Rational Six-Cycles Under Quadratic Iteration

Michael Stoll
Universität Bayreuth

GTEM 3rd annual meeting, University of Warwick
September 8, 2009

Quadratic Iteration

Let $f(c,x) = x^2 + c \in \mathbb{Z}[c,x]$ and define

$$f^0(c,x) = x\,, \qquad f^{n+1}(c,x) = f(c, f^n(c,x)) = (f^n(c,x))^2 + c\,.$$

$(x_0, x_1, \ldots, x_{N-1}) \in \mathbb{Q}^N$ is a rational N-cycle if there is $c \in \mathbb{Q}$ such that

$$x_1 = f(c, x_0)\,, \quad x_2 = f(c, x_1)\,, \quad \ldots\,, \quad x_{N-1} = f(c, x_{N-2})$$
$$\text{and} \qquad x_0 = f(c, x_{N-1})\,,$$

and $x_0, x_1, \ldots, x_{N-1}$ are pairwise distinct.

Question.

For which $N \geq 1$ do there exist rational N-cycles?

Conjecture (Morton, Silverman).

Rational N-cycles do not exist for N large.

Dynamic Modular Curves

Pairs (c, x) such that the sequence $\left(f^n(c, x)\right)_{n \geq 0}$
has (not necessarily minimal) period N
correspond to points on the affine plane curve given by

$$f^N(c, x) - x = 0\,.$$

Dividing off shorter periods, we obtain

$$Y_1^{\mathrm{dyn}}(N) : \Phi_N^*(c, x) := \prod_{d \mid N} \left(f^d(c, x) - x\right)^{\mu(N/d)} = 0\,.$$

It can be shown that $Y_1^{\mathrm{dyn}}(N)$ is smooth and geometrically irreducible;
we denote by $X_1^{\mathrm{dyn}}(N)$ its smooth projective model.
The points in $X_1^{\mathrm{dyn}}(N) \setminus Y_1^{\mathrm{dyn}}(N)$ are called cusps; all of them are rational.

Question, new version.

For which N are there non-cuspidal rational points on $X_1^{\mathrm{dyn}}(N)$?

Small N

It is easy to see that $X_1^{\mathrm{dyn}}(1)$ and $X_1^{\mathrm{dyn}}(2)$ are isomorphic to $\mathbb{P}^1$.
This is still true (but less obvious) for $X_1^{\mathrm{dyn}}(3)$.
So there are lots of rational fixed points, 2- and 3-cycles.

The curve $X_1^{\mathrm{dyn}}(4)$ has genus 2;
it turns out that it is isomorphic to $X_1(16)$,
and all its rational points are cusps.
So there are no rational 4-cycles (P. Morton 1998).

The genus of $X_1^{\mathrm{dyn}}(N)$ grows very fast ($N = 5 \to 14$, $N = 6 \to 34$, $\dots$);
it is not feasible to work with these curves directly when $N \geq 5$.

The Quotient Curve

Observe that $(c, x) \mapsto (c, x^2 + c)$ induces an action of $\mathbb{Z}/N\mathbb{Z}$ on $X_1^{\text{dyn}}(N)$; we denote by $X_0^{\text{dyn}}(N)$ the quotient curve.

If we can find the rational points on $X_0^{\text{dyn}}(N)$,
we can determine $X_1^{\text{dyn}}(N)(\mathbb{Q})$
and hence decide if there are rational N-cycles.

The curve $X_0^{\text{dyn}}(5)$ has genus 2.
Its Jacobian has Mordell-Weil rank 1,
and Chabauty's method can be used to find $X_0^{\text{dyn}}(5)(\mathbb{Q})$.
The result implies that there are no rational 5-cycles
(Flynn-Poonen-Schaefer 1997).

The Case $N = 6$

The curve $X_0^{\text{dyn}}(6)$ is non-hyperelliptic of genus 4.
An affine equation in terms of c and the trace

$$t = x + f(c,x) + f^2(c,x) + \cdots + f^5(c,x)$$

is given by

$$\begin{aligned}256(t^3+t^2-t-1)c^3 + 16(9t^5+7t^4+10t^3+30t^2-19t-37)c^2 \\ + 8(3t^7+t^6+2t^5+2t^4-17t^3+69t^2+52t-48)c \\ + t^9-t^8+2t^7+14t^6+49t^5+175t^4+140t^3+196t^2+448t = 0\end{aligned}$$

It has a smooth model in $\mathbb{P}^1_u \times \mathbb{P}^1_w$ given by

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

where

$$c = \frac{(-u^3-2u^2+5u-10)uw-u^4+3u^3+8u^2-10u+12}{4u^2(uw+u-3)}, \quad t = \frac{2}{u} - 1\,.$$

The Points

We easily find the following ten rational points on $C = X_0^{\text{dyn}}(6)$.

	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	$-\frac{7}{2}$	$-\frac{71}{48}$

$P_0, \ldots, P_4$ are the images of the cusps on $X_1^{\text{dyn}}(6)$.
$P_5, \ldots, P_9$ do not lift to rational points on $X_1^{\text{dyn}}(6)$.
P_9 is the image of six points defined over $\mathbb{Q}(\sqrt{33})$;
the fibers above the other points form single Galois orbits.

Goal. Show that $C(\mathbb{Q}) = \{P_0, P_1, \ldots, P_9\}$!

A Subgroup of the Mordell-Weil Group

Let J be the Jacobian of C,
and we denote by Γ the subgroup of $J(\mathbb{Q})$ generated by the $[P_i - P_j]$.

Theorem.

- $J(\mathbb{Q})$ is torsion-free.
- $\Gamma \cong \mathbb{Z}^3$, and Γ is generated by divisors supported in $\{P_0, P_1, P_2, P_4\}$.

The first assertion follows from $\gcd\bigl(\#J(\mathbb{F}_7), \#J(\mathbb{F}_{13})\bigr) = 1$.
For the second assertion, we consider the homomorphism

$$\Bigl(\bigoplus_{j=0}^{9} \mathbb{Z}P_j\Bigr)^0 \longrightarrow J(\mathbb{Q}) \longrightarrow \bigoplus_{p\in\{3,5,7,11,13\}} J(\mathbb{F}_p)\,.$$

We check that the small elements of its kernel give principal divisors;
the image shows that the rank is at least 3.

Points Mapping to G

We take P_1 as base point for the embedding $\iota : C \to J$.

The saturation of the group $\Gamma \subset J(\mathbb{Q})$ is

$$\bar{\Gamma} = \{D \in J(\mathbb{Q}) : nD \in \Gamma \text{ for some } n \geq 1\}.$$

Theorem.

$$\{P \in C(\mathbb{Q}) : \iota(P) \in \bar{\Gamma}\} = \{P_0, P_1, \ldots, P_9\}$$

For the proof, we use the Chabauty-Coleman method.

Chabauty (1)

Let p be a prime number.
There is a pairing

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

which induces a perfect pairing of $\mathbb{Q}_p$-vector spaces

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

Since Γ has rank $< 4 = \dim_{\mathbb{Q}_p} \Omega^1_J(\mathbb{Q}_p)$,
there is $0 \neq \omega \in \Omega^1_J(\mathbb{Q}_p) \cong \Omega^1_C(\mathbb{Q}_p)$ with $\langle \omega, \bar{\Gamma} \rangle = 0$.

We take $p = 5$ and find for the reduction mod 5 of ω that

$$\bar{\omega} = w \, \frac{du}{\frac{\partial}{\partial w} G(u, w)} \in \Omega^1_C(\mathbb{F}_5)\,.$$

Chabauty (2)

Theorem.

Let $P \in C(\mathbb{F}_5)$ such that $v_P(\bar{\omega}) \le 2$.

Then $\quad \#\{P' \in C(\mathbb{Q}) : \bar{P}' = P, \iota(P') \in \bar{\Gamma}\} \le v_P(\bar{\omega}) + 1$.

Here, $\{P_0, \ldots, P_9\}$ surjects onto $C(\mathbb{F}_5)$, and

- $v_{\bar{P}_j}(\bar{\omega}) = 0$ for $j \neq 3, 7, 9$;
- $v_{\bar{P}_7}(\bar{\omega}) = 1$ and $\bar{P}_7 = \bar{P}_9$.

So a point $P \in C(\mathbb{Q}) \setminus \{P_0, \ldots, P_9\}$ with $\iota(P) \in \bar{\Gamma}$ must satisfy $\bar{P} = \bar{P}_3$.

Computation $\Rightarrow P \mapsto \langle \omega, \iota(P) \rangle$ has only one zero on this residue class.

This finishes the proof of the theorem.

A Sufficient Condition

Recall the **Theorem** we proved:

$$\{P \in C(\mathbb{Q}) : \iota(P) \in \bar{\Gamma}\} = \{P_0, P_1, \ldots, P_9\}$$

Therefore, $\bar{\Gamma} = J(\mathbb{Q})$ implies that $C(\mathbb{Q}) = \{P_0, \ldots, P_9\}$ and then that there are no rational 6-cycles.

For this it is sufficient (and necessary) that $\operatorname{rank} J(\mathbb{Q}) \leq 3$.

So we need an upper bound for the Mordell-Weil rank.
The usual approach (2-descent) appears to be infeasible.
We use the BSD rank conjecture instead.

The L-Series (1)

We want to compute $L'''(J,1)$ (and verify it is nonzero).

We assume that $L(J,s)$ extends to an entire function
and satisfies the usual functional equation.

We need to know the conductor and the bad Euler factors.

The only primes of bad reduction for C are 2 and 8 029 187.
At 8 029 187, our model is regular and has only a node.
At 2, we compute a regular model. We obtain:

- The conductor is $2^2 \cdot 8\,029\,187$;
- the Euler factor at 2 is $(1+T)^2(1+T+2T^2)^2$.

The L-Series (2)

Since the conductor is not too large,
we can compute enough coefficients of $L(J, s)$
to find $L'''(J, 1)$ to reasonable precision.

We check numerically that the functional equation (with sign -1) is OK.

We then use Tim Dokchitser's package to evaluate

$$L'''(J, 1) \approx 0.83601\ldots \neq 0\,.$$

We see that the BSD rank conjecture for J implies that $\bar{\Gamma} = J(\mathbb{Q})$.

Conclusion

Theorem.

If the L-series of J extends to an entire function
and satisfies the usual functional equation,
and if the BSD rank conjecture holds for J,

then there are no rational 6-cycles.

Remarks

The approach used here for finding $C(\mathbb{Q})$ is applicable when

- we can find generators of a finite index subgroup of $J(\mathbb{Q})$;
- $\operatorname{rank} J(\mathbb{Q}) < g(C)$, the genus of C;
- the conductor is not too large.

Given the first two conditions, we can use Chabauty's method, perhaps combined with a Mordell-Weil sieve, to find the rational points on the curve.

The third condition allows us to verify the first condition, assuming the BSD rank conjecture for J.

What About $N = 7$?

If we attempt to extend our approach to rational 7-cycles, we run into a number of difficulties —

- $X_0^{\mathrm{dyn}}(7)$ has genus 16;
- $X_0^{\mathrm{dyn}}(7)$ has bad reduction at

$$p = 84562\,62122\,13597\,75358\,18884\,16725\,49561$$

(and perhaps at 2).

The first implies that computations will be rather involved, the second implies that the conductor is too large.

Reference

M. Stoll, *Rational 6-cycles under iteration of quadratic maps*, LMS J. Comput. Math. **11** (2008), 367–380.