P}$ depending both on P and E such that if $q \nmid \Delta_{2,E,P}$, then the Galois group of this extension is the full group

of affine transformations of a two-dimensional affine \mathbb{F}_q -space, namely

$$\text{Aff}(E_P[q]) = \text{GL}_2(\mathbb{F}_q) \times \mathbb{F}_q^2,$$

where $\text{GL}_2(\mathbb{F}_q)$ acts on \mathbb{F}_q^2 by linear automorphisms. That is, the group law is $(\phi, u) \circ (\psi, v) = (\phi\psi, \phi(v) + u)$. We assume that $\Delta_{2,E,P}$ contains all the prime factors of $\Delta_{1,E}$ and of $x_1y_1z_1$ (as pointed out above, we may assume that $x_1y_1 \neq 0$). By [7], it follows that if q does not divide $\Delta_{2,E,P}$, then

$$\lim_{x \rightarrow \infty} \frac{\#\{p \leq x \mid a_p \equiv q \pmod{p}, p \equiv b \pmod{p}, q \mid \text{ord}_{E(\mathbb{F}_p)}(P)\}}{\pi(x)} = \delta_{q;a,b,P},$$

where

$$\delta_{q;a,b,P} = \frac{\#\{(J, u) \in \text{GL}_2(\mathbb{F}_q) \mid \text{tr}(J) = a, \det(J) = b, u \notin \text{Im}(J - I_2)\}}{\#(\text{GL}_2(\mathbb{F}_q) \times \mathbb{F}_q^2)}.$$

Note first of all that a and b have to be chosen so that $p - a_p + 1 = b - a + 1$ is a multiple of q , so in particular $b \equiv a - 1 \pmod{q}$. Now if

$$(J, u) = \left(\begin{pmatrix} a-1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right)$$

then $\text{tr}(J) = a$, $\det(J) = a - 1 = b$, and

$$u \notin \text{Im}(J - I_2) = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix}, x \in \mathbb{F}_q \right\}.$$

This shows that $\delta_{q;a,a-1,P}$ is positive. We record this conclusion as the following theorem.

Theorem 3. *Let $a \geq 2$ be an integer, E be an elliptic curve defined over \mathbb{Q} with a point of infinite order $P \in E(\mathbb{Q})$. Then there exists $\Delta = \Delta(E, P)$ such that if a fixed prime q does not divide Δ , then the set of primes $p \equiv a - 1 \pmod{q}$ with $a_p \equiv a \pmod{q}$ and $P \pmod{q}$ having order a multiple of q in $E(\mathbb{F}_p)$ has density $\delta_{q;a,a-1,P} > 0$.*

3.2. Proving Theorem 2. Let $a = 3$, let q be a fixed sufficiently large prime (large in a sense that will be made more precise later), and let $P_{q;3,2,P}$ be the set of primes p with the property in the statement of Theorem 2. Finally, let p be a large prime in $P_{q;3,2,P}$. In particular, we may assume that p does not divide the denominators, nor the norms (from \mathbb{K} to \mathbb{Q}) of the numerators of any of the polynomials $P_i(X) \in \mathbb{K}[X]$ appearing in the formula (6) for the terms of the linear recurrence sequence, and that p does not divide the last coefficient c_k of the characteristic polynomial $\Psi(X)$ either. We put

$$L = \text{lcm}\{p^j - 1 \mid 1 \leq j \leq d\}.$$

Note that since by construction $p \equiv 2 \pmod{q}$, we have $p^j - 1 \equiv 2^j - 1 \pmod{q}$ for $j = 1, \dots, k$. Thus, for large q , we have $q \nmid L$. Let T be the period modulo p of $(z_n)_{n \geq 1}$. It follows from a theorem of Silverman [16,

Th. 1]) that $T \mid 2(p - 2)\#E(\mathbb{F}_p)$. Further, since the order of P modulo p is divisible by q , it follows that

$$q \mid T \mid 2(p - 1)(p - a_p + 1).$$

To get a contradiction, we work with the sequence $(u_{n^2})_{n \geq 1}$ for large n , and show that its period modulo p is coprime to q . This will give us the contradiction.

Assume therefore that (5) holds, so in particular there is some n_0 for which

$$(14) \quad u_{(n+mT)^2} \equiv u_{n^2} \pmod{p}$$

for all $n \geq n_0$ and $m \geq 0$. Let π be a prime ideal of \mathbb{K} lying above the rational prime number p . The congruence (14) together with Binet's formula (6) give

$$(15) \quad \sum_{i=1}^s \alpha_i^{n^2} (P_i((n + mT)^2) \alpha_i^{2mnT + m^2T^2} - P_i(n^2)) \equiv 0 \pmod{\pi}.$$

Write \mathcal{S} for the set of primes dividing T together with all primes smaller than some p_0 , where p_0 is a sufficiently large number to be determined later. Let N be the largest divisor of L composed only of primes from \mathcal{S} . Suppose that $m = pN\ell$ for some integer $\ell \geq 0$ in (15) and use the fact that

$$P_i((n + pN\ell)^2) \equiv P_i(n^2) \pmod{\pi},$$

to deduce that

$$(16) \quad \sum_{i=1}^s \alpha_i^{n^2} P_i(n^2) (\beta_i^{2\ell n + pNT\ell^2} - 1) \equiv 0 \pmod{\pi}$$

where $\beta_i := \alpha_i^{pNT}$ for $1 \leq i \leq s$. Once again we postpone the lengthy proof of the next lemma to the appendix.

Lemma 4. *If p_0 is sufficiently large, then the congruence (16) implies that*

$$\beta_i \equiv 1 \pmod{\pi}$$

for $i = 1, \dots, s$.

Thus $\alpha_i^{pTN} \equiv 1 \pmod{\pi}$ for any prime ideal π of the ring of integers $\mathcal{O}_{\mathbb{K}}$ lying above the prime p . However, the order of α_i modulo π divides L , and L is neither a multiple of q , nor of p . Also, by construction, p divides neither L nor $p - a_p + 1$. So, writing b_q for the exponent of q in T , we get that $\alpha_i^{NT/q^{b_q}} \equiv 1 \pmod{\pi}$. Since p is large (and in particular, p does not divide the discriminant of \mathbb{K}), we conclude that p splits in distinct prime ideals π in $\mathcal{O}_{\mathbb{K}}$. The above argument then shows that $\alpha_i^{NT/q^{b_q}} \equiv 1 \pmod{p}$ for all $i = 1, \dots, r$. By the Binet formula (6), this means that pNT/q^{b_q} is a period of $(u_{n^2})_{n \geq 1}$ modulo p . By the assumption (5), it follows that pNT/q^{b_q} is also a period of $(z_n)_{n \geq 1}$. Hence, $T \mid pNT/q^{b_q}$, which is not possible by the definition of b_q . This contradiction completes the p -adic proof.

Appendix

We assemble here some of the calculations used earlier. Write

$$P(X) = a_0X^d + a_1X^{d-1} + a_2X^{d-3} + \dots + a_d.$$

For some nonzero number α consider the polynomial

$$(17) \quad Q(X) := P((2X + 1)^2) - \alpha^3 (P((X + 2)^2)P(X^2)^3 - P((X - 1)^2)P((X + 1)^2)^3).$$

Lemma 5. *If $d = 0$ then $Q(X)$ is the constant a_0 , and if $d > 0$ then*

$$Q(X) = -4da_0^4\alpha^3X^{8d-3} + \text{monomials of lower order in } X.$$

Proof of Lemma 5. If $d = 0$, then $Q(X) = a_0 - \alpha^3(a_0a_0^3 - a_0a_0^3) = a_0$ is constant. Thus we may assume that $d > 0$. Computer experiments with Mathematica for $d = 1, 2, 3$ suggest that the degree of the polynomial

$$(18) \quad P((X + 2)^2)P(X^2)^3 - P((X - 1)^2)P((X + 1)^2)^3$$

is $8d - 3$, and the leading coefficient is $4da_0^4$, motivating the statement of the lemma. To verify this, we compute the first three coefficients of $P((X + i)^2)$ for $i = -1, 0, 1, 2$, factor X^{8d} in the expression (18), change variables using the substitution $y = 1/X$ inside the parentheses, and compute the order of the resulting expression in y . For example,

$$\begin{aligned} P((X + 2)^2) &= a_0(X + 2)^{2d} + a_1(X + 2)^{2d-2} + \dots \\ &= a_0X^{2d} + 4da_0X^{2d-1} + \underbrace{\left(4\binom{2d}{2}a_0 + a_1 \right)}_{\Sigma_1} X^{2d-2} \\ &\quad + \underbrace{\left(8\binom{2d}{3}a_0 + 2(2d-2)a_1 \right)}_{\Sigma_2} X^{2d-3} + \dots \\ P(X^2) &= a_0X^{2d} + a_1X^{2d-2} + \dots \\ P((X - 1)^2) &= a_0(X - 1)^{2d} + a_1(X - 1)^{2d-2} + \dots \\ &= a_0X^{2d} - 2da_0X^{2d-1} + \underbrace{\left(\binom{2d}{2}a_0 + a_1 \right)}_{\Sigma_3} X^{2d-2} \\ &\quad + \left(-\binom{2d}{3}a_0 - (2d-2)a_1 \right) X^{2d-3} + \dots \\ P((X + 1)^2) &= a_0X^{2d} + 2da_0X^{2d-1} + \left(\binom{2d}{2}a_0 + a_1 \right) X^{2d-2} \\ &\quad + \underbrace{\left(\binom{2d}{3}a_0 + (2d-2)a_1 \right)}_{\Sigma_4} X^{2d-3} + \dots \end{aligned}$$

So, putting $y = 1/X$, it remains to notice that

$$\begin{aligned} & (a_0 + 4da_0y + \Sigma_1y^2 + \Sigma_2y^3) \times (a_0 + a_1y^2)^3 \\ & \quad - (a_0 - 2da_0y + \Sigma_3y^2 - \Sigma_4y^3) \times (a_0 + 2da_0y + \Sigma_3y^2 + \Sigma_4y^3)^3 \\ & = (4d)a_0^4y^3 + \text{higher powers of } y, \end{aligned}$$

as required. □

Proof of Lemma 4. Assume for the time being that this congruence does not hold. Up to relabeling the roots $\alpha_1, \dots, \alpha_s$, we may assume that there exist $s_1 < s$ and indices $0 < i_1 < \dots < i_t = s - s_1$ such that

$$\beta_1 \equiv \dots \equiv \beta_{s_1} \equiv 1 \pmod{\pi}$$

and

$$(19) \quad \begin{cases} \beta_{s_1+1} \equiv \dots \equiv \beta_{s_1+i_1} \equiv \gamma_1 \pmod{\pi} \\ \vdots \\ \beta_{s_1+i_{t-1}+1} \equiv \dots \equiv \beta_{s_1+i_t} \equiv \gamma_t \pmod{\pi} \end{cases}$$

where $\gamma_i \not\equiv 1 \pmod{\pi}$ for $i \in \{1, \dots, t\}$ and $\gamma_i \not\equiv \gamma_j \pmod{\pi}$ for distinct i and j in $\{1, \dots, t\}$. Relation (16) becomes

$$(20) \quad \sum_{j=1}^t Q_j(n) (\beta_j^{2\ell n + pNT\ell^2} - 1) \equiv 0 \pmod{\pi}$$

where

$$Q_j(n) = \sum_{i=s_1+i_{j-1}+1}^{s_1+i_j} \alpha_i^{n^2} P_i(n^2)$$

for $j = 1, \dots, t$, with the convention that $i_0 := 0$. Notice that

$$(21) \quad \beta_1, \dots, \beta_t \text{ are distinct modulo } \pi \text{ and none is congruent to } 1$$

by (19). Write

$$\frac{L}{N} := \prod_{r|L/N} r^{a_r}$$

for the prime decomposition of $\frac{L}{N}$. For each prime r dividing $\frac{L}{N}$, choose n_0 with the property

$$\left(\frac{n_0^2 + jpNT}{r} \right) = 1$$

for all $j = 1, \dots, t$. To see that such an n_0 exists, note that for a fixed prime r , the number of possible residue classes for such an n_0 is

$$I_r = \sum_{0 \leq n \leq r-1} \prod_{1 \leq j \leq t} \frac{1}{2} \left(\left(\frac{n^2 + jpN}{r} \right) + 1 \right) + O(1).$$

The $O(1)$ term depends on t and comes from those $n \in \{0, \dots, r - 1\}$ for which $n^2 + jpN \equiv 0 \pmod{r}$. To estimate I_r , expand the inner product,

separate the main term and change the order of summation for the remainder to deduce that

$$2^t I_r = r + \sum_{\substack{J \subset \{1, \dots, t\} \\ J \neq \emptyset}} \sum_{0 \leq n \leq p-1} \left(\frac{\prod_{j \in J} (n^2 + jpN)}{r} \right) + O(1) = r + O(\sqrt{r} + 1),$$

where the implied constant in the O term depends on t . For the above estimate, we use Weil’s bound with the observation that if r does not divide pNT and is larger than t , then the polynomial

$$\prod_{J \subset \{1, \dots, t\}} (x^2 + jpNT)$$

has only simple roots modulo r . This shows that $I_r > 0$ for all r sufficiently large. So, we choose the prime p_0 such that $I_r > 0$ for all $r > p_0$. For each such fixed r , fix n_0 modulo r such that $n_0^2 + jpN$ is a square modulo r and extend it to r^{a_r} in some way. We also choose n_0 modulo p such that $P_i(n_0) \not\equiv 0 \pmod{p}$ for all $i = 1, \dots, s$. This is certainly possible if $p > \sum_{i=1}^s \deg(P_i(X))$. So far, n_0 has been fixed only modulo pL/N , and we continue to denote by n_0 the smallest possible positive value of such a number in the arithmetic progression of common difference pL/N .

We claim that there are positive integers x_{s_1}, \dots, x_s such that

$$(22) \quad \det \begin{pmatrix} (n_0 + pL/Nx_{s_1+i_{j-1}+1})^2 & \cdots & (n_0 + pL/Nx_{s_1+i_{j-1}+1})^2 \\ \alpha_{s_1+i_{j-1}+1} & \cdots & \alpha_{s_1+i_j} \\ (n_0 + pL/Nx_{s_1+i_{j-1}+2})^2 & \cdots & (n_0 + pL/Nx_{s_1+i_{j-1}+2})^2 \\ \alpha_{s_1+i_{j-1}+1} & \cdots & \alpha_{s_1+i_j} \\ \cdots & \cdots & \cdots \\ (n_0 + pL/Nx_{s_1+i_j})^2 & \cdots & (n_0 + pL/Nx_{s_1+i_j})^2 \\ \alpha_{s_1+i_{j-1}+1} & \cdots & \alpha_{s_1+i_j} \end{pmatrix} \neq 0$$

for $j = 1, \dots, t$, and will prove this by an induction argument as follows.

- The statement is clear if $i_j - i_{j-1} = 1$.
- If $i_j - i_{j-1} = 2$ then the statement holds because the ratio

$$\alpha_{s_1+i_j+2} / \alpha_{s_1+i_{j-1}+1}$$

is not a root of unity by the nondegeneracy of the linear recurrence sequence.

- For larger values of $i_j - i_{j-1}$ the claim follows by induction, by first choosing $x_{s_1+i_{j-1}+1}, \dots, x_{s_1+i_{j-1}}$ with the property that the minor of size $(i_j - i_{j-1} - 1) \times (i_j - i_{j-1} - 1)$ from the upper left corner is nonzero, expanding the above determinant over the last row treating $x_{s_1+i_j}$ as an indeterminate, and using the fact that the vanishing of the resulting determinant leads to an S -unit equation in this last variable which can have only finitely many solutions $x_{s_1+i_j}$.

Assuming now that x_1, \dots, x_{s-s_1} are fixed positive integers satisfying (22) for all $j = 1, \dots, t$, assume that p is larger than the norm with respect to the extension $\mathbb{K} \supseteq \mathbb{Q}$ of each of the determinants (22) for $j = 1, \dots, t$. Giving n

the values $n_0 + pL/Nx_1, \dots, n_0 + pL/Nx_{s-s_1}$ in turn and assuming that for some $j \in \{1, \dots, t\}$, we have that $Q_j(n_0 + pL/Nx_i) \equiv 0 \pmod{\pi}$ for all $i \in \{s_1 + i_{j-1} + 1, \dots, s_1 + i_j\}$, we get the system

$$(23) \quad \sum_{i=s_1+i_{j-1}+1}^{s_1+i_j} \alpha_i^{(n_0+pL/Nx_u)^2} P_i(n_0^2) \equiv 0 \pmod{\pi}$$

for $u = s_1 + i_{j-1} + 1, \dots, s_1 + i_j$. Write $\mathbb{F}_q = \mathbb{K}[X]/\pi$ for the residue field. The relation (23) says that the nonzero vector $(P_i(n_0^2))_{s_1+i_{j-1}-1 \leq i \leq s_1+i_j}^T$ in $(\mathbb{F}_q)^{i_j-i_{j-1}}$ is a solution to a homogeneous system of equations whose determinant (22) is nonzero modulo π , which is a contradiction. It follows that there exists n_0 in the appropriate residue class modulo pL/N such that $Q_j(n_0)$ is nonzero modulo π for all $j = 1, \dots, t$.

For each $j = 1, \dots, t$ and for each r dividing $\frac{L}{N}$ we can choose $\ell_j \pmod{r}$ such that

$$2\ell_j n_0 + pNT\ell_j^2 \equiv j \pmod{r}.$$

The claimed choice of $\ell_j \pmod{r}$ of the above congruences is formally given by

$$\ell_j \equiv \frac{1}{pNT}(-n_0 + \sqrt{n_0^2 + jpNT}) \pmod{r},$$

which exists since by construction r does not divide pNT and $n_0^2 + jpNT$ is a quadratic residue modulo r and the square root symbol denotes any choice of square root. By Hensel's lifting lemma (see [2, Sec. 4.3]), we can extend this solution ℓ_j defined modulo r to a solution also written ℓ_j defined modulo r^{ar} , and then by the Chinese Remainder theorem to a solution again written ℓ_j modulo $\frac{L}{N}$. This finally gives a choice of ℓ_j satisfying

$$2\ell_j n_0 + pNT\ell_j^2 \equiv j \pmod{L/N}.$$

Thus

$$\beta_u^{2\ell_j n_0 + pNT\ell_j^2} = (\alpha_u^{pNT})^{j+\lambda_j L/N} = \alpha_u^{pNTj} \alpha_u^{pTL}$$

and so

$$\beta_u^{2\ell_j n_0 + pNT\ell_j^2} \equiv \alpha_u^{pNTj} \equiv \beta_u^j \pmod{\pi}$$

because L is a multiple of the order of α_u modulo π , and the above congruences hold for all $u = 1, \dots, t$. This means that we can write (20) as

$$\sum_{j=1}^t Q_j(n_0)(\beta_j^u - 1) \equiv 0 \pmod{\pi}$$

for all $u = 1, \dots, t$, and $\mathbf{Q} = (Q_j(n_0))_{1 \leq j \leq t}^T$ is not the zero vector in \mathbb{F}_q^t . It follows that

$$\det \begin{vmatrix} \beta_1 - 1 & \beta_2 - 1 & \dots & \beta_t - 1 \\ \beta_1^2 - 1 & \beta_2^2 - 1 & \dots & \beta_t^2 - 1 \\ \dots & \dots & \dots & \dots \\ \beta_1^t - 1 & \beta_2^t - 1 & \dots & \beta_t^t - 1 \end{vmatrix}$$

is divisible by π . Up to a choice of sign, the above determinant is

$$\prod_{i=1}^t (\beta_i - 1) \prod_{1 \leq i < j \leq t} (\beta_i - \beta_j).$$

Thus either $\beta_i \equiv 1 \pmod{\pi}$ for some $i = 1, \dots, t$, or $\beta_i \equiv \beta_j \pmod{\pi}$ for some $1 \leq i < j \leq t$, and neither possibility is compatible with (19). This contradiction proves the lemma. \square

Acknowledgements

We are grateful to both Joe Silverman and an anonymous referee for many suggestions that have improved the exposition, several of which were quite substantial. One of these — not implemented here — is that there may be an almost entirely geometric argument that gives the main result, associating the linear recurrence sequence to a multiplicative group and showing that the relation (5) then forces the elliptic curve to have impossible reduction properties. This paper started during a visit of F. L. to the Max Planck Institute in Fall, 2013 and ended during a conference at CIRM Luminy celebrating the 60th birthday of Professor Igor Shparlinski in April 2016. This author thanks the Max Planck Institute for hospitality and support, Professors Pieter Moree, Francesco Pappalardi and Igor Shparlinski for useful conversations and the organizers of the CIRM event for their invitation.

References

- [1] BACHMAKOV, MARC. Un théorème de finitude sur la cohomologie des courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B* **270** (1970), A999–A1001. MR0269653, Zbl 0194.52303.
- [2] CASSELS, J. W. S. Local fields. London Mathematical Society Student Texts, 3. *Cambridge University Press, Cambridge*, 1986. xiv+360 pp. ISBN: 0-521-30484-9; 0-521-31525-5. MR861410, Zbl 0595.12006, doi: 10.1017/CBO9781139171885.
- [3] DAVID, C.; WU, J. Pseudoprime reductions of elliptic curves. *Canad. J. Math.* **64** (2012), no. 1, 81–101. MR2932170, Zbl 1271.11090, arXiv:1005.3871, doi: 10.4153/CJM-2011-044-x.
- [4] EVEREST, GRAHAM; VAN DER POORTEN, ALF; SHPARLINSKI, IGOR; WARD, THOMAS. Recurrence sequences. Mathematical Surveys and Monographs, 104. *American Mathematical Society, Providence, RI*, 2003. xiv+318 pp. ISBN: 0-8218-3387-1. MR1990179, Zbl 1033.11006, doi: 10.1090/surv/104.
- [5] EVERTSE, JAN-HENDRIK. On sums of S -units and linear recurrences. *Compositio Math.* **53** (1984), no. 2, 225–244. MR0766298, Zbl 0547.10008.
- [6] FATOU, P. Séries trigonométriques et séries de Taylor. *Acta Math.* **30** (1906), no. 1, 335–400. MR1555035, JFM 37.0283.01, doi: 10.1007/BF02418579.
- [7] MELELEO, GIULIO. Questions related to primitive points on elliptic curves and statistics for biquadratic curves over finite fields. Ph.D. thesis, Università degli Studi “Roma Tre”, 2015. http://www.matfis.uniroma3.it/dottorato/TESI/meleleo/2015_04_30-Tesi_Meleleo.pdf.
- [8] MOSS, P. B. The arithmetic of realizable sequences. Ph.D. thesis, Univ. East Anglia, 2003. <https://www.math.stonybrook.edu/theses/thesis03-5/part1.pdf>.

- [9] PAPPALARDI, F. Local conditions for the primitive Lang–Trotter conjecture. *Analytic Theory of Automorphic Forms*, The Institute of Mathematical Sciences Conference videos, 2013. http://ekalavya.imsc.res.in/conference_videos.
- [10] RIBET, KENNETH A. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.* **46** (1979), no. 4, 745–761. MR552524, Zbl 0428.14018, doi: 10.1215/S0012-7094-79-04638-6.
- [11] SCHLICKWEI, HANS PETER. S -unit equations over number fields. *Invent. Math.* **102** (1990), no. 1, 95–107. MR1069241, Zbl 0711.11017, doi: 10.1007/BF01233421.
- [12] SCHMIDT, WOLFGANG M. Norm form equations. *Ann. of Math. (2)* **96** (1972), 526–551. MR0314761, Zbl 0226.10024, doi: 10.2307/1970824.
- [13] SERRE, JEAN-PIERRE. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283, Zbl 0235.14012, doi: 10.1007/BF01405086.
- [14] SILVERMAN, JOSEPH H. The arithmetic of elliptic curves. *Graduate Texts in Mathematics*, 106. Springer-Verlag, New York, 1986. ISBN: 0-387-96203-4. MR0817210, Zbl 0585.14026, doi: 10.1007/978-1-4757-1920-8.
- [15] SILVERMAN, JOSEPH H. Wieferich’s criterion and the abc -conjecture. *J. Number Theory* **30** (1988), no. 2, 226–237. MR0961918, Zbl 0654.10019, doi: 10.1016/0022-314X(88)90019-4.
- [16] SILVERMAN, JOSEPH H. p -adic properties of division polynomials and elliptic divisibility sequences. *Math. Ann.* **332** (2005), no. 2, 443–471. MR2178070, Zbl 1066.11024, arXiv:math/0404412, doi: 10.1007/s00208-004-0608-0.
- [17] SILVERMAN, JOSEPH H.; STEPHENS, NELSON. The sign of an elliptic divisibility sequence. *J. Ramanujan Math. Soc.* **21** (2006), no. 1, 1–17. MR2226354, Zbl 1148.11013, arXiv:math/0402415.
- [18] VAN DER POORTEN, A. J.; SCHLICKWEI, H. P. Additive relations in fields. *J. Austral. Math. Soc. Ser. A* **51** (1991), no. 1, 154–170. MR1119694, Zbl 0747.11017, doi: 10.1017/S144678870003336X.

(F. Luca) SCHOOL OF MATHEMATICS, UNIVERSITY OF THE WITWATERSRAND, PRIVATE BAG 3, WITS 2050, SOUTH AFRICA
Florian.Luca@wits.ac.za

(T. Ward) ZIFF BUILDING, UNIVERSITY OF LEEDS, LEEDS LS2 9JT, UK
t.b.ward@leeds.ac.uk

This paper is available via <http://nyjm.albany.edu/j/2016/22-58.html>.