Punts racionals de corbes I: The Mordell-Weil Sieve

Francesc Bars

Universitat Autònoma de Barcelona

(Barcelona January, 2019,)

Take $K/\mathbb{Q}$ number field.
C/K a smooth, complete, projective curve over K.
$g(C)$ denotes it genus.
Via Magma (think $K = \mathbb{Q}$):
Points(C, Bound:=1000);
one expects that for $g(C) \geq 2$, if $C(\mathbb{Q}) \neq \emptyset$ then for a big height (=bound) some point would appear, (big height will be rare).
If after the use of the above Magma command, Magma does not find any rational point, how to prove that $C(\mathbb{Q}) = \emptyset$?
This is the aim of the first part of this talk.

First approach:

v a place of K

K_v local field at v

Fact: Exist an algorithm to claim $C(K_v) = \emptyset$ or not.

If $C(K_v) = \emptyset$ implies $C(K) = \emptyset$, and we are done.

Fact: Exist an algorithm to decide if $C(K_v) \neq \emptyset \ \forall v$.

Magma has an implementation of the fact for $y^q = f(x)$ via **HasPointsEverywhereLocally(f,q);**

Theorem (Hasse)

Assume $g(C) = 0$.
$C(K) \neq \emptyset$ if and only if $C(K_v) \neq \emptyset \ \forall v$.

For $g(C) \geq 1$ the above theorem is not true in general.

Assume once and for all $g(C) \geq 1$.

(LP):= Assume once and for all that $C(K_v) \neq \emptyset \ \forall v$

Second approach

Assume that we have a explicit map $f : C \to C'$ all defined over K such that $C'(K)$ is finite. Therefore $f^{-1}(C'(K)) \cap C(K) = C(K)$ will give all the points, and if is empty we are done.

A simplest proof of Hasse principle fails on genus 1 curve without rational points proposed by Selmer:

//Veient el cas de Selmer.
K:=Rationals(); Pr $< x, y, z >$*:= ProjectiveSpace*$(K, 2)$*;*
//Indroduïm la corba com un "Model de Gènere 1"
C:=GenusOneModel$(3 * x^3 + 4 * y^3 + 5 * z^3)$*;*
//La següent funció dóna la corba Elíptica E
//i el morfisme m:C− $>$*E (de grau* $9 = 3^2$*)*
C,E,m:=nCovering(C);
//Calculem el Grup de Mordell Weil de E
MordellWeilGroup(E); Points(E: Bound:=100);
//Surt 0, per tant només té un punt, el O
O:=E![0,1,0];
//Calculem les imatges inverses del punt (a Q).
Points(Pullback(m, O));
//No n'hi ha.

Third approach: Descend method

Vague idea: Find a finite family $\phi_a : D_a \to C$ s.t.

$$C(K) = \bigsqcup_a \phi_a(D_a(K))$$

More concretely, assume $\iota : C \hookrightarrow Jac(C)$ (Abel-Jacobi map)
(i.e. assume C has a degree 1 divisor over K)
$[n] : Jac(C) \to Jac(C)$ unramified, thus
$[n]^*(C)$ unramified n-cover of C,

Theorem (Chevalley-Weil)

We have $C(K) = \bigsqcup_{D' : \text{twists of } D \text{ over } K \text{ sat.}(LP)} D'(K)$

Such twists are a finite set: are elements inside the finite group $H^1(k, Jac(C)[n](\overline{K}))$ which satisfy also (LP).

To test descend method in a curve

1. Fix $n \geq 2$,
2. construct all n covers D of C. If no such cover exists then $C(K) = \emptyset$
3. Determine the set of covers associated to the twists of D that satisfies (LP). If no such cover exist then $C(K) = \emptyset$ we are done.
4. Try to compute $D'(K)$.

We are interested in using descend method to prove $C(\mathbb{Q}) = \emptyset$.
For hyperelliptic curves $y^2 = f(x)$ Magma computes
$n = 2$-descent; (i.e. all twist of D 2-covers, without the condition (LP).
TwoCoverDescent(C:$y^2 = f$);
If $\#TwoCoverDescent(C) = 0$ then $C(\mathbb{Q}) = \emptyset$.

//Corba de génere 2
//En aquest cas té punts localment
$K := Rationals(); K < x >:= PolynomialRing(K); a := 7; b := 3;$
H:=HyperellipticCurve$(a * x^6 + b * x^4 + b * x^2 + a);$
Points(H : Bound:=10000);
//No té punts aparentment.
//Quocient de Gènere 1:
HE:=HyperellipticCurve$(a * x^3 + b * x^2 + b * x + a);$
//Corba elíptica corresponent (no usar segon approach):
E:=EllipticCurve(HE); E; Rank(E);
//Veure quants 2 covers hi ha.
#TwoCoverDescent(H);
//Surt zero, finalitzem.

Fourth approach: Mordell-Weil sieve

Begin with an example

$C_d : dy_1^2 = x, dy_2^2 = p(x), deg(p(x)) = 2, i.e. dy_2^2 = p(dy_1^2)$

We have an explicit map (d is not an square):

$$h : C_d \to E : y^2 = xp(x); h(x, y_1, y_2) = (x, dy_1y_2)$$

take p a prime of good reduction and we consider

$$\begin{array}{ccc} C_d(\mathbb{Q}) & \to^h & E(\mathbb{Q}) \\ \downarrow red & & \downarrow \rho \\ C_d(\mathbb{F}_p) & \to^{\overline{h}} & E(\mathbb{F}_p) \end{array}$$

If $\rho(E(\mathbb{Q})) \cap \overline{h}(C_d(\mathbb{F}_p)) = \emptyset$ then

$$C_d(\mathbb{Q}) = \emptyset$$

Take $C_2 : y^2 = 2x^4 + 293x^3 + 10640$, and
$E : y^2 = x(x^2 + 293x + 21280)$
Observe $E(\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \oplus \mathbb{Z}$.
For $p = 13$, $\#E(\mathbb{F}_p) = 16$, $\#\rho(E(\mathbb{Q})) = 8$ and $\#C(\mathbb{F}_p) = 8$ and $\rho(E(\mathbb{Q})) \cap \overline{h}(C_d(\mathbb{F}_p)) = \emptyset$, therefore

$$C_2(\mathbb{Q}) = \emptyset.$$

Let us make such calculations with Magma.

$K := Rationals(); K < x >:= PolynomialRing(K);$
$E := EllipticCurve(x * (x^2 + 293 * x +$
$21280)); Factorization(Conductor(E));$
$MordellWeilGroup(E); Generators(E);$
$h := 2 * x^4 + 293 * x^2 + 10640; C < X, Y, Z >:=$
$HyperellipticCurve(h);$
$A := Coefficient(h, 4); m := map < C- >$
$E|[A * X^2 * Z, A * X * Y, Z^3] >;$
$//Podem\ veure\ que\ de\ fet\ té\ punts\ locals\ arreu$
$HasPointsEverywhereLocally(h, 2);$
$//Podem\ veure\ que\ no\ trobem\ punts\ fins\ a\ altura\ gran(=10000):$
$Points(C : Bound := 10000);$
$//@\ @$

//Busquem un primer de bona reducció "bo", provem $p = 11$.
$K := GF(11); K < x >:= PolynomialRing(K);$
$E := EllipticCurve(x * (x^2 + 293 * x + 21280));$
//Generadors P:=E![380 , 10260]; T1:=E![0,0]; T2:=E![-133,0];
//T1 i T2 tenen ordre 2 (a Q).
//llista de tots els punts (poden haver repeticions).
*PP:=[n*P: n in [0..Order(P)-1]] cat [n*P+T1: n in*
*[0..Order(P)-1]]cat [n*P+T2: n in [0..Order(P)-1]]cat*
*[n*P+T1+T2: n in [0..Order(P)-1]];*
//Convertim a conjunt i contem
#SequenceToSet(PP);
//Contem el nombre de punts de E
#Isetset(Points(E));
*/*Resposta: 12 12*
//Com que surten els mateixos, no podem trobar cap obstrucció.

```
//Mirem ara p = 13.
K := GF(13); K<x>:= PolynomialRing(K);
E:=EllipticCurve(x*(x^2+293*x+21280)); P:=E![380 , 10260];
T1:=E![0,0]; T2:=E![-133,0]; PP:=[n*P: n in [0..Order(P)-1]] cat
[n*P+T1: n in [0..Order(P)-1]]cat [n*P+T2: n in
[0..Order(P)-1]]cat [n*P+T1+T2: n in [0..Order(P)-1]];
PP:=SequenceToSet(PP);
PE:=Isetset(Points(E));
#PP; #PE;
/* Resposta: 8 16
//Com que surten diferents podem trobar una obstrucció
//Construim la corba i el morfisme ara mòdul 13:
```

$h := 2 * x^4 + 293 * x^2 + 10640; C < X, Y, Z >:=$
$HyperellipticCurve(h);$
$A := Coefficient(h, 4);$
$m := map < C -> E | [A * X^2 * Z, A * X * Y, Z^3] >;$
$//Calculem\ les\ imatges\ per\ m\ dels\ punts\ de\ la\ corba:$
$PC:=m(p):\ p\ in\ Points(C);\ PC\ meet\ PP;$
$//Surt\ \emptyset$

Métode general Mordell-Weil sieve

Take $C \to A$, A abelian variety, all over K
s.t. $A(K)$ is a f.g.group (usually $A = Jac(C)$)),
We need explicit, generators $A(K)$ and morphism, and consider (S finite set places):

$$\begin{array}{ccc} C(K) & \to^{f} & A(K) \\ \downarrow & & \downarrow \rho_S \\ \prod_{v \in S} C(K_v) & \to^{\prod f_v} & \prod_{v \in S} A(K_v) \end{array}$$

If $Im(\rho_S) \cap Im(\prod f_v) = \emptyset$ then $C(K) = \emptyset$.
Fact(Bruin-Stoll) Assume C has a degree 1 divisor over K, take $A = Jac(C)$, $\iota = f$ (Abel-Jacobi map), the converse is true.
Problem: Too big $A(K_v)$!!!

Poonen heuristics

Assume once and for all C has a degree 1 divisor over K, and $g(C) \geq 2$

Consider the following diagram (recall, $g(C) \geq 2$)

$$\begin{array}{ccc} C(K) & \hookrightarrow^{\iota} & Jac(C)(K) \\ \downarrow & & \downarrow \rho_S \\ \prod_{v \in S \subset S_{good}} C(\mathbb{F}_v) & \rightarrow^{\prod \iota_v} & \prod_{v \in S} Jac(C)(\mathbb{F}_v) \end{array}$$

where S_{good} places of good reduction of C.

Conjecture (Poonen)

Assume $g(C) \geq 2$. $\exists S \subset S_{good}$ finite s.t. if $C(K) = \emptyset$ then

$$\rho_S(J(K) := Jac(C)(K)) \cap \prod_{v \in S} \iota_v(C(\mathbb{F}_v)) = \emptyset$$

Theorem (Poonen)

Assume above conjecture and $Sha(Jac(C))$ finite. Then

1. *The Brauer-Manin obstruction to the Hasse principle is the only obstruction to the existence of a K-point on a curve C.*
2. *There is an algorithm that takes K and a C/K and decides whether C has a K-point or not.*

Heuristics: (Bruin-Stoll) With $S = \{v = p\}$ the probability that $C(\mathbb{F}_v)$ does not meet the image of $Jac(C)(\mathbb{Q})$ is $>> 1/p$.

Bruin-Stoll, gives (in their web page) an algorithm (for hyperelliptic curves) how to choice S (not inside S_{good}) and integer N and a diagramm:

$$\begin{array}{ccc} C(\mathbb{Q}) & \hookrightarrow^{\iota} & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow \rho \\ \prod_{p\in S} C(\mathbb{F}_p) & \rightarrow^{\prod \iota_p} & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p) \end{array}$$

to compute $A(S,N) := \{a \in J(\mathbb{Q})/N : \rho(a) \in Im(\iota_p), \forall p \in S\}$ and obtain if $A(S,N) = \emptyset$ then $C(\mathbb{Q}) = \emptyset$.

Bruin-Stoll, give (in their web page) a programme in Magma to deal with the above algorithm for hyperelliptic curves $y^2 = f(x)$. As input:

1. $f(x)$;
2. Generators for $Jac(C)(\mathbb{Q})$. This is not direct from Magma, not always is easy task.
3. A rational degree 3 divisor of C. This is also not obvious a priori for general $f(x)$.

We present an example of Mordell-Weil sieve for a genus 3 non-hyperelliptic curve which is bielliptic.
Recall Magma does not compute Jacobians of non-hyperelliptic curves, nowadays.
The $Jac(C)$ has at least two elliptic curves of rank 1 (both are $\overline{\mathbb{Q}}$-isomorphic but not $\mathbb{Q}$-isomorphic.
Thank you to Xavier Xarles, for code in Magma used in this an previous examples
Let us consider:

$$C : -3 * z^4 + y^2 * (y^2 - 7 * z^2) + x^4$$

which is bielliptic, some bielliptic involutions are:
$w_1 : z \leftrightarrow -z, w_2 : x \leftrightarrow -x, w_3 : y \leftrightarrow -y$
where its quotient are elliptic curves s.t. $E_{w_i}(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2$, $i = 1, 2, 3$.

We consider the natural map

$$C(\mathbb{Q}) \to E_1(\mathbb{Q}) \times E_3(\mathbb{Q})$$

and we reduce to a convenient prime $p = 23$, where in such case Mordell-Weil sieve, following Poonen approach, we will obtain $C(\mathbb{Q}) = \emptyset$ by use of the next Magma programme.

Xarles function to make reduction

function redpol(r,pol) R:=Parent(pol); rank:=Rank(R);
k:=Codomain(r); O:=Domain(r); kx:=PolynomialRing(k,rank);
C:=[c: c in Coefficients(pol)]; M:=Monomials(pol); d:=#C;
$crpol := [r(Numerator(C[i]))/r(Denominator(C[i])) : i\ in[1..d]];$
$rpol := \&+[kx!crpol[i] * Monomial(kx, Exponents(M[i])) :$
$i\ in[1..d]];$
return rpol; end function;

$P2 < x, y, z >:= ProjectiveSpace(Rationals(), 2);$
$g := (-3)*z^4+y^2*(y^2-7*z^2)+x^4; C := Curve(P2, g); Genus(C);$
$RationalPoints(C : Bound := 1000);$
$phi1 := iso < C- > C|[x, y, -z], [x, y, -z] >;$
$phi2 := iso < C- > C|[-x, y, z], [-x, y, z] >;$
$phi3 := iso < C- > C|[x, -y, z], [x, -y, z] >;$
$G1 := AutomorphismGroup(C, [phi1]); G2 :=$
$AutomorphismGroup(C, [phi2]); G3 :=$
$AutomorphismGroup(C, [phi3]);$
$CG1, prj := CurveQuotient(G1); Genus(CG1); CG2, prj2 :=$
$CurveQuotient(G2); Genus(CG2); CG3, prj3 :=$
$CurveQuotient(G3); Genus(CG3);$
$pt1 := Setseq(RationalPoints(CG1 : Bound := 100))[1]; pt2 :=$
$Setseq(RationalPoints(CG2 : Bound := 100))[1]; pt3 :=$
$Setseq(RationalPoints(CG3 : Bound := 100))[1];$
$E1, m1 := EllipticCurve(CG1, pt1); E2, m2 :=$

$$E1m, mm1 := MinimalModel(E1); GEm1 := Generators(E1m); prjm1 := Extend(prj * m1 * mm1); Allprjm1 := AllDefiningPolynomials(prjm1);$$
$$E3m, mm3 := MinimalModel(E3); GEm3 := Generators(E3m); prjm3 := Extend(prj3 * m3 * mm3); Allprjm3 := AllDefiningPolynomials(prjm3);$$

$$L := GF(23); red := hom < Integers() -> L|[] >;$$
$$P2L < x, y, z >:= ProjectiveSpace(L, 2);$$
$$Cr := Curve(P2L, Evaluate(redpol(red, g), [x, y, z]));$$
$$pol1, pol2 := HyperellipticPolynomials(E1m);$$
$$Lx := PolynomialRing(L);$$
$$Er := EllipticCurve(Lx!redpol(red, pol1));$$
$$prjmr := map < Cr -> Er|[Evaluate(redpol(red, pol), [x, y, z]) :$$
$$pol\ in\ Allprjm1[2]] >;$$
$$prCr := prjmr(pt) : pt\ in\ Points(Cr); prCr;$$

```
T:=[Er!pt: pt in GEm1];
PP:=[n*T[2]: n in [0..Order(T[2])-1]] cat [n*T[2]+T[1]: n in
[0..Order(T[2])-1]];
PP:=SequenceToSet(PP);
ptCr1 := pt : pt in Points(Cr)|prjmr(pt) in (PP meet prCr);
ptCr1;
```

```
pol1,pol2:=HyperellipticPolynomials(E3m);
Er:=EllipticCurve(Lx!redpol(red,pol1));
prjmr := map< Cr-> Er|[Evaluate(redpol(red, pol), [x, y, z]) :
pol in Allprjm3[2]] >;
T:=[Er!pt: pt in GEm3];
PP:=[n*T[2]: n in [0..Order(T[2])-1]] cat [n*T[2]+T[1]: n in
[0..Order(T[2])-1]];
PP:=SequenceToSet(PP);
ptCr2 := pt : pt in ptCr1|prjmr(pt) in PP;
ptCr2;
//The set ptCr2 is the empty set, thus we are done.
```

$C/\mathbb{Q}$ good curve, $C(\mathbb{Q}) \neq \emptyset$
$\iota : C \hookrightarrow Jac(C)$, the idea is

$$\iota(C(\mathbb{Q})) = \cup_{D \in W} D + L$$

with $L \subseteq Jac(C)(\mathbb{Q})$ of huge index
W small finite set of $Jac(C)(\mathbb{Q})$.
FIRST: $rank_{\mathbb{Q}}(Jac(C)(\mathbb{Q}) \leq genus(C) - 1$
$M \in C(\mathbb{Q})$, p prime

$$B_{p^n}(M) := \{Q \in C(\mathbb{Q}_p) : Q \equiv M (mod\ p^n)\}$$

Chabauty method gives a bound of the $C(\mathbb{Q})$-points in $B_{p^n}(M)$, by the number $Chab_{p^n}(M)$, i.e.

$$\#C(\mathbb{Q}) \cap B_{p^n}(M) \leq Chab_{p^n}(M).$$

Example

$C : y^2 = 2x^6 - 3x^2 - 2x + 1$
$Jac(C)(\mathbb{Q}) = \mathbb{Z}[D := (-2, 11) - (0, 1)]$

Points(C: Range:=1000)
Expected:=$\{(0, 1), (0, -1), (-2, 11), (-2, -11)\}$

Chabauty method, at $p = 3$ gives:

P	$Chab_3(P)$	**Expected**$\cap B_3(P)$
(0,1)	2	$\{(0,1)\}$
(0,-1)	2	$\{(0,-1)\}$
(-2,11)	1	$\{(-2,11)\}$
(-2,-11)	1	$\{(-2,-11)\}$
P	$Chab_9(P)$	**Expected**$\cap B_9(P)$
(0,1)	1	$\{(0,1)\}$
(0,-1)	1	$\{(0,-1)\}$

Corollary

If $P \in C(\mathbb{Q}) \cap (B_9(0,1) \cup B_9(0,-1) \cup B_3(-2,11) \cup B_3(-2,-11))$ then $P \in$ **Expected.**

$P_0 := (0, 1)$

$$\iota : C \hookrightarrow Jac(C); Q \mapsto [Q - P_0].$$

Some calculation gives,
$\iota(0, -1) = -2D$,$\iota(-2, 11) = -3D$, $(\iota(-2, -11) = D)$.
Take $Q \in C(\mathbb{Q})$, then $\iota(Q) = n_Q D$.
p, prime good reduction, write,

$$N_p := order\ [D]; [D] \in Jac(C)(\mathbb{F}_p)$$

$$W_p := \{m \in \mathbb{Z}/N_p : m[D] \in \iota(C(\mathbb{F}_p))\}$$

Observe that Mordell-Weil sieve gives:

$$n_Q (mod\ N_p) \in W_p.$$

p	N_p	W_p
3	13	$\{0, 1, 10, 11\}$
5	21	$\{0, 1, 18, 19\}$
7	65	$\{0, 1, 13, 19, 27, 36, 44, 50, 62, 63\}$
17	39	$\{0, 1, 36, 37\}$
19	234	$\{0, 1, 42, 67, 72, 82, 100, 132, 150, 160, 165, 190, 231, 232\}$
23	16	$\{0, 1, 7, 13, 14\}$
61	208	$\{0, 1, 24, 53, 153, 182, 205, 206\}$

And one obtains

Lemma

If $Q \in C(\mathbb{Q})$ then exist $P \in$ **Expected** such that

$$[Q - P] \in \mathbb{Z}(234D)$$

Because, for example:
$n_Q = -3 + 234mD$,
$[Q - P_0] = n_Q D = \iota((-2, 11)) + m(234D) =$
$[(-2, 11) - P_0] + m(234D)$.

To conclude, use $p = 3$-filtration (good reduction):

$$J(\mathbb{Q}_p) \supseteq J^1(\mathbb{Q}_p) \supseteq J^2(\mathbb{Q}_p) \supseteq \dots$$

with

$$J^m(\mathbb{Q}_p) = \{D \in J(\mathbb{Q}_p) : D \equiv 0 (mod\ p^m)\}$$

$J(\mathbb{Q}_p)/J^1(\mathbb{Q}_p) \cong J(\mathbb{F}_p)$; $J^m(\mathbb{Q}_p)/J^{m+1}(\mathbb{Q}_p) \cong (\mathbb{Z}/p)^{genus(C)}, m \geq 1$

$\#J(\mathbb{F}_3) = 13$; $234 = 2 \cdot 3^2 \cdot 13$, $234D \in J^3(\mathbb{Q}_3)$,
Therefore $Q \in C(\mathbb{Q})$, we obtain:

$$Q \equiv P(mod 3^3); P \in Expected$$

$$Q \in B_{27}(0,1) \cup B_{27}(0,-1) \cup B_{27}(-2,11) \cup B_{27}(-2,-11)$$

and by Chabauty computation

$$Q \in \mathit{Expected}$$

Thus, $C(\mathbb{Q}) =$**Expected**.
MAGMA does for you this example: *Chabauty*().

$C/\mathbb{Q}$, fix $P_0 \in C(\mathbb{Q})$,

$$\iota : C \hookrightarrow Jac(C); P \mapsto [P - P_0]$$

and know $Jac(C)(\mathbb{Q})$, a strategy finite set $W \subset Jac(C)(\mathbb{Q})$ and a subgroup $L \subset J(\mathbb{Q})$ of huge index such that

$$\iota(C(\mathbb{Q})) = \cup_{D \in W} D + L$$

$L_0 := J(\mathbb{Q})$, $W_0 := 0$.
An inductive procedure:
Choose p, prime, good reduction.

$$\begin{array}{ccc} C(\mathbb{Q}) & \to^{\iota} & W_i + L_i \subseteq J(\mathbb{Q}) \\ \downarrow red & & \downarrow red \\ C(\mathbb{F}_p) & \to^{\iota} & J(\mathbb{F}_p) \end{array}$$

$$L_{i+1} := Ker(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p))$$

$$W'_{i+1} := W_i + (L_i / L_{i+1})$$

Satisfies $W'_{i+1} + L_{i+1} = W_i + L_i$.

$$\begin{array}{ccc} C(\mathbb{Q}) & \to^{\iota} & W_i + L_i \subseteq J(\mathbb{Q}) \\ \downarrow red & & \downarrow red \\ C(\mathbb{F}_p) & \to^{\iota} & J(\mathbb{F}_p) \end{array}$$

$$L_{i+1} := Ker(L_i \hookrightarrow J(\mathbb{Q}) \to J(\mathbb{F}_p))$$

$$W'_{i+1} := W_i + (L_i/L_{i+1})$$

Satisfies $W'_{i+1} + L_{i+1} = W_i + L_i$.

$$\begin{array}{ccc} C(\mathbb{Q}) & \to^{\iota} & W'_{i+1} + L_{i+1} \\ \downarrow red & & \downarrow red \\ C(\mathbb{F}_p) & \to^{\iota} & J(\mathbb{F}_p) \end{array} \qquad \leftarrow^{red} \searrow W'_{i+1}$$

$$W_{i+1} := \{w \in W'_{i+1} : red(w) \in \iota(C(\mathbb{F}_p))\}, \text{ and } \iota(C(\mathbb{Q})) \subset W_{i+1} + L_{i+1}.$$

Example (Bugeaud,Mignotte,Stoll,Siksek,Tengely)

Take $C : y^2 - y = x^5 - x$ with $\iota(P) = [P - \infty]$.

$$J(\mathbb{Q}) = \mathbb{Z}[(0,1) - \infty] \oplus \mathbb{Z}[(1,1) - \infty] \oplus \mathbb{Z}[(-1,1) - \infty]$$

Expected:$=\mathcal{U}:=\{\infty, (-1,0), (-1,1), (0,0), (0,1), (1,0), (1,1), (2,-5),$
(2,6),(3,-15),(3,16),(30,-4929),(30,4930),(1/4,15/32),
(1/4,17/32),(-15/16,-185/1024),(-15/16,1209/1024)$\}$
Using primes $p < 10^6$ the authors shown

$$\iota(C(\mathbb{Q})) \subset \iota(\mathcal{U}) + L$$

with $[J(\mathbb{Q}) : L] \sim 3 \times 10^{3240}$.

Height theory, implies P integral $H(P) \leq \mathit{Bound}$ (Baker), and they can conclude for such L that

$$C(\mathbb{Z}) = \{(-1,0),(-1,1),(0,0),(0,1),(1,0),(1,1),(2,-5),$$

(2,6),(3,-15),(3,16),(30,-4929),(30,4930)}.