RATIONAL 6-CYCLES UNDER ITERATION
OF QUADRATIC POLYNOMIALS

MICHAEL STOLL

ABSTRACT. We present a proof, which is conditional on the Birch and Swinnerton-Dyer Conjecture for a specific abelian variety, that there do not exist rational numbers x and c such that x has exact period $N = 6$ under the iteration $x \mapsto x^2 + c$. This extends earlier results by Morton for $N = 4$ and Flynn, Poonen and Schaefer for $N = 5$.

1. INTRODUCTION

In this note, we present a conditional proof that there do not exist rational numbers x and c such that the sequence defined by $x_0 = x$, $x_{n+1} = x_n^2 + c$ (for $n \geq 0$) has exact period 6. The assumptions we have to make are that the L-series of a certain genus 4 curve $X_0^{\mathrm{dyn}}(6)$ extends to an entire function and satisfies the usual kind of functional equation, and that the Jacobian of $X_0^{\mathrm{dyn}}(6)$ satisfies the first part of the Birch and Swinnerton-Dyer conjecture (that asserts equality between the Mordell-Weil rank and the order of vanishing of the L-series at $s = 1$).

This extends a series of investigations on rational cycles under quadratic iteration. It is easy to see that fixed points and 2-cycles are each parameterized by a rational curve; the same is true for 3-cycles. Morton [16] has shown that 4-cycles are parameterized by the modular curve $X_1(16)$; he used this to show that there do not exist rational 4-cycles. Flynn, Poonen, and Schaefer [9] proved that there are no rational 5-cycles and make a preliminary study of 6-cycles. The present paper gives a conditional proof that there are no rational 6-cycles. It is conjectured (see [21, Conj. 3.15, Rk. 3.17]) that there is a universal bound on the number of rational preperiodic points under quadratic iteration. In view of the results obtained so far, it seems reasonable to expect that there are no rational N-cycles when $N > 3$, compare Conjecture 2 in [9]. Poonen [18] shows that this would imply that there can be at most 9 rational preperiodic points.

Let $f^{(0)}(x, c) = x$, $f^{(n+1)}(x, c) = f^{(n)}(x^2 + c, c)$ denote the iterates of $x \mapsto x^2 + c$. For $N \geq 1$, pairs (x, c) such that x is a point of period N under $x \mapsto x^2 + c$ satisfy the equation $\Phi_N(x, c) := f^{(N)}(x, c) - x = 0$. Pairs (x, c) such that x is periodic of

exact order N give rise to points on the affine curve $Y_1^{\mathrm{dyn}}(N)$ with equation

$$\Phi_N^*(x, c) := \prod_{d \mid N} \Phi_d(x, c)^{\mu(N/d)} = 0\,.$$

(For some of the points, the orbit of x actually has exact order a proper divisor of N; see for example [21] for details.) It can be shown that $Y_1^{\mathrm{dyn}}(N)$ is smooth and irreducible; we denote by $X_1^{\mathrm{dyn}}(N)$ its smooth projective model. This curve has an automorphism σ of order N induced by the map $(x, c) \mapsto (x^2 + c, c)$ on $Y_1^{\mathrm{dyn}}(N)$. We denote the quotient $X_1^{\mathrm{dyn}}(N)/\langle\sigma\rangle$ by $X_0^{\mathrm{dyn}}(N)$. There are formulas due to Bousch and Morton for the genera of $X_1^{\mathrm{dyn}}(N)$ and $X_0^{\mathrm{dyn}}(N)$. See [2, 12, 15] or [21, Thm. 4.17].

In this note, we work with $X_0^{\mathrm{dyn}}(6)$, which is a curve of genus 4. Assuming the conjecture of Birch and Swinnerton-Dyer, we determine the set of rational points on this curve, from which we can find the set of rational points on $X_1^{\mathrm{dyn}}(6)$. It turns out that all of these points are "cusps", i.e., they are in the complement of $Y_1^{\mathrm{dyn}}(6)$ and hence do not correspond to pairs (x, c) as above.

We first find a nice model of $X_0^{\mathrm{dyn}}(6)$ (see Section 2 below). There are ten rational points on this curve that are easy to find. We show that they generate a torsion-free subgroup G of rank 3 in the Mordell-Weil group $J(\mathbb{Q})$, where J is the Jacobian of $X_0^{\mathrm{dyn}}(6)$. We further show that there are no other rational points that map into the saturation of this subgroup in $J(\mathbb{Q})$. This is done in Section 3 below. It remains to show that G is a finite-index subgroup of $J(\mathbb{Q})$. It is in this part of the proof that we have to make assumptions on the L-series, since we want to use the Birch and Swinnerton-Dyer conjecture. We compute enough coefficients of the L-series to show that its third derivative at $s = 1$ does not vanish, which, according to the BSD conjecture, implies that the rank of $J(\mathbb{Q})$ is at most 3. See Section 4 below. (Note that a 2-descent on J, which is the usual way to obtain an upper bound on the Mordell-Weil rank for low-genus curves, requires knowledge of the class and unit groups of a number field of degree 119. The necessary computations are utterly infeasible with current technology, even when assuming GRH.)

We have used the MAGMA [13] computer algebra system in order to perform the necessary computations. A script that can be loaded into MAGMA and that performs the relevant computations is available at [26].

This curve $X_0^{\mathrm{dyn}}(6)$ appears to be the first curve of higher genus that is not very special in some way, e.g., hyperelliptic or a modular or Shimura curve, having a large automorphism group, or covering a curve of smaller genus, for which the set of rational points could be explicitly determined (assuming reasonable standard conjectures). The methods used here should be applicable in other cases as well, provided

- we can find a finite-index subgroup of the Mordell-Weil group,
- its rank is less than the genus, and
- the conductor is reasonably small.

2. The Model

In order to obtain a smooth projective model of $X_0^{\mathrm{dyn}}(6)$, we first find an equation for $Y_0^{\mathrm{dyn}}(6)$ (the image of $Y_1^{\mathrm{dyn}}(6)$ in $X_0^{\mathrm{dyn}}(6)$) as an affine plane curve. For a point $(x, c) \in Y_1^{\mathrm{dyn}}(6)$, we consider the "trace" of its orbit,

$$x + (x^2 + c) + f^{(2)}(x, c) + \cdots + f^{(5)}(x, c).$$

The resultant with respect to x of $\Phi_6^*(x, c)$ and $t - \left(f^{(0)}(x, c) + \cdots + f^{(5)}(x, c)\right)$ is a sixth power; one of its sixth roots is

$$
\begin{aligned}
\Psi_6(t, c) = {}& 256(t^3 + t^2 - t - 1)c^3 + 16(9t^5 + 7t^4 + 10t^3 + 30t^2 - 19t - 37)c^2 \\
& + 8(3t^7 + t^6 + 2t^5 + 2t^4 - 17t^3 + 69t^2 + 52t - 48)c \\
& + t^9 - t^8 + 2t^7 + 14t^6 + 49t^5 + 175t^4 + 140t^3 + 196t^2 + 448t \,.
\end{aligned}
$$

(This polynomial was already computed by Morton in [16].) We first resolve the singularities at infinity. Successively getting rid of multiple factors at the edges of the Newton polygon, we arrive at the equation

$$
\begin{aligned}
F(u, v) = {}& (u^4 - u^3)v^3 + (-u^5 + 9u^4 + 6u^3 - 17u^2 + 3u)v^2 \\
& + (4u^4 + 74u^3 - 52u^2 - 54u + 24)v + 4u^4 + 24u^3 + 117u^2 - 261u + 72 \\
& = 0 \,.
\end{aligned}
$$

Here

$$u = \frac{2}{t+1} \quad \text{and} \quad v = 4(c-1) + (t-1)^2 + \frac{2}{t+1} \,,$$

or

$$t = \frac{2}{u} - 1 \quad \text{and} \quad c = \frac{v}{4} - \frac{1}{u^2} + \frac{2}{u} - \frac{u}{4} \,.$$

The curve defined by this equation has three singularities at points (α, β), where

$$3\beta^3 + 32\beta^2 + 69\beta + 72 = 0 \quad \text{and} \quad 18\alpha = 6\beta^2 + 55\beta + 69 \,.$$

From the Newton polygon of F, we see that the regular differentials on the smooth projective model of this curve are contained in the space spanned by ω_0, $u\,\omega_0$, $uv\,\omega_0$, $u^2\,\omega_0$, $u^2v\,\omega_0$, $u^3\,\omega_0$, and $u^3v\,\omega_0$, where

$$\omega_0 = \frac{du}{\frac{\partial}{\partial v}F(u,v)} = -\frac{dv}{\frac{\partial}{\partial u}F(u,v)}\,.$$

(See [11], in particular the example on page 42.) These differentials are regular everywhere except perhaps at the singularities described above. In order to get something regular there, the polynomial that ω_0 is multiplied by has to vanish at the singularities. We obtain the following basis of $\Omega^1_{X_0^{\mathrm{dyn}}(6)}$.

$$\omega_1 = (u^3v + 2u^3 - 3u^2v - u^2 + 3uv + 6)\,\omega_0$$
$$\omega_2 = (u^3v + 2u^3 - u^2v + u^2 + 3u - 6)\,\omega_0$$
$$\omega_3 = (u^3v + 2u^3 - 4u^2v - 3u^2 + 3uv - 3u)\,\omega_0$$
$$\omega_4 = (3u^3v + 4u^3 - 3u^2v + 6u^2 - 6u)\,\omega_0$$

The canonical model of a curve of genus 4 is the intersection of a quadric and a cubic in $\mathbb{P}^3$. We see that u is a rational function of degree 3, which implies that the quadric splits, i.e., it is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ over $\mathbb{Q}$. So there is a model of $X_0^{\mathrm{dyn}}(6)$ that is a smooth curve of bidegree $(3,3)$ in $\mathbb{P}^1 \times \mathbb{P}^1$. To find a suitable second coordinate (besides u), we take the quotient of two differentials vanishing on $u = 0$. This means that the differentials may not contain ω_0 or $uv\,\omega_0$ with a nonzero coefficient. A possible choice is

$$w = \frac{-\omega_1 - \omega_2 + \omega_3 + 2\omega_4}{\omega_4} = \frac{-u^2v + 3uv + 18}{u^2v + 2u^2 + 3u + 6}\,.$$

In terms of u and w, we now have $X_0^{\mathrm{dyn}}(6)$ as a smooth curve in $\mathbb{P}^1 \times \mathbb{P}^1$, with (affine) equation

$$G(u,w) = w^2(w+1)u^3 - (5w^2 + w + 1)u^2 - w(w^2 - 2w - 7)u + (w+1)(w-3) = 0\,.$$

We will denote this curve by C. Note that

$$c = \frac{(-u^3 - 2u^2 + 5u - 10)uw - u^4 + 3u^3 + 8u^2 - 10u + 12}{4u^2(uw + u - 3)}$$

on this model. Note also that the existence of the canonical model shows that $X_0^{\mathrm{dyn}}(6)$ is not hyperelliptic.

Our model has good reduction except at 2 and at $p = 8\,029\,187$. Mod p, we have a node at $(u,w) = (2937959, 7887180)$ with tangent directions defined over $\mathbb{F}_p$. This point is regular on the arithmetic surface given by $G(u,w) = 0$.

Mod 2, there is a node at $(1,0)$ with tangent directions defined over $\mathbb{F}_4$ and a tacnode at $(0,1)$ with local branches again defined over $\mathbb{F}_4$. Both singularities are non-regular points of the arithmetic surface. Resolving these points gives us the

minimal proper regular model over $\mathbb{Z}_2$. The node resolves into a chain of three $\mathbb{P}^1$'s whose ends intersect the original component. Blowing up the tacnode gives a double line, all of whose points are non-regular. Blowing up this line, we obtain a smooth curve of genus 1, meeting the original components in two (regular) points. Therefore, the special fiber of the minimal proper regular model consists of five components A, B, C, C', D, each of multiplicity one. A and B are both elliptic curves with trace of Frobenius -1, the other components are $\mathbb{P}^1$'s. A, B, and D are defined over $\mathbb{F}_2$, C and C' are defined over $\mathbb{F}_4$ and conjugate. The intersection matrix is as follows.

	A	B	C	C'	D
A	-4	2	1	1	0
B	2	-2	0	0	0
C	1	0	-2	0	1
C'	1	0	0	-2	1
D	0	0	1	1	-2

(For some worked examples of how to compute minimal regular models, see [7] or [19].)

The two (separate) intersection points of A and B are swapped by the action of Frobenius. We see that the reduction of the Jacobian has a 2-dimensional abelian and a 2-dimensional toric component (since the dual graph of the special fiber has two independent loops, compare [1, § 9.2]); Frobenius reverses the orientation of both loops. We can summarize our findings in the following lemma.

Lemma 1. *The Jacobian of $C = X_0^{\mathrm{dyn}}(6)$ has conductor $2^2\,p$, where $p = 8\,029\,187$ is the big prime from above. Its Euler factor at 2 is $(1 + T + 2T^2)^2(1 + T)^2$.*

We end this section by showing that $X_0^{\mathrm{dyn}}(6)$ does not have any special geometrical properties that might help us.

Lemma 2. *We have $\mathrm{End}_{\bar{\mathbb{Q}}} J = \mathbb{Z}$. In particular:*

(1) *The automorphism group of $X_0^{\mathrm{dyn}}(6)$ is trivial (even over $\bar{\mathbb{Q}}$).*
(2) *The Jacobian of $X_0^{\mathrm{dyn}}(6)$ is absolutely simple.*
(3) *There is no map of degree ≥ 2 from $X_0^{\mathrm{dyn}}(6)$ to a curve of positive genus (not even over $\bar{\mathbb{Q}}$).*

Proof. We take inspiration from the proof of Prop. 9 in [9]. To make matters more concrete, we formulate a computational lemma.

Lemma 3. *Let C be a curve of genus g over a number field K, with Jacobian J, let v be a finite place of K of good reduction for C, and let $f(T)$ be the Euler factor of $L(C, s)$ at v. If $f \in \mathbb{Q}[T]$ is irreducible, and no monic irreducible factor of*

$$h(T) = \frac{\mathrm{Res}_x\big(f(x), f(Tx)\big)}{(1 - T)^{2g}}$$

has integral coefficients and constant term 1, then $\mathrm{End}_{\bar{K}} J$ embeds into the number field generated by a root of f.

Proof. For the proof, note that the roots of h are all the quotients α/β, where α and β are distinct roots of f. If one of these quotients is a root of unity, then h has a monic irreducible factor that has integral coefficients and constant term 1 (namely, some cyclotomic polynomial). Conversely, if there is such an irreducible factor, then its roots are units in the splitting field of f, and they have absolute value 1 in all complex embeddings (since $|\sigma(\alpha)| = q^{-1/2}$ for all complex embeddings σ and all roots α of f, where q is the size of the residue class field k_v). Hence some α/β is a root of unity.

Now this is the case if and only if, for some $n \geq 2$, there are distinct roots α and β of f such that $\alpha^n = \beta^n$. This in turn is equivalent to the Galois orbit of α^n having size less than $\deg f = 2g$, which means that the characteristic polynomial of the nth power of the v-Frobenius is not irreducible.

Our assumptions therefore imply that all these characteristic polynomials are irreducible. (An argument like this was used in [22] to show that certain genus 2 Jacobians are absolutely simple.) From [28, Thm. 8], we then see that the endomorphism algebra of J over $\bar{k}_v$ is the number field generated by a root of f, and since the endomorphism ring of J (over $\bar{K}$) embeds into this algebra, the claim is proved. (Note that J is simple over k_v since f is irreducible.) $\square$

To prove Lemma 2, we compute the Euler factors at $p = 5$ and $p = 7$. They are

$$1 + 3T + 6T^2 + 6T^3 - 8T^4 + 30T^5 + 150T^6 + 375T^7 + 625T^8 .$$

and

$$1 + 7T + 28T^2 + 94T^3 + 276T^4 + 658T^5 + 1372T^6 + 2401T^7 + 2401T^8 .$$

We observe that both polynomials satisfy the assumptions in Lemma 3 and that the number fields they generate are linearly disjoint over $\mathbb{Q}$. (We can check, for example using MAGMA, that there is no common subfield other than $\mathbb{Q}$.) This proves the first claim.

Statement (1) then follows, since any nontrivial automorphism of the curve would induce a nontrivial automorphism of the Jacobian J. But the only nontrivial automorphism of J is multiplication by -1, and if it would come form an automorphism of the curve, this would imply that the curve is hyperelliptic, which is not the case. Alternatively, we can use the fact that any automorphism of our curve must extend to an automorphism of $\mathbb{P}^1 \times \mathbb{P}^1$. Such automorphisms either perform a Möbius transformation on each of the factors separately, or else this type of automorphism is followed by swapping the two factors. A Gröbner basis computation shows that the only automorphism of $\mathbb{P}^1 \times \mathbb{P}^1$ that fixes the curve is the identity.

If statement (2) were false, then the algebra $\mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End}_{\bar{\mathbb{Q}}} J$ would have zero divisors, which is not the case.

Finally, if the curve covers another curve of positive genus and the map is not an isomorphism, then the other curve has genus strictly between 0 and 4. But then its Jacobian will be a factor of the Jacobian of $X_0^{\text{dyn}}(6)$, so the latter would have to split, contradicting the fact that J is absolutely simple. $\qquad\square$

3. Rational Points

A quick search finds the following ten rational points on C.

	u	w	t	c
P_0	0	∞	∞	∞
P_1	0	-1	∞	∞
P_2	0	3	∞	∞
P_3	∞	0	-1	∞
P_4	1	2	1	∞

	u	w	t	c
P_5	2	1	0	0
P_6	1	∞	1	-2
P_7	∞	-1	-1	-2
P_8	-1	∞	-3	-4
P_9	$-\frac{4}{5}$	-1	$-\frac{7}{2}$	$-\frac{71}{48}$

The first five of these are the "cusps"; these are the points that have to be added to $Y_0^{\text{dyn}}(6)$ in order to obtain a smooth projective curve. It is known that all cusps on $X_1^{\text{dyn}}(N)$ and hence also on $X_0^{\text{dyn}}(N)$ are rational points, for all N. This follows from the Laurent series expansions for the periodic points in terms of $q = (-4c - 3)^{-1/2}$, which have rational coefficients; compare [16]. In fact, the map

$$Y_1^{\text{dyn}}(N) \longrightarrow \mathbb{P}^N, \quad (x, c) \longmapsto \left(1 : x : x^2 + c : \ldots : f^{(N-1)}(x, c)\right)$$

extends to a projective embedding of $X_1^{\text{dyn}}(N)$, where the cusps have coordinates $(0 : 1 : \pm 1 : \ldots : \pm 1)$.

The remaining five points correspond to cycles of length 6 for the given value of c that are stable as a set (or as a cycle) under the action of the absolute Galois group of $\mathbb{Q}$. For the special values $c = 0$ and $c = -2$, these cycles are "predictable"; they come from roots of unity. For $N = 6$, we find cycles containing ζ_9 when $c = 0$ and cycles containing $\zeta_{13} + \zeta_{13}^{-1}$ (this is the one whose trace t is -1) or $\zeta_{21} + \zeta_{21}^{-1}$ (with $t = 1$) when $c = -2$. (We use ζ_n to denote a primitive nth root of unity; these cycles then contain all possible values of the above expressions.)

For $c = -4$, the points in the cycle live in a sextic abelian number field with discriminant $5^3 \cdot 7^4$ and conductor 35; it is the field $\mathbb{Q}(\sqrt{5}, \cos \frac{2\pi}{7})$. Finally, for $c = -\frac{71}{48}$, we find points defined over the *quadratic* field $\mathbb{Q}(\sqrt{33})$; one point in the cycle is $x = -1 + \frac{1}{12}\sqrt{33}$. In particular, this means that $X_1^{\text{dyn}}(6)\left(\mathbb{Q}(\sqrt{33})\right)$ contains an orbit of six non-cuspidal points.

See also the final section of [9], where these points are already found, and the corresponding Galois-stable 6-cycles are described.

We will now prove the following result.

Lemma 4. *Let J denote the Jacobian of $C = X_0^{\mathrm{dyn}}(6)$.*

1. *$J(\mathbb{Q})$ has trivial torsion subgroup.*
2. *The subgroup G of $J(\mathbb{Q})$ generated by the classes of divisors supported in the 10 rational points listed above is isomorphic to $\mathbb{Z}^3$.*
3. *This subgroup is already generated by divisors supported at the cusps.*

Proof. We know that the prime-to-p torsion in $J(\mathbb{Q})$ injects into $J(\mathbb{F}_p)$ for primes of good reduction, so the observation that (as computed by MAGMA)

$$\#J(\mathbb{F}_7) = 2 \cdot 7 \cdot 11 \cdot 47 \quad \text{and} \quad \#J(\mathbb{F}_{13}) = 3 \cdot 17 \cdot 23 \cdot 43$$

shows that $J(\mathbb{Q})$ has trivial torsion subgroup.

The main tool for proving the other assertions is the homomorphism

$$\Phi_S : \bigoplus_{i=0}^{9} \mathbb{Z}P_i \longrightarrow \mathrm{Pic}_C \longrightarrow \prod_{p \in S} \mathrm{Pic}_{C/\mathbb{F}_p} ,$$

where S is a set of primes of good reduction. We take $S = \{3, 5, 7, 11, 13\}$ and compute the kernel of Φ_S. This kernel is a subgroup of rank 9 in $\mathbb{Z}^{10} = \bigoplus \mathbb{Z}P_i$. We apply LLL to it and find that there are six independent elements with very small coefficients (and three large additional basis vectors). We suspect that the small elements come from actual relations between our points; this can then be verified by exhibiting a suitable rational function. (MAGMA provides the necessary functionality for these computations.) Denoting linear equivalence by '$\sim$', we find the following six independent relations.

$$P_0 + P_6 + P_8 \sim P_1 + P_7 + P_9$$
$$P_0 + P_1 + P_2 \sim 2P_3 + P_7$$
$$\sim 2P_4 + P_6$$
$$P_0 + P_2 + P_7 + P_9 \sim P_1 + P_3 + P_5 + P_6$$
$$2P_0 + P_1 + P_6 \sim P_2 + P_3 + 2P_5$$
$$3P_0 + P_3 \sim P_1 + P_2 + P_6 + P_8$$

On the other hand, looking at the image of Φ_S, we see that the degree 0 subgroup of $\mathbb{Z}^{10}$ surjects onto $(\mathbb{Z}/3\mathbb{Z})^3$. Since we know that there is no torsion in $J(\mathbb{Q})$, this implies that the rank of the image of the degree 0 subgroup in $J(\mathbb{Q})$ must be at least 3. The existence of the relations above implies that the rank is at most 3, so the rank is exactly 3, and since there is no torsion, the group must be isomorphic to $\mathbb{Z}^3$.

Finally, from the relations we have given it is easy to verify that P_3 and $P_5, \ldots, P_9$ can be expressed in terms of P_0, P_1, P_2, and P_4. This means that our subgroup is already generated by divisors supported at the latter four points (all of which are cusps). The only relation between the cusps is

$$5P_0 - 10P_1 - 2P_2 + P_3 + 6P_4 \sim 0 \, ;$$

it is perhaps worth noting that this relation is *not* induced by the standard "dynamical units" as provided by [21, Thm. 2.33] or [17], applied to the coordinate ring of $Y_1^{\mathrm{dyn}}(6)$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Our next result is as follows.

Lemma 5. *The ten points $P_0, \ldots, P_9$ are the only rational points whose images in Pic_C are in the saturation of the subgroup described in the previous lemma.*

Proof. We use Chabauty's method (see for example [3, 4, 14, 25]) for the proof. Recall that there is a pairing

$$\Omega^1_J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p \, , \qquad (\omega, Q) \longmapsto \int_0^Q \omega$$

that induces a perfect $\mathbb{Q}_p$-bilinear pairing

$$\Omega^1_J(\mathbb{Q}_p) \times J_1(\mathbb{Q}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow \mathbb{Q}_p \, ,$$

where $J_1(\mathbb{Q}_p)$ denotes the kernel of reduction. If $G \subset J(\mathbb{Q}_p)$ is a subgroup of rank less than $\dim J = 4$, then there must be a nonzero differential ω that kills G under this pairing. Note that ω then also kills the saturation

$$\bar{G} = \{P \in J(\mathbb{Q}_p) : nP \in G \text{ for some } n \geq 1\}$$

of G. We will apply this with $p = 5$ and G the subgroup generated by the known rational points as above.

For points in the kernel of reduction, the integral can be evaluated by formally integrating the power series representing ω in terms of a system of local parameters at the origin and then plugging in the values at Q of these parameters. For practical computations, it is convenient to use the canonical identification $\Omega^1_J(\mathbb{Q}_p) \cong \Omega^1_C(\mathbb{Q}_p)$.

Let $P' \in C(\mathbb{Q})$ be a fixed base-point. Let $Q \in J_1(\mathbb{Q}_p)$. Then Q is represented by a divisor of the form $(Q_1 + Q_2 + Q_3 + Q_4) - 4P'$, where the points $Q_j \in C(\bar{\mathbb{Q}}_p)$ all reduce to P' modulo the prime above p in their field of definition. Let τ be a uniformizer at P' that reduces mod p to a uniformizer at the reduction of P'. The differential ω can be written as $\phi(\tau) \, d\tau$ with a power series $\phi \in \mathbb{Q}_p[\![T]\!]$. Let

$$\lambda = \lambda_1 T + \lambda_2 T^2 + \ldots$$

be its formal integral. Then

$$\int_0^Q \omega = \sum_{j=1}^4 \lambda\big(\tau(Q_j)\big) = \sum_{n=1}^\infty \lambda_n \sum_{j=1}^4 \tau(Q_j)^n \,;$$

the series converges in $\mathbb{Q}_p$. Note that the power sums can be computed from the coefficients of the characteristic polynomial

$$\big(X - \tau(Q_1)\big)\big(X - \tau(Q_2)\big)\big(X - \tau(Q_3)\big)\big(X - \tau(Q_4)\big)\,,$$

which lie in the field of definition of Q.

In our concrete case, we take $P' = P_1$. Applying LLL to the kernel of the reduction map $\bigoplus_{j \neq 1} \mathbb{Z}(P_j - P_1) \to J(\mathbb{F}_5)$, we find a basis of $G \cap J_1(\mathbb{Q}_5)$, given by

$$D_1 = P_7 - P_9$$
$$D_2 = P_0 - 6P_1 + 2P_5 + P_7 + P_8 + P_9$$
$$D_3 = P_0 - 3P_1 + 2P_2 + P_4 + P_6 - P_7 - P_8$$

For each of these, we find D_j' such that $D_j \sim D_j' - 4P'$ and D_j' is effective of degree 4, with points reducing to P'. The point $P' = P_1$ has coordinates $(u, w) = (0, -1)$; we can choose u as a uniformizer at P' and its reduction. The space of regular differentials is spanned by

$$\omega_0 = \frac{du}{\frac{\partial}{\partial w} G(u, w)}, \quad \omega_1 = u\,\omega_0, \quad \omega_2 = w\,\omega_0, \quad \text{and} \quad \omega_3 = uw\,\omega_0\,.$$

We expand each ω_i as a power series in u times du and let $\lambda_i \in u\mathbb{Q}[\![u]\!]$ be its formal integral. Then we evaluate each λ_i at each D_j' as described above. We determine the kernel of the resulting matrix, which gives us the differential ω that kills our subgroup G. We find that reduced mod 5, this differential is $\bar\omega = \bar\omega_2$. It vanishes at the points where $w = 0$ or $u = \infty$. There are two such points in $C(\mathbb{F}_5)$, namely $(\infty, -1)$ and $(\infty, 0)$. At the former, $\bar\omega$ vanishes to first order, which implies that there are at most two rational points in that residue class (see for example [25, Prop. 6.3]). Since we have the points $P_7 = (\infty, -1)$ and $P_9 = (-4/5, -1)$, these must be all the rational points in this residue class. At $(\infty, 0)$, we compute explicitly that the logarithm λ that vanishes on $C(\mathbb{Q})$ on this residue class is

$$\lambda = \gamma\tau\big(1 - (2 + O(5))5\tau + O(5^2)\big)$$

with some constant $\gamma \neq 0$, where 5τ is the uniformizer w at $(\infty, 0)$. So λ has a single zero on this residue class, which is taken care of by $P_3 = (\infty, 0)$. On all other points in $C(\mathbb{F}_5)$, $\bar\omega$ does not vanish, hence there can be at most one rational point in each of these residue classes. Since it is easily checked that $\{P_0, \ldots, P_9\} \to C(\mathbb{F}_5)$ is surjective, this shows that there are no other points P in $C(\mathbb{Q})$ such that $P - P'$ is in G. In fact, there is no such point that maps into the saturation of G in $J(\mathbb{Q}_5)$

(since ω kills $\bar{G}$). So there is no rational point on C mapping into the saturation of G other than those already known. $\qquad\square$

Theorem 6. *If the rank of $J(\mathbb{Q})$ is 3, then $X_0^{\mathrm{dyn}}(6)$ has only the ten rational points listed above. In particular, it then follows that the only rational points on $X_1^{\mathrm{dyn}}(6)$ are the cusps, so that there is no cycle of exact length 6 consisting of rational numbers under an iteration $x \mapsto x^2 + c$.*

Proof. If $J(\mathbb{Q})$ has rank 3, then $J(\mathbb{Q})$ is the saturation of G, the subgroup generated by degree 0 divisors supported on the known rational points, since the latter then has finite index in $J(\mathbb{Q})$. The previous lemma then shows that there are no other rational points on $X_0^{\mathrm{dyn}}(6)$ than those already known. None of the non-cuspidal points among these lift to a rational point on $X_1^{\mathrm{dyn}}(6)$, so the latter curve can have no non-cuspidal rational points. A rational 6-cycle would give rise to a non-cuspidal rational point on this curve, so such a rational 6-cycle cannot exist. $\qquad\square$

4. Bounding the Rank

It remains to show that the rank of $J(\mathbb{Q})$ is 3. We know that the rank is at least 3, so it suffices to show that it is at most 3.

The standard procedure for obtaining an upper bound for the rank is a descent on the Jacobian. However, the complexity of this quickly becomes prohibitive when the genus is not very small and the curve does not have any helpful special features. For example, 2-descent on Jacobians of general non-hyperelliptic genus 3 curves is still in its infancy and so far has been successful in only one example (assuming GRH for the computation). Here, we have a curve of genus 4, and it appears that there are no helpful special properties, see Lemma 2 above. Usually, our best bet is a 2-descent, and for this, the most promising approach seems to be to look at the odd theta characteristics (whose differences generate the 2-torsion subgroup). On a curve of genus 4, there are 120 of them; they correspond to $(1, 1)$-forms on $\mathbb{P}^1 \times \mathbb{P}^1$ that meet the curve tangentially in three points (more precisely, the intersection divisor is twice an effective divisor of degree 3). We can set up the scheme describing these; after a Gröbner basis computation, we find that it has one rational point, and the other 119 points form a single Galois orbit. This means that in order to do anything in the direction of a 2-descent, we would have to compute the ideal class group and fundamental units of a number field of degree 119. Before we are able to perform such computations (even if we allow ourselves to assume GRH), we need very substantial progress in the development of suitable algorithms.

The result on the Galois orbits on the odd theta characteristics can be obtained faster by computing the Gröbner bases of the scheme over $\mathbb{F}_5$ and over $\mathbb{F}_{13}$. We first note that $1 + u + w$ gives rise to the point defined over $\mathbb{Q}$ (the $(1, 1)$-forms are

of the form $a + bu + cw + duw$). Over $\mathbb{F}_5$, the remaining 119 points split into nine orbits of length 7 and four orbits of length 14, whereas over $\mathbb{F}_{13}$, they split into seven orbits of length 17. Since these partitions must refine the orbit partition over $\mathbb{Q}$, there must be a single orbit of length 119.

We can extract some more information. First note that the theta characteristics can be identified with the 2-torsion subgroup $J[2]$ (by sending the unique odd theta characteristic that is defined over $\mathbb{Q}$ to the origin). The Galois action on $J[2]$ must then have orbits of lengths 1 and 119. We will determine the image of Galois in $\mathrm{Sp}_8(\mathbb{F}_2)$ and deduce that the remaining 136 elements also form a single orbit.

First note that the Galois group cannot surject onto $\mathrm{Sp}_8(\mathbb{F}_2)$, since otherwise the Galois action on the non-zero 2-torsion points on J would be transitive. The Frobenius automorphisms at $p = 5$ and 13, acting on $J[2]$, have orders 14 and 17, as we saw above. Up to conjugation, $\mathrm{Sp}_8(\mathbb{F}_2)$ has only two proper subgroups whose order is a multiple of $14 \cdot 17$, namely $\Gamma = \mathrm{GO}_8^-(\mathbb{F}_p)$ of index 120 and $\mathrm{O}_8^-(\mathbb{F}_2)$ of index 240. The latter has no elements of order 14, so the image of Galois in $\mathrm{Sp}_8(\mathbb{F}_2)$ must be Γ.

Since the action of Γ on $J[2]$ has orbits of lengths 1, 119, and 136, our claim follows. It can be checked that the smallest faithful permutation representation of Γ has degree 119 (see [5] or the MAGMA script [26]), so that this is really the smallest possible degree of a number field that we can hope for in a 2-descent computation.

Note that we showed in Lemma 2 that J has no endomorphisms other than the multiplication-by-n maps, so that multiplication-by-2 is the isogeny $J \to J$ of lowest possible degree that can be used for a descent argument. There are no nontrivial Galois-stable subgroups of $J[2]$, so there are no 2-isogenies to other abelian varieties either.

A possible alternative approach to obtaining a bound for the rank assumes the (weak) Birch and Swinnerton-Dyer conjecture [27], plus standard conjectures on analytic continuation and functional equations of L-series, see for example [10, Conj. 3.1.1]. The conjecture predicts that the rank of $J(\mathbb{Q})$ is the same as the order of vanishing of the L-series $L(J, s) = L(C, s)$ at $s = 1$. In order to be able to evaluate the L-series and its derivatives there, we need to compute its coefficients a_n for values of n up to a suitable multiple of the square root of its conductor. Luckily, in our case the conductor $2^2 \cdot 8\,029\,187$ is not too large, so that we can actually perform the computation in reasonable time.

We use Tim Dokchitser's L-series package [6] in its MAGMA implementation. We will not need to find the Euler factor at the large bad prime (it is beyond the necessary range of coefficients). For the other bad prime 2, we found the Euler factor in Section 2. For the good primes, we need the Euler factor up to T^d, where $d = \lfloor \log_p m \rfloor$ and m is the number of coefficients required. This information can be

obtained by counting the number of points in $C(\mathbb{F}_{p^e})$ for $e = 1, \ldots, \min\{d, 4\}$. For a precision of 10^{-20}, we need 183997 coefficients (which we can compute in a day or so). We verify numerically that our L-series satisfies the functional equation it is supposed to satisfy (with sign -1). Then we find that the L-series and its first two derivatives vanish at $s = 1$ to the given precision, whereas $L'''(C, 1) = 0.83601 \ldots$ is clearly nonzero. Assuming (the first part of) the Birch and Swinnerton-Dyer conjecture for J, this implies that $\operatorname{rank} J(\mathbb{Q}) \le 3$. We therefore obtain our main result below.

Theorem 7. *Let J be the Jacobian of $X_0^{\mathrm{dyn}}(6)$. If the L-series $L(J, s)$ extends to an entire function and satisfies the standard functional equation, and if the Birch and Swinnerton-Dyer conjecture is valid for J, then there are no rational cycles of exact length 6 under $x \mapsto x^2 + c$.*

It would be very desirable to get some additional corroboration of the result by also verifying the second part of the Birch and Swinnerton-Dyer conjecture. From the information obtained in Section 2, we can deduce that the Tamagawa number at 2 is $c_2 = 4$, whereas all other Tamagawa numbers are 1. Since there is no torsion in the Mordell-Weil group (see Lemma 4), the conjecture would predict that

$$R\,\Omega\,\#\mathrm{III} = \frac{L'''(J,1)/3!}{4} = 0.03483 \ldots,$$

where R is the regulator of the Mordell-Weil group, Ω is the volume $\int_{J(\mathbb{R})} |\eta|$, where η is a generator of $H^0(\mathcal{J}, \Omega^4_{\mathcal{J}/\operatorname{Spec}\mathbb{Z}})$ for the Néron model $\mathcal{J}$ of J over $\mathbb{Z}$, and III is the Shafarevich-Tate group of J, conjectured to be finite, in which case its order is a square, since C has rational points, see [20].

Up to a small integral factor, Ω can be computed numerically as the determinant of integrals $\int_\gamma \omega$, where γ runs through a basis of the part of the homology $H_1(C(\mathbb{C}), \mathbb{Z})$ that is fixed by complex conjugation, and ω runs through a basis of the $\mathbb{Q}$-defined differentials on C, like the ω_j used in Section 3. This computation does not present any essential problems. See for example [7, § 3.5].

The computation of the regulator is a different matter. For this, we would need to compute the canonical height of points in $J(\mathbb{Q})$. For Jacobians of genus 2 curves, there is an explicit theory of heights (see [8, 23, 24]) that allows us to do that. For Jacobians of curves of genus ≥ 3, however, no comparable results seem to be currently available. So for the time being, we have to leave the numerical verification of the full Birch and Swinnerton-Dyer conjecture for J as a challenge problem.

5. What Next?

Without fundamentally new ideas, it seems unlikely that we can make our result unconditional in the foreseeable future. In another direction, it looks rather hopeless to try to get a similar result for $X_0^{\mathrm{dyn}}(7)$. This curve has genus 16 and bad reduction at the 35-digit prime $p = 84562\,62122\,13597\,75358\,18884\,16725\,49561$ and possibly at 2. In any case, the conductor will be very large (at least p) and so there will be no reasonable chance to use the L-series numerically to obtain information on the rank. It might still be possible to get some information on the subgroup of the Jacobian generated by the cusps (e.g., by making use of dynamical units). It will be very hard, however, to use this information for a Chabauty argument, for example.

Another question is how the large bad primes can be explained or even predicted. We have 3701 for $N = 5$ (the only bad prime for $X_0^{\mathrm{dyn}}(5)$, see [9]; their model is also bad at 2, but this can easily be repaired), 8029187 for $N = 6$ and the 35-digit prime above for $N = 7$. Note that unless we can shed light on this question, it is likely to be very hard to try and prove algebraically that $Y_1^{\mathrm{dyn}}(N)$ is smooth, since such a proof must break down when the characteristic is one of these primes.

The following could be a possible line of attack for a proof that $Y_1^{\mathrm{dyn}}(N)(\mathbb{Q})$ is empty for large N. There is a good description of the formal neighborhoods of the cusps on $X_1^{\mathrm{dyn}}(N)$, using symbolic dynamics. If we could use this to prove, for any odd prime p, that the cusp is the only rational point in its residue class mod p, and also to prove a similar statement modulo a suitable power of 2, then this would imply that a parameter $c \in \mathbb{Q}$ that allows for a cycle of exact length N of rational numbers must be essentially integral (more precisely, its denominator must divide a fixed power of 2). It is then fairly easy to show that N is bounded.

For example, assume that $c \in \mathbb{Z}$ and x is in a cycle. Then x must also be an integer. If $c > 0$, we have $x^2 + c > |x|$, so there cannot be a cycle. For $c = 0$, the only possibilities are $x = 0$ and $x = 1$. For $c = -1$, the only possibilities are $x = 0$ and $x = -1$. If $c < -1$, we have $x^2 + c > |x|$ whenever $|x| \geq \sqrt{|c|} + 1$. So we must have $|x| < \sqrt{|c|} + 1$. But then we also need that $|x^2 + c| < \sqrt{|c|} + 1$, which implies that $\sqrt{|c| - \sqrt{|c|} - 1} < |x| < \sqrt{|c|} + 1$. This interval has length less than 2, so there are at most two possible values for $|x|$. This implies that there must be either a fixed point or a cycle of length 2. Indeed, for any $x \in \mathbb{Z}$, x is a fixed point for $c = x - x^2$, and $(x, -x - 1)$ is a 2-cycle for $c = -x^2 - x - 1$.

In the more general case when $m^2 c \in \mathbb{Z}$ for some fixed integer $m \geq 1$, we can use similar arguments to show that the cycle must be contained in a union of a bounded number of intervals whose lengths are bounded. Since the possible values of x are in the set $\frac{1}{m}\mathbb{Z}$, there must be a bound on their number.

In the spirit of the methods used in this paper, the necessary result for odd primes p would follow from the following two statements.

(1) The cuspidal group (i.e., the group generated by degree zero divisors supported at the cusps) is of finite index in the Mordell-Weil group of the Jacobian of $X_1^{\mathrm{dyn}}(N)$.
(2) For every cusp P, there is a regular differential on $X_1^{\mathrm{dyn}}(N)$, defined over $\mathbb{Q}_p$, that kills the cuspidal group and whose reduction mod p does not vanish at P.

However, we need some additional ideas to approach a proof of either one of these.

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Erg. Math. Grenzgeb. 3. Folge, Bd. 21 (Springer, Berlin Heidelberg, 1990).

[2] T. Bousch, *Sur quelques problèmes de dynamique holomorphe*, PhD thesis (Université de Paris-Sud, Centre d'Orsay, 1992).

[3] C. Chabauty, 'Sur les points rationnels des courbes algébriques de genre supérieur à l'unité', *C. R. Acad. Sci. Paris* 212 (1941) 882–885.

[4] R.F. Coleman, 'Effective Chabauty', *Duke Math. J.* 52 (1985) 765–770.

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of finite groups* (Oxford University Press, Eynsham, 1985).

[6] T. Dokchitser, 'Computing special values of motivic L-functions', *Experiment. Math.* 13 (2004) 137–149.

[7] E.V. Flynn, F. Leprévost, E.F. Schaefer, W.A. Stein, M. Stoll, and J.L. Wetherell, 'Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves', *Math. Comp.* 70 (2001) 1675–1697.

[8] E.V. Flynn, 'An explicit theory of heights', *Trans. Amer. Math. Soc.* 347 (1995) 3003–3015.

[9] E.V. Flynn, B. Poonen, and E.F. Schaefer, 'Cycles of quadratic polynomials and rational points on a genus-2 curve', *Duke Math. J.* 90 (1997) 435–463.

[10] W.W.J. Hulsbergen, *Conjectures in arithmetic algebraic geometry,* 2nd revised edition, (Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden, 1994).

[11] A.G. Khovanskii, 'Newton polyhedra and the genus of complete intersections', *Funct. Anal. and Appl.* 12 (1978) 38–46.(Translated from Russian).

[12] E. Lau and D. Schleicher, 'Internal addresses in the Mandelbrot set and irreducibility of polynomials', SUNY Stony Brook Institute for Mathematical Sciences Preprint #1994–19. See also: arXiv:math/9411238v2 [math.DS]

[13] MAGMA is described in W. Bosma, J. Cannon, and C. Playoust, 'The Magma algebra system I: The user language', *J. Symb. Comp.* 24 (1997) 235–265. (Also see the Magma home page at
http://www.maths.usyd.edu.au:8000/u/magma/ .)

[14] W. McCallum and B. Poonen, 'The method of Chabauty and Coleman', Preprint (2007). Available at
http://math.berkeley.edu/~poonen/papers/chabauty.pdf

[15] P. Morton, 'On certain algebraic curves related to polynomial maps', *Compositio Math.* 103 (1996) 319–350.

[16] P. Morton, 'Arithmetic properties of periodic points of quadratic maps, II', *Acta Arith.* 87 (1998) 89–102.

[17] W. Narkiewicz, 'Polynomial cycles in algebraic number fields', *Colloq. Math.* 58 (1989) 151–155.

[18] B. Poonen, 'The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture', *Math. Z.* 228 (1998) 11–29.

[19] B. Poonen, E.F. Schaefer, and M. Stoll, 'Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$', *Duke Math. J.* 137 (2007) 103–158.

[20] B. Poonen and M. Stoll, 'The Cassels-Tate pairing on polarized abelian varieties', *Ann. of Math.* 150 (1999) 1109–1149.

[21] J.H. Silverman, *The arithmetic of dynamical systems*, Springer Graduate Texts in Mathematics 241, (Springer, New York, 2007).

[22] M. Stoll, 'Two simple 2-dimensional abelian varieties defined over **Q** with Mordell-Weil group of rank at least 19', *C. R. Acad. Sci. Paris* 321 (1995) 1341–1345.

[23] M. Stoll, 'On the height constant for curves of genus two', *Acta Arith.* 90 (1999) 183–201.

[24] M. Stoll, 'On the height constant for curves of genus two, II', *Acta Arith.* 104 (2002) 165–182.

[25] M. Stoll, 'Independence of rational points on twists of a given curve', *Compositio Math.* 142 (2006) 1201–1214.

[26] M. Stoll, MAGMA script accompanying this paper. Available at
http://www.faculty.jacobs-university.de/mstoll/magma/scripts/Xdyn06.magma

[27] J. Tate, 'On the conjectures of Birch and Swinnerton-Dyer and a geometric analog', *Séminaire Bourbaki*, Vol. 9, Exp. No. 306, (Soc. Math. France, Paris, 1995) 415–440.

[28] W.C. Waterhouse and J.S. Milne, 'Abelian varieties over finite fields', *1969 Number Theory Institute*, Stony Brook, N.Y., 1969, Proc. Sympos. Pure Math. 20, (Amer. Math. Soc., Providence, 1971) 53–64.

School of Engineering and Science, Jacobs University Bremen, Campus Ring 1, 28759 Bremen, Germany.

E-mail address: m.stoll@jacobs-university.de