An elliptic divisibility sequence is not a sampled linearly recurrent sequence

Florian Luca

April 23, 2018

The result

Let E be an elliptic curve defined over $\mathbb{Q}$. Assume that E given by an equation of the form

$$y^2 = x^3 + Ax + B \qquad \text{with} \qquad A, B \in \mathbb{Z}, \tag{1}$$

where $\Delta_E = 4A^3 + 27B^2 \neq 0$.

Let

$$P = (x_1/z_1^2, y_1/z_1^3)$$

be rational point of infinite order on the curve E, where x_1, y_1, z_1 are coprime integers. We write

$$nP = (x_n/z_n^2, y_n/z_n^3) \quad \text{for all} \quad n \geq 1.$$

It is known that

$$\log z_n = (c + o(1))n^2 \quad \text{holds as} \quad n \to \infty,$$

with some appropriate constant $c > 0$.

Thus, we ask whether $\{z_n\}_{n\geq 1}$ can be modeled, up to finitely many terms, by $\{u_{n^2}\}_{n\geq 1}$, where $\{u_n\}_{n\geq 1}$ is a linear recurrent sequence of some order $k \geq 1$. We show that this is not the case.

Theorem

There do not exist $k \geq 1$ and a linearly recurrent sequence $\{u_n\}_{n\geq 1}$ of order k such that the formula

$$z_n = u_{n^2} \tag{2}$$

holds for all positive integers n with finitely many exceptions.

We shall give two proofs of Theorem 1, a complex one and a p-adic one. We start with the complex one.

The complex proof

We consider the relation

$$z_n = u_{n^2}$$

for all but finitely many n. Assume that $\{u_n\}_{n\geq 1}$ satisfies the linear recurrence of order $k \geq 1$

$$u_{n+k} = c_1 u_{n+k-1} + \cdots + c_k u_n \qquad (n \geq 1)$$

of characteristic equation

$$\Psi(x) = x^k - c_1 x^{k-1} - \cdots - c_k = \prod_{i=1}^{s} (x - \alpha_i)^{\sigma_i}$$

where $\alpha_1, \ldots, \alpha_s$ are distinct roots of multiplicity $\sigma_1, \ldots, \sigma_s$, respectively. By a result of Silverman, we may assume that $k \geq 2$, otherwise $\{u_n\}_{n\geq 1}$ is either constant or a geometric progression, so the largest prime factor of z_n remains bounded, which is not possible by Silverman's result.

Then

$$u_n = \sum_{i=1}^{s} P_i(n)\alpha_i^n, \tag{3}$$

where

$$P_i(X) \in \mathbb{Q}(\alpha_1, \ldots, \alpha_s)[X]$$

are polynomials of degree at most σ_i for $i = 1, \ldots, s$. Assuming that k is the minimal positive integer such that $\{u_n\}_{n\geq 1}$ is linearly recurrent of order k, we may in fact assume that $P_i(X)$ are of degree exactly σ_i for $i = 1, \ldots, s$. Furthermore, assume that α_i/α_j is a root of unity for some $i \neq j \in \{1, \ldots, s\}$. Let M be a positive integer such that if α_i^M/α_j^M is a root of unity for some $i \neq j$ in $\{1, \ldots, s\}$, then this root of unity is 1. That is, we can take M to be the least common multiple of all the roots of the roots of unity among the members of the set $\{\alpha_i/\alpha_j : i, j \in \{1, \ldots, s\}\}$. In fact, for reasons that will become clear later, we make the following assumption:

Assumption: *Let M be a positive integer with the following property: If $m_1, \ldots, m_k$ are any integers such that*

$$\prod_{i=1}^{s} \alpha_i^{m_i} = \zeta$$

is a root of unity, then $\zeta^M = 1$.

This is possible because the group of roots of unity inside the number field $\mathbb{K} = \mathbb{Q}[\alpha_1, \ldots, \alpha_s]$ is cyclic of some order L, so we can take $M = L$. Then $v_n = u_{M^2 n}$ is also a linearly recurrent sequence of order smaller than k, and the relation (1) implies that the relation

$$z_{Mn} = v_n$$

holds for all but finitely many positive integers n, and this is the same equation as (1) with the point P replaced by the point MP.

So, we may assume that $\{u_n\}_{n\geq 1}$ has the property that no multiplicative combination among the α_i's is a a root of unity different from 1. In particular, α_i/α_j is not a root of unity for any $1 \leq i < j \leq s$. Linear recurrences $\{u_n\}_{n\geq 1}$ with the above property are said to be *nondegenerate*.

An exponential polynomial with infinitely many zeros

Let

$$\rho = \max\{|\alpha_i| : 1 \leq i \leq s\}$$

and relabel the distinct roots of $\Psi(x)$ such that

$$\alpha_1, \ldots, \alpha_r \quad \text{have absolute value equal to} \quad \rho$$

and

$$\alpha_{r+1}, \ldots, \alpha_s \quad \text{have absolute value} \leq \rho^{1-\delta} \quad (\delta > 0).$$

Write

$$\alpha_j = \rho e^{\mathbf{i}\theta_j} \quad \text{for} \quad j = 1, \ldots, r \quad (\text{here} \quad \mathbf{i} = \sqrt{-1}),$$

and

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

where

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

Since

$$z_n = \Psi_n(P),$$

where

$$\Psi_n(X) \in \mathbb{Z}[X] \quad \text{is the} \quad n\text{th} \quad \textit{Division Polynomial},$$

it satisfies the recurrence

$$z_{2n+1} = z_{n+2}z_n^3 - z_{n-1}z_{n+1}^3 \quad \text{for all} \quad n \geq 1.$$

Using (1), we get that if $n \geq n_0$, then

$$\sum_{i=1}^{r} P_i((2n+1)^2)\alpha_i^{(2n+1)^2} = \left(\sum_{i=1}^{r} P_i((n+2)^2)\alpha_i^{(n+2)^2}\right)$$
$$\times \quad \left(\sum_{i=1}^{r} P_i(n^2)\alpha_i^{n^2}\right)^3 - \left(\sum_{i=1}^{r} P_i((n-1)^2)\alpha_i^{(n-1)^2}\right)$$
$$\times \quad \left(\sum_{i=1}^{r} P_i((n+1)^2)\alpha_i^{(n+1)^2}\right)^3 + O\left(n^{8D}\rho^{4(1-\delta/2)n^2}\right). \qquad (4)$$

So, it remains to study the above equation (4). Putting the main terms in one side and the expression inside O in the other side and dividing by ρ^{4n^2+4n}, we get a formula of the type

$$\sum_{i=1}^{L} x_i = O(\rho^{-\delta n^2}), \quad \text{for} \quad i = 1, \ldots, L, \tag{5}$$

where

$$x_i = x_i(n) = Q_i(n)\, e^{\mathbf{i} \sum_{j \in I_i} m_j(n)\theta_j},$$

where we have

$$I_i \subseteq \{1, \ldots, r\},$$

and for each $i \in \{1, \ldots, L\}$ and each $m_j \in I_i$,

$$m_j(n) \quad \text{is some polynomial of degree at most} \quad 2 \quad \text{in} \quad n.$$

In fact, I_i has cardinality at most 4 as a subset of $\{1, \ldots, s\}$ for each $i \in \{1, \ldots, L\}$.

To group like terms, let

$$f_i(X) = \sum_{j \in I_i} m_j(X)\theta_j \in \mathbb{C}[x] \qquad i \in \{1, \ldots, L\},$$

and assume that $\{g_1(X), \ldots, q_t(X)\}$ are distinct representatives of all the classes of equivalence of the polynomials from the set $\{f_1(X), \ldots, f_L(X)\}$ modulo the equivalence relation

$$f_i(X) \equiv_\pi f_j(X) \quad \text{if and only if} \quad \frac{1}{\pi}(f_i(X) - f_j(X)) \in \mathbb{Q}[x].$$

Note that

$$f_i(X) \equiv_\pi f_j(X)$$

implies that

$$e^{\mathbf{i}(f_i(n) - f_j(n))} \quad \text{is monomial in} \quad \alpha_1, \ldots, \alpha_r \quad \text{and a root of unity;}$$

hence, it is 1 by our convention.

Thus, $t = L$; that is $f_i(X)$ are mutually inequivalent modulo the relation $\equiv_\pi$ for $i \in \{1, \ldots, L\}$.

Then the left–hand side of (5) is of the form

$$\sum_{(i,j)\in\mathcal{D}} c_{i,j} n^i e^{f_j(n)} := \sum_{(i,j)\in\mathcal{D}} c_{i,j} y_{i,j}(n), \tag{6}$$

where

$$\mathcal{D} \quad \text{is some subset of} \quad \{0, \ldots, D\} \times \{1, \ldots, L\}.$$

Here, $y_{i,j}(n) := n^i e^{f_j(n)}$, and $\mathcal{D}$ is the subset of all pairs (i, j) with $0 \le i \le D,\ 1 \le j \le L$, such that $c_{i,j} \neq 0$.

Assume that the expression given by expression (6) is not the 0 function of n. Then the expression on the left–hand side of (5) is not constant zero either. Then $L \geq 1$. Further, the height of the vector

$$\mathbf{y}(n) := (y_{i,j}(n))_{(i,j)\in\mathcal{D}}$$

satisfies $H(\mathbf{y}) \geq \rho^{cn}$ for some appropriate positive constant c. It is then an immediate consequence of the Subspace Theorem that all the solutions $\mathbf{y}(n) = (y_{i,j}(n))_{i,j\in\mathcal{D}}$ to inequality

$$\sum_{i,j\in\mathcal{D}} c_{i,j}y_{i,j}(n) = O\left(H(\mathbf{y})^{-2\delta/c}\right)$$

live in finitely many subspaces of $\overline{\mathbb{Q}}^{\#\mathcal{D}}$. That is, there exist finitely many nonzero vectors, say $\mathbf{d} \in \{\mathbf{d}^{(1)}, \ldots, \mathbf{d}^{(u)}\} \subset \overline{\mathbb{Q}}^{\#\mathcal{D}}$ with the property that by denoting $\mathbf{d}^{(k)} = (d_{i,j}^{(k)})_{(i,j)\in\mathcal{D}}$ we must have that for each n, there exists $k \in \{1, \ldots, u\}$ such that

$$\sum_{(i,j)\in\mathcal{D}} d_{i,j}^{(k)} c_{i,j} n^i e^{\mathbf{i}f_j(n)} = 0.$$

As in the proof of the finiteness of the number of non-degenerate solutions to $\mathcal{S}$-unit equation, this leads to the conclusion that for each such n there exist $(i_1, j_1) \neq (i_2, j_2)$ and a finite set of complex numbers $\mathcal{D}_{i_1,j_1,i_2,j_2}$ such that

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

Hence,

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

If $i_1 \neq i_2$, we get right away that n can have only finitely many values. If $i_1 = i_2$ but $j_1 \neq j_2$, then since $f_{j_1}(X)$ and $f_{j_2}(X)$ are not equivalent under the relation $\equiv_R$, then we get again that n can have only finitely many values as well.

To summarize, the only possibility is that (4) holds identically for all n without the O term.
Next, we look at the term involving only one of the α_i from (4) for some $i \in \{1, \ldots, r\}$.
Then we get that, by comparing left and right–hand sides in (4), with

$$\alpha = \alpha_i \quad \text{and} \quad P(X) = P_i(X) \quad \text{(so, ignoring the index)},$$

this term is

$$\begin{aligned} P((2n+1)^2)\alpha^{(2n+1)^2} \quad & - \quad P((n+2)^2)\alpha^{(n+2)^2}\left((P(n^2)\alpha^{n^2}\right)^3 \\ & + \quad P((n-1)^2\alpha^{(n-1)^2}\left(P((n+1)^2)\alpha^{(n+1)^2}\right)^3. \end{aligned}$$

Separating α^{4n^2+4n+1}, we get that its coefficient is the polynomial

$$Q(x) := P((2x+1)^2) - \alpha^3\left(P((x+2)^2)P(x^2)^3 - P((x-1)^2)P((x+1)^2 \right. \tag{7}$$

evaluated in n.

Write

$$P(x) = a_0 X^d + a_1 X^{d-1} + a_2 X^{d-3} + \cdots + a_d.$$

If $d = 0$, then $Q(x) = a_0$ is constant.

Assume now that $d > 0$. Computer experiments with Mathematica for $d = 1, 2, 3$ seemed to indicate the degree of the polynomial

$$P((x+2)^2)P(x^2)^3 - P((x-1)^2)P((x+1)^2)^3 \qquad (8)$$

is $8d - 3$ with leading coefficient $4da_0^4$.

To confirm this, we compute the first three coefficients of $P((X+i)^2)$ for $i = -1, 0, 1, 2$, factor X^{8d} in the expression (8), inside the parentheses make the change of variables $y = 1/X$ and compute the order of the resulting expression in y.

For example,

$$\begin{aligned}
P((X+2)^2) &= a_0(X+2)^{2d} + a_1(X+2)^{2d-2} + \cdots \\
&= a_0X^{2d} + 4da_0X^{2d-1} + \left(4\binom{2d}{2}a_0 + a_1\right)X^{2d-2} \\
&+ \left(8\binom{2d}{3}a_0 + 2(2d-2)a_1\right)X^{2d-3} + \cdots \\
P(X^2) &= a_0X^{2d} + a_1X^{2d-2} + \cdots \\
P((X-1)^2) &= a_0(X-1)^{2d} + a_1(X-1)^{2d-2} + \cdots \\
&= a_0X^{2d} - 2da_0X^{2d-1} + \left(\binom{2d}{2}a_0 + a_1\right)X^{2d-2} \\
&+ \left(-\binom{2d}{3}a_0 - (2d-2)a_1\right)X^{2d-3} + \cdots \\
P((X+1)^2) &= a_0X^{2d} + 2da_0X^{2d-1} + \left(\binom{2d}{2}a_0 + a_1\right)X^{2d-2} \\
&+ \left(\binom{2d}{3}a_0 + (2d-2)a_1\right)X^{2d-3} + \cdots
\end{aligned}$$

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

$$
\begin{aligned}
& \left(a_0 + 4da_0 y + \left(4\binom{2d}{2}a_0 + a_1\right) y^2\right. \\
+ & \left.\left(8\binom{2d}{3}a_0 + 2(2d-2)a_1\right) y^3\right) \times \left(a_0 + a_1 y^2\right)^3 \\
- & \left(a_0 - 2da_0 y + \left(\binom{2d}{2}a_0 + a_1\right) y^2\right. \\
+ & \left.\left(-\binom{2d}{3}a_0 - (2d-2)a_1\right) y^3\right) \times (a_0 + 2da_0 y \\
+ & \left(\binom{2d}{2}a_0 + a_1\right) y^2 + \left(\left(\binom{2d}{3}a_0 + (2d-2)a_1\right) y^3\right)^3 \\
= & (4d)a^4 y^3 + \text{higher powers of} \quad y,
\end{aligned}
$$

which is what we wanted. This shows that

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

This shows that putting everything on the left–hand side in (4), we get a sum of terms containing the sub-sum

$$\rho^{4n^2+4n}\left(\sum_{i=1}^{r} Q_i(n)e^{\mathbf{i}(4n^2+4n)\theta_i}\right),$$

where $Q_i(X)$ has degree $\min\{0, 8\deg(P_i) - 3\}$ for $i = 1, \ldots, r$.

If $r = 1$, we get that this sub-sum coincides with the entire sum and it cannot be constant 0. Thus, $r \geq 2$. Further, separating for each $i \in \{1, \ldots, r\}$ the monomials with non-zero coefficients in $Q_i(X)$, we see that no monomial of the form

$$c_{i,j}n^j e^{\mathbf{i}(4n^2+4n)\theta_i} \qquad i \in \{1, \ldots, r\}, \qquad j \in \{0, \ldots, \deg(Q_i(X))\}$$

can be cancelled by any other such monomial corresponding to some pair of indices $(i_1, j_1) \neq (i, j)$.

So, considering just the leading monomials for each $i \in \{1, \ldots, r\}$ (namely the monomials corresponding to $j = \deg(Q_i(X))$ for each $i \in \{1, \ldots, r\}$), the only possibility is that for all $i \in \{1, \ldots, r\}$, this corresponding monomial is matched with some non diagonal monomial (i.e., monomial involving at least two of the α_i's) arising from expanding the right–hand side of (4). That is, for each $i \in \{1, \ldots, s\}$, there exists $I_i \subseteq \{1, \ldots, r\}$ or cardinality at least two such that for each $j \in I_i$ there are fixed pairs (c_j, d_j) of integers with $c_j > 0$,

$$\sum_{j \in I_i} c_j = 4, \qquad \sum_{j \in I_i} d_j = 4$$

and

$$e^{\mathbf{i}(4n^2+4n)\theta_i} = \prod_{j \in I_i} e^{\mathbf{i}(c_j n^2 + d_j n)\theta_j}.$$

Matching the leading terms above we get that

$$4\theta_i - \sum_{j \in I_i} c_j \theta_j \in \mathbb{Z}\pi. \qquad (9)$$

The above relation implies that the multiplicative combination $\alpha_i^4 \prod_{i\in I_i} \alpha_j^{c_j}$ is a root of unity, and by our convention this root of unity must be 1. Hence, (9) is in fact

$$\theta_i = \sum_{j\in I_i} (c_j/4)\theta_j. \tag{10}$$

This means that θ_i is in the convex hull of θ_j for $j \in I_i$.

If I_i has only two elements of which one is i itself, we get, with $I_i = \{i, j\}$, that

$$(4 - c_i)\theta_i = c_j\theta_j,$$

but this is impossible since α_i/α_j is not a root of unity. Thus, either I_i does not contain i, or it does but then it has at least 3 elements. So, θ_i is in the convex hull of the remaining ones. Plotting them as numbers in $(-1, 1)$ and picking i to be the one to the most left, we get a contradiction. A different way of seeing this last step is to think of $\theta = (\theta_1, \ldots, \theta_r)$ 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 having the coefficient $c_j/4$ on in the position (i, j) if $i \in \{1, \ldots, r\}$ and $j \in I_i$ and 0 otherwise. Then $\mathbf{A}$ is a matrix whose entries are non-negative, has row sums equal to 1 and each row contains at least two nonzero entries. The eigenspace of such a matrix corresponding to the eigenvalue 1 one dimensional spanned by $(1, 1, \ldots, 1)^T$. Hence, $\theta_i = \theta_j$ for $i = 1, \ldots, r$, contradiction.

The p-adic proof

Considerations about orders of points on elliptic curves

For a prime p, we let $E(\mathbb{F}_p)$ be the set of solutions modulo p of the equation (1) modulo p together with the point of infinity. We let

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

Then $a_p \in (-2\sqrt{p}, 2\sqrt{p})$ 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 reduced modulo p.

Otherwise, when $p \mid \Delta_E$, we have $a_p \in \{0, \pm 1\}$. If $p \nmid \Delta_E z_1$, then P can be regarded as a point on $E(\mathbb{F}_p)$ which is not the origin. We let q be a large but fixed prime. We ask what can we say about primes p such that the order of P in $E(\mathbb{F}_p)$ is divisible by q. For this, we use recent joint work of Meleleo.

But first, some group theory.

Let

$$E[q] = \{Q : qQ = O\}, \quad \text{where} \quad O \quad \text{is the point at infinity.}$$

As a $\mathbb{F}_q$-vector space, $E[q]$ can be identified with $\mathbb{F}_q^2$. Adjoining the coordinates of the points $Q \in E[q]$ to $\mathbb{Q}$ we obtain a Galois extension of $\mathbb{Q}$ of Galois group contained in $\mathrm{GL}_2(\mathbb{F}_q)$. Serre's open mapping theorem says that there exists a positive integer $\Delta_{1,E}$ depending on E such that if $q \nmid \Delta_{1,E}$, then this Galois group is the full $\mathrm{GL}_2(\mathbb{F}_q)$. We assume that $\Delta_{1,E}$ is already a multiple of all prime factors of Δ_E.

Suppose now that we want to study the density of the primes p such that a_p and p have prescribed values modulo q, say a and b. Then, one can identify the Jacobian of such a prime p with the equivalence class of a 2×2 matrix in $\mathrm{GL}_2(\mathbb{F}_q)$ whose trace has the value of a_p modulo q and whose determinant has the value p modulo q. That is for given residue classes a and $b \not\equiv 0$ modulo q, the density

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

exists and equals

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

In particular, $\delta_{q;a,b} > 0$ always.

Assume next that we want to throw the point P into the picture and see what happens to its order in $E(\mathbb{F}_p)$ modulo q. Consider

$$E_P[q] = \{R : qR = P\}.$$

Note that by fixing $R_0 \in E_P[q]$, we can identify $E_P[q]$ with $R_0 + E[q]$, and since $E[q]$ was identified with a $\mathbb{F}_q$ vector space of dimension 2, it follows that $E_P[q]$ can be identified with an affine space of dimension two over $\mathbb{F}_q$. Adjoin also 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 which is due to Bashmakov, there exists a constant $\Delta_{2,E,P}$ depending both on P and E such that if $q \nmid \Delta_{2,P,E}$, then the Galois group of this extension is the group of affine transformations of a 2-dimensional affine $\mathbb{F}_q$–space, namely

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

where of course $\mathrm{GL}_2(\mathbb{F}_q)$ acts on $\mathbb{F}_q^2$ by linear automorphism.

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 $x_1 y_1 z_1$. Here, we assume that $x_1 y_1 \neq 0$. It is clear that $y_1 \neq 0$ (otherwise P is of order 2).

If $x_1 = 0$, then we replace P by $2P$, which is still of infinite order, and then $x_1 \neq 0$.

Furthermore, the order of $2P$ modulo p equals the order of P modulo p, or half of it (depending of whether the order of P modulo p is odd or even), and since q is odd, it follows that 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 $2P$.

By results of Meleleo, if q does not divide $\Delta_{2,E,P}$, then

$$\lim_{x\to\infty} \frac{\#\{p \le x : a_p \equiv q \pmod p,\ p \equiv b \pmod p,\ q \mid \mathrm{ord}_{E(\mathbb{F}_p)}(P)\}}{\pi(x)}$$

equals $\delta_{q;a,b,P}$, where

$$\delta_{q;a,b,P} = \frac{\#\{(J,u) \in \mathrm{GL}_2(\mathbb{F}_q) : \mathrm{tr}(J) = a,\ \det(J) = b,\ u \notin \mathrm{Im}(J - I_2)\}}{\#\left(\mathrm{GL}_2(\mathbb{F}_p) \rtimes \mathbb{F}_q^2\right)}.$$

Note first of all that a and b have to be chosen such that

$$p - a_p + 1 = b - a + 1 \quad \text{is a multiple of} \quad q.$$

Thus, $b \equiv a - 1 \pmod q$. Well, take

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

Then

$$\mathrm{tr}(J) = a, \quad \det(J) = a-1 = b \quad \text{and} \quad u \notin \mathrm{Im}(J-I_2) = \left\{\begin{pmatrix} x \\ 0 \end{pmatrix}, x \in \mathbb{F}_q\right\}$$

This shows that $\delta_{q;a,a-1,P} > 0$. We record this as a theorem.

Theorem

Let $a \geq 2$ be a fixed positive integer, and E be an elliptic curve defined over $\mathbb{Q}$ with a point of infinite order P on it. Then there exists Δ depending on E and P such that if q does not divide Δ, then the set of primes $p \equiv a - 1 \pmod{q}$ with $a_p \equiv a \pmod{q}$ and $P \mod q$ having order a multiple of q in $E(\mathbb{F}_q)$ has positive density $\delta_{q;a,a-1,P}$.

The p-adic proof

Let $a = 3$, q be fixed but sufficiently large in a way to be made more precise later and let $P_{q;3,2,P}$ be the set of primes p as in the statement of Theorem 2. We let p be a large prime in $P_{q;3,2,P}$. In particular, we assume that p does not divide the neither 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 formula (3), and that p does not divide the last coefficient c_k of $\Psi(X)$ either. We put

$$L = \text{lcm}[p^j - 1 : 1 \le j \le d].$$

Note that since $p \equiv 2 \pmod{q}$, it follows that $p^j - 1 \equiv 2^j - 1 \pmod{q}$ for $j = 1, \ldots, k$. Thus, for large q, we have that $q \nmid L$.

We now let T be the period modulo p of $\{z_n\}_{n\geq 1}$. It follows from a theorem of Silverman, 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 on the side of the sequence $\{u_{n^2}\}_{n\geq n_0}$ and show that its period modulo p is coprime to q. This will give us the contradiction.

For the time being, we write that

$$u_{(n+mT)^2} \equiv u_{n^2} \pmod p \tag{11}$$

holds for all $n \geq n_0$ and all $m \geq 0$. Let π be a prime ideal of $\mathbb{K}$ sitting above the rational prime number p. Congruence (11) together with Binet's formula (3) give

$$\sum_{i=1}^{s} \alpha_i^{n^2}(P_i((n+mT)^2)\alpha_i^{2mnT+m^2T^2} - P_i(n^2)) \equiv 0 \pmod \pi. \tag{12}$$

We put

$$\mathcal{S} = \{p \mid T\} \cup \{p \leq p_0\},$$

where p_0 is a sufficiently large number to be determined later and let N be the largest divisor of L composed only of primes from $\mathcal{S}$.

We write $m = pN\ell$ for some integer $\ell \geq 0$ in (12) and use the fact that

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

to get that

$$\sum_{i=1}^{s} \alpha_i^{n^2} P_i(n^2)(\beta_i^{2\ell n + pNT\ell^2} - 1) \equiv 0 \pmod{\pi}, \tag{13}$$

where

$$\beta_i := \alpha_i^{pNT} \quad (1 \leq i \leq s).$$

We show that if p_0 is sufficiently large, the above congruences (13) imply that $\beta_i \equiv 1 \pmod{\pi}$ for all $i = 1, \ldots, s$. Assume for the time being that this is not so. In fact, up to relabeling the roots $\alpha_1, \ldots, \alpha_s$, we may assume that there exist $s_1 < s$ and indices $0 < i_1 < \cdots < i_t = s - s_1$ such that

$$\begin{aligned}
&\beta_1 \equiv \cdots \equiv \beta_{s_1} \equiv 1 \pmod{\pi} \\
&\beta_{s_1+1} \equiv \cdots \equiv \beta_{s_1+i_1} \equiv \gamma_1 \pmod{\pi} \\
&\ldots \\
&\beta_{s_1+i_{t-1}+1} \equiv \cdots \equiv \beta_{s_1+i_t} \equiv \gamma_t \pmod{\pi}
\end{aligned}$$

where $\gamma_i \not\equiv 1 \pmod{\pi}$ for $i \in \{1, \ldots, t\}$ and $\gamma_i \not\equiv \gamma_j \pmod{\pi}$ for distinct i and j in $\{1, \ldots, t\}$.

Relation (13) becomes

$$\sum_{j=1}^{t} Q_j(n)(\beta_j^{2\ell n+pNT\ell^2} - 1) \equiv 0 \pmod{\pi}. \tag{14}$$

Here,

$$Q_j(n) = \sum_{i=s_1+i_{j-1}+1}^{s_1+i_j} \alpha_i^{n^2} P_i(n^2) \qquad \text{for} \qquad j = 1, \ldots, t$$

with the convention that $i_0 := 0$. Write

$$L/N := \prod_{r \mid L/N} r^{a_r}.$$

For each prime $r \mid L/N$, choose n_0 with the property

$$\left(\frac{n_0^2 + jpNT}{r}\right) = 1 \qquad \text{for all} \qquad j = 1, \ldots, t.$$

To see that this exist, note that for a fixed r, the number of possible residue classes for such an n_0 is

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

The constant implied by the above $O(1)$ depends on t and comes from the instances $n \in \{0, \ldots, r-1\}$ for which $n^2 + jpN \equiv 0 \pmod r$.

To estimate I_r, we expand the inner product, separate the main term and change the order of summation for the remainder terms getting that

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

where the implied constant in the above O depends on t. For the above estimate, we use Weil's bound with the observation that if $r > t$ and does not divide pNT, then the polynomial

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

has only simple roots modulo r. This shows that $I_r > 0$ for all r sufficiently large.

So, we set 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

$$P_i(n_0) \not\equiv 0 \pmod{p} \quad \text{for all} \quad i = 1, \ldots, s.$$

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 value (first such value) of such a number in the arithmetic progression of ratio pL/N.

Next we claim that there are positive integers $x_{s_1}, \dots, x_s$ such that for each $j = 1, \dots, t$, the determinant

$$\det \begin{vmatrix} \alpha_{s_1+i_{j-1}+1}^{(n_0+pL/Nx_{s_1+i_{j-1}+1})^2} & \cdots & \alpha_{s_1+i_j}^{(n_0+pL/Nx_{s_1+i_{j-1}+1})^2} \\ \alpha_{s_1+i_{j-1}+1}^{(n_0+pL/Nx_{s_1+i_{j-1}+2})^2} & \cdots & \alpha_{s_1+i_j}^{(n_0+pL/Nx_{s_1+i_{j-1}+2})^2} \\ \cdots & \cdots & \cdots \\ \alpha_{s_1+i_{j-1}+1}^{(n_0+pL/Nx_{s_1+i_j})^2} & \cdots & \alpha_{s_1+i_j}^{(n_0+pL/Nx_{s_1+i_j})^2} \end{vmatrix} \neq 0. \qquad (15)$$

We do this one j at a time. The statement is clear if

$$i_j - i_{i_{j-1}} = 1.$$

It also clear if $i_j - i_{j-1} = 2$ because the ratio

$$\alpha_{s_1+i_j+2}/\alpha_{s_1+i_{j-1}+1} \quad \text{is not a root of unity.}$$

For larger values of $i_j - i_{j-1}$ it follows by induction by first choosing $x_{s_1+i_{j-1}+1}, \ldots, x_{s_1+i_j-1}$ such that the minor of size $(i_j - i_{j-1} - 1) \times (i_j - i_{j-1} - 1)$ from the upper left corner is non-zero, 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 $\mathcal{S}$-unit equation in this last variable which can have only finitely many solutions $x_{s_1+i_j}$.

Assuming now that $x_1, \ldots, x_{s-s_1}$ are fixed positive integers such that (15) holds for all $j = 1, \ldots, t$, then we assume that p is larger than the norm (from $\mathbb{K}$ over $\mathbb{Q}$) of each of the determinants (15) for $j = 1, \ldots, t$. Now giving n the values

$$n_0 + pL/Nx_1, \ldots, n_0 + pL/Nx_{s-s_1}$$

and assuming that for some $j \in \{1, \ldots, t\}$, we have that

$$Q_j(n_0+pL/Nx_i) \equiv 0 \pmod{\pi} \quad \text{for all} \quad i \in \{s_1+i_{j-1}+1, \ldots, s_1+i_j\},$$

we get the system

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

This signals the nonzero vector

$$(P_i(n_0^2))^T_{s_1+i_{j-1}-1 \le i \le s_1+i_j} \quad \text{in} \quad \mathbb{F}_q^{i_j-i_{j-1}}$$

(where $\mathbb{F}_q = \mathbb{K}[X]/\pi$) as a solution to an homogeneous system of equations whose determinant (15) is nonzero modulo π; a contradiction.

Hence, there exists n_0 in the correct residue class modulo pL/N such that $Q_j(n_0)$ is nonzero modulo π for all $j = 1, \ldots, t$. It now remains to choose some ℓ's. Well, for each $j = 1, \ldots, t$, and for each r dividing L/N choose ℓ_j such that

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

The solution ℓ_j modulo r of the above congruences are given by

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

which exists since r does not divide pNT and $n_0^2 + jpNT$ is a quadratic residue modulo r. With Hensel's Lemma, we extend this to a solution ℓ_j modulo r^{a_r}, and then with the Chinese Remainder Lemma to a solution ℓ_j modulo L/N. Hence,

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

Thus,

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

therefore

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

because L is a multiple of the order of α_u modulo π, and the above congruences hold for all $u = 1, \ldots, t$. Returning to (14), we get that

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

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

Hence,

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

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

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

So, either $\beta_i \equiv 1 \pmod{\pi}$ for some $i = 1, \ldots, t$, or $\beta_i \equiv \beta_j \pmod{\pi}$ for some $1 \le i < j \le t$, and none is possible.

So, the conclusion is that $\alpha_i^{pTN} \equiv 1 \pmod{\pi}$ and this was true for all prime ideals π of $\mathcal{O}_{\mathbb{K}}$ dividing p. However, the order of α_i modulo π divides L, and L is not a multiple of q or of p. Also, p does not divide either L or $p - a_p + 1$. So, writing a_q for the exponent of q in T, we get that

$$\alpha_i^{NT/q^{a_q}} \equiv 1 \pmod{\pi}.$$

Since p is large (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

$$\alpha_i^{NT/q^{a_q}} \equiv 1 \pmod{p} \quad \text{for all} \quad i = 1, \ldots, r.$$

But then, by the Binet formula (3), we get that pNT/q^{a_q} is a period of $\{u_{n^2}\}_{n\geq 1}$ modulo p. So, also a period of $\{z_n\}_{n\geq 1}$. Hence, $T \mid pNT/q^{a_q}$, which is not possible since T is a multiple of q.

This finishes the p-adic proof.

MERÇI BEAUCOUP!