Scientific Research Publishing

Open Journal of Discrete Mathematics, 2021, 11, 103-113
https://www.scirp.org/journal/ojdm
ISSN Online: 2161-7643
ISSN Print: 2161-7635

Rational Points on Genus 3 Real Hyperelliptic Curves

Brice M. Miayoka, Regis F. Babindamana, Basile G. R. Bossoto

Faculté Des Sciences et Techniques, Université Marien Ngouabi, Brazzaville, Congo
Email: bricemiayo@gmail.com, regis.babindamana@umng.cg, basile.bossoto@umng.cg

How to cite this paper: Miayoka, B.M., Babindamana, R.F. and Bossoto, B.G.R. (2021) Rational Points on Genus 3 Real Hyperelliptic Curves. *Open Journal of Discrete Mathematics*, **11**, 103-113.
https://doi.org/10.4236/ojdm.2021.114008

Received: May 5, 2021
Accepted: October 16, 2021
Published: October 19, 2021

Abstract

We compute rational points on real hyperelliptic curves of genus 3 defined on $\mathbb{Q}$ whose Jacobian have Mordell-Weil rank $r=0$. We present an implementation in sagemath of an algorithm which describes the birational transformation of real hyperelliptic curves into imaginary hyperelliptic curves and the Chabauty-Coleman method to find $C(\mathbb{Q})$. We run the algorithms in Sage on 47 real hyperelliptic curves of genus 3.

Keywords

Hyperelliptic Curve, Jacobian, Coleman Integration, Rational Point

1. Introduction

Let C be a hyperelliptic curve of the genus $g \geq 2$ defined on $\mathbb{Q}$. The Mordell conjecture proved by Fattings, gives that the set of rational points $C(\mathbb{Q})$ is finite. The hyperelliptic curves can be subdivided into two types: those with real models and those with imaginary models. Our objective is to compute the rational points in the case of real hyperelliptic curves of genus 3 whose Jacobian have a Mordel-Weil rank equal to 0. This fits into the particular case where $r < g$ has been considered by Chabauty and the techniques developed by Coleman in 1980 [1], allow us to use the p-adic integration to explicitly computation the set of rational points [2].

Although there is an algorithm by Jennifer Balakrishnan computing Coleman integrals in the case of real hyperelliptic curves in [3], this one is unfortunately not available in Sage. We then use the birational transformation of real hyperelliptic curves into imaginary hyperelliptic curves, because in the latter case, Balakrishnan, Bradshaw and Kedlaya described and implemented in Sage the explicit computation of Coleman integrals on imaginary hyperelliptic curves [4]. We

The AMS classification: MSC2020, 14G05, 11G30.

start with an overview of hyperelliptic curves and the transition from a real hyperelliptic curve to an imaginary hyperelliptic curve in Section 1. In Section 2, we recall the Chabauty-Coleman method and explicit Coleman integration. In Section 3, we describe our algorithm, which is subdivided into three sub-algorithms: the first one that transforms a real curve to an imaginary curve; the second computes the set of rational points of the imaginary hyperelliptic curve found in **Algorithm 3**. **Algorithm 4** is this of Maria Inés de Frutos Fernaandez and Sachi Hashimoto in [5] and its implementation in [6]. To the latter, we added a function allowing it to take the hyperelliptic curves of genus 3 and of rank 0 given by non-monic polynomials. Finally, the third algorithm constructs the rational points of the curve C which is real hyperelliptic from the rational points of the imaginary hyperelliptic curve birationally equivalent to C. In Section 4, we present the results obtained on a list of curves taken from the database of hyperelliptic curves of genus 3 [7].

2. Background on Hyperelliptic Curves

In this section we recall the definition of hyperelliptic curves, the different types of hyperelliptic curves and how to pass from a real hyperelliptic curve to an imaginary hyperelliptic curve. For more detail in this section, we refer the reader to [8] [9]. A hyperelliptic curve of genus $g \geq 2$ over $\mathbb{Q}$ is defined by an equation:

$$y^2 = f(x) \tag{1}$$

where f is a polynomial of $\mathbb{Q}[x]$ of degree $2g+2$ or $2g+1$. This defines a smooth irreducible algebraic curve in the affine plane. Considering its smooth projective model which is obtained by adding one or two points at infinity, we distinguish two types of hyperelliptic curves which differ by the number of rational points at infinity:

- Real hyperelliptic curves: they are those which have two points at infinity. In this case, the polynomial f is of degree $2g+2$;
- Imaginary hyprelliptic curves: they are those which have a one point at infinity. In this case, the polynomial f is of degree $2g+1$.

In this article, we are interested in real hyperelliptic curves.

A real hyperelliptic curve C of genus g over $\mathbb{Q}$ is defined by an absolutely irreducible equation of the form:

$$y^2 = f(x) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1} + f_{2g}x^{2g} + f_{2g-1}x^{2g-1} + \cdots + f_0 \tag{2}$$

where $f_{2g+2} \neq 0$. The two points at infinity correspond to the two square roots of the leading coefficient of f. These points are rational if and only if this leading coefficient is a square, so that its square roots are rational numbers.

Let us soppose that f_{2g+2} is a non-zero square in $\mathbb{Q}$. We set $f_{2g+2} = s^2$. The points at infinity of C are given in projective coordinates by $\infty_1 = (1:s:0)$ and $\infty_2 = (1:-s:0)$, which are rational [9].

The set of rational points on C denoted by $C(\mathbb{Q})$, is defined by:

$$C(\mathbb{Q}) = \{(x,y)\mathbb{Q}^2 \mid y^2 = f(x)\} \cup \{\infty_1, \infty_2\}$$

Let C be a real hyperelliptic curve of genus g over $\mathbb{Q}$ with equation $y^2 = f(x)$. If there exists a *ramified prime divisor* of degree 1 in $\mathbb{Q}$ of C, then the curve C is birationally equivalent to an imaginary hyperelliptic curve $C': y'^2 = f'(x')$ of genus g. Indeed, if we denote $P = (a,b)$ a rational point of the curve C such that P is equal to its image under the hyperelliptic involution $\iota(P) = (a,-b)$ *i.e.*: that $2b = 0$, then P is said to be ramified and in this case the divisor $D = P - \infty_1$ is the ramified prime divisor, then we can make the following change of variable:

$$x = \frac{1+ax'}{x'} \text{ and } y = \frac{y'}{x'^{g+1}} - b \tag{3}$$

In the equation of C, we thus find the equation of C'.

Therefore P is ramified if $b = 0$. By substituting a and $b = 0$ in the equation of C, we get $f(a) = 0$. We conclude that if the polynomial $f(x)$ has at least one root in $\mathbb{Q}$, then the real hyperelliptic curve of equation $y^2 = f(x)$ admits at least one rational ramified point and therefore it is birationally equivalent to an imaginary hyperelliptic curve via the change of variables below.

We are interested in real hyperelliptic curves of genus 3 having at least one rational point of ramification and whose Jacobians have Mordell-Weil rank 0.

3. Background Chabauty-Coleman Method and Coleman Integration

In this section we recall the Chabauty-Coleman method used to compute the rartional points in part 2 of our algorithm. We also give a brief reminder on Coleman integrals. For more details see [10].

3.1. Chabauty-Coleman Method

Let C be a smooth projective curve over the rational numbers of genus at least 2. From the work of Faltings, we know that $C(\mathbb{Q})$ is finite, but the proof of Faltings does not explicitly give the set $C(\mathbb{Q})$. However, before Faltings' work, Chabauty considered the following configuration. Let p be a prime number and $P \in C(\mathbb{Q}_p)$. We consider the following inclusion:

$$\iota_P : C \to J, Q \to [Q - P].$$

Let $\overline{J(\mathbb{Q})}$ be the p-adic closure of $J(\mathbb{Q})$ and define $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} = \iota_P\left(C(\mathbb{Q}_p)\right) \cap \overline{J(\mathbb{Q})}$. Chabauty proved the following case of Mordell's conjecture:

Theorem 2.1. Let $C/\mathbb{Q}$ be a curve of genus $g \geq 2$ such that the Mordell-Weil the rank of the Jacobian J of C over Q is less than g, and let p be a prime number, then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.

Chabauty's result was then reinterpreted and made effective by Coleman, who showed what follows:

Theorem 2.2. Let C be as above and suppose that p is a prime number of good

reduction for C. If $p > 2g$, then:

$$\#C(\mathbb{Q}) \le \#C(\mathbb{F}_p) + 2g - 2.$$

The Chabauty-Coleman method uses the theory of p-adic integrations on curves to construct the p-adic integrals of 1-forms on $C(\mathbb{Q}_p)$ which vanish on $C(\mathbb{Q})$ and which allow in practice to explain the set of rational points which are contained in the intersection of the set of zeros of the integrals of *g-r-independent* forms on the base change of C to $\mathbb{Q}_p$.

3.2. Computing Coleman Integrations

In order to Compute $C(\mathbb{Q})$, we need to evaluate $\int_P^Q \omega$ for $\omega \in \Omega_C^1(\mathbb{Q}_p)$ where $\Omega_C^1(\mathbb{Q}_p)$ is the g-dimensional vector space of regular 1-forms on C. Let $\omega_{i_{(0\le i\le 2g-1)}}$ be a differential basis of $H_{dR}^1(C)$ with $\omega_i = x^i \frac{dx}{2y}$, then we can write $\omega = df_i + \sum_{i=0}^{2g-1} a_i \omega_i$ where $a_i \in \mathbb{Q}_i$ and f_i is in the Monsky-Washnitzer (MW) weak completion of the coordinate ring of C deprived of the Weierstrass points [11]. And let $P, Q \in C(\mathbb{Q}_p)$. So:

$$\int_P^Q \omega = f_i(Q) - f_i(P) + \sum_{i=0}^{g-1} a_i \int_P^Q \omega_i$$

Suppose that p is a prime of good reduction for C and let $\bar{C}$ be the reduction of C modulo p. Then there is a natural reduction $red : C(\mathbb{Q}) \to \bar{C}(\mathbb{Q}_p)$ which sends the points of $C(\mathbb{Q}_p)$ to the points of $\bar{C}(\mathbb{F}_p)$. If $P \in C(\mathbb{Q}_p)$, denote by $\bar{P} \in \bar{C}(\mathbb{F}_p)$ the reduction of P modulo p. We say that two points $P, Q \in C(\mathbb{Q}_p)$ are in the same residue disk if they have the same reduction modulo p. To compute $\int_P^Q \omega_i$, we consider two cases: P and Q are in the same residue disk and P and Q are in the residue disks different. Algorithms in both cases are given below (**Algorithm 1**, **Algorithm 2**). For more details see [4].

4. The Algorithm

In this section, we specialize in the case that interests us, where C is a hyperelliptic curve of genus 3 given by a model of even degree defined by:

$$y^2 = f(x),$$

where $f(x) \in \mathbb{Q}[x]$ is monic of degree 8 (to avoid the leading coefficient of the polynomial f is not a square in $\mathbb{Q}$) and having at least one root in $\mathbb{Q}$. We assume that the Jacobian J of C has a Mordell-Weil rank 0 over $\mathbb{Q}$. Our goal is to compute $C(\mathbb{Q})$. Since our hyperelliptic curve is given by a polynomial having at least one root in $\mathbb{Q}$. Then from Section 1, we can find at least one hyperelliptic curve of odd degree model isomorphic to C. We have implemented the algorithm bellow on Sage (**Algorithm 3**), which determines, the curve C' isomorphic to C.

Algorithm 1. $P,Q \in C(\mathbb{C}_p)$ are in the same residue disk (tiny Integrals).

Input: C hyperelliptic curve over an unramified extension K of $\mathbb{Q}_p$ with p a prime of good ordinary reduction, Points P, Q on C.

Output: $\int_P^Q \omega_i$.

1) Construct an linear interpolation $x(t), y(t)$ from P to Q.

2) Formally integrate the power series in t: $\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_{P(t)}^{Q(t)} x(t)^i \frac{d(x(t))}{2y(t)}$.

3) Return $\int_P^Q \omega_i$.

Algorithm 2. P,Q are in different residue disks, we use Frobenius to ϕ.

Input: C hyperelliptic curve over an unramified extension K of $\mathbb{Q}_p$ with p a prime of good reduction Points P, Q on C.

Output: $\int_P^Q \omega_i$.

1) Find Teichmüller points P,Q in the disks of P,Q.

2) Compute the tiny integrals $\int_P^{P'} \omega_i$ and $\int_Q^{Q'} \omega_i$.

3) Calculate the action of Frobenius on each basis element $(\phi^m)^* \omega_i = \sum_j^{2g-1} M_{ij}\omega_j + df_i$.

4) Change of variables gives $\sum_{j=0}^{2g-1}(M-I)\int_{P'}^{Q'} \omega_j = f_i(Q) - f_i(Q)$ and solving the linear system gives the integrals $\int_{P'}^{Q'} \omega_i$.

5) Correct endpoints to recover $\int_P^Q \omega_i - \int_P^{P'} \omega_i + \int_{P'}^{Q'} \omega_i + \int_{Q'}^{Q} \omega_i$.

6) Return $\int_P^Q \omega_i$.

Algorithm 3. Transformation of a genus 3 real hyperelliptic curve in a genus 3 imaginary hyperelliptic curve.

1) Function TransformationCurves($C: y^2 = f(x)$).

2) Computation of the roots of f.

3) Choose a root of f.

4) $a \leftarrow f(a) = 0$.

5) Compute: $F = x^{2g+2} f\left(\frac{1+ax}{x}\right)$.

6) C' = Hyperelliptic(F).

7) Return C'.

The hyperelliptic curve C' obtained in this algorithm is given by an equation of the form:

$$y^2 = F(x)$$

where $F(x) \in \mathbb{Q}[x]$ not necessarily monic of degree 7.

Such a model has a unique point at inifinity which we denote by ∞. The jacobian J' of C' also has a rank of Mordell-Weil 0 on $\mathbb{Q}$.

Let $p \geq 7$ a prime number such that C' has a good reduction mod p (donte that p must not be divisible by the dominant coefficient of F). We now want, probably to count rational points of C' so that we can count the set of rational

points of C. For this, we use the algorithm described in [5] which we transcribe here (**Algorithm 4**).

Note that the output of this algorithm is a finite subset $C'\left(\mathbb{Q}_p\right)$ containing $C'\left(\mathbb{Q}\right)$, which is returned as three separate subsets:

- The set $C'\left(\mathbb{Q}\right)$ of rational points of C'.
- The set of points Q in $C'\left(\mathbb{Q}_p\right)\backslash C'\left(\mathbb{Q}\right)$ such that $\left[Q-\infty\right]\in J\left(\mathbb{Q}_p\right)$ is 2-torsion.
- The set of points Q in $C'\left(\mathbb{Q}_p\right)\backslash C'\left(\mathbb{Q}\right)$ such that $\left[Q-\infty\right]\in J\left(C'\left(\mathbb{Q}\right)\right)$ is an n-torsion point for.

In this paper we are interested that at the set $C'\left(\mathbb{Q}\right)$ of rational points of C'.

Note that the implementation of this algorithm only took into account the hyperelliptic curves defined by a polynomial monic [5]. Since, in most of the cases that have processed the hyperelliptic curve it was defined by a polynomial no monic. So we had to add to the code in Sage of [6] a function allowing this algorithm to take into account polynomial not necessarily monic.

Here we present the code for this function in SageMath Software [12].

```
def rational_ponts_of_H(H, p0, pts):
    p=find_good_p(H, p0)
    pts0=list(pts)
    pts=[]
    for a in pts0:
        if a[2]!=1 and a[2]!=0:
            pts.append(H(a[0]/a[2], a[1]/(a[2])^4, 1))
        else :
            pts.append(a)
    def_poly=H.hyperelliptic_polynomials()[0]
    lead_coeff=def_poly.leading_coefficient()
    assert lead_coeff%p!=0
    def_poly_new=def_poly(lead_coeff*def_poly.parent().0)/lead_coeff^8
    H_old=H
    H= HyperellipticCurve(def_poly_new)
    pts_old= pts
    pts=[]
    for a in pts_old:
        if a[2]==0:
            pts.append(H(0,1,0))
        else:
            pts.append(H(a[0]/lead_coeff, a[1]/lead_coeff^4))
    pts=list(set(pts))
    E=Chabauty_Coleman(H, p0, pts)
    points=[]
    for a in E:
            if a[2]==0:
                points.append(H_old([0, 1, 0]))

            else:
                points.append(H_old([a[0]*lead_coeff, a[1]*lead_coeff^4, a[2]]))
    return p, points
```

We give below the steps of **Algorithm 4**, for more details see [5].

Step 1 (Required precision.) We need to choose the p-adic precision N and the t-adic precision M to guarantee that, in Step 3, we will obtain all the roots of $f_i\left(pt\right)$ in $\mathbb{Z}_p$. Set $N=2p+4$ and $M=2p+1$ is sufficient for p prime $p>2g=6$ [2].

Algorithm 4. Chabauty-Coleman method for genus 3 rank 0 hyperelliptic curve.

1) Function Chabauty-Coleman(C', p, $C'(\mathbb{Q})_{\text{know}}$).
2) Set the p-adic precision N to $2p+4$.
3) Set the t-adic precision M to $2p+1$.
4) Initialize found-points := empty list.
5) for each $P \in C(\mathbb{F}_p)$ up to the standard involution ι do.
6) Compute $f_1; f_2$ and f_3 in local coordinates.
7) for each point $Q \in C(\mathbb{Q}_p)$ corresponding to a common zero of the f_i do.
8) Add Q and $\iota(Q)$ to found-points.
9) end for.
10) end for.
11) return $\mathbb{Q}$ -points of C'.

Step 2 (Annihilator) A basis of the space of differentials $H^0\left(C'_{\mathbb{Q}_p}, \Omega^1\right)$; is given by $\{\omega_0, \omega_1, \omega_2\}$ where $\omega_i = \left(x^i/2y\right)dx$. For each $i = 0;1;2$, define:

$$f_i(z) = \int_\infty^z \omega_i$$

where ∞ denotes the point at infinity. The functions $f_i(z)$ are zero on all rational points of C', but not identically zero.

Step 3 (Searching in residue discs.) For each point $\overline{P} \in C(\mathbb{F}_p)$, we compute the set of $\mathbb{Q}_p$ -rational points P reducing to $\overline{P}$ such that $f_i(P) = 0$ for $i = 0;1;2$. To perform this computation, we consider two different cases:

1) If there is a point $P \in C'(\mathbb{Q})_{known}$ reducing to $\overline{P}$, then we expand each ω_i in terms of a uniformizer t at P and we formally integrate to obtain three power series $f_i(t)$, that parametrize the integrals of the ω_i between P and any other point in the residue disc.

2) Otherwise, we start by finding a Q_p -point P reducing to $\overline{P} = (\overline{x}_0; \overline{y}_0)$ (note that $\overline{P}$ cannot be ∞ in this case). If $\overline{y}_0 = 0$ we can take $P = (\overline{x}_0; 0)$ where x_0 is the Hensel lift of $\overline{x_0}$ to a root of $F(x)$. Otherwise, we can take $P = (x_0; y_0)$ where x_0 is any lift of x_0 to $\mathbb{Z}_p$ and y_0 is obtained from y_0 by applying Hensels Lemma to $y^2 = F(x_0)$. Then we set $f_i(t) = \overline{f}_i(t) + \int_\infty^z \omega_i$; where each $\overline{f}_i(t)$ parametrizes the integral of ω_i between P and any other point in the residue disc.

Step 4 (Identifying the rational points.) Now, for each of the points Q found in Step 3, we attempt to reconstruct Q as a Q-rational point, using Sage. If this is not possible, then $[Q - \infty]$ must be a torsion point in $J(\mathbb{Q}_p)$, because J has rank 0.

Once we have the rational points of C' we can reconstruct the rational points of C. Note that C has the same number of rational points as C' and being a curve given by a model of even degree, it has two points at infinity that we note ∞^+ and ∞^-.

We use above algorithms to determine the rational points of C from the rational points of C' (**Algorithm 5**).

Note also that, if after reconstruction, we do not have the at inifinity, we must

Algorithm 5. Computation of the rational points of C.

1) Function RationalPoints-of-$C(C,\ C'(\mathbb{Q}))$.
2) Initilize found-ponits = empty list.
3) Add $P=(a,0)$ to found-points.
4) for each $Q(x',y')\in C'(\mathbb{Q})$ such that $x'\neq a$ do.
5) Compute $P(x,y)\in C(\mathbb{Q})$ such that.
6) $x=\frac{1+ax'}{x'}$ and $y=\frac{y'}{x'^4}$.
7) end for.
8) Add P and $\iota(P)$ to found-points.
9) **return** $\mathbb{Q}$-points of C.

add them because they are known in advance in our case these are the coordinate points $(1:1:0)$ and $(1:-1:0)$.

5. Example

We run our algorithms in Sage on a list of 47 hyperelliptic curves of genus 3 and rank 0, obtained from the database [7] giving the models of even degree polynomials having at least one root in $\mathbb{Q}$.

Our implementation proves that for each of the studied curves, the set of rational points is equal to the set of rational points of naive height at most 10^5.

Figure 1 shows how many of the curves in our list have certain number of rational points.

We observe that the maximun of the points is 4 and that a majority of the curves have three rational points.

We conclude this section, showing how the algorithms work on a particular curve and we show an example of a curve which does not have rational points at infinity.

5.1. Example

Consider a hyperelliptic curve C of genus 3 given by:

$$C: y^2 = x^8 - 4x^7 + 4x^6 + 2x^5 - 8x^4 + 8x^3 + x^2 - 4x.$$

The function **RankBound** in **Magma** shows that the jacobian J of C has a rank of Mordell-Weil 0. Then we can apple the algorithms described above to compute the number of rational points of C. We proceed as follows:

Let's pose $f(x) = x^8 - 4x^7 + 4x^6 + 2x^5 - 8x^4 + 8x^3 + x^2 - 4x$. It is easy see that f vanishes into $0\in\mathbb{Q}$. Therefore, the curve C is $\mathbb{Q}$-isomorphic a imaginary hyperelliptic curve that denote C'.

Step 1: Compute of the equation of C'

Let $y^2 = F(x)$ the equation of the curve C'. By Algorithm 3, we have $F(x) = x^8 f\left(\frac{1+ax}{x}\right)$ with $a=0$, then C' is given by:

$$C': y^2 = -4x^7 + x^6 + 8x^5 - 8x^4 + 2x^3 + 4x^2 - 4x + 1.$$

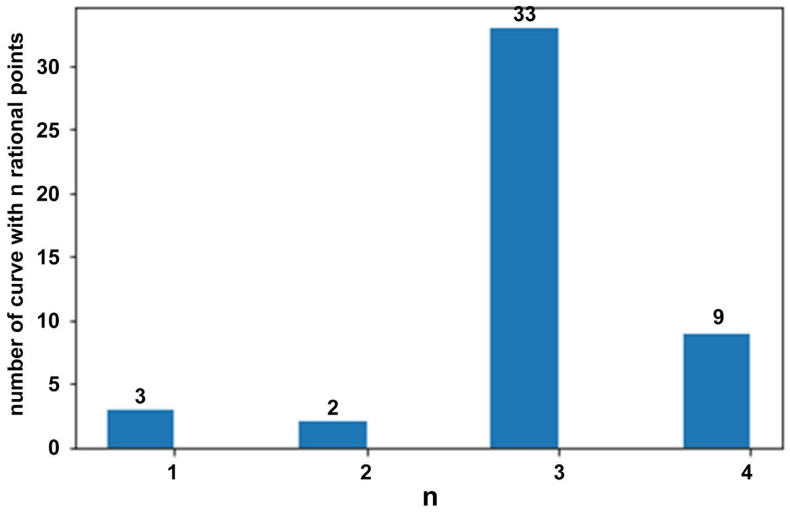

Figure 1. Number of hyperelliptic curves of genus 3 given by a model of even degree in the list and n points rationels.

Step 2 Computing rational points of C'

Using **Magma** we find that the set of rational points of C' with a height bounded by 10^5 is:

$$C'(\mathbb{Q})_{\text{know}} = \{\infty, (0,-1), (0,1), (1,0)\}.$$

Since the curve has good reduction modulo $7 > 6$, we run the **Algorithm 4** using this prime. The points of $C'(\mathbb{F}_7)$ are as follows:

$$\{\overline{\infty}, \overline{(1;0)}, \overline{(0;1)}, \overline{(0;6)}\}.$$

After Hensel lifting each of these points to a point of $C'(\mathbb{Q}_7)$, we write $f_0(z), f_1(z)$ and $f_2(z)$ in local coordinates, we obtained:

$$f_0(z) = -\frac{1}{4}z - \frac{9}{32}z^3 - \frac{1767}{2560}z^5 - \frac{62103}{28672}z^7 - \frac{9063575}{1179648}z^9 - \frac{338395653}{11534336}z^{11} - \frac{25665563035}{218103808}z^{13} + O(z^{15})$$

$$f_1(z) = -\frac{1}{4}z - \frac{25}{96}z^3 - \frac{321}{512}z^5 - \frac{55933}{28672}z^7 - \frac{8124485}{1179648}z^9 - \frac{302419335}{11534336}z^{11} - \frac{22889075713}{218103808}z^{13} + O(z^{15})$$

$$f_2(z) = -\frac{1}{4}z - \frac{23}{96}z^3 - \frac{1451}{2560}z^5 - \frac{50195}{28672}z^7 - \frac{7261675}{1179648}z^9 - \frac{269617641}{11534336}z^{11} - \frac{20370900655}{218103808}z^{13} + O(z^{15}).$$

Then we use the **PARI/GP function polrootspadic** to compute the common zeros of the $f_0(z) \bmod 7^{18}$, $f_1(z) \bmod 7^{18}$ and $f_2(z) \bmod 7^{18}$. We notice, that they have the common zeros in the discs $\overline{\infty}, \overline{(1;0)}, \overline{(0;1)}$ and $\overline{(0;6)}$ which correspond respectively to the points $\infty, (1,0), (0,1)$ and $(0,-1)$.

Therefore, we have shown that $C'(\mathbb{Q}) = \{\infty, (0;-1), (0;1), (1;0)\}$.

Step 3 Determination of the rational points of C

We now move on to the phase of constructing the rational points of C from $C'(\mathbb{Q})$ using Algorithm 5. We start adding the point used for the variable change *i.e.*: $P1(a=0;0)$ and the points at infinity ∞^+ and ∞^-. Let $Q=(1,0)\in C'(\mathbb{Q})$, we compute the point $P2(x;y)\in C(\mathbb{Q})$ such that $x=\frac{1+ax'}{x'}$ and $y=\frac{y'}{x'^4}$ Hence $P2=(1;0)$. Since Q is the only point in C' whose the x-coordinate is different from $a=0$, Algorithm 5 stops here. Therefore:

$$C(\mathbb{Q})=\{\infty^+,\infty^-,(0;0),(1;0)\}.$$

We check that we have the same result using **Magma** with a height of 10^5.

In our list, we found case of a hyperelliptic curve whose polynomial f is not monic and its leading coefficient is not a square in $\mathbb{Q}$. So the curve has no pints at infinity. We present it in the following example.

5.2. Example

Let be the hyperelliptic curve:

$$C: y^2=-3x^8-8x^7-18x^6-18x^5-15x^4+2x^3+5x^2+8x.$$

This curve does not have rational points at infinity since the leading coefficient of the polynomial defining the curve is not a square in $\mathbb{Q}$.

By Algorithm 3, the curve C is transformed into the imaginary hyperelliptic curve C' given by:

$$C': y^2=8x^7+5x^6+2x^5-15x^4-18x^3-18x^2-8x-3.$$

Using Magma, we have:

$$C'(\mathbb{Q})_{\text{know}}=\{\infty\}.$$

Since the curve has good reduction modulo 7, we run Algorithm 4 and we find that $C'(\mathbb{Q})=\{\infty\}$.

Since C' has only one rational point, then C will only have one rational point too which will be none other than the point used for the change of variable. By Algorithm 5, we get $C(\mathbb{Q})=\{(0,0)\}$.

6. Conclusion

In this paper, we have presented the computation of rational points on hyperelliptic curves of genus 3 given by an even degree model and whose Jacobian has a Mordell-Weil rank 0, using the isomorphism between the real hyperelliptic curve and the imaginary hyperelliptic curve. Our calculations show that the rational points on C are the same as when we search on Magma with a height of at most 10^5.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Coleman, R.F. (1985) Effective Chabauty. *Duke Mathematical Journal*, **52**, 765-770. https://doi.org/10.1215/S0012-7094-85-05240-8

[2] Balakrishnan, J.S., Bianchi, F., Cantoral-Farfán, V., Çiperiani, M. and Etropolski, A. (2018) Chabauty-Coleman Experiments for Genus 3 Hyperelliptic Curves. In: Balakrishnan, J., Folsom, A., Lalín, M. and Manes, M., Eds., *Research Directions in Number Theory*, Springer, Cham, 67-90. https://doi.org/10.1007/978-3-030-19478-9_3

[3] Balakrishnan, J.S. (2015) Coleman Integration for Even-Degree Models of Hyperelliptic Curves. *LMS Journal of Computation and Mathematics*, **18**, 258-265. https://doi.org/10.1112/S1461157015000029

[4] Balakrishnan, J.S., Bradshaw, R.W. and Kedlaya, K.S. (2010) Explicit Coleman Integration for Hyperelliptic Curves. In: Hanrot, G., Morain, F. and Thomé, E., Eds., *Algorithmic Number Theory*, *ANTS* 2010. Lecture Notes in Computer Science. Springer, Berlin, 16-31. https://doi.org/10.1007/978-3-642-14518-6_6

[5] de Frutos Fernaandez, M.I. and Hashimoto, S. (2019) Computing Rational Points on Rank 0 Genus 3 Hyperelliptic Curves. *arXiv*, 190904808v2, 1-10.

[6] de Frutos Fernaandez, M.I. and Hashimoto, S. (2019) Sage Code. https://github.com/sachihashimoto/rational-points-hyperelliptic

[7] Booker, A., Platt, D., Sijsling, J. and Sutherland, A. (2018) Genus 3 Hyperelliptic Curves. 1-4. http://math.mit.edu/~drew/lmfdb_genus3_hyperelliptic.txt

[8] Jacobson, M.J., Scheidler, R. and Stein, A. (2009) Cryptographic Aspects of Real Hyperelliptic Curves. *Cryptology ePrint Archive*, 1-28.

[9] Stoll, M. (2014) Arithmetic of Hyperelliptic Curves. Screen Version of August 1, 2014, **1**, 1-35.

[10] McCallum, W. and Poonen, B. (2012) The Method of Chabauty and Coleman, Explicit Methods in Number Theory. In: *Panoramas et Synthèses*, Société Mathématique de France, Paris, **36**, 99-117.

[11] Balakrishnan, J.S. (2011) Coleman Integration for Hyperelliptic Curves: Algorithms and Applications. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA.

[12] Zimmermann, P. (2017) The Sage Developers Sagemath, the Sage Mathematics Software System (Version 9.1).