Rational Points on Curves embedded in a Product of elliptic Curves

Evelina Viada

BIRS Workshop ”Specialisation and Effectiveness in Number Theory”
August 28 - September 2, 2022

Effectivity

Theorem (Faltings Theorem)

The set of rational points on an algebraic curve of genus ≥ 2 is finite.

The result of Faltings is not effective, in the sense that it does not give any method for finding the rational points on C.

This is due to the non existence of an effective bound for the height of the points in $C(\mathbb{Q})$.
Points of bounded height and bounded degree are finitely many.
(Only finitely many integral points in $\mathbb{R}^n$ in a ball of given a radius)

Effective Methods

The method of Chabauty-Coleman provides a bound on the number of rational points on curves with Jacobian of $\mathbb{Q}$-rank strictly smaller than the genus.

Example

Flynn gives **explicit** examples: he finds the rational points for a selection of curves of genus 2 with Jacobian of $\mathbb{Q}$-rank 1.

An innovative application in the context of Chabauty's method is given by J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*.

The Manin-Dem'janenko method applies to curves that admit many $\mathbb{Q}$-independent morphisms towards an abelian variety.

Example

Kulesz, Girard, Matera, Schost and others find all rational points on some families of curves: these curves have genus 2 (resp. 3) and elliptic Jacobian of $\mathbb{Q}$-rank 1 (resp. 2) with some special properties. For instance with factors given by a Weierstrass equation $y^2 = x^3 + a^2x$, with a square-free integer and such that the Mordell-Weil group has rank 1.

No explicit height's bound

The bounds for the height must be worked out with *ad hoc* methods case by case and for the technique to be successful the equations of the curve must be of a special shape and small genus.

Notations

- Ambient variety:
  E an elliptic curve defined over $\overline{\mathbb{Q}}$.
  $E^N = E \times \cdots \times E$.
- The k-rational points for k a number field and $\mathcal{C}$ an algebraic curve are denoted by $\mathcal{C}(k)$.

Anomalous Intersections

Algebraic subgroups of E^N

- An algebraic subgroup B of dimension $N-s$ is the kernel of a matrix $\phi_B \in \mathrm{Mat}_{s,N}(\mathrm{End}(E))$ of rank s

$$\phi_B = \begin{pmatrix} b_{11} & \dots & b_{1,N} \\ \vdots & \vdots & \vdots \\ b_{s,1} & \dots & b_{s,N} \end{pmatrix} : E^N \to E^s$$

$$\phi_B : (x_1, \dots, x_N) \to (b_{11}x_1 + \dots + b_{1N}x_N, \dots, b_{s1}x_1 + \dots + b_{sN}x_N).$$

- Up to constants, $\deg B$ is the volume of the lattice generated by the rows.

Case $N = 2$

An algebraic Subgroup of E^2 is given, up to some torsion, by

$$B = \{b_1 X_1 + b_2 X_2 = 0$$

Consider an algebraic curve $\mathcal{C} \subset E^2$ with rank $E(\mathbb{Q}) = 1$, i.e. $E(\mathbb{Q}) = \langle g_1 \rangle$
Then a point $P = (P_1, P_2) \in \mathcal{C}(\mathbb{Q}) \subset E(\mathbb{Q})^2$ has the form

$$P = (a_1 g_1, a_2 g_1)$$

and therefore is a point in

$$B = \{a_2 X_1 - a_1 X_2 = 0$$

So

$$P \in \mathcal{C} \cap B.$$

If the set

$$\mathcal{C} \cap \bigcup_{dim B = 1} B$$

has bounded height, then $\mathcal{C}(\mathbb{Q})$ has bounded height.

For C of genus ≥ 2,

$$C \cap \bigcup_{dim B = 1} B$$

has bounded height.
This is part of the Anomalous Intersection Conjecture (AIC).
If $E(\mathbb{Q})$ has rank 1 and $C \in E^2$, the proof is effective.

Theorem (AIC)

Let C be weak-transverse in E^N. Then the set

$$C \cap \cup_{\dim B \leq N-2} B \quad \text{is finite.}$$

Here B ranges over all algebraic subgroups of dimension $\leq N-2$.

This theorem implies Faltings Theorem for $C \in E^N$.

Weakness of the method

If $\mathcal{C} \subset E^2$ and rank $E(\mathbb{Q}) = 2$, then there is no subgroup containing P, so no equation and therefore no intersection and no result and maybe no hope.

This is the limit for the effective Mordell Conjecture.

Families of curves of increasing genus

Consider the elliptic curve

$$E : \{y^2 = x^3 + x - 1$$

and the cartesian product

$$E \times E \subset \mathbb{P}^2 \times \mathbb{P}^2$$

where (x_1, y_1) resp. (x_2, y_2) are the affine coordinates of the first resp. second factor.

$E(\mathbb{Q})$ has rank 1.

The Family $\mathcal{C}_n$

Definition

Let $\{\mathcal{C}_n\}_n$ be the family of curves $\mathcal{C}_n \subseteq E^2$ defined for $n \geq 1$ via the additional equation

$$x_1^n = y_2.$$

In affine coordinates

$$\mathcal{C}_n = \begin{cases} y_1^2 & = x_1^3 + x_1 - 1 \\ y_2^2 & = x_2^3 + x_2 - 1 \\ x_1^n & = y_2 \end{cases}$$

The $\mathcal{C}_n$ have genus $4n+2$.

Our explicit bound on the height of $\mathcal{C}_n(\mathbb{Q})$ implies:

The rational points on the curves are

$$\mathcal{C}_n(\mathbb{Q}) = \{(1, \pm 1) \times (1, 1)\}.$$

The Family $\mathcal{D}_n$

Definition

Let $\{\mathcal{D}_n\}_n$ be the family of curves $\mathcal{D}_n \subseteq E^2$ defined for $n \geq 1$ via the additional equation

$$\Phi_n(x_1) = y_2,$$

where $\Phi_n(x)$ is the n-th cyclotomic polynomial.

In affine coordinates

$$\mathcal{D}_n = \begin{cases} y_1^2 & = x_1^3 + x_1 - 1 \\ y_2^2 & = x_2^3 + x_2 - 1 \\ \Phi_n(x_1) & = y_2 \end{cases}$$

The $\mathcal{D}_n$ have increasing genus.

Our explicit bound on the height of $\mathcal{D}_n(\mathbb{Q})$ implies that:

$$\mathcal{D}_1(\mathbb{Q}) = (2, \pm 3) \times (1, 1)$$
$$\mathcal{D}_2(\mathbb{Q}) = (2, \pm 3) \times (2, 3)$$
$$\mathcal{D}_{3^k}(\mathbb{Q}) = (1, \pm 1) \times (2, 3)$$
$$\mathcal{D}_{47^k}(\mathbb{Q}) = (1, \pm 1) \times (13, 47)$$
$$\mathcal{D}_{p^k}(\mathbb{Q}) = \varnothing \text{ if } p \neq 3, 47 \text{ or } p = 2 \text{ and } k > 1$$
$$\mathcal{D}_6(\mathbb{Q}) = (1, \pm 1) \times (1, 1) \text{ and } (2, \pm 3) \times (2, 3)$$
$$\mathcal{D}_n(\mathbb{Q}) = (1, \pm 1) \times (1, 1) \text{ if } n \neq 6 \text{ has at least two distinct prime factors.}$$

The $\mathbb{Q}(\sqrt{-3})$-rational points

Let E be defined by the equation

$$y^2 = x^3 + 2.$$

Consider the family $C_n \in E^2$

$E(\mathbb{Q}(\sqrt{-3}))$ has rank 2.

But E has CM by $\mathbb{Z}[\zeta]$ and $E(\mathbb{Q}(\sqrt{-3}))$ has $\mathbb{Z}[\zeta]$-rank 1.

So there is $B = \{a_1 X_1 + a_2 X_2 = 0$ that contains P
Then $\mathrm{End}(\mathrm{E}) = \mathbb{Z}[\zeta]$ for $\zeta = \frac{-1+\sqrt{-3}}{2}$ a primitive cube root of 1.
Let $g = (-1 : 1 : 1)$ and $O = (0 : 1 : 0)$ in $E(\mathbb{Q})$.

The $\mathbb{Q}(\sqrt{-3})$-rational points on the family $C_n \in E^2$

In affine coordinates

$$C_n = \begin{cases} y_1^2 &= x_1^3 + 2 \\ y_2^2 &= x_2^3 + 2 \\ x_1^n &= y_2 \end{cases}$$

Our explicit bound on the height of $C_n(\mathbb{Q}(\sqrt{-3}))$ implies:

$$\begin{aligned}
&C_n(\mathbb{Q}(\sqrt{-3})) \setminus \{(O,O)\} = \\
&= \{(ag, bg) \mid a = \pm 1, \pm\zeta, \pm\zeta^2 \text{ and } b = 1, \zeta, \zeta^2\} && \text{if } n \equiv 0 \pmod 6 \\
&= \{(ag, bg) \mid a = \pm 1 \text{ and } b = -1, -\zeta, -\zeta^2\} && \text{if } n \equiv \pm 1 \pmod 6 \\
&= \{(ag, bg) \mid a = \pm 1 \text{ and } b = 1, \zeta, \zeta^2\} && \text{if } n \equiv \pm 2 \pmod 6 \\
&= \{(ag, bg) \mid a = \pm 1, \pm\zeta, \pm\zeta^2 \text{ and } b = -1, -\zeta, -\zeta^2\} && \text{if } n \equiv 3 \pmod 6,
\end{aligned}$$

The $\mathbb{Q}(\sqrt{-3})$-rational points on the family $\mathcal{D}_n$

In affine coordinates

$$\mathcal{D}_n = \begin{cases} y_1^2 & = x_1^3 + 2 \\ y_2^2 & = x_2^3 + 2 \\ \Phi_n(x_1) & = y_2 \end{cases}$$

Our explicit bound on the height of $\mathcal{D}_n(\mathbb{Q}(\sqrt{-3}))$ implies that:

$$\mathcal{D}_n(\mathbb{Q}(\sqrt{-3})) = \{(O,O)\}$$

if $n = 1, 2,$ or $n = 2p^k$ for $k \geq 1$ and p a prime number

$$\mathcal{D}_n(\mathbb{Q}(\sqrt{-3})) = \{(\pm g, g)\} \cup \{(O,O)\} \qquad \text{otherwise.}$$

Main results on Bounded Height

Let E be an elliptic curve given in the form

$$y^2 = x^3 + Ax + B.$$

with A, B algebraic integers.
Let $\hat{h}$ be the Néron-Tate height on E^N.
Let $h(\mathcal{C})$ be the normalised height of $\mathcal{C}$.

Theorem (VV2022: Veneziano, V. (generalization of N=2 Checcoli, Veneziano, V. 2018))

Let E be a non-CM elliptic curve and let $\mathcal{C}$ be a curve transverse in E^N. Then all the points P of rank at most $N-1$ on $\mathcal{C}$ have Néron-Tate height explicitely bounded as follows:

$$\hat{h}(P) \leq D(N) \cdot h(\mathcal{C})(\deg \mathcal{C})^{N-1} + D_2(N,E)(\deg \mathcal{C})^N + D_3(N,E).$$

The constants are given by:

$$D(N) = 4N! \left(\frac{N^2(N-1)^2 3^N}{4^{N-3}} N!(N-1)!^4 \right)^{N-1},$$

$$D_2(N,E) = D_1(N) \left(N^2 C(E) + 3^N \log 2 \right),$$

$$D_3(N,E) = (N+1)C(E) + 1,$$

Theorem (VV2022: Veneziano, V.)

Let E be an elliptic curve with Complex Multiplication by the field K and let $\mathcal{C}$ be a curve transverse in E^N. Then all the points P of $\mathrm{End}(\mathrm{E})$-rank at most $N-1$ on $\mathcal{C}$ have Néron-Tate height explicitely bounded as follows:

$$\hat{h}(P) \leq C_1(N,E) \cdot h(\mathcal{C})(\deg \mathcal{C})^{N-1} + C_2(N,E)(\deg \mathcal{C})^N + C_3(N,E).$$

The constants are given by:

$$\begin{aligned}
C(N) &= N! \left(N \cdot N! \cdot (2N)!^2\right)^{N-1}, \\
C_1(N,E) &= c(N) f^N |D_K|^{N^2 - \frac{3}{2}N + 1} + 1, \\
C_2(N,E) &= c(N) f^N |D_K|^{N^2 - \frac{3}{2}N + 1} \left(N^2 C(E) + 3^N \log 2 + 1\right), \\
C_3(N,E) &= N(N+1)C(E) + 3^N \log 2 + 1.
\end{aligned}$$

where D_K is the discriminant of the field of complex multiplication and f is the conductor of $\mathrm{End}(\mathrm{E})$.

Invariants of the curves

Theorem

Let $\mathcal{C}$ be the curve given in E^2 cut by the additional equation

$$p(x_1) = y_2,$$

with $p(X) \in k[X]$ a non-constant polynomial of degree n. Then

$$\deg \mathcal{C} = 6n + 9$$

and

$$h(\mathcal{C}) \leq 2 \deg \mathcal{C} \left(h_W(p) + \log n + 2c_1(E) \right)$$

where $h_W(p) = h_W(1 : p_0 : \ldots : p_n)$ is the height of the coefficients of $p(X)$.

Applying Theorem VV in Explicit Examples

Choice of the ambient variety. Elliptic curves without CM and of rank 1 over $\mathbb{Q}$:

$$E_1 : y^2 = x^3 + x - 1,$$
$$E_2 : y^2 = x^3 - 26811x - 7320618,$$
$$E_3 : y^2 = x^3 - 675243x - 213578586,$$
$$E_4 : y^2 = x^3 - 110038419x + 12067837188462,$$
$$E_5 : y^2 = x^3 - 2581990371x - 50433763600098.$$

$$\deg \mathcal{C}_n = 6n+9,$$
$$h(\mathcal{C}_n) \leq 6(2n+3)\log(3+|A|+|B|).$$

The $\mathcal{C}_n$ have genus $4n+2$.

$$\deg \mathcal{D}_n = 6\varphi(n)+9,$$
$$h(\mathcal{D}_n) \leq 6(2\varphi(n)+3)\left(2^{\omega_2(n)}\log 2 + 2\log(3+|A|+|B|)\right),$$

where $\varphi(n)$ is the Euler function, $\omega_2(n)$ is the number of distinct odd prime factors of n.
The $\mathcal{D}_n$ have increasing genus.

Plug the invariants in Theorem VV

For every $n \geq 1$ and every point $P \in \mathcal{C}_n(\mathbb{Q})$ we have

$$\hat{h}(P) \leq 1301\,(4c_6(E))\,(2n+3)^2 + 4c_6(E).$$

For every $n \geq 2$ and every point $P \in \mathcal{D}_n(\mathbb{Q})$ we have

$$\hat{h}(P) \leq 1302\left(2^{\omega_2(n)}\log 2 + 4c_6(E)\right)(2\varphi(n)+3)^2 + 4c_6(E)$$

were $c_6(E) = \log(3+|A|+|B|)$.

Applying Theorem VV to explicit examples

Let E be the elliptic curve

$$E : y^2 = x^3 + 2.$$

This curve E has complex multiplication by a third root of 1, given by

$$(x, y) \mapsto (\zeta x, y)$$

with $\zeta = \frac{-1+\sqrt{-3}}{2}$.
Its discriminant is 1728 and its j-invariant is 0.
The field of complex multiplication is $K = \mathbb{Q}(\zeta)$, which has discriminant $D_K = -3$, $\mathrm{End}(\mathrm{E}) = \mathbb{Z}[\zeta]$ and conductor $f = 1$.
The set

$$E(K) = \langle g, \zeta \cdot g \rangle_{\mathbb{Q}}$$

for $g = (-1, 1)$. Moreover $\hat{h}(g) \approx 1.1319$.

Computing the relevant coefficients we get

$$\begin{aligned} C(E) &\leq 6.211 \\ C_1(2,E) &\leq 2101 \\ C_2(2,E) &\leq 67638 \\ C_3(2,E) &\leq 13.1 \end{aligned}$$

We proved that

$$\begin{aligned} \deg \mathcal{C}_n &= 6n+9, \\ h(\mathcal{C}_n) &\leq 6\log 5(2n+3), \\ \deg \mathcal{D}_n &= 6\varphi(n)+9, \\ h(\mathcal{D}_n) &\leq 6(2\varphi(n)+3)\left(\varphi(n)\log 2+\log 5\right). \end{aligned}$$

Plagging all in our CM theorem VV it follows that

$$\hat{h}(P) \leq 644391 \cdot (2n+3)^2 + 28 \tag{1}$$

if $P \in \mathcal{C}_n(K)$, while

$$\hat{h}(P) \leq 644391 \cdot (2\varphi(n)+3)^2 + 28 \tag{2}$$

if $P \in \mathcal{D}_n(K)$.

Applying a generalisation of a result of Stoll, we see that

$$C_n(K) = C_n(O_K) \text{ for } n > 21$$

and only the curves with $n \leq 20$ need to be checked for additional points.
It can be checked that $E(O_K) = \{\pm g, \pm\zeta g, \pm\zeta^2 g\}$, from which we obtain the points listed above.

A computer calculation shows that there are no other points on $\mathcal{C}_n(K)$ for $n \leq 20$, which completes the proof of the theorem.

Search algorithm by K. Belabas, B. Allombert

20

Algorithm 1 Checking for rational points on $\mathcal{C}_n(K)$

1: $E :=$ the elliptic curve defined by $y^2 = x^3 + 2$
2: g := the point $(-1, 1) \in E(\mathbb{Q})$
3: ζ a primitive third root of unity
4: **for** n $= 1$ **to** 20 **do**
5: Ma := the upper bound for $|a|$ in equation (22)
6: Mb := the upper bound for $|b|$ in equation (23)
7: p $:= 7$
8: Initialize L to a list containing all pairs of integers (a, b) with $|a| \leq$ Ma and $1 \leq b \leq$ Mb
9: c $:= 0$
10: **while true do**
11: g2 := the reduction modulo p of the point ζg
12: NL := the cardinality of L
13: $E_p :=$ the reduction of E modulo p
14: Np := the cardinality of E_p
15: Mpa $:= \min($Ma, Np $- 1)$
16: Mpb $:= \min($Mb, Np $- 1)$
17: **for** a $= -$Mpa **to** Mpa **do**
18: ag := the point [a]g $\in E_p$
19: **for** b $= 1$ **to** Mpb **do**
20: ag := the point ag + g2 in E_p
21: **if** ag is the point at infinity **then**
22: Remove the pair (a, b) from L
23: **next**
24: **end if**
25: x := the first coordinate of the point ag
26: **if** The congruence $X^3 + 2 \equiv$ x^{2*n} (mod p) has no solution **then**
27: Remove from L all pairs (a, b) such that $a \equiv$ a (mod Np) and $b \equiv$ b (mod Np)
28: **end if**
29: **end for**
30: **end for**
31: **if** The cardinality of L is equal to c **then**
32: c $:=$ c $+ 1$
33: **end if**
34: **if** The cardinality of L is zero, **or** c > 15 **then**
35: **break**
36: **end if**
37: p := the next prime after p which is congruent to 1 modulo 3
38: **end while**
39: **end for**

Example for $N = 3$

Let $\mathcal{C} \in E^3$ with rank $E(\mathbb{Q}) = 2$.
For instance $E := \{y^2 = x^3 - 3x + 1$ has rank 2. Let $\mathcal{C}$ be defined in E^3 by the equations $x_1 = y_2$ and $x_2 = y_3$. Compute all invariants, plug them in Theorem VV and for $P \in \mathcal{C}(\mathbb{Q})$ you get

$$\hat{h}(P) \leq 10^{22}$$

NOT IMPLEMENTABLE

Use the fact that there are generators of $E(\mathbb{Q})$ with angle of 45 degree to improve the bound to

$$\hat{h}(P) \leq 10^{19}$$

Use sharp comparison of $h(P)$ and $\hat{h}(P)$ to improve the bound to

$$\hat{h}(P) \leq 10^{16}$$

Maybe implementable

A hope to overcome the rank condition

Consider $E := \{y^2 = x^3 - 3x + 1$ has rank 2.
Let $\mathcal{C}$ be defined in E^2 by the equation $x_1 = y_2$.

No effective theorem applies in this case.

With Fabien Pazuki we investigate the possibility to reduce the problem of bounding the height of the rational points to some strong conjectures on the height properties of the generators of $E(\mathbb{Q})$. It seams that in this specific case the conjectures can be checked by hand using a computer program.

THANK YOU