

Uniform bounds for the number of rational points of families of curves of genus 2^{*}

P. Gaudry¹, L. Kulesz², G. Matera², É. Schost³

¹ LIX, École Polytechnique, F-91128 Palaiseau Cedex, France,
gaudry@lix.polytechnique.fr.

² Instituto de Desarrollo Humano

Universidad Nacional de General Sarmiento
Campus Universitario, José M. Gutiérrez entre José L. Suárez y Verdi
(1613) Los Polvorines, Pcia. de Buenos Aires, Argentina
{lkulesz,gmatera}@ungs.edu.ar.

³ Laboratoire GAGE, École Polytechnique, F-91128 Palaiseau cedex, France,
schost@gage.polytechnique.fr.

Abstract We construct an infinite family $\{\mathcal{C}_{a,b}\}_{a,b \in \mathbb{Q}}$ of curves of genus 2 defined over \mathbb{Q} , with two independent morphisms to a family of elliptic curves $\{\mathcal{E}_{a,b}\}_{a,b \in \mathbb{Q}}$. When any of these elliptic curves $\mathcal{E}_{a,b}$ has rank 1 over \mathbb{Q} , we obtain (modulo a conjecture of S. Lang, proved for special cases) a uniform bound for the number of rational points of the curve $\mathcal{C}_{a,b}$, and an algorithm which finds all the rational points of the curve $\mathcal{C}_{a,b}$.

1 Introduction

Diophantine geometry is mainly concerned with the search for integer or rational solutions of multivariate polynomial equation systems

$$f_1(X_1, \dots, X_n) = 0, \dots, f_r(X_1, \dots, X_n) = 0, \quad (1)$$

where f_1, \dots, f_r are polynomials in $\mathbb{Z}[X_1, \dots, X_n]$.

Typical problems of diophantine geometry are the following decision problems:

- (i) Does there exist a solution $(x_1, \dots, x_n) \in \mathbb{Z}^n$ of the system (1)?
- (ii) Does there exist a solution $(x_1, \dots, x_n) \in \mathbb{Q}^n$ of the system (1)?

As the set of points

$$V := \{x \in \mathbb{C}^n : f_1(x) = 0, \dots, f_n(x) = 0\}$$

defines a \mathbb{Q} -definable algebraic variety, we may rephrase the problems above in the following way:

* Research was partially supported by the following Argentinian and French grants :
UBA-CYT X198, PIP CONICET 4571, ECOS A99E06.

- (i) Does there exist a point $(x_1, \dots, x_n) \in \mathbb{Z}^n$ in the variety V ?
- (ii) Does there exist a point $(x_1, \dots, x_n) \in \mathbb{Q}^n$ in the variety V ?

A point $(x_1, \dots, x_n) \in \mathbb{Q}^n \cap V$ is called a *rational point* (or \mathbb{Q} -*rational point*) of the variety V .

Problem (i) is the so-called Hilbert’s 10th Problem over \mathbb{Z} and was proved to be *undecidable* by Y. Matiyasevich [Mat70]. On the other hand, it is not known whether there exists an algorithm which solves Problem (ii), known as Hilbert’s 10th Problem over \mathbb{Q} (see [Poo01]). Let us finally remark that the first order theory over \mathbb{Q} is also undecidable [Rob49].

Furthermore, it is not even known whether there exists an algorithm solving Problem (ii) in the case of algebraic plane curves, i.e., an algorithm answering the following question:

- (ii’) Given a polynomial $f \in \mathbb{Q}[X, Y]$, does there exist a \mathbb{Q} -rational point in the algebraic plane curve $\mathcal{C} := \{(x, y) \in \mathbb{C}^2 : f(x, y) = 0\}$?

Nevertheless, in the case of Problem (ii’) we have qualitative results such as Faltings’ Theorem [Fal83], which roughly asserts that the set of \mathbb{Q} -rational points of a \mathbb{Q} -definable smooth curve of genus at least 2 is finite. The genus of a curve \mathcal{C} is a geometric invariant which measures how complicated are the singularities of the curve \mathcal{C} . Curves of genus 0 are isomorphic to a conic, and curves of genus 1 with a rational point are elliptic curves (see Section 2).

Problem (i) and (ii) are related to the use of *arithmetic circuits* as data structures in computer science. Arithmetic circuits have been extensively used to modelize algebraic computations (see e.g. [Par95] or [BCS97]). In particular, the use of arithmetic circuits as data structures has been proved to be very useful for the design of efficient algorithms for the solution of multivariate parametric polynomial equation systems (see e.g. [KP96], [GHM⁺98], [GHH⁺97], [HKP⁺00]).

The general context of parametric polynomial equation solving can be described as follows:

Let $\Gamma(T, X)$ be a system of polynomial equations in the variables $X := (X_1, \dots, X_n)$, depending on parameters $T := (T_1, \dots, T_m)$. Thus any parameter point $t \in \mathbb{C}^m$ determines a *specific* problem instance $\Gamma(t, X)$. Let us assume that any such problem instance admits a finite, nonempty set of solutions belonging to \mathbb{C}^n . Let Y be a new variable. The output of a typical algorithm which “solves” the system is a (parametric) arithmetic circuit $\beta(T, Y)$ of length L , which represents a univariate polynomial $F(T, Y)$ describing the projection of the solution set of the parametric system $\Gamma(T, X)$ on a suitable straight-line. We are interested in minimizing the length L of the circuit representation of the polynomial $F(T, Y)$. This leads us to the following problem:

Let $f \in \mathbb{Q}[Y]$ be a given univariate polynomial. Find a *short* circuit with *rational* parameters which evaluates the polynomial f .

It is well-known that the vector of coefficients of a univariate polynomial $f \in \mathbb{Q}[Y]$ of degree d represented by an arithmetic circuit of length L belongs to a \mathbb{Q} -definable algebraic variety of $\mathbb{C}^{L^{O(1)}}$ (see e.g. [BCS97]). Therefore, our problem can be easily restated as the search for a rational solution of a suitable algebraic variety of $\mathbb{C}^{L^{O(1)}}$. The existence of an arithmetic circuit of length L representing the given polynomial f is then equivalent to the existence of a rational solution of a suitable instance of Problem (ii).

In connection with Problems (i) and (ii) and Faltings' Theorem, we have the following conjecture of S. Lang [Lan86]:

Conjecture A. *Let V a variety of general type defined over a number field \mathbb{K} . Then, the set $V(\mathbb{K})$ of \mathbb{K} -rational points of V is contained in a subvariety of V of codimension greater than 1.*

Conjecture A in its full generality is very difficult to attack and we do not know of any attempt in this direction. On the other hand, L. Caporaso, J. Harris and B. Mazur showed the following consequence of this conjecture in the case of algebraic curves (see [CHM95], [CHM97]):

Theorem 1. *If Conjecture A is true, then for any number field \mathbb{K} and any integer $g \geq 2$, there exists an integer $B(\mathbb{K}, g)$ such that any non-singular \mathbb{K} -definable curve of genus g has at most $B(\mathbb{K}, g)$ \mathbb{K} -rational points.*

This (conjectural) result generalizes Mordell's Conjecture, now Faltings' Theorem, which asserts that the set of \mathbb{K} -rational points of any \mathbb{K} -definable curve of genus ≥ 2 is finite.

We know very few results in the direction of Theorem 1. In [Kul99], the author constructs an infinite family of \mathbb{Q} -definable curves of genus 2 which covers the elliptic curve $\mathcal{E}_a : Y^2 = X^3 - a^2X$ and obtains a uniform bound for the cardinality of the set of rational points of any member of this family.

In this article we obtain this kind of estimates for more general families of curves of genus two. Let us also remark that such estimates also implies the existence of an algorithm computing the set of rational points of any member of the families under consideration by exhaustive search. In order to simplify the exposition we will restrict ourselves to the analysis of \mathbb{Q} -rational points of \mathbb{Q} -definable curves, but proofs also hold for any number field \mathbb{K} .

2 Generalities

In this section we recall some notions and results about elliptic curves, heights and morphisms. Details can be found in [Kna92] and [Sil86].

2.1 Elliptic Curves

A nonsingular homogeneous cubic polynomial $F(X_0, X_1, X_2)$ of $\mathbb{Q}[X_0, X_1, X_2]$ defines a (projective) *elliptic curve* if it vanishes on at least one rational point. It can be shown that any elliptic curve \mathcal{E} over \mathbb{Q} is isomorphic to the projective closure of an affine curve of equation $Y^2 = X^3 + AX + B$ for some $A, B \in \mathbb{Z}$ with $4A^3 + 27B^2 \neq 0$.

We denote by $\Delta(\mathcal{E})$ and $j(\mathcal{E})$ the *discriminant* and the *j-invariant* of the elliptic curve \mathcal{E} defined as follows:

$$\Delta(\mathcal{E}) = 16(4A^3 - 27B^2), \quad j(\mathcal{E}) = 1728 \frac{(4A)^3}{\Delta(\mathcal{E})}.$$

Elliptic curves with the same j -invariant are isomorphic.

In 1922, L.J. Mordell proved the following theorem, conjectured by H. Poincaré:

Theorem 2. *Let \mathcal{E} be an elliptic curve over \mathbb{Q} . Then $\mathcal{E}(\mathbb{Q})$ is a finitely generated abelian group.*

We denote the torsion subgroup of $\mathcal{E}(\mathbb{Q})$ and the rank of the free part of $\mathcal{E}(\mathbb{Q})$ by $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ and $r_{\mathbb{Q}}(\mathcal{E})$ respectively. In 1976, B. Mazur proved the following result, conjecture of Beppo Levi in 1908 [Maz78]:

Theorem 3. *For any elliptic curve \mathcal{E} defined over \mathbb{Q} , the torsion subgroup $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups: $\mathbb{Z}/m\mathbb{Z}$ for $m \leq 10$ or 12, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $m \leq 4$.*

Let $n \in \mathbb{Z} \setminus \{0\}$ and $P \in \mathcal{E}$. We denote by $[n]$ the morphism of multiplication by n in \mathcal{E} , namely:

$$[n] : \mathcal{E} \rightarrow \mathcal{E} \\ P \mapsto \underbrace{P + \dots + P}_{n \text{ times}}.$$

The degree of this morphism is n^2 .

2.2 Heights

Let x be a rational number. Let us write $x = \frac{x_1}{x_2}$ with $x_1 \in \mathbb{Z}$, $x_2 \in \mathbb{N}^*$ and $\gcd(x_1, x_2) = 1$. We define the (naive) *height* of x , $h(x)$, as the quantity $h(x) := \log(\max\{|x_1|, |x_2|\})$.

Let \mathcal{C} be a \mathbb{Q} -definable algebraic curve of \mathbb{A}^2 and $P = (x, y)$ be a rational point of $\mathcal{C}(\mathbb{Q})$. We define the (naive) height of P , $h(P)$, as $h(P) = h(x)$.

Suppose now that the curve \mathcal{C} has genus two. Then it has been shown that \mathcal{C} is defined by an equation of the form $Y^2 = p(X)$, where $p(X)$ is a polynomial of $\mathbb{Q}[X]$ of degree 6. If we assume further that there exists a \mathbb{Q} -definable morphism mapping the curve \mathcal{C} to a \mathbb{Q} -definable elliptic curve \mathcal{E} , then it can be shown

that \mathcal{C} is defined by an equation of the form $Y^2 = aX^6 + bX^4 + cX^2 + d$, where $a, b, c, d \in \mathbb{Q}$ (see [CaF196]).

In this work we are going to consider the family of curves $\{\mathcal{C}_{a,b}\}_{a,b \in \mathbb{Q}}$ defined by the equation $Y^2 = aX^6 + bX^4 + bX^2 + a$. Let us denote by $\mathcal{E}_{a,b}$ the elliptic curve defined by the equation $Y^2 = aX^3 + bX^2 + bX + a$. Let $\phi_1, \phi_2 : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ be the morphisms $\phi_1(X, Y) = (X^2, Y)$ and $\phi_2(X, Y) = (\frac{1}{X^2}, \frac{Y}{X^3})$. Then that for any $(a, b) \in \mathbb{Q}^2$ the morphisms ϕ_1, ϕ_2 map the curve $\mathcal{C}_{a,b}$ to the elliptic curve $\mathcal{E}_{a,b}$.

Let us observe that, from the definition of the (naive) height of a rational point of an algebraic curve, we easily deduce that, for any $(a, b) \in \mathbb{Q}^2$ and any $P \in \mathcal{C}_{a,b}$, the following identity holds:

$$h(\phi_1(P)) = h(\phi_2(P)). \quad (2)$$

On the other hand, we have the notion of a *canonical height* of rational point of an elliptic curve \mathcal{E} defined over \mathbb{Q} . Let \mathcal{E} be an elliptic curve defined over \mathbb{Q} and let P be a rational point in $\mathcal{E}(\mathbb{Q})$. We define the canonical height of P , $\hat{h}(P)$, by the formula $\hat{h}(P) = \lim_{n \rightarrow \infty} 4^{-n} h([2^n]P)$. The canonical height $\hat{h}(P)$ satisfies the following properties:

- Theorem 4.** (i) $\hat{h}(P) = h(P) + O(1)$.
(ii) $\hat{h}(mP) = m^2 \hat{h}(P)$ for any $m \in \mathbb{Z}$.
(iii) $\langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q))$ is bi-additive.
(iv) Given n points $P_1, \dots, P_n \in \mathcal{E}(\mathbb{Q})$, P_1, \dots, P_n are independent if and only if the $n \times n$ matrix with entries $\langle P_i, P_j \rangle$ is invertible.

In this paper we will make use of the following conjecture, due to S. Lang:

Conjecture B: *There exists a constant c such that for any elliptic curve \mathcal{E} defined over \mathbb{Q} of discriminant Δ and any rational point $P \in \mathcal{E}(\mathbb{Q})$ of infinite order, the estimate $\hat{h}(P) > ch(\Delta)$ holds.*

Let us remark that Lang's Conjecture B has been proved to be true for elliptic curves with complex multiplication (see [Sil94]).

Theorem 4(i) asserts that for any point $P \in \mathcal{E}(\mathbb{Q})$ of an elliptic curve \mathcal{E} defined over \mathbb{Q} , the difference $\hat{h}(P) - h(P)$ can be bounded by a constant depending only on the elliptic curve \mathcal{E} . J. Silverman found the following explicit estimates for the difference $\hat{h}(P) - h(P)$ in terms of the discriminant Δ and the j -invariant j of the elliptic curve \mathcal{E} under consideration [Sil90]:

Theorem 5. *If \mathcal{E} is a \mathbb{Q} -definable elliptic curve, then for any point P of $\mathcal{E}(\mathbb{Q})$ we have the estimates:*

$$-\frac{1}{4}h(j) - \frac{1}{6}h(\Delta) - 1.946 \leq \hat{h}(P) - h(P) \leq \frac{1}{6}h(\Delta) + \frac{1}{6}h(j) + 2.14. \quad (3)$$

2.3 Independent Morphisms

Let \mathcal{C} be a nonsingular \mathbb{Q} -definable curve of \mathbb{P}^2 , let \mathcal{E} be a \mathbb{Q} -definable elliptic curve and let us assume that there exist l \mathbb{Q} -definable morphisms ϕ_1, \dots, ϕ_l mapping \mathcal{C} to \mathcal{E} . These morphisms may be considered as elements of the ring $k(\mathcal{C})^2$, where $k(\mathcal{C})$ denotes the field of rational functions of the curve \mathcal{C} .

Definition 1. *We say that the morphisms ϕ_1, \dots, ϕ_l are independent if the relation $\sum_{i=1}^l n_i \phi_i = P \in \mathcal{E}(\mathbb{Q})$ (i.e., $\sum_{i=1}^l n_i \phi_i$ is a constant in $k(\mathcal{C})^2$) implies $n_i = 0$ for $1 \leq i \leq l$.*

In 1967, J.W. Cassels found a very useful characterization of the independence of morphisms [Cas68]:

Lemma 1. *Let ϕ_1, \dots, ϕ_l be morphisms mapping a curve \mathcal{C} to an elliptic curve \mathcal{E} . Let D be the $(l \times l)$ -matrix whose (i, j) -entry is given by the expression:*

$$\frac{1}{2}(d(\phi_i + \phi_j) - d(\phi_i) - d(\phi_j))$$

for $1 \leq i, j \leq l$, where $d(\psi)$ denotes the degree of the morphism $\psi : \mathbb{C} \rightarrow \mathbb{C}$. Then the morphisms ϕ_1, \dots, ϕ_l are independent over \mathbb{Q} if and only if $\det(D) \neq 0$ holds.

In the context of the curves $\mathcal{C}_{a,b}$, a direct computation shows that $(\phi_1 + \phi_2)(X, Y) = (f_+(X), Yg_+(X))$ and $(\phi_1 - \phi_2)(X, Y) = (f_-(X), Yg_-(X))$ where

$$f_+(X) = \frac{-2aX^3 - 3aX^2 - 2aX + bX^2}{a(X^4 + 2X^3 + 2X^2 + 2X + 1)},$$

$$f_-(X) = \frac{2aX^3 - 3aX^2 + 2aX + bX^2}{a(X^4 - 2X^3 + 2X^2 - 2X + 1)}.$$

This shows that the degrees of the maps $\phi_1, \phi_2, \phi_1 \pm \phi_2$ are respectively 2, 2, 4. By Lemma 1 we easily deduce that ϕ_1 and ϕ_2 are independent over \mathbb{Q} .

3 Our Results

3.1 Dem'janenko–Manin's Method

As expressed in Introduction, we know that a curve of genus ≥ 2 has at most finitely many rational points. Unfortunately, there remains unsolved the very difficult problem of the explicit computation of the set of rational points of a given curve. Up to now, there are two methods which allow us to compute this set:

- 1) The Chabauty's method [Cha41], made effective by Coleman [Col85].

2) The Dem'janenko's method [Dem68], generalized by Manin [Man69].

These methods apply to particular cases. More precisely, Chabauty's method applies to curves of genus g whose Jacobian has rank $< g$ over \mathbb{Q} , and Dem'janenko–Manin's method applies to curves that admit l independent morphisms to an elliptic curve of rank $< l$ over \mathbb{Q} .

Dem'janenko–Manin's method relies on the following result (see [Dem68], [Cas68], [Ser89]):

Theorem 6. *If ϕ_1, \dots, ϕ_l are independent morphisms over \mathbb{Q} and $l > r_{\mathbb{Q}}(\mathcal{E})$ holds, then $\mathcal{C}(\mathbb{Q})$ is a finite set, and all its elements can be effectively computed.*

Let us consider the family of curves $\{\mathcal{C}_{a,b}\}_{a,b \in \mathbb{Q}}$ defined in Section 2.2. We have shown that there exist two independent morphisms of degree two mapping the curve $\mathcal{C}_{a,b}$ to the elliptic curve $\mathcal{E}_{a,b}$, namely, $\phi_1(X, Y) = (X^2, Y)$ and $\phi_2(X, Y) = (\frac{1}{X^2}, \frac{Y}{X^3})$. Let us assume that $\mathcal{E}_{a,b}$ has rank one over \mathbb{Q} .

Now we sketch the proof of Theorem 6 for the family of curves $\{\mathcal{C}_{a,b}\}_{a,b \in \mathbb{Q}}$. Let us remark that the proof of Theorem 6 also provides an *algorithm* which finds all the rational points on any curve of the family $\{\mathcal{C}_{a,b}\}_{a,b \in \mathbb{Q}}$.

Let R be a generator of the free part of $\mathcal{E}_{a,b}(\mathbb{Q})$. For any point P in $\mathcal{C}_{a,b}(\mathbb{Q})$, there exist integers n, m and points $T_1, T_2 \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$ satisfying the following identities:

$$\phi_1(P) = [n]R + T_1$$

$$\phi_2(P) = [m]R + T_2.$$

On the other hand, from Theorem 3 we deduce that the choice $u = 8 \cdot 9 \cdot 7 \cdot 5$ implies the relation $[u]T = 0$ for any $T \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$. Then, we have

$$[u]\phi_1(P) = [un]R,$$

$$[u]\phi_2(P) = [um]R.$$

Therefore,

$$\hat{h}(\phi_1(P)) = n^2 \hat{h}(R), \tag{4}$$

$$\hat{h}(\phi_2(P)) = m^2 \hat{h}(R).$$

Let us observe that the following estimate holds:

$$\begin{aligned} |\hat{h}(\phi_1(P)) - \hat{h}(\phi_2(P))| &\leq |\hat{h}(\phi_1(P)) - h(\phi_1(P))| + |\hat{h}(\phi_2(P)) - h(\phi_2(P))| + \\ &+ |h(\phi_1(P)) - h(\phi_2(P))|. \end{aligned} \tag{5}$$

If $\phi_1(P) \pm \phi_2(P) \notin \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$, Equations (2), (3), (4) and (5) imply the existence of a constant k (depending only on $\mathcal{E}_{a,b}$, ϕ_1 and ϕ_2) such that $|m^2 - n^2| < k$. This implies the estimate

$$\min(|n|, |m|) < \frac{k}{2}. \quad (6)$$

Therefore, we can compute all the \mathbb{Q} -rational points of \mathcal{C} satisfying the condition $\phi_1(P) \pm \phi_2(P) \notin \mathcal{E}(\mathbb{Q})_{\text{tors}}$.

Now suppose $\phi_1(P) \pm \phi_2(P) \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$. Taking into account that the morphisms ϕ_1 and ϕ_2 are independent over \mathbb{Q} we conclude that there exists only a finite set of rational points P such that the condition $\phi_1(P) \pm \phi_2(P) \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$ holds. These points can be determined by a direct computation. Then in this case we also obtain effectively all the \mathbb{Q} -rational points of the curve $\mathcal{C}_{a,b}$.

3.2 A Uniform Bound

Taking into account the identity $h(\phi_1(x, y)) = h(\phi_2(x, y)) = h(x^2)$, from estimates (3), (5) and Theorem 5 we deduce the following estimates for any point $P \in \mathcal{C}_{a,b}(\mathbb{Q})$:

$$\begin{aligned} |\hat{h}(\phi_1(P)) - \hat{h}(\phi_2(P))| &\leq |\hat{h}(\phi_1(P)) - h(\phi_1(P))| + |\hat{h}(\phi_2(P)) - h(\phi_2(P))| \\ &\leq \frac{1}{2}h(j) + \frac{1}{3}h(\Delta) + 4.28, \end{aligned} \quad (7)$$

where j and Δ denote the invariant and the discriminant of the curve $\mathcal{E}_{a,b}$.

Let us suppose that the rank of the elliptic curve $\mathcal{E}_{a,b}(\mathbb{Q})$ is 1. Let R be a generator of the free part of the group $\mathcal{E}_{a,b}(\mathbb{Q})$. Then, for any point P of $\mathcal{C}_{a,b}(\mathbb{Q})$, there exist integers n, m and points $T_1, T_2 \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$ such that the following estimates hold:

$$\phi_1(P) = [n]R + T_1,$$

$$\phi_2(P) = [m]R + T_2.$$

Suppose now that $n \neq \pm m$ holds. Then estimate (7) implies $(n^2 - m^2)\hat{h}(R) \leq \frac{1}{2}h(j) + \frac{1}{3}h(\Delta) + 4.28$. Therefore, from estimate (6) we deduce the following inequality:

$$\min(|n|, |m|) < \frac{\frac{1}{2}h(j) + \frac{1}{3}h(\Delta) + 4.28}{2\hat{h}(R)}.$$

On the other hand, if $n = \pm m$, we have $\phi_1(P) \pm \phi_2(P) \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$. Taking into account that $\#(\mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}) \leq 16$ (see Theorem 3), $d(\phi_1 \pm \phi_2) = 4$ and that for any x -coordinate we have two y -coordinates, we deduce that there are at most $4 \cdot 16 \cdot 2 \cdot 2 = 256$ points $P \in \mathcal{C}_{a,b}(\mathbb{Q})$ such that $\phi_1(P) \pm \phi_2(P) \in \mathcal{E}_{a,b}(\mathbb{Q})_{\text{tors}}$. In conclusion, we obtain the following result:

Theorem 7. *If the rank of the elliptic curve $\mathcal{E}_{a,b}(\mathbb{Q})$ is 1, the following estimate holds:*

$$\#(\mathcal{C}_{a,b}(\mathbb{Q})) \leq 64 \frac{\left(\frac{1}{2}h(j) + \frac{1}{3}h(\Delta) + 4.28\right)}{\hat{h}(R)} + 256.$$

Corollary 1. *Under the assumption of the validity of Lang's Conjecture B, we have the estimate:*

$$\#(\mathcal{C}_{a,b}(\mathbb{Q})) \leq 64 \frac{\left(\frac{1}{2}h(j) + \frac{1}{3}h(\Delta) + 4.28\right)}{ch(\Delta)} + 256 \leq k_1 h(j) + k_2,$$

where k_1 and k_2 are universal constants independent of the curve $\mathcal{C}_{a,b}(\mathbb{Q})$.

Furthermore, if $h(\Delta) \geq h(j)$, then we have

$$\#(\mathcal{C}_{a,b}(\mathbb{Q})) \leq k_3,$$

where k_3 are a universal constant independent of the curve $\mathcal{C}_{a,b}(\mathbb{Q})$.

Let us remark that Corollary 1 generalizes the results of [Kul99]. In that work, the author considers the family of elliptic curves $\{\mathcal{E}_a\}_{a \in \mathbb{Q}}$ defined by the equation $Y^2 = X^3 - a^2X$. The curve \mathcal{E}_a has complex multiplication (hence Conjecture B holds), and its j -invariant is 1728 for any $a \in \mathbb{Q}$.

By making the replacement $X := -2/3 aX + 1/3 a$, we see that the curve \mathcal{E}_a is isomorphic to the curve of equation $Y^2 = -6 aX^3 + 9aX^2 + 9aX - 6 a$ and then, by Corollary 1, we obtain for any $a \in \mathbb{Q}$ a uniform bound for all the rational points of the genus 2-curve of equation $Y^2 = -2/3 aX^6 + aX^4 + aX^2 - 2/3 a$.

References

- [BCS97] P. Bürgisser, M. Clausen, and M.A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, Berlin Heidelberg New York, 1997.
- [CHM97] L. Caporaso, J. Harris, and B. Mazur. Uniformity of rational points. *Journal of the AMS*, 10(1): 1–35, 1997.
- [CHM95] L. Caporaso, J. Harris, and B. Mazur. How many rational points can a curve have? In R.H. Dijkgraaf et al., editors, *The moduli space of curves. Proceedings of the conference held on Texel Island, Netherlands*, volume 129 of *Progress in Mathematics*, pages 13–31, Basel, 1995. Birkhäuser.
- [Cas68] J.W.S. Cassels. On a theorem of Dem'janenko. *J. London Math. Soc.*, 43:61–66, 1968.
- [CaFl96] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Mordell-Weil arithmetic of curves of genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.
- [Cha41] C. Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *Comptes Rendus de l'Académie des Sciences de Paris*, 212:1022–1024, 1941.
- [Col85] R.F. Coleman. Effective Chabauty. *Duke Math. Journal*, 52:765–770, 1985.

- [Dem68] V. Dem'janenko. Rational points of a class of algebraic curves. *Trans. of the AMS*, 66:246–272, 1968.
- [Fal83] G. Faltings. Finiteness theorems for abelian varieties over number fields. *Inventiones Math.*, 73(3):349–366, 1983.
- [GHH⁺97] M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, and L.M. Pardo. Lower bounds for diophantine approximation. *Journal of Pure and Applied Algebra*, 117,118:277–317, 1997.
- [GHM⁺98] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, and L.M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.
- [HKP⁺00] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *Journal of Complexity*, 16(1):70–109, 2000.
- [Kna92] A. Knapp. *Elliptic Curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.
- [KP96] T. Krick and L.M. Pardo. A computational method for diophantine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 193–254, Basel, 1996. Birkhäuser.
- [Kul99] L. Kulesz. Application de la méthode de Dem'janenko–Manin à certaines familles de courbes de genre 2 et 3. *Journal of Number Theory*, 76(1):130–146, 1999.
- [Lan86] S. Lang. Hyperbolic and diophantine analysis, *Bulletin of the AMS*, 14(2): 159–205, 1986.
- [Man69] Y. Manin. The p -torsion of elliptic curves is uniformly bounded (in russian). *Izv. Akad. Nauk SSSR*, 33:459–465, 1969.
- [Mat70] Y. Matiyasevich. The Diophantineness of enumerable sets. (Russian) *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.
- [Maz78] B. Mazur. Rational isogenies of prime degree. *Inventiones Math.*, 44:129–169, 1978.
- [Par95] L.M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, M. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAEECC-11*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69, Berlin Heidelberg New York, 1995. Springer.
- [Poo01] B. Poonen. Computing rational points on curves. To appear in *Proceedings of the Millennium Conference on Number Theory, May 21–26, 2000*.
- [Rob49] J. Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949.
- [Ser89] J.-P. Serre. *Lectures on Mordell–Weil Theorem*, volume E 15 of *Aspects of Mathematics*. Fried. Vieweg & Sohn, Braunschweig/Wiesbaden, 1989.
- [Sil86] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Berlin Heidelberg New York, 1986.
- [Sil90] J.H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Mathematics of Computation*, 55(192):723–743, 1990.
- [Sil94] J.H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, Berlin Heidelberg New York, 1994.