Chabauty without the Mordell-Weil group

Michael Stoll

Universität Bayreuth

Jahrestagung SPP 1489

Osnabrück

September 29, 2015

Example

Example

Say, we would like to solve the Generalized Fermat Equation

$$x^5 + y^5 = z^{17}.$$

Example

Say, we would like to solve the Generalized Fermat Equation

$$x^5 + y^5 = z^{17}.$$

Proposition (Dahmen & Siksek 2014).
Let p be an odd prime. If the only rational points on the curve

$$C_p \colon 5y^2 = 4x^p + 1$$

are the obvious ones (namely, ∞ and $(1, \pm 1)$),
then the only primitive integral solutions of $x^5 + y^5 = z^p$
are the trivial ones.

Example

Say, we would like to solve the Generalized Fermat Equation

$$x^5 + y^5 = z^{17}.$$

Proposition (Dahmen & Siksek 2014).
Let p be an odd prime. If the only rational points on the curve

$$C_p \colon 5y^2 = 4x^p + 1$$

are the obvious ones (namely, ∞ and $(1, \pm 1)$),
then the only primitive integral solutions of $x^5 + y^5 = z^p$
are the trivial ones.

(Dahmen and Siksek show this for $p = 7$ and $p = 19$
and deal with $p = 11$ and $p = 13$ in another way, assuming GRH.)

Why the Usual Approach Does Not Work

Why the Usual Approach Does Not Work

So we would like to show that $C_{17}(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$.

Why the Usual Approach Does Not Work

So we would like to show that $C_{17}(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$.

The usual approach is to embed C_{17} into its Jacobian variety J_{17},
to determine the group $J_{17}(\mathbb{Q})$ (up to finite index),
and then to apply Chabauty's method
(which uses p-adic analysis to isolate $C_{17}(\mathbb{Q})$ inside $J_{17}(\mathbb{Q})$).

Why the Usual Approach Does Not Work

So we would like to show that $C_{17}(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$.

The usual approach is to embed C_{17} into its Jacobian variety J_{17},
to determine the group $J_{17}(\mathbb{Q})$ (up to finite index),
and then to apply Chabauty's method
(which uses p-adic analysis to isolate $C_{17}(\mathbb{Q})$ inside $J_{17}(\mathbb{Q})$).

The first step is to compute the 2-Selmer group $\mathrm{Sel}_2 J_{17} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
Since $J_{17}(\mathbb{Q})[2] = 0$, this gives rank $J_{17}(\mathbb{Q}) \le 2$.
We know the point $[(1,1) - \infty]$ of infinite order, so rank $J_{17}(\mathbb{Q}) \ge 1$,
and (assuming finiteness of Sha) therefore rank $J_{17}(\mathbb{Q}) = 2$.

Why the Usual Approach Does Not Work

So we would like to show that $C_{17}(\mathbb{Q}) = \{\infty, (1, \pm 1)\}$.

The usual approach is to embed C_{17} into its Jacobian variety J_{17},
to determine the group $J_{17}(\mathbb{Q})$ (up to finite index),
and then to apply Chabauty's method
(which uses p-adic analysis to isolate $C_{17}(\mathbb{Q})$ inside $J_{17}(\mathbb{Q})$).

The first step is to compute the 2-Selmer group $\mathrm{Sel}_2 J_{17} \cong (\mathbb{Z}/2\mathbb{Z})^2$.
Since $J_{17}(\mathbb{Q})[2] = 0$, this gives rank $J_{17}(\mathbb{Q}) \le 2$.
We know the point $[(1,1) - \infty]$ of infinite order, so rank $J_{17}(\mathbb{Q}) \ge 1$,
and (assuming finiteness of Sha) therefore rank $J_{17}(\mathbb{Q}) = 2$.

But we are unable to find another independent point,
so we cannot proceed with Chabauty's method.

The Usual Approach and its Problems

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

- Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

• Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;

worst case is $\ell = p$.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

- Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

- Can get painful even for $p = 2$ and moderate g.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

- Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

- Can get painful even for $p = 2$ and moderate g.

2. Find $P_1, \ldots, P_r \in J(\mathbb{Q})$ such that $\langle P_1, \ldots, P_r \rangle + J(\mathbb{Q})_{\text{tors}} \twoheadrightarrow \mathrm{Sel}_p J$.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

• Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

• Can get painful even for $p = 2$ and moderate g.

2. Find $P_1, \ldots, P_r \in J(\mathbb{Q})$ such that $\langle P_1, \ldots, P_r \rangle + J(\mathbb{Q})_{\mathrm{tors}} \twoheadrightarrow \mathrm{Sel}_p J$.

Problems: rank bound not tight, large generators,
high-dimensional search space.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

• Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

• Can get painful even for $p = 2$ and moderate g.

2. Find $P_1, \ldots, P_r \in J(\mathbb{Q})$ such that $\langle P_1, \ldots, P_r \rangle + J(\mathbb{Q})_{\mathrm{tors}} \twoheadrightarrow \mathrm{Sel}_p J$.

Problems: rank bound not tight, large generators,
high-dimensional search space.

• The most serious stumbling block in many cases.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p\, J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

- Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

- Can get painful even for $p = 2$ and moderate g.

2. Find $P_1, \ldots, P_r \in J(\mathbb{Q})$ such that $\langle P_1, \ldots, P_r \rangle + J(\mathbb{Q})_{\mathrm{tors}} \twoheadrightarrow \mathrm{Sel}_p\, J$.

Problems: rank bound not tight, large generators,
high-dimensional search space.

- The most serious stumbling block in many cases.

3. If $r < g$, use Chabauty plus Mordell-Weil Sieve to determine $C(\mathbb{Q})$.

The Usual Approach and its Problems

Let C be a nice curve of genus g over $\mathbb{Q}$.

1. Compute a Selmer group $\mathrm{Sel}_p J$, where $J = \mathrm{Jac}(C)$.

Global Part: Class groups and units of number fields

• Usually OK for $p = 2$, C hyperelliptic, moderate g (GRH).

Local Part: Computation of $J(\mathbb{Q}_\ell)/pJ(\mathbb{Q}_\ell)$ for bad primes ℓ;
worst case is $\ell = p$.

• Can get painful even for $p = 2$ and moderate g.

2. Find $P_1, \ldots, P_r \in J(\mathbb{Q})$ such that $\langle P_1, \ldots, P_r \rangle + J(\mathbb{Q})_{\mathrm{tors}} \twoheadrightarrow \mathrm{Sel}_p J$.

Problems: rank bound not tight, large generators,
high-dimensional search space.

• The most serious stumbling block in many cases.

3. If $r < g$, use Chabauty plus Mordell-Weil Sieve to determine $C(\mathbb{Q})$.

• If we get here, we usually win!

The Idea

The Idea

In joint work with Bjorn Poonen
we used only the 2-Selmer group and its statistical behavior
(as determined by Bhargava and Gross)
to show that Chabauty's method at $p = 2$ applies
to 'most' hyperelliptic curves C of odd degree to show $C(\mathbb{Q}) = \{\infty\}$.

The Idea

In joint work with Bjorn Poonen
we used only the 2-Selmer group and its statistical behavior
(as determined by Bhargava and Gross)
to show that Chabauty's method at $p = 2$ applies
to 'most' hyperelliptic curves C of odd degree to show $C(\mathbb{Q}) = \{\infty\}$.

The idea is to make this work for concrete curves C
to show that $C(\mathbb{Q})$ does not contain unknown points.

The Idea

In joint work with Bjorn Poonen
we used only the 2-Selmer group and its statistical behavior
(as determined by Bhargava and Gross)
to show that Chabauty's method at $p = 2$ applies
to 'most' hyperelliptic curves C of odd degree to show $C(\mathbb{Q}) = \{\infty\}$.

The idea is to make this work for concrete curves C
to show that $C(\mathbb{Q})$ does not contain unknown points.

Pro: No need to find many independent points in $J(\mathbb{Q})$.

The Idea

In joint work with Bjorn Poonen
we used only the 2-Selmer group and its statistical behavior
(as determined by Bhargava and Gross)
to show that Chabauty's method at $p = 2$ applies
to 'most' hyperelliptic curves C of odd degree to show $C(\mathbb{Q}) = \{\infty\}$.

The idea is to make this work for concrete curves C
to show that $C(\mathbb{Q})$ does not contain unknown points.

Pro: No need to find many independent points in $J(\mathbb{Q})$.
Con: Does not always work, even when Selmer rank $< g$.

The Idea

In joint work with Bjorn Poonen
we used only the 2-Selmer group and its statistical behavior
(as determined by Bhargava and Gross)
to show that Chabauty's method at $p = 2$ applies
to 'most' hyperelliptic curves C of odd degree to show $C(\mathbb{Q}) = \{\infty\}$.

The idea is to make this work for concrete curves C
to show that $C(\mathbb{Q})$ does not contain unknown points.

Pro: No need to find many independent points in $J(\mathbb{Q})$.
Con: Does not always work, even when Selmer rank $< g$.
Pro: Necessary conditions are likely satisfied when g is not very small.

Method

Method

Setting:

$C/\mathbb{Q}$ nice curve with Jacobian J;

$P_0 \in C(\mathbb{Q})$, gives embedding $i\colon C \hookrightarrow J$;

$\Gamma \subset J(\mathbb{Q})$ a subgroup with saturation $\overline{\Gamma}$;

p a prime number; $X \subset C(\mathbb{Q}_p)$, e.g., a residue disk.

Method

Setting:

$C/\mathbb{Q}$ nice curve with Jacobian J;

$P_0 \in C(\mathbb{Q})$, gives embedding $\iota\colon C \hookrightarrow J$;

$\Gamma \subset J(\mathbb{Q})$ a subgroup with saturation $\overline{\Gamma}$;

p a prime number; $X \subset C(\mathbb{Q}_p)$, e.g., a residue disk.

For $P \in J(\mathbb{Q}_p)$ set

$$q(P) = \{\pi_p(Q) : Q \in J(\mathbb{Q}_p), \exists n \geq 0\colon p^n Q = P\} \subset \frac{J(\mathbb{Q}_p)}{pJ(\mathbb{Q}_p)}$$

where $\pi_p\colon J(\mathbb{Q}_p) \to J(\mathbb{Q}_p)/pJ(\mathbb{Q}_p)$,

and for $S \subset J(\mathbb{Q}_p)$ set $q(S) = \bigcup_{P \in S} q(P)$.

Method

Method

$\Gamma \subset J(\mathbb{Q})$ subgroup with saturation $\overline{\Gamma}$

$q(P) = \{\pi_p(Q) : Q \in J(\mathbb{Q}_p), \exists n \geq 0 \colon p^n Q = P\}$

Method

$\Gamma \subset J(\mathbb{Q})$ subgroup with saturation $\overline{\Gamma}$

$q(P) = \left\{\pi_p(Q) : Q \in J(\mathbb{Q}_p), \exists n \geq 0\colon p^n Q = P\right\}$

$$
\begin{array}{ccccccccc}
C(\mathbb{Q}) \cap X & \hookrightarrow & C(\mathbb{Q}) & \overset{i}{\hookrightarrow} & J(\mathbb{Q}) & \overset{\pi}{\twoheadrightarrow} & \dfrac{J(\mathbb{Q})}{pJ(\mathbb{Q})} & \overset{\delta}{\hookrightarrow} & \mathrm{Sel}_p\, J \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & \swarrow{\scriptstyle \sigma} & \\
X & \hookrightarrow & C(\mathbb{Q}_p) & \overset{i}{\hookrightarrow} & J(\mathbb{Q}_p) & \overset{\pi_p}{\twoheadrightarrow} & \dfrac{J(\mathbb{Q}_p)}{pJ(\mathbb{Q}_p)} & &
\end{array}
$$

Method

$\Gamma \subset J(\mathbb{Q})$ subgroup with saturation $\overline{\Gamma}$

$q(P) = \{\pi_p(Q) : Q \in J(\mathbb{Q}_p), \exists n \geq 0 \colon p^n Q = P\}$

$$\begin{array}{ccccccccc}
C(\mathbb{Q}) \cap X & \hookrightarrow & C(\mathbb{Q}) & \stackrel{i}{\hookrightarrow} & J(\mathbb{Q}) & \stackrel{\pi}{\twoheadrightarrow} & \frac{J(\mathbb{Q})}{pJ(\mathbb{Q})} & \stackrel{\delta}{\hookrightarrow} & \mathrm{Sel}_p\, J \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & \swarrow \sigma & \\
X & \hookrightarrow & C(\mathbb{Q}_p) & \stackrel{i}{\hookrightarrow} & J(\mathbb{Q}_p) & \stackrel{\pi_p}{\twoheadrightarrow} & \frac{J(\mathbb{Q}_p)}{pJ(\mathbb{Q}_p)} & &
\end{array}$$

Proposition.

If (1) $\ker \sigma \subset \delta\pi(\Gamma)$ and (2) $q(i(X) + \Gamma) \cap \mathrm{im}\, \sigma \subset \pi_p(\Gamma)$, then $C(\mathbb{Q}) \cap X \subset i^{-1}(\overline{\Gamma})$.

Method

$\Gamma \subset J(\mathbb{Q})$ subgroup with saturation $\overline{\Gamma}$

$q(P) = \left\{\pi_p(Q) : Q \in J(\mathbb{Q}_p), \exists n \geq 0 \colon p^n Q = P\right\}$

$$\begin{array}{ccccccccc}
C(\mathbb{Q}) \cap X & \hookrightarrow & C(\mathbb{Q}) & \overset{i}{\hookrightarrow} & J(\mathbb{Q}) & \overset{\pi}{\twoheadrightarrow} & \dfrac{J(\mathbb{Q})}{pJ(\mathbb{Q})} & \overset{\delta}{\hookrightarrow} & \mathrm{Sel}_p J \\
\big\downarrow & & \big\downarrow & & \big\downarrow & & \big\downarrow & \swarrow{\scriptstyle \sigma} & \\
X & \hookrightarrow & C(\mathbb{Q}_p) & \overset{i}{\hookrightarrow} & J(\mathbb{Q}_p) & \overset{\pi_p}{\twoheadrightarrow} & \dfrac{J(\mathbb{Q}_p)}{pJ(\mathbb{Q}_p)} & &
\end{array}$$

Proposition.
If (1) $\ker\sigma \subset \delta\pi(\Gamma)$ and (2) $q(i(X) + \Gamma) \cap \operatorname{im}\sigma \subset \pi_p(\Gamma)$, then $C(\mathbb{Q}) \cap X \subset i^{-1}(\overline{\Gamma})$.

Corollary.
If $P_0 \in X$, X is contained in (half) a residue disk,
$\ker\sigma \subset \delta\pi(J(\mathbb{Q})[p^\infty])$ and $q(i(X) + J(\mathbb{Q})[p^\infty]) \cap \operatorname{im}\sigma \subset \pi_p(J(\mathbb{Q})[p^\infty])$, then

$$C(\mathbb{Q}) \cap X = \{P_0\}.$$

Odd Degree Hyperelliptic Curves

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

- q is locally constant in an explicit way.

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

- q is locally constant in an explicit way.
- To compute q, need to halve points in $J(\mathbb{Q}_2)$.
  This can be done explicitly.

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

- q is locally constant in an explicit way.
- To compute q, need to halve points in $J(\mathbb{Q}_2)$.
  This can be done explicitly.
- If C is given as $y^2 = f(x)$ and $L = \mathbb{Q}[x]/\langle f \rangle$, then have compatible maps
  $$\mu\colon J(\mathbb{Q}) \to \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \hookrightarrow L^{\square}, \qquad \mu_2\colon J(\mathbb{Q}_2) \to \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \hookrightarrow L_2^{\square}, \qquad r\colon L^{\square} \to L_2^{\square},$$
  where $L_2 = L \otimes_{\mathbb{Q}} \mathbb{Q}_2$ and $R^{\square} = R^{\times}/(R^{\times})^2$.

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

- q is locally constant in an explicit way.
- To compute q, need to halve points in $J(\mathbb{Q}_2)$.
  This can be done explicitly.
- If C is given as $y^2 = f(x)$ and $L = \mathbb{Q}[x]/\langle f \rangle$, then have compatible maps
  $\mu\colon J(\mathbb{Q}) \to \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} \hookrightarrow L^\square, \qquad \mu_2\colon J(\mathbb{Q}_2) \to \dfrac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \hookrightarrow L_2^\square, \qquad r\colon L^\square \to L_2^\square,$
  where $L_2 = L \otimes_{\mathbb{Q}} \mathbb{Q}_2$ and $R^\square = R^\times/(R^\times)^2$.
- Can compute $\mathrm{Sel}_2\, C$ and $\mathrm{Sel}_2\, J$ as a subset and subgroup of $L^\square$.

Odd Degree Hyperelliptic Curves

We want to turn this into an algorithm
when $p = 2$ and C is a hyperelliptic curve of odd degree.

- q is locally constant in an explicit way.
- To compute q, need to halve points in $J(\mathbb{Q}_2)$.
  This can be done explicitly.
- If C is given as $y^2 = f(x)$ and $L = \mathbb{Q}[x]/\langle f \rangle$, then have compatible maps
  $\mu\colon J(\mathbb{Q}) \to \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} \hookrightarrow L^\square, \qquad \mu_2\colon J(\mathbb{Q}_2) \to \dfrac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} \hookrightarrow L_2^\square, \qquad r\colon L^\square \to L_2^\square,$
  where $L_2 = L \otimes_{\mathbb{Q}} \mathbb{Q}_2$ and $R^\square = R^\times/(R^\times)^2$.
- Can compute $\mathrm{Sel}_2\, C$ and $\mathrm{Sel}_2\, J$ as a subset and subgroup of $L^\square$.
- So work with $L^\square$ and $L_2^\square$ instead of $J(\mathbb{Q})/2J(\mathbb{Q})$ and $J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)$.

The Algorithm

The Algorithm

1. Compute $\mathrm{Sel}_2\, C \subset \mathrm{Sel}_2\, J \subset L^{\square}$.

The Algorithm

1. Compute $\mathrm{Sel}_2\, C \subset \mathrm{Sel}_2\, J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2\, J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\text{known}}$.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\mathrm{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^\square$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\text{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^\square$.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\mathrm{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\mathrm{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:

   a. If $X \cap C(\mathbb{Q})_{\mathrm{known}} = \emptyset$:
      if $\mu_2(X) \cap r(\mathrm{Sel}_2 C) \neq \emptyset$ then return FAIL, else continue with next X.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\mathrm{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:

   a. If $X \cap C(\mathbb{Q})_{\mathrm{known}} = \emptyset$:
      if $\mu_2(X) \cap r(\mathrm{Sel}_2 C) \neq \emptyset$ then return FAIL, else continue with next X.

   b. Pick $P_0 \in X \cap C(\mathbb{Q})_{\mathrm{known}}$ and compute $Y = \mu_2(q(i_{P_0}(X) + J(\mathbb{Q})[2^\infty]))$

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\text{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:
   a. If $X \cap C(\mathbb{Q})_{\text{known}} = \emptyset$:
      if $\mu_2(X) \cap r(\mathrm{Sel}_2 C) \neq \emptyset$ then return FAIL, else continue with next X.
   b. Pick $P_0 \in X \cap C(\mathbb{Q})_{\text{known}}$ and compute $Y = \mu_2(q(i_{P_0}(X) + J(\mathbb{Q})[2^\infty]))$
   c. If $Y \cap r(\mathrm{Sel}_2 J) \not\subset R$ then return FAIL.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\text{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:
   a. If $X \cap C(\mathbb{Q})_{\text{known}} = \emptyset$:
      if $\mu_2(X) \cap r(\mathrm{Sel}_2 C) \neq \emptyset$ then return FAIL, else continue with next X.
   b. Pick $P_0 \in X \cap C(\mathbb{Q})_{\text{known}}$ and compute $Y = \mu_2(q(i_{P_0}(X) + J(\mathbb{Q})[2^\infty]))$
   c. If $Y \cap r(\mathrm{Sel}_2 J) \not\subset R$ then return FAIL.
7. Return $C(\mathbb{Q})_{\text{known}}$.

The Algorithm

1. Compute $\mathrm{Sel}_2 C \subset \mathrm{Sel}_2 J \subset L^{\square}$.
2. If $\ker(r) \cap \mathrm{Sel}_2 J \not\subset \mu(J(\mathbb{Q})[2^\infty])$, then return FAIL.
3. Search for rational points on C; this gives $C(\mathbb{Q})_{\mathrm{known}}$.
4. Let $\mathcal{X}$ be a partition of $C(\mathbb{Q}_2)$ into (half) residue disks X.
5. Set $R = \mu_2(J(\mathbb{Q})[2^\infty]) \subset L_2^{\square}$.
6. For each $X \in \mathcal{X}$, do:
   a. If $X \cap C(\mathbb{Q})_{\mathrm{known}} = \emptyset$:
      if $\mu_2(X) \cap r(\mathrm{Sel}_2 C) \neq \emptyset$ then return FAIL, else continue with next X.
   b. Pick $P_0 \in X \cap C(\mathbb{Q})_{\mathrm{known}}$ and compute $Y = \mu_2(q(i_{P_0}(X) + J(\mathbb{Q})[2^\infty]))$
   c. If $Y \cap r(\mathrm{Sel}_2 J) \not\subset R$ then return FAIL.
7. Return $C(\mathbb{Q})_{\mathrm{known}}$.

Remark. Can leave out 2-adic condition for $\mathrm{Sel}_2 J$.

Applications

Applications

(1) $5y^2 = 4x^p + 1$:
Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $r(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $r|_{\mathrm{Sel}_2 J_p}$ is injective.

Applications

(1) $5y^2 = 4x^p + 1$:

Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $r(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $r|_{\mathrm{Sel}_2 J_p}$ is injective. This gives

Theorem.
$x^5 + y^5 = z^p$ has only trivial solutions for $p \leq 53$ (under GRH for $p \geq 23$).

Applications

(1) $5y^2 = 4x^p + 1$:
Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $r(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $r|_{\mathrm{Sel}_2 J_p}$ is injective. This gives

Theorem.
$x^5 + y^5 = z^p$ has only trivial solutions for $p \leq 53$ (under GRH for $p \geq 23$).

(2) Similar application to FLT (via $y^2 = 4x^p + 1$).

Applications

(1) $5y^2 = 4x^p + 1$:
Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $r(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $r|_{\mathrm{Sel}_2 J_p}$ is injective. This gives

Theorem.
$x^5 + y^5 = z^p$ has only trivial solutions for $p \leq 53$ (under GRH for $p \geq 23$).

(2) Similar application to FLT (via $y^2 = 4x^p + 1$).

(3) The set of integral points on $Y^2 - Y = X^{21} - X$ is $\{-1, 0, 1\} \times \{0, 1\}$.

Applications

(1) $5y^2 = 4x^p + 1$:
Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $r(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $r|_{\mathrm{Sel}_2 J_p}$ is injective. This gives

Theorem.
$x^5 + y^5 = z^p$ has only trivial solutions for $p \leq 53$ (under GRH for $p \geq 23$).

(2) Similar application to FLT (via $y^2 = 4x^p + 1$).

(3) The set of integral points on $Y^2 - Y = X^{21} - X$ is $\{-1, 0, 1\} \times \{0, 1\}$.

(4) Elliptic curve Chabauty variant proves that the only rational points on
$y^2 = 81x^{10} + 420x^9 + 1380x^8 + 1860x^7 + 3060x^6 - 66x^5 + 3240x^4 - 1740x^3 + 1320x^2 - 480x + 69$
are the two points at infinity.
(Note: $g = \operatorname{rank} J(\mathbb{Q}) = 4$.)

Applications

(1) $5y^2 = 4x^p + 1$:
Obtain a three-element set $Z \subset \mathbb{Q}_2(\sqrt[p]{2})^\square$ that $r(\mathrm{Sel}_2 J_p)$ has to avoid; also check that $r|_{\mathrm{Sel}_2 J_p}$ is injective. This gives

Theorem.
$x^5 + y^5 = z^p$ has only trivial solutions for $p \le 53$ (under GRH for $p \ge 23$).

(2) Similar application to FLT (via $y^2 = 4x^p + 1$).

(3) The set of integral points on $Y^2 - Y = X^{21} - X$ is $\{-1, 0, 1\} \times \{0, 1\}$.

(4) Elliptic curve Chabauty variant proves that the only rational points on
$y^2 = 81x^{10} + 420x^9 + 1380x^8 + 1860x^7 + 3060x^6 - 66x^5 + 3240x^4 - 1740x^3 + 1320x^2 - 480x + 69$
are the two points at infinity.
(Note: $g = \operatorname{rank} J(\mathbb{Q}) = 4$.)

(5) More to come!

Thank You!