UNIVERSITÄT BAYREUTH

An Application of “Selmer Group Chabauty” to Arithmetic Dynamics

Michael Stoll

Universität Bayreuth

MIT

November 19, 2019

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x] .$$

The iterates of f_c are

$f_c^{\circ 0}(x) = x ,$

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

The iterates of f_c are

$$f_c^{\circ 0}(x) = x\,, \quad f_c^{\circ 1}(x) = f_c(x) = x^2 + c\,,$$

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

The iterates of f_c are

$$f_c^{\circ 0}(x) = x\,, \quad f_c^{\circ 1}(x) = f_c(x) = x^2 + c\,, \quad f_c^{\circ 2}(x) = f_c(f_c(x)) = (x^2 + c)^2 + c\,, \quad \ldots\,,$$

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

The iterates of f_c are

$$f_c^{\circ 0}(x) = x\,, \quad f_c^{\circ 1}(x) = f_c(x) = x^2 + c\,, \quad f_c^{\circ 2}(x) = f_c(f_c(x)) = (x^2 + c)^2 + c\,, \quad \ldots\,,$$
$$f_c^{\circ (n+1)}(x) = f_c(f_c^{\circ n}(x)) = f_c^{\circ n}(f_c(x))\,, \quad \ldots\,.$$

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

The iterates of f_c are

$$f_c^{\circ 0}(x) = x\,, \quad f_c^{\circ 1}(x) = f_c(x) = x^2 + c\,, \quad f_c^{\circ 2}(x) = f_c(f_c(x)) = (x^2 + c)^2 + c\,, \quad \ldots\,,$$
$$f_c^{\circ (n+1)}(x) = f_c(f_c^{\circ n}(x)) = f_c^{\circ n}(f_c(x))\,, \quad \ldots\,.$$

Question.
For which c and n is $f_c^{\circ n}$ irreducible in $\mathbb{Q}[x]$?

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

The iterates of f_c are

$$f_c^{\circ 0}(x) = x\,, \quad f_c^{\circ 1}(x) = f_c(x) = x^2 + c\,, \quad f_c^{\circ 2}(x) = f_c(f_c(x)) = (x^2 + c)^2 + c\,, \quad \ldots\,,$$
$$f_c^{\circ(n+1)}(x) = f_c(f_c^{\circ n}(x)) = f_c^{\circ n}(f_c(x))\,, \quad \ldots\,.$$

Question.
For which c and n is $f_c^{\circ n}$ irreducible in $\mathbb{Q}[x]$?

Conjecture.
For all $c \in \mathbb{Q}$, if $f_c^{\circ 2}$ is irreducible, then $f_c^{\circ n}$ is irreducible for all n.

Iterates of quadratic polynomials

Let $c \in \mathbb{Q}$ and define

$$f_c(x) = x^2 + c \in \mathbb{Q}[x]\,.$$

The iterates of f_c are

$$f_c^{\circ 0}(x) = x\,, \quad f_c^{\circ 1}(x) = f_c(x) = x^2 + c\,, \quad f_c^{\circ 2}(x) = f_c(f_c(x)) = (x^2 + c)^2 + c\,, \quad \ldots\,,$$
$$f_c^{\circ(n+1)}(x) = f_c(f_c^{\circ n}(x)) = f_c^{\circ n}(f_c(x))\,, \quad \ldots\,.$$

Question.
For which c and n is $f_c^{\circ n}$ irreducible in $\mathbb{Q}[x]$?

Conjecture.
For all $c \in \mathbb{Q}$, if $f_c^{\circ 2}$ is irreducible, then $f_c^{\circ n}$ is irreducible for all n.

Remark.
$f_c^{\circ 2}$ reducible $\iff$ $c = -t^2$ or $1/c = 4t^2(t^2 - 1)$ with $t \in \mathbb{Q}$.

A criterion

Lemma.
Assume that $n \geq 1$, $f_c^{\circ n}$ is irreducible and $f_c^{\circ(n+1)}$ is reducible.
Then the constant term of $f_c^{\circ(n+1)}$ must be a square.

A criterion

Lemma.
Assume that $n \geq 1$, $f_c^{\circ n}$ is irreducible and $f_c^{\circ(n+1)}$ is reducible.
Then the constant term of $f_c^{\circ(n+1)}$ must be a square.

Proof.
$f_c^{\circ(n+1)}(x) = f_c^{\circ n}(x^2 + c)$ is an even polynomial.

A criterion

Lemma.
Assume that $n \geq 1$, $f_c^{\circ n}$ is irreducible and $f_c^{\circ(n+1)}$ is reducible.
Then the constant term of $f_c^{\circ(n+1)}$ must be a square.

Proof.
$f_c^{\circ(n+1)}(x) = f_c^{\circ n}(x^2 + c)$ is an even polynomial.
So $x \mapsto -x$ induces an involution on the set of irreducible factors of $f_c^{\circ(n+1)}$.

A criterion

Lemma.
Assume that $n \geq 1$, $f_c^{\circ n}$ is irreducible and $f_c^{\circ(n+1)}$ is reducible.
Then the constant term of $f_c^{\circ(n+1)}$ must be a square.

Proof.
$f_c^{\circ(n+1)}(x) = f_c^{\circ n}(x^2 + c)$ is an even polynomial.
So $x \mapsto -x$ induces an involution on the set of irreducible factors of $f_c^{\circ(n+1)}$.
Fixed points of this involution correspond to factors of $f_c^{\circ n}$.

A criterion

Lemma.
Assume that $n \geq 1$, $f_c^{\circ n}$ is irreducible and $f_c^{\circ(n+1)}$ is reducible.
Then the constant term of $f_c^{\circ(n+1)}$ must be a square.

Proof.
$f_c^{\circ(n+1)}(x) = f_c^{\circ n}(x^2 + c)$ is an even polynomial.
So $x \mapsto -x$ induces an involution on the set of irreducible factors of $f_c^{\circ(n+1)}$.
Fixed points of this involution correspond to factors of $f_c^{\circ n}$.
So when $f_c^{\circ(n+1)}$ is reducible, it factors as $f_c^{\circ(n+1)}(x) = h(x)h(-x)$,
and $f_c^{\circ(n+1)}(0) = h(0)^2$. (Note that $\deg h$ is even, since $n \geq 1$.) ❑

A criterion

Lemma.
Assume that $n \geq 1$, $f_c^{\circ n}$ is irreducible and $f_c^{\circ(n+1)}$ is reducible.
Then the constant term of $f_c^{\circ(n+1)}$ must be a square.

Proof.
$f_c^{\circ(n+1)}(x) = f_c^{\circ n}(x^2 + c)$ is an even polynomial.
So $x \mapsto -x$ induces an involution on the set of irreducible factors of $f_c^{\circ(n+1)}$.
Fixed points of this involution correspond to factors of $f_c^{\circ n}$.
So when $f_c^{\circ(n+1)}$ is reducible, it factors as $f_c^{\circ(n+1)}(x) = h(x)h(-x)$,
and $f_c^{\circ(n+1)}(0) = h(0)^2$. (Note that $\deg h$ is even, since $n \geq 1$.) ❑

Remark.
$f_c^{\circ(n+1)}$ can be irreducible even though its constant term is a square;
e.g., $f_{1/3}^{\circ 2}(x) = x^4 + \frac{2}{3}x^2 + \frac{4}{9}$ is irreducible.

What is known

We define $A_n(c)$ to be the constant term of $f_c^{\circ n}$:

$$A_0(c) = 0\,, \quad A_1(c) = c\,, \quad A_2(c) = c^2 + c\,, \quad \ldots, \quad A_{n+1}(c) = A_n(c)^2 + c\,, \quad \ldots.$$

What is known

We define $A_n(c)$ to be the constant term of $f_c^{\circ n}$:

$$A_0(c) = 0\,, \quad A_1(c) = c\,, \quad A_2(c) = c^2 + c\,, \quad \ldots\,, \quad A_{n+1}(c) = A_n(c)^2 + c\,, \quad \ldots\,.$$

Proposition.
Let $c \in \mathbb{Q}$. Then

❶ $A_3(c)$ is a square $\iff$ $c = 0$.

❷ $A_4(c)$ is a square $\iff$ $c \in \{0, -1\}$.

What is known

We define $A_n(c)$ to be the constant term of $f_c^{\circ n}$:

$$A_0(c) = 0\,, \quad A_1(c) = c\,, \quad A_2(c) = c^2 + c\,, \quad \ldots, \quad A_{n+1}(c) = A_n(c)^2 + c\,, \quad \ldots.$$

Proposition.
Let $c \in \mathbb{Q}$. Then

❶ $A_3(c)$ is a square $\iff$ $c = 0$.

❷ $A_4(c)$ is a square $\iff$ $c \in \{0, -1\}$.

Proof (sketch; [Jones, Hindes et al.]).
$y^2 = A_3(x)$ is a rank-zero elliptic curve,
$y^2 = A_4(x)$ is a hyperelliptic genus-3 curve with rank-zero Jacobian. ❑

What is known

We define $A_n(c)$ to be the constant term of $f_c^{\circ n}$:

$$A_0(c) = 0\,, \quad A_1(c) = c\,, \quad A_2(c) = c^2 + c\,, \quad \ldots\,, \quad A_{n+1}(c) = A_n(c)^2 + c\,, \quad \ldots\,.$$

Proposition.

Let $c \in \mathbb{Q}$. Then

❶ $A_3(c)$ is a square $\iff$ $c = 0$.

❷ $A_4(c)$ is a square $\iff$ $c \in \{0, -1\}$.

Proof (sketch; [Jones, Hindes et al.]).

$y^2 = A_3(x)$ is a rank-zero elliptic curve,

$y^2 = A_4(x)$ is a hyperelliptic genus-3 curve with rank-zero Jacobian. ❑

Conclusion.

If $c \in \mathbb{Q}$ is such that $f_c^{\circ 2}$ is irreducible, then $f_c^{\circ 4}$ is irreducible.

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.
Equivalently, $a_5(x)$ is a square only for $x = 0$, where $a_5(x) = x^{16} A_5(1/x)$.

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.
Equivalently, $a_5(x)$ is a square only for $x = 0$, where $a_5(x) = x^{16}A_5(1/x)$.
Write

$$C\colon y^2 = a_5(x) = x^{15} + (x^7 + (x^3 + (x+1)^2)^2)^2 ;$$

this is an odd degree hyperelliptic curve of genus $g = 7$.

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.
Equivalently, $a_5(x)$ is a square only for $x = 0$, where $a_5(x) = x^{16} A_5(1/x)$.
Write

$$C\colon y^2 = a_5(x) = x^{15} + (x^7 + (x^3 + (x+1)^2)^2)^2;$$

this is an odd degree hyperelliptic curve of genus $g = 7$.

Its Jacobian variety J has 2-Selmer rank 2,

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.
Equivalently, $a_5(x)$ is a square only for $x = 0$, where $a_5(x) = x^{16} A_5(1/x)$.
Write

$$C\colon y^2 = a_5(x) = x^{15} + (x^7 + (x^3 + (x+1)^2)^2)^2\,;$$

this is an odd degree hyperelliptic curve of genus $g = 7$.

Its Jacobian variety J has 2-Selmer rank 2,
but we are unable to find points of infinite order in $J(\mathbb{Q})$.
So standard Chabauty techniques cannot be applied.

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.
Equivalently, $a_5(x)$ is a square only for $x = 0$, where $a_5(x) = x^{16}A_5(1/x)$.
Write

$$C\colon y^2 = a_5(x) = x^{15} + (x^7 + (x^3 + (x+1)^2)^2)^2;$$

this is an odd degree hyperelliptic curve of genus $g = 7$.

Its Jacobian variety J has 2-Selmer rank 2,
but we are unable to find points of infinite order in $J(\mathbb{Q})$.
So standard Chabauty techniques cannot be applied.

We will instead use "Selmer Group Chabauty".

The goal

We want to show that $A_5(c)$ is a square only for $c = 0$.
Equivalently, $a_5(x)$ is a square only for $x = 0$, where $a_5(x) = x^{16} A_5(1/x)$.
Write

$$C \colon y^2 = a_5(x) = x^{15} + (x^7 + (x^3 + (x+1)^2)^2)^2 ;$$

this is an odd degree hyperelliptic curve of genus $g = 7$.

Its Jacobian variety J has 2-Selmer rank 2,
but we are unable to find points of infinite order in $J(\mathbb{Q})$.
So standard Chabauty techniques cannot be applied.

We will instead use "Selmer Group Chabauty".

We have three rational points on C whose image in J has odd order:

$$C(\mathbb{Q})_{\text{odd}} = \{\infty,\ (0,1),\ (0,-1)\}.$$

The idea

$$C(\mathbb{Q}) \xhookrightarrow{\ i\ } J(\mathbb{Q}) \twoheadrightarrow \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \xhookrightarrow{\ \delta\ } \mathrm{Sel}_2(J)$$

The idea

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d, hook] & J(\mathbb{Q}) \arrow[r, two heads] \arrow[d, hook] & \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, hook, "\delta"] & \color{red}{\mathrm{Sel}_2(J)} \arrow[d, "\sigma"] \\
C(\mathbb{Q}_2) \arrow[r, hook, "i"] & J(\mathbb{Q}_2) \arrow[rr, two heads] & & \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)}
\end{tikzcd}$$

The idea

$$
\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d, hook] & J(\mathbb{Q}) \arrow[r, two heads] \arrow[d, hook] & \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, hook, "\delta"] & \color{red}{\mathrm{Sel}_2(J)} \arrow[d, "\sigma"] \\
C(\mathbb{Q}_2) \arrow[r, hook, "i"] & J(\mathbb{Q}_2) \arrow[rr, two heads] \arrow[d, two heads, "\log"] & & \dfrac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \arrow[d, two heads, "\overline{\log}"] \\
& \mathbb{Z}_2^g \arrow[rr, two heads] & & \mathbb{F}_2^g
\end{tikzcd}
$$

The idea

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d, hook] & J(\mathbb{Q}) \arrow[r, two heads] \arrow[d, hook] & \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, hook, "\delta"] & \mathrm{Sel}_2(J) \arrow[d, "\sigma"] \\
C(\mathbb{Q}_2) \arrow[r, hook, "i"] & J(\mathbb{Q}_2) \arrow[rr, two heads] \arrow[d, two heads, "\log"] & & \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \arrow[d, two heads, "\overline{\log}"] \\
& \mathbb{Z}_2^g \arrow[rr, two heads] & & \mathbb{F}_2^g
\end{tikzcd}$$

We check that σ is injective.

The idea

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d, hook] & J(\mathbb{Q}) \arrow[r, two heads] \arrow[d, hook] & \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, hook, "\delta"] & \mathrm{Sel}_2(J) \arrow[d, "\sigma"] \\
C(\mathbb{Q}_2) \arrow[r, hook, "i"] & J(\mathbb{Q}_2) \arrow[rr, two heads] \arrow[d, two heads, "\log"] & & \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \arrow[d, two heads, "\overline{\log}"] \\
& \mathbb{Z}_2^g \arrow[rr, two heads] & & \mathbb{F}_2^g
\end{tikzcd}$$

We check that σ is injective.

Let $P \in C(\mathbb{Q}) \setminus C(\mathbb{Q})_{\mathrm{odd}}$ and write $i(P) = 2^n \cdot Q$ with $Q \in J(\mathbb{Q})$ and n maximal.

The idea

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d, hook] & J(\mathbb{Q}) \arrow[r, two heads] \arrow[d, hook] & \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, hook, "\delta"] & \mathrm{Sel}_2(J) \arrow[d, "\sigma"] \\ C(\mathbb{Q}_2) \arrow[r, hook, "i"] & J(\mathbb{Q}_2) \arrow[rr, two heads] \arrow[d, two heads, "\log"] & & \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \arrow[d, two heads, "\overline{\log}"] \\ & \mathbb{Z}_2^g \arrow[rr, two heads] & & \mathbb{F}_2^g \end{tikzcd}$$

We check that σ is injective.

Let $P \in C(\mathbb{Q}) \setminus C(\mathbb{Q})_{\mathrm{odd}}$ and write $i(P) = 2^n \cdot Q$ with $Q \in J(\mathbb{Q})$ and n maximal.

Then $\overline{2^{-n} \log i(P)} = \overline{\log Q} = \overline{\log}\sigma\delta(Q) \in \overline{\log}\sigma(\mathrm{Sel}_2(J))$.

The idea

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "i"] \arrow[d, hook] & J(\mathbb{Q}) \arrow[r, two heads] \arrow[d, hook] & \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \arrow[r, hook, "\delta"] & \mathrm{Sel}_2(J) \arrow[d, "\sigma"] \\
C(\mathbb{Q}_2) \arrow[r, hook, "i"] & J(\mathbb{Q}_2) \arrow[rr, two heads] \arrow[d, two heads, "\log"] & & \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \arrow[d, two heads, "\overline{\log}"] \\
& \mathbb{Z}_2^g \arrow[rr, two heads] & & \mathbb{F}_2^g
\end{tikzcd}$$

We check that σ is injective.

Let $P \in C(\mathbb{Q}) \setminus C(\mathbb{Q})_{\mathrm{odd}}$ and write $i(P) = 2^n \cdot Q$ with $Q \in J(\mathbb{Q})$ and n maximal.

Then $\overline{2^{-n} \log i(P)} = \overline{\log Q} = \overline{\log}\sigma\delta(Q) \in \overline{\log}\sigma(\mathrm{Sel}_2(J))$.

We show $\forall P \in C(\mathbb{Q}_2) \setminus C(\mathbb{Q})_{\mathrm{odd}}\colon \overline{2^{-n} \log i(P)} \notin \overline{\log}\sigma(\mathrm{Sel}_2(J))$.

This implies that $C(\mathbb{Q}) = C(\mathbb{Q})_{\mathrm{odd}}$.

The Selmer group

Let θ be a root of a_5 (which is irreducible) and set $K = \mathbb{Q}(\theta)$.

The Selmer group

Let θ be a root of a_5 (which is irreducible) and set $K = \mathbb{Q}(\theta)$.
For every field extension $L/\mathbb{Q}$, there is an injective homomorphism

$$\delta_L \colon J(L)/2J(L) \to (L \otimes_{\mathbb{Q}} K)^\times/(L \otimes_{\mathbb{Q}} K)^{\times 2};$$

The 2-Selmer group can be identified with the subgroup of $K^\times/K^{\times 2}$ whose elements have image in $\operatorname{im} \delta_{\mathbb{Q}_v}$ under the obvious map, for all v.

The Selmer group

Let θ be a root of a_5 (which is irreducible) and set $K = \mathbb{Q}(\theta)$.
For every field extension $L/\mathbb{Q}$, there is an injective homomorphism

$$\delta_L \colon J(L)/2J(L) \to (L \otimes_{\mathbb{Q}} K)^\times/(L \otimes_{\mathbb{Q}} K)^{\times 2};$$

The 2-Selmer group can be identified with the subgroup of $K^\times/K^{\times 2}$ whose elements have image in $\operatorname{im} \delta_{\mathbb{Q}_v}$ under the obvious map, for all v.
The discriminant of a_5,

$$\operatorname{disc}(a_5) = 13 \cdot 24554691821639909$$

is odd and squarefree and the class group of K is trivial,
which implies that

$$\operatorname{Sel}_2(J) \subset \mathcal{O}_K^\times/\mathcal{O}_K^{\times 2}.$$

The Selmer group

Let θ be a root of a_5 (which is irreducible) and set $K = \mathbb{Q}(\theta)$.
For every field extension $L/\mathbb{Q}$, there is an injective homomorphism

$$\delta_L \colon J(L)/2J(L) \to (L \otimes_{\mathbb{Q}} K)^\times/(L \otimes_{\mathbb{Q}} K)^{\times 2};$$

The 2-Selmer group can be identified with the subgroup of $K^\times/K^{\times 2}$ whose elements have image in $\operatorname{im} \delta_{\mathbb{Q}_v}$ under the obvious map, for all v.
The discriminant of a_5,

$$\operatorname{disc}(a_5) = 13 \cdot 245546918216399909$$

is odd and squarefree and the class group of K is trivial,
which implies that

$$\operatorname{Sel}_2(J) \subset \mathcal{O}_K^\times/\mathcal{O}_K^{\times 2}.$$

The injectivity of σ follows from that of

$$\mathcal{O}_K^\times/\mathcal{O}_K^{\times 2} \to \mathbb{Z}_2[\theta]^\times/\mathbb{Z}_2[\theta]^{\times 2}.$$

The local image at 2

Any point $Q \in J(L)$ is represented by a divisor of the form $D - d \cdot \infty$ with D effective and not containing a Weierstrass point in its support.

The local image at 2

Any point $Q \in J(L)$ is represented by a divisor of the form $D - d \cdot \infty$ with D effective and not containing a Weierstrass point in its support. Let $a \in L[x]$ be the monic polynomial of degree d whose roots are the x-coordinates of the points in D (with multiplicity). Then

$$\delta_L(Q) = (-1)^d a(\theta) \in L[\theta]^\times / L[\theta]^{\times 2}.$$

The local image at 2

Any point $Q \in J(L)$ is represented by a divisor of the form $D - d \cdot \infty$ with D effective and not containing a Weierstrass point in its support. Let $a \in L[x]$ be the monic polynomial of degree d whose roots are the x-coordinates of the points in D (with multiplicity). Then

$$\delta_L(Q) = (-1)^d a(\theta) \in L[\theta]^\times / L[\theta]^{\times 2}.$$

Proposition.
There are points in $J(\mathbb{Q}_2)$ with a-polynomials

$$x^d - 2, \quad d \in \{1, 2, \ldots, 7\}, \qquad x^d - 4, \quad d \in \{3, 5\}$$

that represent a basis of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

The local image at 2

Any point $Q \in J(L)$ is represented by a divisor of the form $D - d \cdot \infty$ with D effective and not containing a Weierstrass point in its support. Let $a \in L[x]$ be the monic polynomial of degree d whose roots are the x-coordinates of the points in D (with multiplicity). Then

$$\delta_L(Q) = (-1)^d a(\theta) \in L[\theta]^\times / L[\theta]^{\times 2}.$$

Proposition.
There are points in $J(\mathbb{Q}_2)$ with a-polynomials

$$x^d - 2, \quad d \in \{1, 2, \ldots, 7\}, \qquad x^d - 4, \quad d \in \{3, 5\}$$

that represent a basis of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

$\rightsquigarrow$ We can determine $\operatorname{im} \delta_{\mathbb{Q}_2}$ and $\mathrm{Sel}_2(J)$.

The 2-adic abelian logarithm

$$\underline{\omega} = \left(\frac{dx}{y}, \frac{x\,dx}{y}, \ldots, \frac{x^{g-1}\,dx}{y}\right)$$

is a basis of the space of regular differentials on C.

The 2-adic abelian logarithm

$$\underline{\omega} = \left(\frac{dx}{y}, \frac{x\,dx}{y}, \ldots, \frac{x^{g-1}\,dx}{y}\right)$$

is a basis of the space of regular differentials on C.

We define the logarithm on the image of $C(\bar{\mathbb{Q}}_2)$ by

$$\log i(P) = \int_{\infty}^{P} \underline{\omega} \in \bar{\mathbb{Q}}_2^g$$

and extend to $J(\bar{\mathbb{Q}}_2)$ by linearity.

The 2-adic abelian logarithm

$$\underline{\omega} = \left(\frac{dx}{y}, \frac{x\,dx}{y}, \ldots, \frac{x^{g-1}\,dx}{y}\right)$$

is a basis of the space of regular differentials on C.
We define the logarithm on the image of $C(\bar{\mathbb{Q}}_2)$ by

$$\log i(P) = \int_\infty^P \underline{\omega} \in \bar{\mathbb{Q}}_2^g$$

and extend to $J(\bar{\mathbb{Q}}_2)$ by linearity.

Let $P_0 = (0, 1) \in C(\mathbb{Q})_{\mathrm{odd}}$. Since $i(P_0)$ is torsion, $\log i(P_0) = 0$.
Near P_0, we can expand log as a g-tuple of formal power series in $t = x$.

The 2-adic abelian logarithm

$$\underline{\omega} = \left(\frac{dx}{y}, \frac{x\,dx}{y}, \ldots, \frac{x^{g-1}\,dx}{y}\right)$$

is a basis of the space of regular differentials on C.

We define the logarithm on the image of $C(\bar{\mathbb{Q}}_2)$ by

$$\log i(P) = \int_\infty^P \underline{\omega} \in \bar{\mathbb{Q}}_2^g$$

and extend to $J(\bar{\mathbb{Q}}_2)$ by linearity.

Let $P_0 = (0, 1) \in C(\mathbb{Q})_{\text{odd}}$. Since $i(P_0)$ is torsion, $\log i(P_0) = 0$.

Near P_0, we can expand log as a g-tuple of formal power series in $t = x$.

Proposition.

These power series converge in $\bar{\mathbb{Q}}_2$ on points (ξ, η) with $v_2(\xi) > \frac{2}{2g+1}$.

The 2-adic abelian logarithm

$$\underline{\omega} = \left(\frac{dx}{y}, \frac{x\,dx}{y}, \dots, \frac{x^{g-1}\,dx}{y}\right)$$

is a basis of the space of regular differentials on C.

We define the logarithm on the image of $C(\bar{\mathbb{Q}}_2)$ by

$$\log i(P) = \int_\infty^P \underline{\omega} \in \bar{\mathbb{Q}}_2^g$$

and extend to $J(\bar{\mathbb{Q}}_2)$ by linearity.

Let $P_0 = (0, 1) \in C(\mathbb{Q})_{\mathrm{odd}}$. Since $i(P_0)$ is torsion, $\log i(P_0) = 0$.

Near P_0, we can expand log as a g-tuple of formal power series in $t = x$.

Proposition.

These power series converge in $\bar{\mathbb{Q}}_2$ on points (ξ, η) with $v_2(\xi) > \frac{2}{2g+1}$.

$\rightsquigarrow$ We can determine a basis of the $\mathbb{Z}_2$-lattice $\mathbb{Z}_2^g \simeq \log J(\mathbb{Q}_2) \subset \mathbb{Q}_2^g$.

Points near P_0

Compose log with the isomorphism to $\mathbb{Z}_2^g$ to obtain

$$\log' \colon J(\mathbb{Q}_2) \twoheadrightarrow \mathbb{Z}_2^g\,.$$

Points near P_0

Compose log with the isomorphism to $\mathbb{Z}_2^g$ to obtain

$$\mathrm{log}'\colon J(\mathbb{Q}_2) \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}_2^g .$$

With respect to our $\mathbb{Z}_2$-basis, we have

$$\overline{\mathrm{log}'}\sigma(\mathrm{Sel}_2(J)) = \big\langle (0,1,0,0,0,1,0),(0,0,1,1,1,1,0) \big\rangle \subset \mathbb{F}_2^g .$$

Points near P_0

Compose log with the isomorphism to $\mathbb{Z}_2^g$ to obtain

$$\log'\colon J(\mathbb{Q}_2) \twoheadrightarrow \mathbb{Z}_2^g .$$

With respect to our $\mathbb{Z}_2$-basis, we have

$$\overline{\log'}\sigma(\mathrm{Sel}_2(J)) = \big\langle (0,1,0,0,0,1,0),(0,0,1,1,1,1,0)\big\rangle \subset \mathbb{F}_2^g .$$

We can compute the power series $\underline{\ell}(t)$ expressing $\log'$ near P_0 giving

$$\log' i\big((2t,*)\big) = \big(t + O(2^2), t^2 + O(2^2), O(2^2), 2t^4 + O(2^2), O(2^2), 2t^3 + O(2^2), O(2^2)\big) .$$

Points near P_0

Compose log with the isomorphism to $\mathbb{Z}_2^g$ to obtain

$$\log'\colon J(\mathbb{Q}_2) \twoheadrightarrow \mathbb{Z}_2^g .$$

With respect to our $\mathbb{Z}_2$-basis, we have

$$\overline{\log'}\sigma(\mathrm{Sel}_2(J)) = \big\langle (0,1,0,0,0,1,0),(0,0,1,1,1,1,0) \big\rangle \subset \mathbb{F}_2^g .$$

We can compute the power series $\underline{\ell}(t)$ expressing $\log'$ near P_0 giving

$$\log' i\big((2t,*)\big) = \big(t + O(2^2), t^2 + O(2^2), O(2^2), 2t^4 + O(2^2), O(2^2), 2t^3 + O(2^2), O(2^2)\big) .$$

For t odd, we find $\quad \overline{\log' i((2t,*))} = (1,1,0,0,0,0,0) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$.

Points near P_0

Compose log with the isomorphism to $\mathbb{Z}_2^g$ to obtain

$$\log'\colon J(\mathbb{Q}_2) \longrightarrow\!\!\!\!\rightarrow \mathbb{Z}_2^g\,.$$

With respect to our $\mathbb{Z}_2$-basis, we have

$$\overline{\log'}\sigma(\mathrm{Sel}_2(J)) = \big\langle (0,1,0,0,0,1,0), (0,0,1,1,1,1,0) \big\rangle \subset \mathbb{F}_2^g\,.$$

We can compute the power series $\underline{\ell}(t)$ expressing $\log'$ near P_0 giving

$$\log' i\big((2t,*)\big) = \big(t + O(2^2), t^2 + O(2^2), O(2^2), 2t^4 + O(2^2), O(2^2), 2t^3 + O(2^2), O(2^2)\big)\,.$$

For t odd, we find $\overline{\log' i((2t,*))} = (1,1,0,0,0,0,0) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$.
For $t \neq 0$ even, we get $\overline{2^{-n}\log' i((2t,*))} = (1,0,0,0,0,0,0) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$.

Points near P_0

Compose log with the isomorphism to $\mathbb{Z}_2^g$ to obtain

$$\log' \colon J(\mathbb{Q}_2) \twoheadrightarrow \mathbb{Z}_2^g .$$

With respect to our $\mathbb{Z}_2$-basis, we have

$$\overline{\log'}\sigma(\mathrm{Sel}_2(J)) = \big\langle (0,1,0,0,0,1,0), (0,0,1,1,1,1,0) \big\rangle \subset \mathbb{F}_2^g .$$

We can compute the power series $\underline{\ell}(t)$ expressing $\log'$ near P_0 giving

$$\log' i\big((2t,*)\big) = \big(t + O(2^2), t^2 + O(2^2), O(2^2), 2t^4 + O(2^2), O(2^2), 2t^3 + O(2^2), O(2^2)\big) .$$

For t odd, we find $\overline{\log' i((2t,*))} = (1,1,0,0,0,0,0) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$.
For $t \neq 0$ even, we get $\overline{2^{-n}\log' i((2t,*))} = (1,0,0,0,0,0,0) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$.

Conclusion.
$(0,\pm 1)$ are the only points $P \in C(\mathbb{Q})$ with $v_2(x(P)) > 0$.

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$, we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \left(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\right).$$

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$, we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \bigl(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\bigr) .$$

We find that $\overline{2^{-n} \log' i(P_{2t})} = (0, 0, 0, 0, 0, 0, 1) \notin \overline{\log'} \sigma(\mathrm{Sel}_2(J))$ for all $t \in \mathbb{Z}_2$.

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$, we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \left(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\right).$$

We find that $\overline{2^{-n} \log' i(P_{2t})} = (0, 0, 0, 0, 0, 0, 1) \notin \overline{\log'} \sigma(\mathrm{Sel}_2(J))$ for all $t \in \mathbb{Z}_2$.

Conclusion.
∞ is the only point $P \in C(\mathbb{Q})$ with $v_2(x(P)) < 0$.

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$, we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \bigl(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\bigr)\,.$$

We find that $\overline{2^{-n} \log' i(P_{2t})} = (0, 0, 0, 0, 0, 0, 1) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$ for all $t \in \mathbb{Z}_2$.

Conclusion.

∞ is the only point $P \in C(\mathbb{Q})$ with $v_2(x(P)) < 0$.

The (possibly) remaining rational points P have $x(P) \equiv -3 \bmod 8$.

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$,
we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \big(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\big)\,.$$

We find that $\overline{2^{-n}\log' i(P_{2t})} = (0,0,0,0,0,0,1) \notin \overline{\log'}\sigma(\mathrm{Sel}_2(J))$ for all $t \in \mathbb{Z}_2$.

Conclusion.
∞ is the only point $P \in C(\mathbb{Q})$ with $v_2(x(P)) < 0$.

The (possibly) remaining rational points P have $x(P) \equiv -3 \bmod 8$.
We check that $\delta_{\mathbb{Q}_2} i(P) \notin \sigma(\mathrm{Sel}_2(J))$.

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$, we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \big(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\big).$$

We find that $\overline{2^{-n} \log' i(P_{2t})} = (0, 0, 0, 0, 0, 0, 1) \notin \overline{\log'} \sigma(\mathrm{Sel}_2(J))$ for all $t \in \mathbb{Z}_2$.

Conclusion.
∞ is the only point $P \in C(\mathbb{Q})$ with $v_2(x(P)) < 0$.

The (possibly) remaining rational points P have $x(P) \equiv -3 \bmod 8$.
We check that $\delta_{\mathbb{Q}_2} i(P) \notin \sigma(\mathrm{Sel}_2(J))$.

Conclusion.
There are no points $P \in C(\mathbb{Q})$ with $v_2(x(P)) = 0$.

Other points

To deal with points P near ∞, i.e., such that $v_2(x(P)) < 0$, we expand $\log'$ in terms of $t = y/x^{g+1}$; this gives

$$\log' i(P_{2t}) = \left(O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), O(2^2), -t + 2t^2 + O(2^2)\right).$$

We find that $\overline{2^{-n} \log' i(P_{2t})} = (0, 0, 0, 0, 0, 0, 1) \notin \overline{\log'} \sigma(\mathrm{Sel}_2(J))$ for all $t \in \mathbb{Z}_2$.

Conclusion.
∞ is the only point $P \in C(\mathbb{Q})$ with $v_2(x(P)) < 0$.

The (possibly) remaining rational points P have $x(P) \equiv -3 \bmod 8$.
We check that $\delta_{\mathbb{Q}_2} i(P) \notin \sigma(\mathrm{Sel}_2(J))$.

Conclusion.
There are no points $P \in C(\mathbb{Q})$ with $v_2(x(P)) = 0$.
So $C(\mathbb{Q}) = \{\infty, (0, 1), (0, -1)\}$.

Further results

We have shown that

❸ $A_5(c)$ is a square $\iff$ $c = 0$.

Further results

We have shown that

❸ $A_5(c)$ is a square $\iff c = 0$.

Lemma.

If $1 < m \mid n$ and $c \in \mathbb{Q}$ such that $A_n(c)$ is a square,
then $\pm A_m(c)$ is a square. If $m \equiv n \bmod 2$, then $A_m(c)$ is a square.

Further results

We have shown that

❸ $\quad A_5(c)$ is a square $\iff$ $c = 0$.

Lemma.

If $1 < m \mid n$ and $c \in \mathbb{Q}$ such that $A_n(c)$ is a square,
then $\pm A_m(c)$ is a square. If $m \equiv n \bmod 2$, then $A_m(c)$ is a square.

❹ $\quad A_6(c)$ is a square $\iff$ $c \in \{0, -1\}$. [$\rightsquigarrow$ genus 2 curve of rank 1]

Further results

We have shown that

❸ $A_5(c)$ is a square $\iff$ $c = 0$.

Lemma.
If $1 < m \mid n$ and $c \in \mathbb{Q}$ such that $A_n(c)$ is a square,
then $\pm A_m(c)$ is a square. If $m \equiv n \bmod 2$, then $A_m(c)$ is a square.

❹ $A_6(c)$ is a square $\iff$ $c \in \{0, -1\}$. [$\rightsquigarrow$ genus 2 curve of rank 1]

❺ $A_7(c)$ is a square $\iff$ $c = 0$. [under GRH; $\mathrm{Sel}_2(J) = 0$]

Further results

We have shown that

❸ $A_5(c)$ is a square $\iff$ $c = 0$.

Lemma.
If $1 < m \mid n$ and $c \in \mathbb{Q}$ such that $A_n(c)$ is a square,
then $\pm A_m(c)$ is a square. If $m \equiv n \bmod 2$, then $A_m(c)$ is a square.

❹ $A_6(c)$ is a square $\iff$ $c \in \{0, -1\}$. [$\rightsquigarrow$ genus 2 curve of rank 1]

❺ $A_7(c)$ is a square $\iff$ $c = 0$. [under GRH; $\mathrm{Sel}_2(J) = 0$]

❻ $A_{10}(c)$ is a square $\iff$ $c \in \{0, -1\}$. [work with $y^2 = -a_5(x)$]

Further results

We have shown that

❸ $A_5(c)$ is a square $\iff$ $c = 0$.

Lemma.
If $1 < m \mid n$ and $c \in \mathbb{Q}$ such that $A_n(c)$ is a square,
then $\pm A_m(c)$ is a square. If $m \equiv n \bmod 2$, then $A_m(c)$ is a square.

❹ $A_6(c)$ is a square $\iff$ $c \in \{0, -1\}$. [$\rightsquigarrow$ genus 2 curve of rank 1]

❺ $A_7(c)$ is a square $\iff$ $c = 0$. [under GRH; $\mathrm{Sel}_2(J) = 0$]

❻ $A_{10}(c)$ is a square $\iff$ $c \in \{0, -1\}$. [work with $y^2 = -a_5(x)$]

Theorem.
Let $c \in \mathbb{Q}$ such that $f_c^{\circ 2}$ is irreducible [$\rightsquigarrow c \notin \{0, -1\}$].
Then $f_c^{\circ 6}$ is irreducible. Assuming GRH, $f_c^{\circ 10}$ is also irreducible.

Further results

We have shown that

❸ $A_5(c)$ is a square $\iff$ $c = 0$.

Lemma.

If $1 < m \mid n$ and $c \in \mathbb{Q}$ such that $A_n(c)$ is a square,
then $\pm A_m(c)$ is a square. If $m \equiv n \bmod 2$, then $A_m(c)$ is a square.

❹ $A_6(c)$ is a square $\iff$ $c \in \{0, -1\}$. [$\rightsquigarrow$ genus 2 curve of rank 1]

❺ $A_7(c)$ is a square $\iff$ $c = 0$. [under GRH; $\mathrm{Sel}_2(J) = 0$]

❻ $A_{10}(c)$ is a square $\iff$ $c \in \{0, -1\}$. [work with $y^2 = -a_5(x)$]

Theorem.

Let $c \in \mathbb{Q}$ such that $f_c^{\circ 2}$ is irreducible [$\rightsquigarrow c \notin \{0, -1\}$].
Then $f_c^{\circ 6}$ is irreducible. Assuming GRH, $f_c^{\circ 10}$ is also irreducible.

Proof.

By the above, $A_n(c) \neq \square$ for $n = 3, 4, 5, 6, 8, 9, 10$ and for $n = 7$ under GRH. ❑

Generalization

The method applies in a similar way to curves of the form

$$C\colon y^2 = x^{2g+1} + h(x)^2 \qquad \text{with } h \in \mathbb{Z}[x],\ \deg h \le g \text{ and } h(0) \text{ odd}$$

to show that $C(\mathbb{Q}) = \{\infty, (0, h(0)), (0, -h(0))\}$.

Generalization

The method applies in a similar way to curves of the form

$$C\colon y^2 = x^{2g+1} + h(x)^2 \qquad \text{with } h \in \mathbb{Z}[x],\ \deg h \le g \text{ and } h(0) \text{ odd}$$

to show that $C(\mathbb{Q}) = \{\infty, (0, h(0)), (0, -h(0))\}$.

The key step is the explicit description of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

Generalization

The method applies in a similar way to curves of the form

$$C\colon y^2 = x^{2g+1} + h(x)^2 \qquad \text{with } h \in \mathbb{Z}[x],\ \deg h \le g \text{ and } h(0) \text{ odd}$$

to show that $C(\mathbb{Q}) = \{\infty, (0, h(0)), (0, -h(0))\}$.

The key step is the explicit description of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

We have implemented the method for the case that $h(1)$ is even
and have run it for $g = 5$ on all the $16\,808$ suitable h
with coefficients in $\{-3, \ldots, 3\}$ and positive leading coefficient:

Generalization

The method applies in a similar way to curves of the form

$$C\colon y^2 = x^{2g+1} + h(x)^2 \qquad \text{with } h \in \mathbb{Z}[x],\ \deg h \le g \text{ and } h(0) \text{ odd}$$

to show that $C(\mathbb{Q}) = \{\infty, (0, h(0)), (0, -h(0))\}$.

The key step is the explicit description of $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

We have implemented the method for the case that $h(1)$ is even and have run it for $g = 5$ on all the 16 808 suitable h with coefficients in $\{-3, \ldots, 3\}$ and positive leading coefficient:

dim Sel	0	1	2	3	4	5	avg. # Sel	total	perc.
success	3307	5786	2553	309	7	0	2.314	11962	71.2%
more pts.	0	693	1204	644	133	6	5.102	2680	15.9%
failure	0	668	1004	436	57	1	4.517	2166	12.9%
total	3307	7147	4761	1389	197	7	3.042	16808	100.0%

Thank You!