INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus
Mathématique

Nguyen Xuan Tho

Rational points on a certain genus 2 curve

Volume 361 (2023), p. 1071-1073

Published online: 7 September 2023

https://doi.org/10.5802/crmath.471

Les Comptes Rendus. Mathématique *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2023, Vol. 361, p. 1071-1073
https://doi.org/10.5802/crmath.471

Number theory / *Théorie des nombres*

Rational points on a certain genus 2 curve

Nguyen Xuan Tho [a]

[a] Hanoi University of Science and Technology
E-mail: tho.nguyenxuan1@hust.edu.vn

Abstract. We give a correct proof to the fact that all rational points on the curve

$$y^2 = (x^2+1)(x^2+3)(x^2+7)$$

are $\pm\infty$ and $(\pm 1, \pm 8)$. This corrects previous works of Cohen [3] and Duquesne [4, 5].

2020 Mathematics Subject Classification. 14G05, 14H99.

Funding. This paper is funded by the Ministry of Education and Training of Vietnam under the project B2022-CTT-03, 2022-2023.

Manuscript received 26 October 2022, accepted 31 January 2023.

1. Introduction

The goal of this paper is to prove the following theorems

Theorem 1. *All rational points on the curve*

$$\mathscr{C}_1 : y^2 = (x^2+1)(x^2+3)(x^2+7) \tag{1}$$

are $\pm\infty$ *and* $(\pm 1, \pm 8)$.

The available proofs of Theorems 1 in [3] and [4] are unfortunately incorrect. The curve (1) appeared in the work of Flynn and Wetherell [6]. However, Flynn and Wetherell also pointed out that their method failed in determining all rational points on the curve (1). Duquesne later gave an incorrect proof of Theorem 1 in his thesis [4, pp. 64–69]. Duquesne also reported Theorem 1 in [5, Theorem 4] and refered to his thesis for the proof. Furthermore, Duquesne's proof was reproduced in Cohen's book [3, Theorem 13.3.10, pp. 459–462]. Duquesne argued as the following: since $\mathbb{Q}(i)$ is a unique factorization domain and

$$(x+i)(x^2+3)(x-i)(x^2+7) = y^2,$$

it follows that

$$\begin{cases} \alpha y_1^2 = (x+i)(x^2+3), \\ \alpha y_2^2 = (x-i)(x^2+7), \end{cases}$$

where α can be taken as a divisor of the resultant of $(x+i)(x^2+3)$ and $(x-i)(x^2+7)$. The problem is that polynomials $(x+i)(x^2+3)$ and $(x-i)(x^2+7)$ have odd (three) degrees and so the denominator of x needs to be considered. Specifically, write $x = X/Z$, where $X, Z \in \mathbb{Z}$ and $\gcd(X, Z) = 1$, so (1) takes the form

$$Y^2 = (X^2 + Z^2)(X^2 + 3Z^2)(X^2 + 7Z^2).$$

Certainly,

$$\begin{cases} \beta Y_1^2 = (X^2 + 3Z^2)(X + iZ), \\ \beta Y_2^2 = (X^2 + 7Z^2)(X - iZ), \end{cases} \tag{2}$$

where $\beta \in \mathbb{Q}(i)$. Now

$$\text{Resultant}_X((X^2 + 3Z^2)(X + iZ), (X^2 + 7Z^2)(X - iZ)) = -2^7 \cdot 3 \cdot i \cdot Z^9,$$

so that β may be taken as a squarefree divisor of $2 \cdot 3 \cdot Z$ in $\mathbb{Z}[i]$. Certainly $\gcd(\beta, Z) = 1$, otherwise $\gcd(X, Z) > 1$, so $\beta | 2 \cdot 3$. Just as for α. However, the system (2) on dividing by Z^3 corresponds to

$$\begin{cases} \dfrac{\beta}{Z} \cdot y_1^2 = (x^2 + 3)(x + i), \\ \dfrac{\beta}{Z} \cdot y_2^2 = (x^2 + 7)(x - i), \end{cases}$$

so that the original α has to depend on (the square-free part of) Z.

For a specific example, consider the curve

$$y^2 = (x^2 + 1)(x^2 + 15)(x^2 + 18),$$

where the resultant of $(x + i)(x^2 + 15)$ and $(x - i)(x^2 + 18)$ equals $-2^2 \cdot 3^2 \cdot 7 \cdot 17i$. The curve has a rational point with $x = 3/5$, at which point

$$\begin{aligned} (x + i)(x^2 + 15) &= (1 - i)^{15}(4 + i) \cdot \frac{3}{125} \\ &\equiv (1 - i)(4 + i) \cdot 3 \cdot 5 \pmod{\mathbb{Z}[i]^2}. \end{aligned}$$

The resultant technique will work when applied to polynomials of even degree.

In the next sections, we will prove Theorem 1. The main tools are the elliptic curve Chabauty method in combination with Bruin and Stoll's fake-2 Selmer set [2], which have been implemented in MAGMA [1]. See Stoll [7, 8] for concrete examples. The MAGMA codes for the computation of the 2-fake Selmer sets for each curve $\mathscr{C}_1$ and $\mathscr{C}_2$ are given. The MAGMA codes for the elliptic curve Chabauty routine are available at https://www.overleaf.com/read/mgsfpypvvbrb

2. A proof of Theorem 1

Step 1. We compute the fake-2 Selmer set $\mathrm{Sel}^{(2)}_{\text{fake}}(\mathscr{C}_1)$:
MAGMA codes:

```
P<x> := PolynomialRing(Rationals());
C1 := HyperellipticCurve((x^2+1)*(x^2+3)*(x^2+7));
Sel, mSel := TwoCoverDescent(C1);
#Sel;
A<th> := Domain(mSel);
Sel eq {mSel(x0 - th): x0 in
{th+1,1,-1}};
```

Output:

```
3
true
```

The last line shows that for every rational point $(x, y) \in \mathscr{C}(\mathbb{Q})$, there exists $a \in \mathbb{Q}$ such that

$$x - \alpha \in a\mathbb{Q}(\alpha)^2 \quad \forall\, \alpha \in \{i, \sqrt{-3}, \sqrt{-7}\}, \tag{3}$$

$$\text{or} \quad \frac{x-\alpha}{1-\alpha} \in a\mathbb{Q}(\alpha)^2 \quad \forall\, \alpha \in \{i, \sqrt{-3}, \sqrt{-7}\}, \tag{4}$$

$$\text{or} \quad \frac{x-\alpha}{-1-\alpha} \in a\mathbb{Q}(\alpha)^2 \quad \forall\, \alpha \in \{i, \sqrt{-3}, \sqrt{-7}\}. \tag{5}$$

Step 2. We use the elliptic curve Chabauty method:

Case (3). Then

$$\mathscr{E}_1 : z^2 = (x - i)(x - \sqrt{-7})(x^2 + 3),$$

where $z \in K = \mathbb{Q}(i, \sqrt{-7})$. The curve $\mathscr{E}_1$ has rank 2. The elliptic curve Chabauty routine in MAGMA [1] works at $p = 5$ and shows that there are no points (x, z) in $\mathscr{E}_1(K)$ with the rational x-coordinate.

Case (4). Then

$$\mathscr{E}_2 : z^2 = 2(1 - i)(1 - \sqrt{-3})(x - i)(x - \sqrt{-3})(x^2 + 7),$$

where $z \in K = \mathbb{Q}(i, \sqrt{-3})$. The curve $\mathscr{E}_2$ has rank 2. The elliptic curve Chabauty routine works at $p = 5$ with the auxiliary prime 13, and shows that every point $(x, z) \in \mathscr{E}_2(K)$ with $x \in \mathbb{Q}$ satisfies $x = \pm 1$. Hence in (1), we have $x = \pm 1$ and $y = \pm 8$.

Case (5). By taking the complex conjugate and mapping x to $-x$, we have Case (4). Hence $x = \pm 1$ and $y = \pm 8$.

Acknowledgment

The author would like to thanks Professor Andrew Bremner for his help during the preparation of this paper.

References

[1] W. Bosma, J. Cannon, C. Playoust, "The MAGMA algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.

[2] N. Bruin, M. Stoll, "Two cover descent on hyperelliptic curves", *Math. Comput.* **78** (2009), no. 268, p. 2347-2370.

[3] H. Cohen, *Number Theory. Volume II: Analytic and Mordern Tools*, Graduate Texts in Mathematics, vol. 240, Springer, 2007.

[4] S. Duquesne, "Calculs Effectifs des Points Entiers et Rationnels sur les Courbes", PhD Thesis, Université Bordeaux I, 2001.

[5] ———, "Points rationnels et méthode de Chabauty elliptique", *J. Théor. Nombres Bordeaux* **15** (2003), no. 1, p. 99-113.

[6] E. V. Flynn, J. L. Wetherell, "Finding Rational Points on Bielliptic Genus 2 Curves", *Manuscr. Math.* **100** (1999), no. 4, p. 519-533.

[7] M. Stoll, "Slides of the talk *Rational Diophantine quintuples and diagonal genus 5 curves*", https://www.mathe2.uni-bayreuth.de/stoll/talks/Manchester-2017-print.pdf.

[8] ———, "Rational Diophantine quintuples and diagonal genus 5 curves", *Acta Arith.* **190** (2019), no. 3, p. 239-261.