UNIVERSITÄT BAYREUTH

Descent and Covering Collections
Part II: Descent Theory

Michael Stoll

Universität Bayreuth

NATO Advanced Study Institute

Ohrid

September 3, 2014

Local Solubility

Recall:

Definition.

A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

Local Solubility

Recall:

Definition.
A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

We have seen on Monday
that we can decide whether a given curve is ELS or not.

Local Solubility

Recall:

Definition.
A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

We have seen on Monday
that we can decide whether a given curve is ELS or not.

This gives a way of showing that $C(\mathbb{Q}) = \emptyset$.

Local Solubility

Recall:

Definition.

A (nice) curve C over $\mathbb{Q}$ is said to be everywhere locally soluble or ELS, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

We have seen on Monday
that we can decide whether a given curve is ELS or not.

This gives a way of showing that $C(\mathbb{Q}) = \emptyset$.

Conversely, it is easy to show that $C(\mathbb{Q}) \neq \emptyset$:
Just find a point $P_0 \in C(\mathbb{Q})$!

Heuristics

Order all equations $y^2 = f(x)$ with integral coefficients
of hyperelliptic curves of fixed genus $g \geq 2$ by height $H(f) = \max_j |f_j|$.
Denote that family by $\mathcal{F}_g$.

Heuristics

Order all equations $y^2 = f(x)$ with integral coefficients of hyperelliptic curves of fixed genus $g \geq 2$ by height $H(f) = \max_j |f_j|$. Denote that family by $\mathcal{F}_g$.

Expectation/Conjecture.

The set of curves in $\mathcal{F}_g$ with rational points has density zero.

Heuristics

Order all equations $y^2 = f(x)$ with integral coefficients of hyperelliptic curves of fixed genus $g \geq 2$ by height $H(f) = \max_j |f_j|$. Denote that family by $\mathcal{F}_g$.

Expectation/Conjecture.

The set of curves in $\mathcal{F}_g$ with rational points has density zero.
(**Bhargava** (2013): The (upper) density is $o(2^{-g})$. More on Friday!)

Heuristics

Order all equations $y^2 = f(x)$ with integral coefficients
of hyperelliptic curves of fixed genus $g \geq 2$ by height $H(f) = \max_j |f_j|$.
Denote that family by $\mathcal{F}_g$.

Expectation/Conjecture.

The set of curves in $\mathcal{F}_g$ with rational points has density zero.
(**Bhargava** (2013): The (upper) density is $o(2^{-g})$. More on Friday!)

Proposition.

The set of ELS curves in $\mathcal{F}_g$ has a density $\delta_g > 0$.

Heuristics

Order all equations $y^2 = f(x)$ with integral coefficients
of hyperelliptic curves of fixed genus $g \geq 2$ by height $H(f) = \max_j |f_j|$.
Denote that family by $\mathcal{F}_g$.

Expectation/Conjecture.

The set of curves in $\mathcal{F}_g$ with rational points has density zero.
(**Bhargava** (2013): The (upper) density is $o(2^{-g})$. More on Friday!)

Proposition.

The set of ELS curves in $\mathcal{F}_g$ has a density $\delta_g > 0$.

We have $\delta_2 \approx 0.85$; as g grows, δ_g gets closer to 1, but $\limsup_{g \to \infty} \delta_g < 1$.

Heuristics

Order all equations $y^2 = f(x)$ with integral coefficients of hyperelliptic curves of fixed genus $g \geq 2$ by height $H(f) = \max_j |f_j|$. Denote that family by $\mathcal{F}_g$.

Expectation/Conjecture.

The set of curves in $\mathcal{F}_g$ with rational points has density zero. (**Bhargava** (2013): The (upper) density is $o(2^{-g})$. More on Friday!)

Proposition.

The set of ELS curves in $\mathcal{F}_g$ has a density $\delta_g > 0$.

We have $\delta_2 \approx 0.85$; as g grows, δ_g gets closer to 1, but $\limsup_{g\to\infty} \delta_g < 1$.

Conclusion: We need a way of proving $C(\mathbb{Q}) = \emptyset$ even when C is ELS!

A Double Cover

Let $C\colon y^2 = f(x)$ be hyperelliptic over $\mathbb{Q}$ with $f \in \mathbb{Z}[x]$
and assume that $f = f_1 f_2$ in $\mathbb{Z}[x]$ with (at least one of) $\deg f_1$, $\deg f_2$ even.

A Double Cover

Let $C\colon y^2 = f(x)$ be hyperelliptic over $\mathbb{Q}$ with $f \in \mathbb{Z}[x]$
and assume that $f = f_1 f_2$ in $\mathbb{Z}[x]$ with (at least one of) $\deg f_1$, $\deg f_2$ even.

Assume that $P = (\xi, \eta) \in C(\mathbb{Q})$: $\quad \eta^2 = f(\xi) = f_1(\xi) f_2(\xi)$.
Then there is a unique squarefree $d \in \mathbb{Z}$
such that $f_1(\xi) = d\eta_1^2$ and $f_2(\xi) = d\eta_2^2$ with $\eta_1, \eta_2 \in \mathbb{Q}$.

A Double Cover

Let $C\colon y^2 = f(x)$ be hyperelliptic over $\mathbb{Q}$ with $f \in \mathbb{Z}[x]$
and assume that $f = f_1 f_2$ in $\mathbb{Z}[x]$ with (at least one of) $\deg f_1$, $\deg f_2$ even.

Assume that $P = (\xi, \eta) \in C(\mathbb{Q})$: $\quad \eta^2 = f(\xi) = f_1(\xi) f_2(\xi)$.
Then there is a unique squarefree $d \in \mathbb{Z}$
such that $f_1(\xi) = d\eta_1^2$ and $f_2(\xi) = d\eta_2^2$ with $\eta_1, \eta_2 \in \mathbb{Q}$.

Let $D_d\colon dy_1^2 = f_1(x), dy_2^2 = f_2(x)$ and $\pi_d\colon D_d \to C$, $(x, y_1, y_2) \mapsto (x, dy_1 y_2)$.
The above then means that $P \in \pi_d\bigl(D_d(\mathbb{Q})\bigr)$.

A Double Cover

Let $C\colon y^2 = f(x)$ be hyperelliptic over $\mathbb{Q}$ with $f \in \mathbb{Z}[x]$
and assume that $f = f_1 f_2$ in $\mathbb{Z}[x]$ with (at least one of) $\deg f_1$, $\deg f_2$ even.

Assume that $P = (\xi, \eta) \in C(\mathbb{Q})$: $\quad \eta^2 = f(\xi) = f_1(\xi) f_2(\xi)$.
Then there is a unique squarefree $d \in \mathbb{Z}$
such that $f_1(\xi) = d\eta_1^2$ and $f_2(\xi) = d\eta_2^2$ with $\eta_1, \eta_2 \in \mathbb{Q}$.

Let $D_d\colon dy_1^2 = f_1(x), dy_2^2 = f_2(x)$ and $\pi_d\colon D_d \to C$, $(x, y_1, y_2) \mapsto (x, dy_1 y_2)$.
The above then means that $P \in \pi_d\big(D_d(\mathbb{Q})\big)$.

Conclusion:

$$C(\mathbb{Q}) = \bigcup_{d \text{ squarefree}} \pi_d\big(D_d(\mathbb{Q})\big) .$$

Restricting the Twists

We write everything homogeneously:

$$D_d\colon dy_1^2 = F_1(x,z), \qquad dy_2^2 = F_2(x,z)$$

with F_1, F_2 homogeneous of even degree and coprime.

Restricting the Twists

We write everything homogeneously:

$$D_d\colon dy_1^2 = F_1(x,z), \qquad dy_2^2 = F_2(x,z)$$

with F_1, F_2 homogeneous of even degree and coprime.

Now assume that the prime p divides d
and that we have a $\mathbb{Q}_p$-rational point on D_d with image $(\xi : \zeta)$ in $\mathbb{P}^1$.
We can then assume ξ and ζ to be coprime p-adic integers.

Restricting the Twists

We write everything homogeneously:

$$D_d\colon dy_1^2 = F_1(x,z), \qquad dy_2^2 = F_2(x,z)$$

with F_1, F_2 homogeneous of even degree and coprime.

Now assume that the prime p divides d
and that we have a $\mathbb{Q}_p$-rational point on D_d with image $(\xi : \zeta)$ in $\mathbb{P}^1$.
We can then assume ξ and ζ to be coprime p-adic integers.

Modulo p, we then find

$$0 \equiv d\eta_1^2 = F_1(\xi,\zeta) \qquad \text{and} \qquad 0 \equiv d\eta_2^2 = F_2(\xi,\zeta)\,,$$

so $\bar{\zeta}x - \bar{\xi}z$ is a common linear factor of $\bar{F}_1$ and $\bar{F}_2$.

Restricting the Twists

We write everything homogeneously:

$$D_d \colon dy_1^2 = F_1(x,z), \qquad dy_2^2 = F_2(x,z)$$

with F_1, F_2 homogeneous of even degree and coprime.

Now assume that the prime p divides d
and that we have a $\mathbb{Q}_p$-rational point on D_d with image $(\xi : \zeta)$ in $\mathbb{P}^1$.
We can then assume ξ and ζ to be coprime p-adic integers.

Modulo p, we then find

$$0 \equiv d\eta_1^2 = F_1(\xi,\zeta) \qquad \text{and} \qquad 0 \equiv d\eta_2^2 = F_2(\xi,\zeta)\,,$$

so $\bar{\zeta}x - \bar{\xi}z$ is a common linear factor of $\bar{F}_1$ and $\bar{F}_2$.

This means that p divides the resultant $\mathrm{Res}(F_1, F_2) \in \mathbb{Z}$.

Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$F(x,z) = f_m x^m + f_{m-1} x^{m-1} z + \ldots + f_1 x z^{m-1} + f_0 z^m$$
$$G(x,z) = g_n x^n + g_{n-1} x^{n-1} z + \ldots + g_1 x z^{n-1} + g_0 z^n$$

Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$F(x,z) = f_m x^m + f_{m-1}x^{m-1}z + \ldots + f_1 x z^{m-1} + f_0 z^m$$
$$G(x,z) = g_n x^n + g_{n-1}x^{n-1}z + \ldots + g_1 x z^{n-1} + g_0 z^n$$

Then the $(n+m)\times(n+m)$ determinant

$$\mathrm{Res}(F,G) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{vmatrix}$$

Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$F(x,z) = f_m x^m + f_{m-1}x^{m-1}z + \ldots + f_1 x z^{m-1} + f_0 z^m$$
$$G(x,z) = g_n x^n + g_{n-1}x^{n-1}z + \ldots + g_1 x z^{n-1} + g_0 z^n$$

Then the $(n+m)\times(n+m)$ determinant

$$\mathrm{Res}(F,G) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{vmatrix}$$

Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$F(x,z) = f_m x^m + f_{m-1} x^{m-1} z + \ldots + f_1 x z^{m-1} + f_0 z^m$$
$$G(x,z) = g_n x^n + g_{n-1} x^{n-1} z + \ldots + g_1 x z^{n-1} + g_0 z^n$$

Then the $(n+m) \times (n+m)$ determinant

$$\mathrm{Res}(F,G) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ & & & & & & & \\ & & & & & & & \end{vmatrix}$$

Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$F(x,z) = f_m x^m + f_{m-1}x^{m-1}z + \ldots + f_1 x z^{m-1} + f_0 z^m$$
$$G(x,z) = g_n x^n + g_{n-1}x^{n-1}z + \ldots + g_1 x z^{n-1} + g_0 z^n$$

Then the $(n+m)\times(n+m)$ determinant

$$\mathrm{Res}(F,G) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 \\ & & & & & & & \\ & & & & & & & \end{vmatrix}$$

Digression: The Resultant of Two Binary Forms

Let F and G be two binary forms over a field k:

$$F(x,z) = f_m x^m + f_{m-1} x^{m-1} z + \ldots + f_1 x z^{m-1} + f_0 z^m$$
$$G(x,z) = g_n x^n + g_{n-1} x^{n-1} z + \ldots + g_1 x z^{n-1} + g_0 z^n$$

Then the $(n+m) \times (n+m)$ determinant

$$\mathrm{Res}(F,G) = \begin{vmatrix} f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \cdots & 0 \\ 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & f_m & f_{m-1} & \cdots & f_1 & f_0 \\ g_n & g_{n-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 0 & g_n & g_{n-1} & \cdots & g_1 & g_0 & 0 \\ 0 & \cdots & 0 & g_n & g_{n-1} & \cdots & g_1 & g_0 \end{vmatrix}$$

is the Resultant of F and G.

The Resultant (2)

The resultant obeys the following rules (exercise!):

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\mathrm{Res}(G, F) = (-1)^{(\deg F)(\deg G)}\mathrm{Res}(F, G)$.

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\text{Res}(G, F) = (-1)^{(\deg F)(\deg G)}\text{Res}(F, G)$.
- $\text{Res}(F, c) = c^{\deg F}$ if c is constant.

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\text{Res}(G, F) = (-1)^{(\deg F)(\deg G)} \text{Res}(F, G)$.
- $\text{Res}(F, c) = c^{\deg F}$ if c is constant.
- $\text{Res}(F, -\beta x + \alpha z) = F(\alpha, \beta)$.

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\text{Res}(G, F) = (-1)^{(\deg F)(\deg G)} \text{Res}(F, G)$.
- $\text{Res}(F, c) = c^{\deg F}$ if c is constant.
- $\text{Res}(F, -\beta x + \alpha z) = F(\alpha, \beta)$.
- $\text{Res}(F, GH) = \text{Res}(F, G)\,\text{Res}(F, H)$.

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\text{Res}(G, F) = (-1)^{(\deg F)(\deg G)} \text{Res}(F, G)$.
- $\text{Res}(F, c) = c^{\deg F}$ if c is constant.
- $\text{Res}(F, -\beta x + \alpha z) = F(\alpha, \beta)$.
- $\text{Res}(F, GH) = \text{Res}(F, G)\,\text{Res}(F, H)$.
- $\text{Res}(F, G) = \text{Res}(F, G + FH)$ if $\deg F + \deg H = \deg G$.

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\text{Res}(G, F) = (-1)^{(\deg F)(\deg G)} \text{Res}(F, G)$.
- $\text{Res}(F, c) = c^{\deg F}$ if c is constant.
- $\text{Res}(F, -\beta x + \alpha z) = F(\alpha, \beta)$.
- $\text{Res}(F, GH) = \text{Res}(F, G)\,\text{Res}(F, H)$.
- $\text{Res}(F, G) = \text{Res}(F, G + FH)$ if $\deg F + \deg H = \deg G$.
- $\text{Res}(F \circ \gamma, G \circ \gamma) = \det(\gamma)^{(\deg F)(\deg G)} \text{Res}(F, G)$ for $\gamma \in GL(2, k)$.

The Resultant (2)

The resultant obeys the following rules (exercise!):

- $\text{Res}(G, F) = (-1)^{(\deg F)(\deg G)}\text{Res}(F, G)$.
- $\text{Res}(F, c) = c^{\deg F}$ if c is constant.
- $\text{Res}(F, -\beta x + \alpha z) = F(\alpha, \beta)$.
- $\text{Res}(F, GH) = \text{Res}(F, G)\,\text{Res}(F, H)$.
- $\text{Res}(F, G) = \text{Res}(F, G + FH)$ if $\deg F + \deg H = \deg G$.
- $\text{Res}(F \circ \gamma, G \circ \gamma) = \det(\gamma)^{(\deg F)(\deg G)}\text{Res}(F, G)$ for $\gamma \in GL(2, k)$.

Most importantly:

- $\text{Res}(F, G) = 0$ if and only if F and G have a common factor.

A Finiteness Statement

Recall the curve $D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$

and that $p \mid d$, $D_d(\mathbb{Q}_p) \neq \emptyset$ together imply $p \mid \mathrm{Res}(F_1, F_2)$.

A Finiteness Statement

Recall the curve $D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$
and that $p \mid d$, $D_d(\mathbb{Q}_p) \neq \emptyset$ together imply $p \mid \mathrm{Res}(F_1, F_2)$.

Conclusion: If $p \mid d$, but $p \nmid \mathrm{Res}(F_1, F_2)$, then D_d is not ELS, so $D_d(\mathbb{Q}) = \emptyset$.

A Finiteness Statement

Recall the curve $D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$

and that $p \mid d$, $D_d(\mathbb{Q}_p) \neq \emptyset$ together imply $p \mid \mathrm{Res}(F_1, F_2)$.

Conclusion: If $p \mid d$, but $p \nmid \mathrm{Res}(F_1, F_2)$, then D_d is not ELS, so $D_d(\mathbb{Q}) = \emptyset$.

Proposition.
Let $C\colon y^2 = f_1(x)f_2(x)$ as above and set

$$S = \left\{ d \in \mathbb{Z} : d \text{ squarefree and } \forall p\colon p \mid d \Rightarrow p \mid \mathrm{Res}(F_1, F_2) \right\}.$$

A Finiteness Statement

Recall the curve $D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$

and that $p \mid d$, $D_d(\mathbb{Q}_p) \neq \emptyset$ together imply $p \mid \mathrm{Res}(F_1, F_2)$.

Conclusion: If $p \mid d$, but $p \nmid \mathrm{Res}(F_1, F_2)$, then D_d is not ELS, so $D_d(\mathbb{Q}) = \emptyset$.

Proposition.

Let $C\colon y^2 = f_1(x)f_2(x)$ as above and set

$$S = \{d \in \mathbb{Z} : d \text{ squarefree and } \forall p\colon p \mid d \Rightarrow p \mid \mathrm{Res}(F_1, F_2)\}.$$

Then S is finite and

$$C(\mathbb{Q}) = \bigcup_{d \in S} \pi_d\big(D_d(\mathbb{Q})\big).$$

A Finiteness Statement

Recall the curve $D_d\colon dy_1^2 = F_1(x,z), \quad dy_2^2 = F_2(x,z)$
and that $p \mid d$, $D_d(\mathbb{Q}_p) \neq \emptyset$ together imply $p \mid \mathrm{Res}(F_1, F_2)$.

Conclusion: If $p \mid d$, but $p \nmid \mathrm{Res}(F_1, F_2)$, then D_d is not ELS, so $D_d(\mathbb{Q}) = \emptyset$.

Proposition.
Let $C\colon y^2 = f_1(x)f_2(x)$ as above and set

$$S = \bigl\{d \in \mathbb{Z} : d \text{ squarefree and } \forall p\colon p \mid d \Rightarrow p \mid \mathrm{Res}(F_1, F_2)\bigr\}.$$

Then S is finite and

$$C(\mathbb{Q}) = \bigcup_{d \in S} \pi_d\bigl(D_d(\mathbb{Q})\bigr).$$

In particular: $\forall d \in S\colon D_d$ not ELS implies $C(\mathbb{Q}) = \emptyset$.

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x) f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\mathrm{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{vmatrix}$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x) f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\operatorname{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 2 & 1 & 2 \end{vmatrix}$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\mathrm{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 \end{vmatrix}$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\operatorname{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & -1 & 4 & 0 \\ 0 & 0 & -1 & 4 \end{vmatrix}$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x) f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\mathrm{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 5 & -1 \\ 0 & 0 & -1 & 4 \end{vmatrix}$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x) f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\mathrm{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 5 & -1 \\ 0 & 0 & -1 & 4 \end{vmatrix} = \begin{vmatrix} 5 & -1 \\ -1 & 4 \end{vmatrix}$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute:

$$\operatorname{Res}(F_1, F_2) = \begin{vmatrix} -1 & -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} -1 & -1 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 5 & -1 \\ 0 & 0 & -1 & 4 \end{vmatrix} = \begin{vmatrix} 5 & -1 \\ -1 & 4 \end{vmatrix} = 19\,.$$

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute $\mathrm{Res}(F_1, F_2) = 19$, so $S = \{1, -1, 19, -19\}$.

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x) f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute $\mathrm{Res}(F_1, F_2) = 19$, so $S = \{1, -1, 19, -19\}$.

Since $f_2(\xi) > 0$ for all $\xi \in \mathbb{R}$, we have $D_d(\mathbb{R}) = \emptyset$ for $d < 0$.

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x) f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute $\mathrm{Res}(F_1, F_2) = 19$, so $S = \{1, -1, 19, -19\}$.

Since $f_2(\xi) > 0$ for all $\xi \in \mathbb{R}$, we have $D_d(\mathbb{R}) = \emptyset$ for $d < 0$.

Also $D_d(\mathbb{F}_3) = \emptyset$ and so $D_d(\mathbb{Q}_3) = \emptyset$ for $d \equiv 1 \bmod 3$
($\bar{F}_1(1, 0) = -1 \neq \Box$, $\bar{f}_2(0) = -1$, $\bar{f}_1(1) = -1$, $\bar{f}_2(-1) = -1$).

An Example

Consider

$$C\colon y^2 = (-x^2 - x + 1)(x^4 + x^3 + x^2 + x + 2) = f_1(x)f_2(x)\,.$$

Then C is ELS (exercise! — use that $f(0) = 2$, $f(1) = -6$, $f(-2) = -12$).

We compute $\mathrm{Res}(F_1, F_2) = 19$, so $S = \{1, -1, 19, -19\}$.

Since $f_2(\xi) > 0$ for all $\xi \in \mathbb{R}$, we have $D_d(\mathbb{R}) = \emptyset$ for $d < 0$.

Also $D_d(\mathbb{F}_3) = \emptyset$ and so $D_d(\mathbb{Q}_3) = \emptyset$ for $d \equiv 1 \bmod 3$
$(\bar{F}_1(1,0) = -1 \neq \square,\ \bar{f}_2(0) = -1,\ \bar{f}_1(1) = -1,\ \bar{f}_2(-1) = -1)$.

Conclusion: For all $d \in S$, we have that D_d is not ELS, so $C(\mathbb{Q}) = \emptyset$.

A Generalization

Question: What makes our construction work?

A Generalization

Question: What makes our construction work?

Answer: The morphism $\pi\colon D \to C$, $(x, y_1, y_2) \mapsto (x, y_1 y_2)$, where

$$D\colon y_1^2 = f_1(x)\,, \quad y_2^2 = f_2(x)\,,$$

is an unramified double cover.

A Generalization

Question: What makes our construction work?

Answer: The morphism $\pi \colon D \to C$, $(x, y_1, y_2) \mapsto (x, y_1 y_2)$, where

$$D \colon y_1^2 = f_1(x)\,, \quad y_2^2 = f_2(x)\,,$$

is an unramified double cover.

This is used (in the form '$\mathrm{Res}(F_1, F_2) \neq 0$') for the finiteness statment.

A Generalization

Question: What makes our construction work?

Answer: The morphism $\pi\colon D \to C$, $(x, y_1, y_2) \mapsto (x, y_1 y_2)$, where

$$D\colon y_1^2 = f_1(x), \quad y_2^2 = f_2(x),$$

is an unramified double cover.

This is used (in the form 'Res$(F_1, F_2) \neq 0$') for the finiteness statment.

(Note: We need (at least one of) $\deg f_1$ and $\deg f_2$ to be even
for the cover to be unramified; otherwise it ramifies above infinity.)

A Generalization

Question: What makes our construction work?

Answer: The morphism $\pi\colon D \to C$, $(x, y_1, y_2) \mapsto (x, y_1 y_2)$, where

$$D\colon y_1^2 = f_1(x)\,, \quad y_2^2 = f_2(x)\,,$$

is an unramified double cover.

This is used (in the form 'Res$(F_1, F_2) \neq 0$') for the finiteness statment.

(Note: We need (at least one of) $\deg f_1$ and $\deg f_2$ to be even
for the cover to be unramified; otherwise it ramifies above infinity.)

The result extends to general unramified double covers.

General Double Covers

Theorem.

Let C and D be nice curves over $\mathbb{Q}$
such that there is an unramified double cover $\pi\colon D \to C$.

General Double Covers

Theorem.

Let C and D be nice curves over $\mathbb{Q}$
such that there is an unramified double cover $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of squarefree $d \in \mathbb{Z}$ such that D_d is ELS,
where $\pi_d\colon D_d \to C$ is the corresponding twist of π,
is finite and computable,

General Double Covers

Theorem.
Let C and D be nice curves over $\mathbb{Q}$
such that there is an unramified double cover $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of squarefree $d \in \mathbb{Z}$ such that D_d is ELS,
where $\pi_d\colon D_d \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{d \in \mathrm{Sel}(\pi)} \pi_d\bigl(D_d(\mathbb{Q})\bigr)\,.$$

General Double Covers

Theorem.

Let C and D be nice curves over $\mathbb{Q}$
such that there is an unramified double cover $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of squarefree $d \in \mathbb{Z}$ such that D_d is ELS,
where $\pi_d\colon D_d \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{d \in \mathrm{Sel}(\pi)} \pi_d\bigl(D_d(\mathbb{Q})\bigr)\,.$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

General Double Covers

Theorem.

Let C and D be nice curves over $\mathbb{Q}$
such that there is an unramified double cover $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of squarefree $d \in \mathbb{Z}$ such that D_d is ELS,
where $\pi_d\colon D_d \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{d \in \mathrm{Sel}(\pi)} \pi_d\bigl(D_d(\mathbb{Q})\bigr) .$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

The set $\mathrm{Sel}(\pi)$ is called the Selmer set of π.

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Let $\pi\colon D \to C$ be an unramified covering
that is in addition geometrically Galois:

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Let $\pi\colon \mathrm{D} \to \mathrm{C}$ be an unramified covering
that is in addition geometrically Galois:

The extension $\bar{\mathbb{Q}}(\mathrm{C}) \subset \bar{\mathbb{Q}}(\mathrm{D})$ of function fields is a Galois extension
($\iff$ the group of deck transformations of $\mathrm{D}(\mathbb{C}) \to \mathrm{C}(\mathbb{C})$ has order $\deg \pi$).

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Let $\pi \colon D \to C$ be an unramified covering
that is in addition geometrically Galois:
The extension $\bar{\mathbb{Q}}(C) \subset \bar{\mathbb{Q}}(D)$ of function fields is a Galois extension
($\iff$ the group of deck transformations of $D(\mathbb{C}) \to C(\mathbb{C})$ has order $\deg \pi$).
Note that this is automatic when $\deg \pi = 2$.

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Let $\pi\colon D \to C$ be an unramified covering
that is in addition geometrically Galois:

The extension $\bar{\mathbb{Q}}(C) \subset \bar{\mathbb{Q}}(D)$ of function fields is a Galois extension
($\iff$ the group of deck transformations of $D(\mathbb{C}) \to C(\mathbb{C})$ has order $\deg \pi$).

Note that this is automatic when $\deg \pi = 2$.

A twist of π is a covering $\pi'\colon D' \to C$ that over $\bar{\mathbb{Q}}$ is isomorphic to π:
there is an isomorphism $\phi\colon D_{\bar{\mathbb{Q}}} \to D'_{\bar{\mathbb{Q}}}$ such that $\pi' \circ \phi = \pi$.

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Let $\pi\colon D \to C$ be an unramified covering
that is in addition geometrically Galois:

The extension $\bar{\mathbb{Q}}(C) \subset \bar{\mathbb{Q}}(D)$ of function fields is a Galois extension
($\iff$ the group of deck transformations of $D(\mathbb{C}) \to C(\mathbb{C})$ has order $\deg \pi$).

Note that this is automatic when $\deg \pi = 2$.

A twist of π is a covering $\pi'\colon D' \to C$ that over $\bar{\mathbb{Q}}$ is isomorphic to π:
there is an isomorphism $\phi\colon D_{\bar{\mathbb{Q}}} \to D'_{\bar{\mathbb{Q}}}$ such that $\pi' \circ \phi = \pi$.

Twists of π are classified by the elements of $H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$.

Generalizing Further

Not every curve over $\mathbb{Q}$ allows unramified double covers over $\mathbb{Q}$.
However, we can generalize the preceding theorem to more general covers.

Let $\pi \colon D \to C$ be an unramified covering
that is in addition geometrically Galois:

The extension $\bar{\mathbb{Q}}(C) \subset \bar{\mathbb{Q}}(D)$ of function fields is a Galois extension
($\iff$ the group of deck transformations of $D(\mathbb{C}) \to C(\mathbb{C})$ has order $\deg \pi$).

Note that this is automatic when $\deg \pi = 2$.

A twist of π is a covering $\pi' \colon D' \to C$ that over $\bar{\mathbb{Q}}$ is isomorphic to π:
there is an isomorphism $\phi \colon D_{\bar{\mathbb{Q}}} \to D'_{\bar{\mathbb{Q}}}$ such that $\pi' \circ \phi = \pi$.

Twists of π are classified by the elements of $H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$.
(For example, $H^1(\mathbb{Q}, \{\pm 1\}) \cong \mathbb{Q}^\times/\text{squares} \triangleq \{\text{squarefree integers}\}$.)

The General Descent Theorem

Theorem.

Let C and D be nice curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi \colon D \to C$.

The General Descent Theorem

Theorem.

Let C and D be nice curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$ such that D_ξ is ELS,
where $\pi_\xi\colon D_\xi \to C$ is the corresponding twist of π,
is finite and computable,

The General Descent Theorem

Theorem.

Let C and D be nice curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$ such that D_ξ is ELS,
where $\pi_\xi\colon D_\xi \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr).$$

The General Descent Theorem

Theorem.

Let C and D be nice curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$ such that D_ξ is ELS,
where $\pi_\xi\colon D_\xi \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr)\,.$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

The General Descent Theorem

Theorem.

Let C and D be nice curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi \colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$ such that D_ξ is ELS,
where $\pi_\xi \colon D_\xi \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr).$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

As before, the set $\mathrm{Sel}(\pi)$ is called the Selmer set of π.

The General Descent Theorem

Theorem.

Let C and D be nice curves over $\mathbb{Q}$ such that there is an unramified and geometrically Galois covering $\pi\colon D \to C$.
Then the set $\mathrm{Sel}(\pi)$ of $\xi \in H^1(\mathbb{Q}, \mathrm{Aut}(\pi))$ such that D_ξ is ELS,
where $\pi_\xi\colon D_\xi \to C$ is the corresponding twist of π,
is finite and computable, and we have

$$C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr)\,.$$

In particular, if $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

As before, the set $\mathrm{Sel}(\pi)$ is called the Selmer set of π.

The computability holds 'in principle'.
On Friday, we will see one case in which it is also practical.

Discussion: Practice

If we can compute $\mathrm{Sel}(\pi)$ for some covering $\pi \colon D \to C$, then:

Discussion: Practice

If we can compute $\mathsf{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathsf{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

Discussion: Practice

If we can compute $\mathsf{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathsf{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.
- Otherwise, we obtain a finite list of curves D_ξ, $\xi \in \mathsf{Sel}(\pi)$, with coverings $\pi_\xi\colon D_\xi \to C$ such that $C(\mathbb{Q}) = \bigcup_{\xi \in \mathsf{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr)$: the family $(\pi_\xi)_{\xi \in \mathsf{Sel}(\pi)}$ is a covering collection for C.

Discussion: Practice

If we can compute $\mathsf{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathsf{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.
- Otherwise, we obtain a finite list of curves D_ξ, $\xi \in \mathsf{Sel}(\pi)$, with coverings $\pi_\xi\colon D_\xi \to C$ such that $C(\mathbb{Q}) = \bigcup_{\xi \in \mathsf{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr)$: the family $(\pi_\xi)_{\xi \in \mathsf{Sel}(\pi)}$ is a covering collection for C.

If we can determine $D_\xi(\mathbb{Q})$ for all $\xi \in \mathsf{Sel}(\pi)$, then we also know $C(\mathbb{Q})$.

Discussion: Practice

If we can compute $\mathsf{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathsf{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.
- Otherwise, we obtain a finite list of curves D_ξ, $\xi \in \mathsf{Sel}(\pi)$, with coverings $\pi_\xi\colon D_\xi \to C$ such that $C(\mathbb{Q}) = \bigcup_{\xi \in \mathsf{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr)$: the family $(\pi_\xi)_{\xi \in \mathsf{Sel}(\pi)}$ is a covering collection for C.

If we can determine $D_\xi(\mathbb{Q})$ for all $\xi \in \mathsf{Sel}(\pi)$, then we also know $C(\mathbb{Q})$.

The D_ξ are more complicated than C (for example, the genus is larger).

Discussion: Practice

If we can compute $\mathrm{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.
- Otherwise, we obtain a finite list of curves D_ξ, $\xi \in \mathrm{Sel}(\pi)$, with coverings $\pi_\xi\colon D_\xi \to C$ such that $C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\big(D_\xi(\mathbb{Q})\big)$: the family $(\pi_\xi)_{\xi \in \mathrm{Sel}(\pi)}$ is a covering collection for C.

If we can determine $D_\xi(\mathbb{Q})$ for all $\xi \in \mathrm{Sel}(\pi)$, then we also know $C(\mathbb{Q})$.

The D_ξ are more complicated than C (for example, the genus is larger).
But there may be morphisms $\phi\colon D_\xi \to C'$ to other curves.
If we can find $C'(\mathbb{Q})$ and this set is finite, then we can compute $D_\xi(\mathbb{Q})$:

Discussion: Practice

If we can compute $\mathrm{Sel}(\pi)$ for some covering $\pi\colon D \to C$, then:

- If $\mathrm{Sel}(\pi) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.
- Otherwise, we obtain a finite list of curves D_ξ, $\xi \in \mathrm{Sel}(\pi)$, with coverings $\pi_\xi\colon D_\xi \to C$ such that $C(\mathbb{Q}) = \bigcup_{\xi \in \mathrm{Sel}(\pi)} \pi_\xi\bigl(D_\xi(\mathbb{Q})\bigr)$: the family $(\pi_\xi)_{\xi \in \mathrm{Sel}(\pi)}$ is a covering collection for C.

If we can determine $D_\xi(\mathbb{Q})$ for all $\xi \in \mathrm{Sel}(\pi)$, then we also know $C(\mathbb{Q})$.

The D_ξ are more complicated than C (for example, the genus is larger).
But there may be morphisms $\phi\colon D_\xi \to C'$ to other curves.
If we can find $C'(\mathbb{Q})$ and this set is finite, then we can compute $D_\xi(\mathbb{Q})$:
for each $P \in C'(\mathbb{Q})$, check the fiber $\phi^{-1}(P)$ for rational points.

Discussion: Theory

If C possesses a rational divisor class of degree 1, then C can be embedded into its Jacobian variety J.

Discussion: Theory

If C possesses a rational divisor class of degree 1,
then C can be embedded into its Jacobian variety J.

For each $n \geq 2$,
we then obtain an unramified and geometrically Galois covering of C
by pulling C back under the multiplication-by-n map of J.

Discussion: Theory

If C possesses a rational divisor class of degree 1,
then C can be embedded into its Jacobian variety J.

For each $n \geq 2$,
we then obtain an unramified and geometrically Galois covering of C
by pulling C back under the multiplication-by-n map of J.
We write $\mathrm{Sel}_n(C)$ for the associated Selmer set.

Discussion: Theory

If C possesses a rational divisor class of degree 1,
then C can be embedded into its Jacobian variety J.

For each $n \geq 2$,
we then obtain an unramified and geometrically Galois covering of C
by pulling C back under the multiplication-by-n map of J.
We write $\mathrm{Sel}_n(C)$ for the associated Selmer set.

Conjecture. $C(\mathbb{Q}) = \emptyset \iff \exists n\colon \mathrm{Sel}_n(C) = \emptyset$.

Discussion: Theory

If C possesses a rational divisor class of degree 1,
then C can be embedded into its Jacobian variety J.

For each $n \geq 2$,
we then obtain an unramified and geometrically Galois covering of C
by pulling C back under the multiplication-by-n map of J.
We write $\mathrm{Sel}_n(C)$ for the associated Selmer set.

Conjecture. $C(\mathbb{Q}) = \emptyset \iff \exists n\colon \mathrm{Sel}_n(C) = \emptyset$.

In particular, this would imply that the question '$C(\mathbb{Q}) = \emptyset$?' is decidable.

Discussion: Theory

If C possesses a rational divisor class of degree 1,
then C can be embedded into its Jacobian variety J.

For each $n \geq 2$,
we then obtain an unramified and geometrically Galois covering of C
by pulling C back under the multiplication-by-n map of J.
We write $\mathrm{Sel}_n(C)$ for the associated Selmer set.

Conjecture. $C(\mathbb{Q}) = \emptyset \iff \exists n\colon \mathrm{Sel}_n(C) = \emptyset$.

In particular, this would imply that the question '$C(\mathbb{Q}) = \emptyset$?' is decidable.

On Friday, we will consider $\mathrm{Sel}_2(C)$ for C hyperelliptic.