Mordel-Weil rank effective computation by 2-descent

Thibaut Misme

PARI/GP Workshop
January, 2024

Motivation

Let C be a nice algebraic curve.

Motivation

Let C be a nice algebraic curve.

$$\text{What is } C(\mathbb{Q}) \text{ ?}$$

Motivation

Let C be a nice algebraic curve.

What is $C(\mathbb{Q})$?

Classic process is to apply Chabauty-Coleman method when $\mathrm{rk}_{\mathbb{Q}}(\mathrm{Jac}(C)) < g(C)$

Motivation

Theorem (Mordell-Weil)

Let K be a number field, J be an abelian variety over K. There exists $r = rank_K(J) \in \mathbb{N}$, such that

$$J(K) \simeq \underbrace{J_{torsion}(K)}_{finite} \times \mathbb{Z}^r$$

Being given C (its equation), how to compute $r = rank_{\mathbb{Q}}(\mathrm{Jac}(C))$ in order to check Chabauty-Coleman condition for $K = \mathbb{Q}$?

2-descent: Introduction

2-descent algorithm is inspired by the Mordell-Weill theorem's proof, which ends up checking $J(\mathbb{Q})/2J(\mathbb{Q})$ finiteness.

In fact:

$$J(\mathbb{Q})/2J(\mathbb{Q}) \simeq J[2](\mathbb{Q}) \times (\mathbb{Z}/2\mathbb{Z})^r$$

$\rightsquigarrow$ If we can compute $J[2](\mathbb{Q})$, it is enough to find $|J(\mathbb{Q})/2J(\mathbb{Q})|$ to get r

2-descent: p-adic's help

Problem

It's difficult to generate points from $C(\mathbb{Q})$ and for $J(\mathbb{Q})$ as well

2-descent: p-adic's help

Problem

It's difficult to generate points from $C(\mathbb{Q})$ and for $J(\mathbb{Q})$ as well

Idea: Consider p-adic numbers

$$C(\mathbb{F}_p) \text{ computable} \rightsquigarrow \text{points in } C(\mathbb{Q}_p) \text{ (Hensel)}$$

$$\rightsquigarrow \text{points in } J(\mathbb{Q}_p) \text{ (Abel-Jacobi)}$$

2-descent: p-adic's help

Problem

It's difficult to generate points from $C(\mathbb{Q})$ and for $J(\mathbb{Q})$ as well

Idea: Consider p-adic numbers

$$C(\mathbb{F}_p) \text{ computable} \rightsquigarrow \text{points in } C(\mathbb{Q}_p) \text{ (Hensel)}$$

$$\rightsquigarrow \text{points in } J(\mathbb{Q}_p) \text{ (Abel-Jacobi)}$$

Bonus: p-adic structure

$|J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)| = |J[2](\mathbb{Q}_p)|$ $(p \neq 2)$

$\rightsquigarrow J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ computable

2-descent: Selmer group

Problem

$J(\mathbb{Q})/2J(\mathbb{Q}) \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ is not injective

2-descent: Selmer group

Problem

$J(\mathbb{Q})/2J(\mathbb{Q}) \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ is not injective

$\rightsquigarrow$ We consider all primes

2-descent: Selmer group

Problem

$J(\mathbb{Q})/2J(\mathbb{Q}) \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ is not injective

$\rightsquigarrow$ We consider all primes

Idea: Hasse's principle

Cohomology yields a **finite** group **Sel** $= Sel^{(2)}(\mathbb{Q})$ s.t. $J(\mathbb{Q})/2J(\mathbb{Q}) \subset Sel$ with better **computational properties**.

2-descent: Selmer group

Selmer group construction

2-descent: Selmer group

Selmer group construction

$$0 \to J[2] \to J(\overline{\mathbb{Q}}) \xrightarrow{2} J(\overline{\mathbb{Q}}) \to 0$$

2-descent: Selmer group

Selmer group construction

$$0 \to J[2] \to J(\overline{\mathbb{Q}}) \xrightarrow{2} J(\overline{\mathbb{Q}}) \to 0$$

$$\begin{array}{ccccc} J(\mathbb{Q})/2J(\mathbb{Q}) & \hookrightarrow & {\color{red}H^1(\mathbb{Q}, J[2])} & \to & H^1(\mathbb{Q}, J) \\ \downarrow & & \downarrow res_p & & \downarrow \\ J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \hookrightarrow & H^1(\mathbb{Q}_p, J[2]) & \to & H^1(\mathbb{Q}_p, J) \end{array}$$

2-descent: Selmer group

Selmer group construction

$$0 \to J[2] \to J(\overline{\mathbb{Q}}) \xrightarrow{2} J(\overline{\mathbb{Q}}) \to 0$$

$$\begin{array}{ccccc} J(\mathbb{Q})/2J(\mathbb{Q}) & \hookrightarrow & H^1(\mathbb{Q}, J[2]) & \to & H^1(\mathbb{Q}, J) \\ \downarrow & & \downarrow res_p & & \downarrow \\ J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) & \hookrightarrow & H^1(\mathbb{Q}_p, J[2]) & \to & H^1(\mathbb{Q}_p, J) \end{array}$$

definition: Selmer group

$$Sel := \{\phi \in H^1(\mathbb{Q}, J[2]) \mid \forall p, res_p(\phi) \in J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)\}$$
$$:= \bigcap_p res_p^{-1}(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))$$

Selmer group

$J(\mathbb{Q})/2J(\mathbb{Q}) \subset Sel \subset H^1(\mathbb{Q}, J[2])$ is a **finite**,
but **abstract** group,
equipped with a morphism, deduced from the **Weil Pairing**:

$$Sel \xrightarrow{H^1(w)} L^*/(L^*)^2$$

Selmer group

$J(\mathbb{Q})/2J(\mathbb{Q}) \subset$ *Sel* $\subset H^1(\mathbb{Q}, J[2])$ is a **finite**,
but **abstract** group,
equipped with a morphism, deduced from the **Weil Pairing**:

$$Sel \xrightarrow{H^1(w)} L^*/(L^*)^2$$

- $L^*/(L^*)^2$ is effective:
  $L = \mathbb{Q}[y]/\chi(y)$ is an algebra defined by $J[2]$

Selmer group

$J(\mathbb{Q})/2J(\mathbb{Q}) \subset Sel \subset H^1(\mathbb{Q}, J[2])$ is a **finite**,
but **abstract** group,
equipped with a morphism, deduced from the **Weil Pairing**:

$$Sel \xrightarrow{H^1(w)} L^*/(L^*)^2$$

- $L^*/(L^*)^2$ is effective:
  $L = \mathbb{Q}[y]/\chi(y)$ is an algebra defined by $J[2]$
- $H^1(w)$ is injective (in some determined cases)
  in opposite with $J(\mathbb{Q})/2J(\mathbb{Q}) \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$

2-descent: Selmer group

Computation of *Sel*

2-descent: Selmer group

Computation of Sel

$$Sel \xrightarrow{H^1(w)} wSel \subset \overbrace{L^*/(L^*)^2}^{effective}$$

Definition

$wSel := H^1(w)(Sel)$

2-descent: Selmer group

Computation of *Sel*

$$\textcolor{red}{Sel} \xrightarrow{H^1(w)} wSel \subset \overbrace{L^*/(L^*)^2}^{effective}$$

Definition

$wSel := H^1(w)(Sel)$

Problem

How can one recognize $wSel$ in $L^*/(L^*)^2$?

2-descent: Selmer group

Problem

How can one recognize *wSel* in $L^*/(L^*)^2$?

2-descent: Selmer group

Problem

How can one recognize *wSel* in $L^*/(L^*)^2$?

$$\begin{array}{ccc} Sel & \xrightarrow{H^1(w)} & wSel \subset \overbrace{L^*/(L^*)^2}^{effective} \\ \downarrow res_p & & \downarrow res_p \\ \underbrace{J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)}_{computable} & \xrightarrow{H^1(w)} & \underbrace{L_p^*/(L_p^*)^2}_{effective} \end{array}$$

Identification (from the def of Sel)

$$wSel = \{x \in L^*/(L^*)^2 \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\} \cap ker(\mathcal{N})$$

2-descent: Selmer group

Problem

How can one recognize *wSel* in $L^*/(L^*)^2$?

Identification

$$wSel = \{x \in L^*/(L^*)^2 \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\} \cap ker(\mathcal{N})$$

2-descent: Selmer group

Problem

How can one recognize *wSel* in $L^*/(L^*)^2$?

Identification

$$wSel = \{x \in L^*/(L^*)^2 \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\} \cap ker(\mathcal{N})$$

Problem

- $L^*/(L^*)^2$ is a vector space of infinite dimension

2-descent: Selmer group

Problem

How can one recognize $wSel$ in $L^*/(L^*)^2$?

Identification

$$wSel = \{x \in L^*/(L^*)^2 \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\} \cap ker(\mathcal{N})$$

Problem

- $L^*/(L^*)^2$ is a vector space of infinite dimension
- infinite amount of Selmer conditions (primes to check)

2-descent: Selmer group

Problem

How can one recognize $wSel$ in $L^*/(L^*)^2$?

Identification

$$wSel = \{x \in L^*/(L^*)^2 \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\} \cap ker(\mathcal{N})$$

Problem

- $L^*/(L^*)^2$ is a vector space of infinite dimension
- infinite amount of Selmer conditions (primes to check)

Solution (Hyperelliptic case)

If p is a **good reduction** prime($\neq 2$) and $H^1(w)$ **is injective**, $res_p(wSel) = ker(val_p) \cap ker(\mathcal{N})$

2-descent: Selmer group

Problem

How can one recognize *wSel* in $L^*/(L^*)^2$?

Solution (Hyperelliptic case)

If p is a **good reduction** prime($\neq 2$) and $H^1(w)$ **is injective**,
$res_p(wSel) = ker(val_p) \cap ker(\mathcal{N})$

2-descent: Selmer group

Problem

How can one recognize $wSel$ in $L^*/(L^*)^2$?

Solution (Hyperelliptic case)

If p is a **good reduction** prime($\neq 2$) and $H^1(w)$ **is injective**, $res_p(wSel) = ker(val_p) \cap ker(\mathcal{N})$

$S = \{\text{primes of } \textbf{bad} \text{ reduction}\} \cup \{2\}$ (finite)
$\tilde{H} := (\bigcap_{p \notin S} ker(val_p)) \cap ker(\mathcal{N})$
finite dimension and computable

Selmer computation

$wSel = \{x \in \tilde{H} \mid \forall p \in S \ res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$
$\rightsquigarrow$ **finite amount of calculation**

2-descent: Selmer group

Sum-up: Selmer

2-descent: Selmer group

Sum-up: Selmer

It's difficult to compute $|J(\mathbb{Q})/2J(\mathbb{Q})|$

2-descent: Selmer group

Sum-up: Selmer

It's difficult to compute $|J(\mathbb{Q})/2J(\mathbb{Q})|$

$\rightsquigarrow$ we compute the **upper-bound** $|Sel| = |wSel|$:
Recognizing *wSel* in the computable finite dimensional subspace $\tilde{H}$ by checking a finite amount of p-adic conditions.

2-descent: Selmer group

Sum-up: Selmer

It's difficult to compute $|J(\mathbb{Q})/2J(\mathbb{Q})|$

$\rightsquigarrow$ we compute the **upper-bound** $|Sel| = |wSel|$:
Recognizing *wSel* in the computable finite dimensional subspace $\tilde{H}$ by checking a finite amount of p-adic conditions.

(We obtain a finite amount of conditions because we know **exactly** the image of *wSel* by p-adic reduction with good primes)

2-descent: Selmer Group

How big is $J(\mathbb{Q})/2J(\mathbb{Q})$ **in** *Sel* **?**

2-descent: Selmer Group

How big is $J(\mathbb{Q})/2J(\mathbb{Q})$ in *Sel* ?

Cohomology gives us a group $Ш[2](\mathbb{Q})$ s.t. :

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to Sel \to Ш[2](\mathbb{Q}) \to 0$$

2-descent: Selmer Group

How big is $J(\mathbb{Q})/2J(\mathbb{Q})$ **in** *Sel* **?**

Cohomology gives us a group $\text{Ш}[2](\mathbb{Q})$ s.t. :

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to Sel \to \text{Ш}[2](\mathbb{Q}) \to 0$$

Conjecture

$\text{Ш}[2](\mathbb{Q})$ is "reasonably often" trivial

$\rightsquigarrow$ it is not very restrictive to only compute Sel

$\rightsquigarrow$ when it is not, try 3-descent

Algorithm

Reminder

$S = \{$primes of **bad** reduction$\}$

$$\begin{array}{ccc} Sel & \xrightarrow{H^1(w)} & wSel \subset \overbrace{\tilde{H}}^{computable} \\ \downarrow res_p & & \downarrow res_p \\ \underbrace{J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)}_{computable} & \xrightarrow{H^1(w)} & \underbrace{L_p^*/(L_p^*)^2}_{effective} \end{array}$$

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

- Compute $J[2]$ and its $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

- Compute $J[2]$ and its $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action
- Find $S = \{$primes of **bad** reduction$\} \cup \{2\}$ (compute the discriminant of the curve)

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

- Compute $J[2]$ and its $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action
- Find $S = \{\text{primes of } \textbf{bad} \text{ reduction}\} \cup \{2\}$ (compute the discriminant of the curve)
- Compute $\forall p \in S$

$$H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) \subset L_p^*/(L_p^*)^2$$

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

- Compute $J[2]$ and its $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action
- Find $S = \{\text{primes of } \textbf{bad} \text{ reduction}\} \cup \{2\}$ (compute the discriminant of the curve)
- Compute $\forall p \in S$

$$H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) \subset L_p^*/(L_p^*)^2$$

(compute random point on $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ + their image by $H^1(w)$ until you find $|J[2](\mathbb{Q}_p)|$ of them different)

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

- Compute $J[2]$ and its $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action
- Find $S = \{\text{primes of } \textbf{bad} \text{ reduction}\} \cup \{2\}$ (compute the discriminant of the curve)
- Compute $\forall p \in S$

$$H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) \subset L_p^*/(L_p^*)^2$$

 (compute random point on $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$
 $+$ their image by $H^1(w)$ until you find $|J[2](\mathbb{Q}_p)|$ of them different)

- Find an explicit finite basis of $\tilde{H} \subset L^*/(L^*)^2$

Algorithm: $H^1(w)$ injective

When $H^1(w)$ is injective

- Compute $J[2]$ and its $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ action
- Find $S = \{\text{primes of } \textbf{bad} \text{ reduction}\} \cup \{2\}$ (compute the discriminant of the curve)
- Compute $\forall p \in S$

$$H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) \subset L_p^*/(L_p^*)^2$$

(compute random point on $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ + their image by $H^1(w)$ until you find $|J[2](\mathbb{Q}_p)|$ of them different)

- Find an explicit finite basis of $\tilde{H} \subset L^*/(L^*)^2$ (In practice: BNF on a field of degree $|J[2]| = 2^{2*g(C)}$)

Algorithm: $H^1(w)$ injective

- ...
- Compute

$$wSel = \{x \in \tilde{H} \mid \forall p \in S\ res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

Algorithm: $H^1(w)$ injective

- ...
- Compute

$$wSel = \{x \in \tilde{H} \mid \forall p \in S \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

(check the Selmer conditions on every element of the basis of $\tilde{H}$ + linear algebra)

Algorithm: $H^1(w)$ injective

- ...
- Compute

  $$wSel = \{x \in \tilde{H} \mid \forall p \in S \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

  (check the Selmer conditions on every element of the basis of $\tilde{H}$ + linear algebra)
- $dim_{\mathbb{F}_2}|J[2](\mathbb{Q})| + rank + dim_{\mathbb{F}_2}|Ш[2](\mathbb{Q})|$
  $= dim_{\mathbb{F}_2}|Sel| = dim_{\mathbb{F}_2}|wSel|$

2-descent: requirements

Sum-up: Computable requirements for perfoming 2-descent

	Hyperelliptic	medium genus
$J[2](\overline{\mathbb{Q}})$ + Galois action	$\surd$	Mascot
$J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$	$\surd$	$\surd$
$H^1(w)$ injective	$\surd$ or Stoll	?

Algorithm: $H^1(w)$ NOT injective

Algorithm: $H^1(w)$ NOT injective

1. **Compute** $H^1(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))$

Algorithm: $H^1(w)$ NOT injective

1. Compute $H^1(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))$

Problem 1

$|H^1(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))| < |J[2](\mathbb{Q}_p)|$

$\rightsquigarrow$ we need to control

$KF_p := ker(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{H^1(w)} L_p^*/(L_p^*)^2)$

Algorithm: $H^1(w)$ NOT injective

1. Compute $H^1(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))$

Problem 1

$|H^1(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))| < |J[2](\mathbb{Q}_p)|$

$\rightsquigarrow$ we need to control

$KF_p := ker(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{H^1(w)} L_p^*/(L_p^*)^2)$

Solution 1

KF_p could be controlled in practice if we can perform the division by 2

Algorithm: $H^1(w)$ NOT injective

2. **Compute wSel**

Algorithm: $H^1(w)$ NOT injective

2. Compute wSel

Problem 2

$$\forall p \notin S,\ H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) < ker(val_p)$$

Algorithm: $H^1(w)$ NOT injective

2. Compute wSel

Problem 2

$\forall p \notin S,\ H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)) < ker(val_p)$

$$wSel := \{x \in \tilde{H} \mid \forall p \ res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

Algorithm: $H^1(w)$ NOT injective

2. Compute wSel

$$wSel := \{x \in \tilde{H} \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

Solution 2: compute wSel

- Compute the old way an upper-bound:

$$wSel_{Fake} = \{x \in \tilde{H} \mid \forall p \in S \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

Algorithm: $H^1(w)$ NOT injective

2. Compute wSel

$$wSel := \{x \in \tilde{H} \mid \forall p \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

Solution 2: compute wSel

- Compute the old way an upper-bound:

$$wSel_{Fake} = \{x \in \tilde{H} \mid \forall p \in S \; res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

- "effective Cebotarev theorem"
  $\rightsquigarrow$ target specific primes to add to the Selmer conditions, hoping to upgrade $wSel_{Fake}$

Algorithm: $H^1(w)$ NOT injective

2. Compute wSel

$$wSel := \{x \in \tilde{H} \mid \forall p \ res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

Solution 2: compute wSel

- Compute the old way an upper-bound:

$$wSel_{Fake} = \{x \in \tilde{H} \mid \forall p \in S \ res_p(x) \in H^1(w)(J(\mathbb{Q}_p)/2J(\mathbb{Q}_p))\}$$

- "effective Cebotarev theorem"
$\rightsquigarrow$ target specific primes to add to the Selmer conditions, hoping to upgrade $wSel_{Fake}$
- **Remark**: even if we reach $wSel$, we could probably not be able to detect it

Algorithm: $H^1(w)$ NOT injective

3. $|wSel| \neq |Sel|$

Algorithm: $H^1(w)$ NOT injective

3. $|wSel| \neq |Sel|$

Problem 3

$|J[2](\mathbb{Q})| + |J(\mathbb{Q})/2J(\mathbb{Q})| + |Ш[2](\mathbb{Q})| = |Sel| = |wSel| \times |KF| \leq |wSel_{Fake}| \times |KF|$

$(KF := ker(Sel \xrightarrow{H^1(w)} L^*/(L^*)^2)$

Algorithm: $H^1(w)$ NOT injective

3. $|wSel| \neq |Sel|$

Problem 3

$|J[2](\mathbb{Q})| + |J(\mathbb{Q})/2J(\mathbb{Q})| + |Ш[2](\mathbb{Q})| = |Sel| =$
$|wSel| \times |KF| \leq |wSel_{Fake}| \times |KF|$
$(KF := ker(Sel \xrightarrow{H^1(w)} L^*/(L^*)^2)$

Solution 3

$KF = (\cap_{p \in S} KF_p) \bigcap (\cap_{p \in A} KF_p)$
with: - $A \subset \{good\ primes\}$ is known if "Effective Cebotarev"
- KF_p should be effectively computable if p is a good prime

Conclusion

Change of paradigm:
We probably couldn't be able to certify $|Sel|$ in the general case.

Conclusion

Change of paradigm:
We probably couldn't be able to certify $|Sel|$ in the general case.
But we would try to be able to set several process aiming to narrow the bound of $|Sel|$, hoping for reaching a point low enough for our purposes (for instance lower than the genus in the Chabauty-Coleman frame)