THE NUMBER OF RATIONAL ITERATED PREIMAGES OF THE ORIGIN UNDER UNICRITICAL POLYNOMIAL MAPS

KAORU SANO

Abstract. We study rational iterated preimages of the origin under unicritical maps $f_{d,c}(x) = x^d + c$. Earlier works of Faber–Hutz–Stoll and Hutz–Hyde–Krause established finiteness and conditional bounds in the quadratic case. Building on this, we prove that for $d = 2$ and $c \in \mathbb{Q} \setminus \{0, -1\}$ there are no rational fourth preimages of the origin, and for all $d \geq 3$ there are no rational second preimages outside trivial cases. The proof relies on geometric analysis of preimage curves, the elliptic Chabauty method, and Diophantine reduction. As a result, we determine the number of rational iterated preimages of 0 under $f_{d,c}$ for all $d \geq 2$.

Contents

1. Introduction

Let L be a number field. Fix an integer $d \geq 2$ and $c \in L$, and define an endomorphism $f_{d,c}$ of affine line by

$$f_{d,c} \colon \mathbb{A}^1 \longrightarrow \mathbb{A}^1; \quad x \mapsto x^d + c.$$

For $a \in L$, the rational iterated preimage of a is the set

$$\bigcup_{N \geq 1} f_{d,c}^{-N}(a)(L) = \{x \in \mathbb{A}^1(L) \mid f_{d,c}^{\circ N}(x) = a \text{ for some } N \geq 1\},$$

where $f_{d,c}^{\circ N}$ is the N-th iterate of $f_{d,c}$, and $f_{d,c}^{-N}(a)$ is the preimage of a under $f_{d,c}^{\circ N}$. Finding an L-rational iterated preimage of a under $f_{d,c}$ amounts to solving complicated polynomial equations. When we vary c, the problem is reduced to determining L-rational points (c, x) of the preimage curves $Y^{\mathrm{pre}}(d, N, a)$ defined by $f_{d,c}^{\circ N}(x) - a = 0$, or its normal projective model $X^{\mathrm{pre}}(d, N, a)$. To study the

Date: October 17, 2025.

uniformity of the number of rational points of such curves, define the quantities

$$\kappa(d,a,L) \coloneqq \sup_{c\in L}\left\{ \# \bigcup_{N\geq 1} f_{d,c}^{-N}(a)(L) \right\}$$

$$\overline{\kappa}(d,a,L) \coloneqq \limsup_{c\in L}\left\{ \# \bigcup_{N\geq 1} f_{d,c}^{-N}(a)(L) \right\}$$

for an integer $d \geq 2$ and a point $a \in \mathbb{A}^1(L)$. In [FHI+09] and [HHK11], they deal with the uniformity of the number of rational iterated preimages under quadratic polynomial maps $f_{2,c}$.

Theorem 1.1.

(i) [FHI+09, Theorem 1.2 for $B = 1$] *For all $a \in \mathbb{A}^1(L)$, the quantity $\kappa(2,a,L)$ is finite.*

(ii) [HHK11, Theorem 1.3] *There is a finite set $S \subset \overline{\mathbb{Q}}$ such that we have*

$$\overline{\kappa}(2,a,L) = \begin{cases} 10 & \text{if } a = -1/4, \\ 6 & \text{if } a \text{ is one of the three third critical values}, \\ 4 & \text{if } a \in S \cap L, \\ 6 & \text{otherwise.} \end{cases}$$

The explicit value $\kappa(2,0,\mathbb{Q})$ is conditionally given in [FHS11].

Theorem 1.2 ([FHS11, Theorem 1.3])**.** *Suppose that for $c \in \mathbb{Q}\setminus\{0,-1\}$ the morphism $f_{2,c}$ admits no rational fourth preimages of 0. Then $\kappa(2,0,\mathbb{Q}) = 6$.*

Moreover, they proved that the morphism $f_{2,c}$ admits no rational fourth preimages of 0 for $c \in \mathbb{Q}\setminus\{0,-1\}$ under the Birch–Swinnerton-Dyer conjecture for the Jacobian of $X^{\mathrm{pre}}(2,4,0)$. This paper aims to remove the assumptions of 1.2 and extend it to unicritical polynomial maps of high degrees.

Theorem 1.3. *The following statements hold.*

(i) *For a rational number $c \in \mathbb{Q}\setminus\{0,-1\}$, the morphism $f_{2,c}$ admits no rational fourth preimages of 0.*

(ii) *For an integer $d \geq 3$ and a rational number $c \in \mathbb{Q}$, assume that $c \neq 0,-1$ if d is even, and assume that $c \neq 0$ if d is odd. Then, the morphism $f_{d,c}$ admits no rational second preimages of 0.*

As a corollary, we get the following result.

Corollary 1.4. *For even $d \geq 3$, we have the equality*

$$\# \bigcup_{N\geq 1} f_{d,c}^{-N}(0)(\mathbb{Q}) = \begin{cases} 3 & \text{for } c = -1, \\ 1 & \text{for } c = 0, \\ 2 & \text{for } c = -(d\text{-th power of rationals other than } 0,\pm 1), \text{ and} \\ 0 & \text{for other rationals.} \end{cases}$$

For odd $d \geq 3$, we have the equality

$$\# \bigcup_{N\geq 1} f_{d,c}^{-N}(0)(\mathbb{Q}) = \begin{cases} 1 & \text{for } c = -(d\text{-th power of rationals}), \text{ and} \\ 0 & \text{for other rationals.} \end{cases}$$

Hence, we have

$$\kappa(d,0,\mathbb{Q}) = \begin{cases} 6 & \text{for } d = 2, \\ 3 & \text{for even } d \geq 3, \text{ and} \\ 1 & \text{for odd } d \geq 3. \end{cases}$$

We will prove 1.3 by the following strategy. For $d = 2$, we exploit the geometry of the degree 2 cover

$$\pi\colon X^{\mathrm{pre}}(2,4,0) \longrightarrow X^{\mathrm{pre}}(2,3,0) \cong E$$

with

$$E : v^2 = u^3 - u + 1,$$

analyze ramification above $E[2]$, and pass to suitable base changes to obtain finite étale double covers of $X^{\mathrm{pre}}(2,4,0)$. This reduces the problem to lower-genus curves C_D classified by a class $[D] \in R^\times/(R^\times)^2$ for $R = \mathbb{Z}[1/2, 1/23]$. We determine $C_D(\mathbb{Q})$ via the elliptic Chabauty method due to [Bru03].

Theorem 1.5. *For $D = (-1)^{\varepsilon_0}2^{\varepsilon_1}23^{\varepsilon_2}$ with $\varepsilon_i \in \{0,1\}$ $(0 \le i \le 2)$, let C_D be the affine plane curve defined by*

$$D^2y^4 = x^3 - x + 1.$$

Then, $C_D(\mathbb{Q})$ is non-empty only if $D = \pm 1$. Moreover, we have

$$C_1(\mathbb{Q}) = C_{-1}(\mathbb{Q}) = \{(0, \pm 1), (\pm 1, \pm 1)\}.$$

Then, we obtain the assertion in the quadratic case.

For the case $d \ge 3$, the conclusion follows even from a Diophantine reduction to the results of [DM97] on the consequences of modularity.

Remark 1.6. There is an arboreal perspective for 1.3 and the previous works [FHI$^+$09, FHS11], and [HHK11]. Fix a. The iterated preimages of a by $f_{d,c}$ form a rooted d-ary tree T_d, and the absolute Galois group acts via the arboreal representation

$$\rho_{f,a} : \mathrm{Gal}(\overline{L}/L) \longrightarrow \mathrm{Aut}(T_d).$$

The uniformity results on the rational iterated preimages are equivalent to the fact that rational vertices cannot persist beyond a uniform level. This picture is consistent with the expectation that, for generic c, the image of $\rho_{f,a}$ is large and rational constraints become increasingly scarce deeper in the tree. See [Odo85] and [Jon13] for these expectations.

Remark 1.7. We may be able to generalize the method used in the proof of 1.5 to the curves defined by

$$D^2y^4 = f(x) \tag{1.1}$$

for $f \in \mathbb{Q}[x]$ having no rational roots and $\deg f = 3$. Moreover, we can use the method to determine the perfect squares in elliptic divisibility sequences (see [Rey12, NS24] for the study of perfect powers in elliptic divisibility sequences in general). Although generalized n-descent for curves of genus 3 has already been developed in [BPS16], it needs heavy computational costs, and often needs to assume the BSD conjecture or the generalized Riemann Hypothesis. This is the reason that [FHS11] needed the BSD conjecture. Our method seems to be comparatively computationally light.

Although the explicit descent on the Jacobians of the curve

$$y^p = f(x)$$

for a prime number p is dealt with in [Sch95, PS97, Sto01, BS09, Mou12, Cre13], our curve (1.1) is out of their scope.

Organization of this paper. In Section 2.1, we recall some geometric facts on $X^{\mathrm{pre}}(2,N,0)$ developped in [FHI$^+$09] and [FHS11]. In Section 2.2, we list some arithmetic facts on a specific elliptic curve. In Section 3 and Section 4 involves the proof of 1.3 (i) and (ii), respectively. In Section 3.1, we define integral models of curves under consideration, and we investigate their singularities and étaleness of some morphisms. In Section 3.2 we reduce the proof of 1.3 (i) to the determination of rational points of C_D's. In Section 3.3, we completely determine the rational points of C_D's. In Section 3.4, we complete the proof of 1.3(i).

Acknowledgement

The author would like to thank Professor Bjorn Poonen for providing a geometric perspective that clarified both the elementary and the more intricate calculations in this work. The author is also grateful to Professor Shun'ichi Yokoyama for his helpful advice on the use of Magma, and to Professor Yasuhiro Ishitsuka and Professor Hiroyasu Miyazaki for their valuable comments.

2. Preliminaries

2.1. **Geometry.** In this subsection, we recall some geometric facts on the preimage curves for $d = 2$ given in [FHI+09] and [FHS11]. Let k be a field of characteristic different from 2. For $a \in k$, define an algebraic set

$$Y^{\mathrm{pre}}(2, N, a) \coloneqq V(f_{2,c}^{\circ N}(x) - a) \subset \mathbb{A}^2_k = \operatorname{Spec} k[c, x],$$

and a morphism $\iota\colon Y^{\mathrm{pre}}(2, N, a) \longrightarrow \mathbb{A}^N$ by

$$\iota(c, x) = (f_{2,c}^{\circ(N-1)}(x), f_{2,c}^{\circ(N-2)}(x), \dots, f_{2,c}(x), x).$$

Note that the order of the polynomials defining ι is the reverse of that in [FHS11]. If $Y^{\mathrm{pre}}(2, N, a)$ is geometrically irreducible, let $X^{\mathrm{pre}}(2, N, a)$ be the unique complete nonsingular curve birational to $Y^{\mathrm{pre}}(2, N, a)$. We have the following lemma.

Lemma 2.1 ([FHS11, Lemma 4.1, Theorem 4.2, and Corollary 4.3])**.**

(i) *The morphism $\iota\colon Y^{\mathrm{pre}}(2, N, a) \longrightarrow \mathbb{A}^N$ is a closed immersion. If $\mathbb{A}^N$ has coordinates $z_1, z_2, \dots, z_N$, then the ideal defining the image of ι is*

$$I = (z_1^2 + z_i - z_{i+1}^2 - a : 1 \le i \le N - 1).$$

(ii) *Let $W, Z_1, Z_2, \dots, Z_N$ be the homogeneous coordinate of $\mathbb{P}^N$, and identify $\mathbb{A}^N$ with the subset of $\mathbb{P}^N$ where $W \neq 0$. Then, the projective closure of the image of ι is a complete intersection of the closed set defined by the homogeneous ideal*

$$J = (Z_1^2 + Z_i W - Z_{i+1}^2 - aW^2 : 1 \le i \le N - 1).$$

(iii) *The points of $V(J)$ on the hyperplane $W = 0$ have homogeneous coordinates*

$$[0, \epsilon_1, \epsilon_2, \dots, \epsilon_N], \quad \epsilon_i = \pm 1.$$

Moreover, they are all nonsingular points of $V(J)$.

(iv) *If $Y^{\mathrm{pre}}(2, N, a)$ is nonsingular, then we have $X^{\mathrm{pre}}(2, N, a) \cong V(J)$ and the complement of the affine part $X^{\mathrm{pre}}(2, N, a) \setminus Y^{\mathrm{pre}}(2, N, a)$ consists 2^{N-1} points.*

(v) *If $Y^{\mathrm{pre}}(2, N, a)$ is nonsingular, then the curve $X^{\mathrm{pre}}(2, N, a)$ can be defined over k, and it is both nonsingular and geometrically irreducible.*

Proof. See [FHS11, Section 4] for (i)–(iv) and [FHI+09, Proposition 4.8] for (v). Note that the coordinates in [FHS11] are chosen to satisfy $f_{2,c}^{\circ i}(z_0) = z_i$, and the coordinates in this paper are arranged to satisfy $f_{2,c}^{\circ i}(z_i) = a$. □

Lemma 2.2.

(i) *The complete curve $X^{\mathrm{pre}}(2, 3, 0)$ is isomorphic to the elliptic curve*

$$E : v^2 = u^3 - u + 1$$

over $\mathbb{Q}$. The birational transform $E \dashrightarrow Y^{\mathrm{pre}}(2, 3, 0)$ is given by

$$x = \frac{v}{u^2 - 1}, \quad c = -\frac{1}{(u^2 - 1)^2}.$$

(ii) *If $[U, V, S]$ is the homogeneous coordinate of E, the isomorphism $E \xrightarrow{\sim} X^{\mathrm{pre}}(2, 3, 0)$ is defined by*

$$[U, V, S] \mapsto \begin{cases} [U^2 - S^2, S^2, US, VS] & \text{if } S \neq 0, \\ [V^2 - S^2, US, U^2, UV] & \text{if } V^2 - S^2 \neq 0, \end{cases}$$

and the inverse is given by

$$[W, Z_1, Z_2, Z_3] \mapsto \begin{cases} [Z_2, Z_3, Z_1] & \text{if } Z_i \neq 0 \text{ for some } i, \\ [(W + Z_1)Z_3, Z_1Z_2 + Z_1W + W^2, Z_2Z_3] & \text{if } Z_1Z_2 + Z_1W + W^2 \neq 0. \end{cases}$$

Note that these expressions coincide with each other at the intersection of the loci.

Proof. See [FHS11, Lemma 5.2] for the statement on birational transformation. We can check the coincidence of the two expressions as follows

$$\begin{aligned}
[U^2 - S^2, S^2, US, VS] &= [U^3 - US^2, US^2, U^2S, UVS] \\
&= [V^2S - S^3, US^2, U^2S, UVS] \\
&= [V^2 - S^2, US, U^2, UV], \text{ and} \\
[Z_2, Z_3, Z_1] &= [Z_2^2 Z_3, Z_2 Z_3^2, Z_1 Z_2 Z_3] \\
&= [(W + Z_1)Z_1 Z_3, Z_2(Z_1^2 + WZ_2), Z_1 Z_2 Z_3] \\
&= [(W + Z_1)Z_1 Z_3, Z_1^2 Z_2 + W(Z_1^2 + Z_1 W), Z_1 Z_2 Z_3] \\
&= [(W + Z_1)Z_3, Z_1 Z_2 + Z_1 W + W^2, Z_2 Z_3].
\end{aligned}$$

□

2.2. **Arithmetic.** This subsection lists some arithmetic facts on curves, which we will use in the proof of 1.3 (i). Almost all facts in this subsection are checked using Magma [BCP97].

Lemma 2.3. *Let $K = \mathbb{Q}(\theta)$ be the number field generated by an element θ with the minimal polynomial*

$$f(t) = t^3 - t + 1.$$

Let $\mathcal{O}_K$ be the ring of integers of K. Then, the following statements hold.

(i) *The discriminant of K is -23.*
(ii) *The only prime ideal 23 ramifies in K, and we can write $(23) = \mathfrak{p}_1\mathfrak{p}_2^2$ with distinct non-zero prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of K. Moreover, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are generated by $\beta_1 := 3\theta^2 - 4$ and $\beta_2 := 3\theta^2 - 1$, respectively.*
(iii) *The class number of K is 1.*
(iv) *The unit group of $\mathcal{O}_K$ is generated by ± 1 and θ, and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Lemma 2.4. *Let E be the elliptic curve defined by*

$$E : v^2 = u^3 - u + 1$$

with the point O at infinity. Let K, θ, $\mathfrak{p}_1$, and $\mathfrak{p}_2$ be as in 2.3. Then, the following statements hold.

(i) *The Mordell–Weil group $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z}$, and is generated by $Q_0 := (1, -1)$.*
(ii) *There are 10 known rational points in $X^{\mathrm{pre}}(2, 4, 0)$ as follows.*

	$X^{\mathrm{pre}}(2,4,0)(\mathbb{Q})$	$\mu \circ \pi(P_i)$	$= mQ_0$
P_1	$[0,1,1,1,1]$	$[1,1,1]$	$= -Q_0$
P_2	$[0,-1,1,1,1]$	$[-1,-1,1]$	$= 2Q_0$
P_3	$[0,1,-1,1,1]$	$[-1,1,1]$	$= -2Q_0$
P_4	$[0,-1,-1,1,1]$	$[1,-1,1]$	$= Q_0$
P_5	$[0,1,1,-1,1]$	$[1,-1,1]$	$= Q_0$
P_6	$[0,-1,1,-1,1]$	$[-1,1,1]$	$= -2Q_0$
P_7	$[0,1,-1,-1,1]$	$[-1,-1,1]$	$= 2Q_0$
P_8	$[0,-1,-1,-1,1]$	$[1,1,1]$	$= -Q_0$
P_9	$[1,0,0,0,0]$	$[0,1,0]$	$= O$
P_{10}	$[1,-1,0,-1,0]$	$[0,1,1]$	$= 3Q_0$,

where $\pi\colon X^{\mathrm{pre}}(2,4,0) \longrightarrow X^{\mathrm{pre}}(2,3,0)$ is the projection $[W, Z_1, Z_2, Z_3, Z_4] \mapsto [W, Z_1, Z_2, Z_3]$, and $\mu\colon X^{\mathrm{pre}}(2,3,0) \longrightarrow E$ is the isomorphism defined in 2.2 (ii).

(iii) *The morphism π ramifies at the points with $Z_4 = 0$. Precisely, these points are P_9, P_{10}, and 6 points written as*

$$[1, f_{2,c_0}^3(0) f_{2,c_0}^2(0), f_{2,c_0}(0), 0],$$

where c_0's are the roots of

$$F(c) := f_{2,c}^{\circ 4}(0) / f_{2,c}^{\circ 2}(0) = c^6 + 3c^5 + 3c^4 + 3c^3 + 2c^2 + 1 = 0.$$

(iv) *The discriminant of F is $58673 = 23 \cdot 2551$. Moreover, we have*

$$F(c) = \begin{cases} (c+4)^2(c+18)(c^3 + 4c + 2) & \text{over } \mathbb{F}_{23} \\ (c+477)^2(c^4 + 1600c^3 + 1162c^2 + 297c + 1869) & \text{over } \mathbb{F}_{2551}. \end{cases}$$

(v) *Define the map* $(x-T)\colon E(\mathbb{Q}) \longrightarrow K^\times/(K^\times)^2$ *by*

$$P \mapsto \begin{cases} (u-\theta)(K^\times)^2 & \text{for } P=(u,v)\neq O,\\ (K^\times)^2 & \text{for } P=O. \end{cases}$$

Then, the map $(x-T)$ *is a homomorphism with the kernel* $2E(\mathbb{Q})$*, and its image equals*

$$\{(K^\times)^2, -\theta(K^\times)^2\}.$$

3. Proof of main results for $d=2$

In this section, we prove 1.3 (i). To avoid the calculation of the Mordell-Weil rank of the Jacobian of $X^{\mathrm{pre}}(2,4,0)$, we efficiently use the geometric information of the surjection $\pi\colon X^{\mathrm{pre}}(2,4,0) \longrightarrow X^{\mathrm{pre}}(2,3,0)$ and a tricky argument based on the 2-descent of the elliptic curve

$$E : v^2 = u^3 - u + 1,$$

which is isomorphic to $X^{\mathrm{pre}}(2,3,0)$.

3.1. **Integral models and their geometry.** In this section, we study the models of $X^{\mathrm{pre}}(2,4,0)$ and E over $R=\mathbb{Z}[\frac{1}{2},\frac{1}{23}]$. Consider the projective R-schemes $\mathcal{E}$, $\mathcal{F}$ $\mathcal{X}_3$, and $\mathcal{X}_4$ defined by the following homogeneous ideals

$$\begin{aligned} I_{\mathcal{E}} &= (V^2S - U^3 + US^2 - S^3) \subset R[U,V,S],\\ I_{\mathcal{F}} &= (T^4 - U^3S + US^3 - S^4) \subset R[U,T,S],\\ I_{\mathcal{X}_3} &= (Z_1^2 + Z_iW - Z_{i+1}^2 : 1\le i\le 2) \subset R[W,Z_1,Z_2,Z_3], \text{ and}\\ I_{\mathcal{X}_4} &= (Z_1^2 + Z_iW - Z_{i+1}^2 : 1\le i\le 3) \subset R[W,Z_1,Z_2,Z_3,Z_4], \end{aligned}$$

respectively. Note that $\mathcal{E}$ and $\mathcal{F}$ are smooth (see 3.4 (i)), and the generic fiber of $\mathcal{E}$ equals E in 2.4. The self-morphisms $[2]$ and T_{3Q_0} on E can be extended to $\mathcal{E}$. We use the same notation for the extended morphisms.

Let $\varphi\colon \mathcal{E} \longrightarrow \mathcal{E}$ be either $[2]$ or $T_{3Q_0}\circ[2]$. Let π be the composition of the morphisms $\mathrm{pr}\colon \mathcal{X}_4 \longrightarrow \mathcal{X}_3$ and $\mu\colon \mathcal{X}_3 \xrightarrow{\sim} \mathcal{E}$ defined by

$$\mathrm{pr}\colon [W,Z_1,Z_2,Z_3,Z_4] \mapsto [W,Z_1,Z_2,Z_3], \text{ and}$$

$$\mu\colon [W,Z_1,Z_2,Z_3] \mapsto \begin{cases} [Z_2,Z_3,Z_1] & \text{if } Z_i\neq 0 \text{ for some } i,\\ [(W+Z_1)Z_3, Z_1Z_2+Z_1W+W^2, Z_2Z_3] & \text{if } Z_1Z_2+Z_1W+W^2\neq 0, \end{cases}$$

which is dealt with in 2.2. Let π be the composition $\mu\circ\mathrm{pr}$. Note that μ is an isomorphism of schemes over R. Let $\psi\colon \mathcal{F} \longrightarrow \mathcal{E}$ be the morphism defined by

$$\psi\colon [U,T,S] \mapsto \begin{cases} [US, T^2, S^2] & \text{if } S\neq 0,\\ [UT^2, U^3 - US^2 + S^3, ST^2] & \text{if } U^3 - US^2 + S^3 \neq 0. \end{cases}$$

Let $\mathcal{X}_4'$ and $\mathcal{X}_4''$ be the projective schemes over R given by the following Cartesian diagrams.

$$\begin{array}{ccccc} \mathcal{X}_4 & \xleftarrow{\varphi'} & \mathcal{X}_4' & \xleftarrow{\psi'} & \mathcal{X}_4''\\ \pi\downarrow & & \pi'\downarrow & & \downarrow\pi''\\ \mathcal{E} & \xleftarrow{\varphi} & \mathcal{E} & \xleftarrow{\psi} & \mathcal{F} \end{array}$$

Before proving the flatness of each scheme, we provide sufficient conditions for the flatness of algebras over a principal ideal domain.

Lemma 3.1. *Let* R_0 *be a ring and* n *and* m *be positive integers with* $m\le n$*. For polynomials* $F_i(T_i,T_{i+1},\dots,T_n)$ $(1\le i\le m)$ *in* $R'=R_0[T_1,T_2,\dots,T_n]$*, suppose that* F_i *is monic in* T_i *up to multiplying a unit in* R_0*. Let* I *be the ideal* $(F_1,F_2,\dots,F_m)$*. Then, the following statements hold.*

(i) *For* $g\in R'$*, set* $r_0=g$*, and* r_{i+1} *for* $0\le i\le m-1$ *be the remainder of* r_i *by* F_{i+1} *as polynomials in the variable* T_{i+1}*. Then,* g *is in* I *if and only if* $r_m=0$ *holds.*

(ii) *Suppose that* R_0 *is a principal ideal domain. Then, the* R_0*-algebra* R'/I *is flat.*

Proof. (i) If $r_m = 0$, the polynomial g is obviously in I.

Assume that g is in I. Then, there are polynomials $g_{i,0} \in R'$ $(1 \leq i \leq m)$ such that

$$r_0 = g = \sum_{i=1}^{m} g_{i,0} F_i.$$

Divide each $g_{i,0}$ for $2 \leq i \leq m$ by F_1 as polynomials in the variable T_1, and write the quotient $q_{i,1}$ and the remainder $g_{i,1}$. Set $g_{1,1} = \sum_{i=2}^{m} q_{i,1} + g_{1,0}$. Then, we have the equalities

$$r_0 = \sum_{i=1}^{m} g_{i,1} F_i, \text{ and } \quad r_1 = \sum_{i=2}^{m} g_{i,1} F_i.$$

By inductively running the same process replacing the role of r_0 and F_1 with r_j and F_{j+1} for $j = 1, 2, \dots m-1$, we get the polynomials $g_{i,j} \in R'$ $(j+1 \leq i \leq m)$ such that

$$r_j = \sum_{i=j+1}^{m} g_{i,j+1} F_i, \text{ and } \quad r_{j+1} = \sum_{i=j+2}^{m} g_{i,j+1} F_i.$$

This observation shows that $r_m = 0$.

(ii) Since the flatness over a principal ideal domain R_0 is equivalent to R_0-torsion freeness, it is enough to show that for $g \in R'$, there exists an element $a \in R_0 \setminus \{0\}$ such that ag is in I if and only if g is itself in I. Suppose that ag is in I for some $a \in R_0 \setminus \{0\}$. Set r_i and r'_i for $1 \leq i \leq m$ as in the statement of (i) for g and ag, respectively. Then, we have $r'_i = a r_i$. Thus, $r'_m = 0$ if and only if $r_m = 0$. By (i), we obtain the assertion. □

Lemma 3.2.

(i) *The R-scheme $\mathcal{X}_4$ is flat over R.*
(ii) *The R-scheme $\mathcal{E}$ is flat over R.*
(iii) *The R-scheme $\mathcal{F}$ is flat over R.*

Proof. (i) Two affine open subschemes

$$\mathcal{X}_4 \cap D_+(W) \cong \operatorname{Spec} R[Z_1, Z_2, Z_3, Z_4]/(Z_{i+1}^2 - Z_1^2 - Z_i : 1 \leq i \leq 3), \text{ and}$$
$$\mathcal{X}_4 \cap D_+(Z_1) \cong \operatorname{Spec} R[Z_2, Z_3, Z_4, W]/(Z_4^2 - Z_3 W - 1, Z_3^2 - Z_2 W - 1, Z_2^2 - W - 1).$$

covers the R-scheme $\mathcal{X}_4$. Three affine open subschemes

$$\mathcal{E} \cap D_+(U) \cong \operatorname{Spec} R[V, S]/(V^2 S - S^3 + S^2 - 1),$$
$$\mathcal{E} \cap D_+(V) \cong \operatorname{Spec} R[U, S]/(S - U^3 + U S^2 - S^3), \text{ and}$$
$$\mathcal{E} \cap D_+(S) \cong \operatorname{Spec} R[U, V]/(V^2 - U^3 + U - 1).$$

cover the scheme $\mathcal{E}$. Three affine open subschemes

$$\mathcal{F} \cap D_+(U) \cong \operatorname{Spec} R[T, S]/(T^4 - S + S^3 - S^4),$$
$$\mathcal{F} \cap D_+(T) \cong \operatorname{Spec} R[U, S]/(1 - U^3 S + U S^3 - S^4), \text{ and}$$
$$\mathcal{F} \cap D_+(S) \cong \operatorname{Spec} R[U, T]/(T^4 - U^3 + U - 1).$$

cover the scheme $\mathcal{F}$. All of them are flat over R by 3.1 (ii). □

For an R-scheme $\mathcal{X}$ and a prime ideal (p) of R, let $\kappa(p)$ denote the residue field of R at (p), $\mathcal{X}_p$ denote the fiber $\mathcal{X} \times_{\operatorname{Spec} R} \operatorname{Spec} \kappa(p)$, and $\mathcal{X}_{\overline{p}}$ denote the scheme $\mathcal{X}_p \times_{\kappa(p)} \operatorname{Spec} \overline{\kappa(p)}$, where $\overline{\kappa(p)}$ is the algebraic closure of $\kappa(p)$. For an R-morphism $\phi\colon \mathcal{X} \longrightarrow \mathcal{Y}$ of R-schemes $\mathcal{X}$ and $\mathcal{Y}$, let $\phi_p\colon \mathcal{X}_p \longrightarrow \mathcal{Y}_p$ and $\phi_{\overline{p}}\colon \mathcal{X}_{\overline{p}} \longrightarrow \mathcal{Y}_{\overline{p}}$ be the induced morphisms.

Lemma 3.3. *For a flat finite R-morphism $\phi\colon \mathcal{X} \longrightarrow \mathcal{Y}$ of R-schemes, ϕ is étale if and only if for all maximal ideal $(p) \in \operatorname{Spec} R$, the morphism $\phi_{\overline{p}}$ is étale.*

Proof. Assume that $\phi_{\overline{p}}$ is étale for all maximal ideal $(p) \in \operatorname{Spec} R \setminus \{(0)\}$. Since $\phi_{\overline{p}}$ is étale, it is smooth, and so is ϕ_p by the definition of smoothness. By the finiteness of $\phi_{\overline{p}}$, it is étale. Since the étaleness is an open condition, ϕ is itself étale.

The opposite implication is true because the base change of an étale morphism is étale. □

On the ramification and the singular locus, we have the following lemma.

Lemma 3.4. *Let notation be as above. The following statements hold.*

(i) *The schemes $\mathcal{E}$ and $\mathcal{F}$ are smooth.*
(ii) *For all $(p) \in \operatorname{Spec} R \setminus \{(2551)\}$, the scheme $(\mathcal{X}_4)_{\overline{p}}$ is regular. The scheme $(\mathcal{X}_4)_{\overline{2551}}$ is singular only at $[1, -308, 13, -477, 0] \in (\mathcal{X}_4)_{\overline{2551}}(\overline{\mathbb{F}_{2551}})$. In particular, the singular point is outside $\pi_{\overline{p}}^{-1}(O) \cup \pi_{\overline{p}}^{-1}(3Q_0)$, where note that we abuse the notation for the $\mathbb{F}_p$-rational points $O = [0, 1, 0]$ and $3Q_0 = [0, 1, 1]$ over all primes $p \in \mathcal{P}$.*
(iii) *The singular point $[1, -308, 13, -477, 0] \in (\mathcal{X}_4)_{\overline{2551}}$ is an ordinary double point.*
(iv) *For all $(p) \in \operatorname{Spec} R$ and all closed point $x \in \pi_{\overline{p}}^{-1}(O) \cup \pi_{\overline{p}}^{-1}(3Q_0)$, the ramification degree of $\pi_{\overline{p}}$ at x equals 2.*
(v) *The genus of $(\mathcal{X}_4)_p$ is 5 for all $(p) \in \operatorname{Spec} R \setminus \{(2551)\}$, and is 4 for $(p) = (2551)$.*
(vi) *For all $(p) \in \operatorname{Spec} R$, the schemes $(\mathcal{X}_4')_p$ and $(\mathcal{X}_4'')_p$ are integral.*
(vii) *For all $(p) \in \operatorname{Spec} R$, the scheme $(\mathcal{X}_4')_{\overline{p}}$ is regular at all closed point $x' \in \pi_{\overline{p}}'^{-1}(\mathcal{E}_{\overline{p}}[2])$.*
(viii) *For all $(p) \in \operatorname{Spec} R$ and all closed point $x' \in \pi_{\overline{p}}'^{-1}(\mathcal{E}_{\overline{p}}[2])$, the ramification degree of $\pi_{\overline{p}}'$ at x' is 2.*
(ix) *The morphism $\psi_{\overline{p}}$ is étale outside $\mathcal{E}_{\overline{p}}[2]$ for all $(p) \in \operatorname{Spec} R$. For all closed point $\mathfrak{f} \in \psi_{\overline{p}}^{-1}(\mathcal{E}_{\overline{p}}[2])$, the ramification degree of $\psi_{\overline{p}}$ at f equals 2.*

Proof. (i) We can check the regularity of $\mathcal{E}$ and $\mathcal{F}$ at the closed point by the Jacobian criterion. Since $\mathcal{E}$ and $\mathcal{F}$ are flat over R, they are regular at all points.

(ii) Since $\mathcal{E}$ is smooth, the curve $(\mathcal{X}_4)_{\overline{p}}$ is smooth at all points other than the points at which $\pi_{\overline{p}}$ ramifies. Ramification points of $\pi_{\overline{p}}$ is given as in 2.4 (iii) over all $p \in \mathcal{P}$. In particular, these points are in the open subset $(W \neq 0)$. This open subset is isomorphic to the affine scheme $Y^{\mathrm{pre}}(2, 4, 0)_{\overline{p}} = V(f_{2,c}^{\circ 4}(x)) \subset (\mathbb{A}^2_{x,c})_{\overline{p}}$. By the Jacobian criterion, a point $(0, c_0)$ is a singular point of $Y^{\mathrm{pre}}(2, 4, 0)_{\overline{p}}$ if and only if c_0 is a multiple root of $f_{2,c}^{\circ 4}(0)$. Such c_0 exists only over 2551 by 2.4 (iv). Moreover, such c_0 for $p = 2551$ is -477. The point $(x, c) = (0, -477)$ corresponds to $[1, -308, 13, -477, 0] \in (\mathcal{X}_4)_{\overline{2551}}(\overline{\mathbb{F}_{2551}})$.

(iii) The direct calculation shows that the Hessian of $f_{2,c}^{\circ 4}(x)$ at $(x, c) = (0, -477)$, is non-degenerate. Hence, it is an ordinary double point of $Y^{\mathrm{pre}}(2, 4, 0)_{\overline{2551}}$ (see [Sta18, Tag 0C49]).

(iv) Since the sets $\pi_{\overline{p}}^{-1}(O)$ and $\pi_{\overline{p}}^{-1}(3Q_0)$ consists of only one smooth point $P_9 = [1, 0, 0, 0, 0]$ and $P_{10} = [1, -1, 0, -1, 0]$, respectively, and the degree of $\pi_{\overline{p}}$ is 2, the statement holds.

(v) For $p \in \mathcal{P} \setminus \{2551\}$, the curve $(\mathcal{X}_4)_{\overline{p}}$ is smooth, and $\pi_{\overline{p}}$ ramifies at 8 points as similar to 2.4 (iii). Hence, the Riemann-Hurwitz formula shows that the genus of $\mathcal{X}_{\overline{p}}$ is 5.

Let $\nu \colon \widetilde{\mathcal{X}} \longrightarrow (\mathcal{X}_4)_{\overline{2551}}$ be the normalization of $(\mathcal{X}_4)_{\overline{2551}}$. It is enough to show that the genus of $\widetilde{\mathcal{X}}$ is 4. Since the singular point of $(\mathcal{X}_4)_{\overline{2551}}$ is a single ordinary double point by (iii), its preimage by ν consists of two points. Hence, the morphism $\nu_{\overline{2551}} \circ \pi$ ramifies at 6 points, and is of degree 2. The Riemann-Hurwitz shows that the genus of $\widetilde{\mathcal{X}}$ is 4.

(vi) Since the extensions of function fields induced by φ_p and $\varphi_p \circ \psi_p$ are separable extensions, the function fields of $(\mathcal{X}_4')_p$ and $(\mathcal{X}_4'')_p$ are reduced.

Assume that $(\mathcal{X}_4'')_p$ (resp. $(\mathcal{X}_4')_p$) is not irreducible, and let $\mathcal{C}$ be an irreducible component. Since the morphism π'' (resp. π') is of degree 2, and its restriction to each irreducible component is dominant, $\mathcal{C}$ is birational to $\mathcal{F}_p$ (resp. $(\mathcal{E})_p$). Hence, the genus of $\mathcal{C}$ is 3 (resp. 1). However, since the restriction of the morphism $\varphi_p' \circ \psi_p'$ (resp. φ_p') to $\mathcal{C}$ is dominant, the genus of $\mathcal{C}$ is more than or equal to that of $(\mathcal{X}_4)_p$, which is 4 or 5 by (v). This is a contradiction.

(vii) Since φ is étale, the morphism $\varphi_{\overline{p}}$ is étale, in particular smooth. Since $\varphi_{\overline{p}}(x')$ is a regular point of $(\mathcal{X}_4)_{\overline{p}}$ by (ii), the assertion holds (see [Liu02, Chapter 4, Theorem 3.36]).

(viii) Let x' be an element of the fiber $\pi_{\overline{p}}'^{-1}(e)$ for some $e \in \mathcal{E}_{\overline{p}}[2](\overline{\kappa(p)})$. Note that x' is a regular point by (vii). The set $\pi_{\overline{p}}^{-1}(\varphi_{\overline{p}}(e))$ consists of a single regular point, either P_9 or P_{10}. Since the scheme $\mathcal{X}_{\overline{p}}$ is defined as the fiber product, the point x' is the unique point of $\pi_{\overline{p}}'^{-1}(e)$. Therefore, the ramification degree of $\pi_{\overline{p}}'$ at x' equals the degree of $\pi_{\overline{p}}'$, which is 2.

(ix) For $e \in (\mathcal{E}_{\overline{p}} \setminus \mathcal{E}_{\overline{p}}[2])(\overline{\mathbb{F}_p})$, the fiber $\psi_{\overline{p}}'^{-1}(e)$ consists of two regular points. For $e \in \mathcal{E}_{\overline{p}}[2]$, the fiber $\psi_{\overline{p}}'^{-1}(e)$ consists of a single regular point. Since the degree of $\psi_{\overline{p}}'$ is 2, the assertion holds. □

Proposition 3.5. *Let notation be as above. Let $\widetilde{\mathcal{X}_4''}$ be the partial normalization of $\mathcal{X}_4''$ at $(\pi' \circ \psi')^{-1}(\mathcal{E}[2])$, i.e., the scheme given by glueing $\mathcal{X}_4'' \setminus (\pi' \circ \psi')^{-1}(\mathcal{E}[2])$ and the normalization of $\mathcal{X}_4'' \setminus$*

$\big(\mathrm{Sing}(\mathcal{X}_4'') \setminus (\pi' \circ \psi')^{-1}(\mathcal{E}[2])\big)$. *Let* $\nu\colon \widetilde{\mathcal{X}_4}'' \longrightarrow \mathcal{X}_4''$ *be the canonical morphism. Then, the morphism* $\psi' \circ \nu\colon \widetilde{\mathcal{X}_4}'' \longrightarrow \mathcal{X}_4'$ *is finite étale of degree* 2.

Proof. Only the étaleness is non-trivial. By 3.3, it suffices to check étaleness fiberwise. Let η, ξ, and η' be the generic points of $\mathcal{E}[2], \pi'^{-1}(\mathcal{E}[2])$, and $\psi^{-1}(\mathcal{E}[2])$, respectively. Then, the rings

$$A \coloneqq \mathcal{O}_{\mathcal{E},\eta}, \quad B \coloneqq \mathcal{O}_{\mathcal{X}_4',\xi}, \text{ and } \quad A_1 \coloneqq \mathcal{O}_{\mathcal{F},\eta'}$$

are DVR. Moreover, since the ramification degrees of the extensions A_1/A and B/A are both equal to 2. Hence, letting B_1 be the integral closure of $B \otimes_A A_1$ in the fraction field at a generic point of $(\pi' \circ \psi' \circ \nu)^{-1}(\mathcal{E}[2])$, we can see that B_1/B is unramified by the Abhyankar's Lemma [Sta18, Tag 0BRM]. Hence, the morphism $\psi' \circ \nu$ is étale on $(\pi' \circ \psi' \circ \nu)^{-1}(\mathcal{E}[2])$ by the purity of the branch locus (see [Sta18, Tag 0BMB]).

Let U be the open subscheme $\mathcal{X}_4'' \setminus (\pi' \circ \psi')^{-1}(\mathcal{E}[2])$. Then, restriction of ν to $\nu^{-1}(U)$ is isomorphism. Since ψ' is étale on U, the morphism $\psi' \circ \nu$ is étale on $\nu^{-1}(U)$. Consequently, $\psi' \circ \nu$ is étale on the whole space $\widetilde{\mathcal{X}_4}''$. □

3.2. **Reduction to curves C_D of lower genus.** Let $X_4 = X^{\mathrm{pre}}(2,4,0)$, X_4', X_4'', $\widetilde{X_4}''$, F be the generic fiber of $\mathcal{X}_4$, $\mathcal{X}_4'$, $\mathcal{X}_4''$, $\widetilde{\mathcal{X}_4}''$, and F respectively. Then, we have the diagram

$$\begin{array}{ccccccc} X_4 & \xleftarrow{\varphi'} & X_4' & \xleftarrow{\psi'} & X_4'' & \xleftarrow{\nu} & \widetilde{X_4}'' \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi'} & & \downarrow{\scriptstyle\pi''} & & \\ E & \xleftarrow{\varphi} & E & \xleftarrow{\psi} & F & & \end{array}$$

commutes. For a rational point $x \in X_4(\mathbb{Q})$, the point $\pi(x)$ is in the image $\varphi(E(\mathbb{Q}))$ for either $\varphi = [2]$ or $T_{3Q_0} \circ [2]$ since the Mordell-Weil group $E(\mathbb{Q})$ is generated by Q_0 by 2.4(i). Thus, it lifts to $x' \in X_4'(\mathbb{Q})$. By the projectivity of $\mathcal{X}_4'$, the point x' lifts to a section $x' \in \mathcal{X}_4'(\operatorname{Spec} R)$, where $R = \mathbb{Z}[\frac{1}{2}, \frac{1}{23}]$. Taking the fiber product, we get the following diagram:

$$\begin{array}{ccccccc} \operatorname{Spec} R & \longleftarrow & \operatorname{Spec} R & \xleftarrow{\varpi} & \operatorname{Spec} R' & & \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x'} & \llcorner & \downarrow{\scriptstyle \widetilde{x}''} & & \\ \mathcal{X}_4 & \xleftarrow{\varphi'} & \mathcal{X}_4' & \xleftarrow{\psi'} & \mathcal{X}_4'' & \xleftarrow{\nu} & \widetilde{\mathcal{X}_4}'' \\ \downarrow{\scriptstyle\pi} & & \llcorner\ \downarrow{\scriptstyle\pi'} & & \llcorner\ \downarrow{\scriptstyle\pi''} & & \\ \mathcal{E} & \xleftarrow{\varphi} & \mathcal{E} & \xleftarrow{\psi} & \mathcal{F} & & \end{array}$$

By 3.5, the morphism $\psi' \circ \nu$ is finite étale of degree 2. Hence, the morphism ϖ is finite étale of degree 2. The following proposition lets us write R' down explicitly.

Proposition 3.6. *Let* $R = \mathbb{Z}[1/p_i : 1 \le i \le n]$ *with distinct prime numbers* $p_1 = 2, p_2, \ldots, p_n$. *For* $D = (-1)^{\varepsilon_0} \prod_{1 \le i \le n} p_i^{\varepsilon_i}$ *with some* $\varepsilon_i \in \{0,1\}$ $(0 \le i \le n)$, *let* $R_D \coloneqq R[x]/(x^2 - D)$. *Then,* R_D *is a finite étale* R*-algebra of degree* 2. *Moreover, any finite étale* R*-algebra of degree* 2 *is given in this way.*

Proof. At first, it is easy to see that the R-algebra R_D in the statement is finite étale of degree 2 over R since 2 is invertible in R.

Any finite étale covering of $\operatorname{Spec} R$ is automatically a Galois étale covering of $\operatorname{Spec} R$ with Galois group $\mathbb{Z}/2\mathbb{Z}$, thus, a μ_2-torsor over $\operatorname{Spec} R$. The group $H^1_{\text{ét}}(\operatorname{Spec} R, \mu_2)$ classifies μ_2-torsors over $\operatorname{Spec} R$ up to ismorphisms. We have the following exact sequence of étale sheaves on $\operatorname{Spec} R$:

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{G}_m \xrightarrow{(\cdot)^2} \mathbb{G}_m \longrightarrow 1$$

since 2 is invertible in R. Taking the long exact sequence, we obtain the exact sequence

$$R^\times \xrightarrow{(\cdot)^2} R^\times \longrightarrow H^1_{\text{ét}}(\operatorname{Spec} R, \mu_2) \longrightarrow H^1_{\text{ét}}(\operatorname{Spec} R, \mathbb{G}_m).$$

Here, we note that $H^1_{\text{ét}}(\operatorname{Spec} R, \mathbb{G}_m) \cong \mathrm{Pic}(R)$ by [Poo17, Proposition 6.6.1], and it is a trivial group since R is a principal ideal domain. Therefore, the group $R^\times/(R^\times)^2$ classifies finite étale coverings of $\operatorname{Spec} R$ of degree 2. Each $[D] \in R^\times/(R^\times)^2$ is represented by $(-1)^{\varepsilon_0} \prod_{1 \le i \le n} p_i^{\varepsilon_i}$ for some $\varepsilon_i \in \{0,1\}$ $(0 \le i \le n)$. Finally, since R_D's for distinct $[D]$ are not isomorphic to each other, we obtain

$2^{n+1}(= \#R^\times/(R^\times)^2)$ isomorphic classes of finite étale R-algebras of degree 2. Hence, these R_D's represent all the isomorphic classes. □

Now, let D be as in 3.6 such that $R' \cong R_D$. If $D = 1$, taking the generic fiber, we conclude that $\mathfrak{f} \coloneqq \pi'' \circ \widetilde{\nu}''(\widetilde{x}'')$ is an element of $F(\mathbb{Q} \times \mathbb{Q}) = F(\mathbb{Q}) \times F(\mathbb{Q})$ such that $\psi(\mathfrak{f})$ is in $E(\mathbb{Q})$, which is equivalent to that $\psi(\mathfrak{f})$ is in the diagonal of $E(\mathbb{Q} \times \mathbb{Q}) = E(\mathbb{Q}) \times E(\mathbb{Q})$.

If $D \neq 1$, taking the generic fiber, we conclude that $\mathfrak{f} \coloneqq \pi'' \circ \widetilde{\nu}''(\widetilde{x}'')$ is an element of $F(\mathbb{Q}(\sqrt{D}))$ such that $\psi(\mathfrak{f})$ is in $E(\mathbb{Q})$. If $\mathfrak{f}$ is a point at infinity, it equals $[1:0:0]$. Its image in E under $[2] \circ \psi$ and $T_{3Q_0} \circ [2] \circ \psi$ are O and $3Q_0$, respectively. Assume that $\mathfrak{f}$ is in the affine part of F. Letting $\mathfrak{f} = (u, t')$, $\psi(\mathfrak{f})$ is in $E(\mathbb{Q})$ if and only if u and t'^2 are rational numbers. Thus, t' is a multiple of a rational number and $\sqrt{D}$, or is itself a rational number. If t' is a rational number, then (u, t') is a rational point of $F = C_1$. If t' is a multiple of a rational number t and $\sqrt{D}$, then (u, t) is a $\mathbb{Q}$-rational point of the curve

$$C_D : D^2t^4 = u^3 - u + 1.$$

Let $\psi_D \colon C_D \longrightarrow E; (u, t) \mapsto (u, Dt^2)$.

Consequently, for any rational point $x \in X_4(\mathbb{Q})$, the point $\pi(x)$ equals $\varphi \circ \psi_D(u, t)$ for some $D = (-1)^{\varepsilon_0}2^{\varepsilon_1}23^{\varepsilon_2}$, $(u, t) \in C_D(\mathbb{Q})$, and $\varphi = [2]$ or $T_{3Q_0} \circ [2]$. Hence, if we obtain the complete list of the rational points of C_D, we can determine all the rational points of X_4.

3.3. **Rational points of C_D.** This subsection aims to prove 1.5. Let K, $\mathcal{O}_K$, θ, $\mathfrak{p}_1 = \beta_1\mathcal{O}_K$, and $\mathfrak{p}_2 = \beta_2\mathcal{O}_K$ be as in 2.3. This section focuses on the determination of the rational points of the affine plane curves

$$C_D \colon D^2y^4 = x^3 - x + 1$$

for $D = (-1)^{\varepsilon_0}2^{\varepsilon_1}23^{\varepsilon_2}$ with $\varepsilon_i \in \{0, 1\}$ $(0 \leq i \leq 2)$. Here, note that we change the notation of variables from the previous subsections to save symbols.

Proof of 1.5. For $(x, y) \in C_D(\mathbb{Q})$, since we have

$$(D^2y)^4 = (D^2x)^3 - D^4(D^2x) + D^6,$$

there are integers X, Y, and $Z > 0$ with

$$D^2y = Y/Z^3,\ D^2x = X/Z^4, \text{ and } (X, Y) = (X, Z) = 1.$$

The equation

$$Y^4 = X^3 - D^4XZ^8 + D^6Z^{12} \tag{3.1}$$

holds. Put

$$A \coloneqq X - D^2\theta Z^4, \quad B \coloneqq X^2 + D^2\theta XZ^4 + D^4(\theta^2 - 1)Z^8,$$

and write

$$A = D_As_A^4, \quad B = D_Bs_B^4$$

with $D_A, D_B, s_A, s_B \in \mathcal{O}_K \setminus \{0\}$ such that D_A and D_B are fourth power free, and D_AD_B is in $(K^\times)^4$. Then, we have the following lemma.

Lemma 3.7. *Let notation be as above.*

(i) *If a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ divides D_A or D_B, it divides all D_A, D_B, D and X.*
(ii) *$2\mathcal{O}_K$ does not divide D_A nor D_B.*
(iii) *$\mathfrak{p}_1$ does not divide D_A nor D_B.*
(iv) *$\mathfrak{p}_2$ does not divide D_A nor D_B.*
(v) *We have $(D_A, D_B) = (1, 1)$, $(-\theta, -\theta^3)$, (θ^2, θ^2), or $(-\theta^3, -\theta)$*

Proof. (i) Assume that $\mathfrak{p}$ divides either D_A or D_B. Since D_A and D_B are fourth power free and the product D_AD_B is in $(K^\times)^4$, both D_A and D_B are divided by $\mathfrak{p}$. For two elements $a, b \in \mathcal{O}_K$, let $\gcd(a, b)$ be the largest ideal dividing both a and b. Since we have the relation

$$\gcd(D_A, D_B) | \gcd(A, B) | D^4(3\theta^2 - 1)Z^8,$$

$\mathfrak{p}$ divides D, $3\theta^2 - 1$, or Z. Since the valuations $v_\mathfrak{p}(D_A)$ and $v_\mathfrak{p}(D_B)$ are even by 2.4 (v), $\mathfrak{p}$ divides $D^4(3\theta^2 - 1)Z^8$ twice, and hence $\mathfrak{p}$ divides D or Z. The equality $X = A + D^2\theta Z^4 = D_As_A^4 + D^2\theta Z^4$ implies that $\mathfrak{p}$ divides X. Since Z is coprime to X, $\mathfrak{p}$ does not divide Z, and hence $\mathfrak{p}$ divides D.

(ii) Assume the contrary. If 4 does not divide X, then the 2-adic valuations of both sides of (3.1) are distinct. Thus, 4 divides X. Put $X' = X/4$. We have

$$Y^4 = 64(X'^3 - (D/2)^4 X' Z^8 + (D/2)^6 Z^{12}).$$

Again, comparing the 2-adic valuations of both sides, we see that 4 divides Y. Put $Y' = Y/4$. Noting that $D/2$ and Z are odd integers, we have the following congruence relations

$$\begin{aligned} 0 \equiv 4Y' &= (X')^3 - (D/2)X'Z^8 + (D/2)^6 Z^{12} \\ &\equiv (X')^3 - X' + 1. \end{aligned}$$

However, 2 does not divide the value $(X')^3 - X' + 1$ for all integers X', which is a contradiction.

(iii) Assume the contrary. As in (ii), the valuations $v_{\mathfrak{p}_1}(D_A)$ and $v_{\mathfrak{p}_1}(D_B)$ are even and positive. Since D_A and D_B are fourth power free, we have $v_{\mathfrak{p}_1}(D_A) = v_{\mathfrak{p}_1}(D_B) = 2$. By (i), $\mathfrak{p}_1$ divides D and X. By the definition of D, the valuation $v_{\mathfrak{p}_1}(D)$ equals 1 in this situation. Since X and Z are prime to each other, Z is not divided by $\mathfrak{p}_1$. We have the equation

$$D_B s_B^4 = X^2 + D^2\theta X Z^4 + D^4(\theta^2 - 1)Z^8 \tag{3.2}$$

by the definition of D_B and s_B. By dividing by D^4Z^8 and completing the square, we get

$$D_B \left(\frac{s_B}{DZ^2}\right)^4 - \frac{3\theta^2 - 4}{4} = \left(\frac{X}{D^2Z^4} + \frac{\theta}{2}\right)^2. \tag{3.3}$$

If $v_{\mathfrak{p}_1}(s_B) > 0$, the $\mathfrak{p}_1$-adic valuation of both sides of (3.3) are distinct. Thus, we obtain $v_{\mathfrak{p}_1}(s_B) = 0$. Moreover, since we have

$$\begin{aligned} v_{\mathfrak{p}_1}(\text{left hand side of (3.2)}) &= v_{\mathfrak{p}_1}(D_B) = 2, \\ v_{\mathfrak{p}_1}(\text{right hand side of (3.2)}) &\begin{cases} = 0 & \text{if } v_{\mathfrak{p}_1}(X) = 0, \text{ and} \\ \geq 4 & \text{if } v_{\mathfrak{p}_1}(X) \geq 2, \end{cases} \end{aligned}$$

we obtain $v_{\mathfrak{p}_1}(X) = 1$. On the other hand, by the definition of D_A and s_A, we have

$$D_A s_A^4 = X - D^2\theta Z^4. \tag{3.4}$$

In our situation, we get

$$\begin{aligned} v_{\mathfrak{p}_1}(\text{left hand side of (3.4)}) &\equiv 2 \mod 4, \text{ and} \\ v_{\mathfrak{p}_1}(\text{right hand side of (3.4)}) &= 1. \end{aligned}$$

This is a contradiction.

(iv) Assume the contrary. As in the argument of the proof of (iii), we have $v_{\mathfrak{p}_2}(D_A) = v_{\mathfrak{p}_2}(D_B) = 2$. By (iii), we have $v_{\mathfrak{p}_1}(D_A) = v_{\mathfrak{p}_1}(D_B) = 0$. Since X is a rational integer, and the ramification degree $e_{\mathfrak{p}_2/23}$ is 2, we have

$$v_{23}(X) = \frac{1}{2} v_{\mathfrak{p}_2}(X).$$

By (i), they are positive integers. Thus, $v_{\mathfrak{p}_2}(X)$ is a positive even integer. If $v_{\mathfrak{p}_2}(X) \geq 3$ holds, we have

$$\begin{aligned} v_{\mathfrak{p}_2}(\text{left hand side of (3.2)}) &\equiv 2 \mod 4, \text{ and} \\ v_{\mathfrak{p}_2}(\text{right hand side of (3.2)}) &= 4. \end{aligned}$$

This is a contradiction. Thus, the value $v_{\mathfrak{p}_2}(X)$ must be equal to 2, and we get

$$v_{\mathfrak{p}_1}(X) = v_{23}(X) = \frac{1}{2} v_{\mathfrak{p}_2}(X) = 1.$$

Then, we obtain the equalities

$$\begin{aligned} v_{\mathfrak{p}_1}(\text{left hand side of (3.3)}) &\equiv 0 \mod 4, \text{ and} \\ v_{\mathfrak{p}_1}(\text{right hand side of (3.3)}) &= 2. \end{aligned}$$

This is a contradiction.

(v) By (i), only the prime ideal dividing D can divide D_A or D_B. Such prime ideals are $2\mathcal{O}_K$, $\mathfrak{p}_1$, or $\mathfrak{p}_2$. (ii), (iii), and (iv) implies that they do not divide D_A and D_B. Hence, D_A and D_B are both units of $\mathcal{O}_K$. The assertion follows from 2.4 (v) and 2.3 (iv). □

Proof of 1.5 (continued). Let C_D°, C_{D_A,D_B}, and C'_{D_B} be the curves defined as follows

$$C_D^\circ : y^4 = x^3 - D^4x + D^6$$

$$C_{D_A,D_B} : \begin{cases} D_A s_A^4 = x - D^2\theta \\ D_B s_B^4 = x^2 + D^2\theta x + D^4(\theta^2 - 1) \\ D_A D_B = s^4 \end{cases}$$

$$C'_{D_B} : y^2 = D_B x^4 - (3\theta^2 - 4)/4.$$

Then, we have the following morphisms

$$\begin{array}{ccccc} C_D & \ni & (\frac{x}{D^2}, \frac{s_A s_B s}{D^2}) & & (x,y) \\ \sim\uparrow & & \uparrow & & \downarrow \\ C_D^\circ & \ni & (x, s_A s_B s) & & (D^2x, D^2y) \\ \uparrow & & \uparrow & & \\ C_{D_A,D_B} & \ni & (x, s_A, s_B, s) & & \\ \downarrow & & \downarrow & & \\ C'_{D_B} & \ni & (\frac{s_B}{D}, \frac{x}{D^2} + \frac{\theta}{2}) & & (x,y) \\ \downarrow\xi & & \downarrow & & \downarrow \\ \mathbb{P}^1 & \ni & \frac{x}{D^2} & & y - \frac{\theta}{2} \end{array}$$

For all rational points $P \in C_D(\mathbb{Q})$, there is a tuple $(D_A, D_B) = (1,1), (-\theta, -\theta^3), (\theta^2, \theta^2), (-\theta^3, -\theta)$ such that P is an image of a K-rational point $(x, s_A, s_B, s) \in C_{D_A,D_B}(K)$ with $x \in \mathbb{Q}$. Let $P' \in C'_{D_B}(K)$ be the image of (x, s_A, s_B, s). Then, the value $\xi(P')$ is a rational number. Hence, we can solve our task by the following procedure using Magma.

(i) Find a K-rational point $P_0 \in C'_{D_B}(K)$ by using the command `RationalPoints`. Using the command `EllipticCurve` for $C_{D'_B}$ and P_0, we obtain an elliptic curve E_{D_B} and an isomorphism $\varphi_{D_B} : C'_{D_B} \longrightarrow E_{D_B}$ which sends P_0 to the unit element O.

(ii) Get an abstract abelian group G and an embedding $m : G \hookrightarrow E_{D_B}(K)$ such that the index of its image in $E_{D_B}(K)$ is finite and coprime to 6.

(iii) Use the command `Chabauty` for m and $\xi \circ \varphi_{D_B}^{-1} : E_{D_B} \longrightarrow \mathbb{P}^1$ with index bound 6. It tells us the set

$$S = \left\{ g \in G \;\middle|\; \xi \circ \varphi_{D_B}^{-1} \circ m(g) \in \mathbb{P}^1(\mathbb{Q}) \right\}$$

and an integer I whose prime divisors are only 2 or 3. The output I means that if the index $[E_{D_B}(K) : m(G)]$ is coprime to I, the set S equals the set of all points of $E_{D_B}(K)$ whose image under $\xi \circ \varphi_{D_B}^{-1}$ is in $\mathbb{P}^1(\mathbb{Q})$. Since we constructed G as its index is coprime to 6 in (ii), this is the case if the computation stops.

We write the computational code in Section A for $D_B = 1$. One can check the other cases by changing n to 1, 2, and 3 in the code. By these computations, for $D_B = (-\theta)^n$ with $0 \le n \le 3$, we obtain that the set

$$S' = \left\{ Q \in C'_{D_B}(K) \mid \xi(Q) \in \mathbb{P}^1(\mathbb{Q}) \right\}$$

is as follows

$$S' = \begin{cases} \{[1,-1,0], [\theta, (\theta-2)/2, 1], [1,1,0], [-\theta, (\theta-2)/2, 1]\} & n = 0 \\ \{[-\theta^2+1, (\theta+2)/2, 1], [\theta^2-1, (\theta+2)/2, 1)\} & n = 1 \\ \emptyset & n = 2 \\ \{[\theta^2-1, \theta/2, 1], [-\theta^2+1, \theta/2, 1]\} & n = 3 \end{cases}$$

where we regard C'_{D_B} is embedded into the weighted projective space $\mathbb{P}(1,2,1)$. The image of these points under ξ is either 0 or ± 1. This means that the original point $P = (x,y) \in C_D(\mathbb{Q})$ satisfies $x \in \{0, \pm 1\}$. Hence, we obtain the equality

$$x^3 - x + 1 = 1.$$

Consequently, the value D must be ± 1, and our assertion holds. □

3.4. **Completion of proof.** Now, we are ready to prove our main theorem for $d = 2$.

Proof of 1.3(i). Let notation be as in Section 2.1. By Section 3.2, for any rational point $x \in X_4(\mathbb{Q})$, the point $\pi(x)$ equals O, $3Q_0$, or $\varphi \circ \psi_D(u,t)$ for some $D = (-1)^{\varepsilon_0} 2^{\varepsilon_1} 23^{\varepsilon_2}$, $(u,t) \in C_D(\mathbb{Q})$, and $\varphi = [2]$ or $T_{3Q_0} \circ [2]$. Assume that it is in the latter case. By 1.5, the value D must be ± 1, and (u,t) is in $\{(0,\pm 1), (\pm 1, \pm 1)\}$. The image of each (u,t) in $E(\mathbb{Q})$ is as follow:

$$E \xleftarrow{\varphi} E \xleftarrow{\psi_1} C_1 \qquad E \xleftarrow{\varphi} E \xleftarrow{\psi_{-1}} C_{-1}$$

$$-2Q_0 \xleftarrow{[2]} (1,1) = -Q_0 \longleftarrow (1,\pm 1) \qquad 2Q_0 \xleftarrow{[2]} (1,-1) = Q_0 \longleftarrow (1,\pm 1)$$
$$Q_0 \xleftarrow{T_{3Q_0}\circ[2]} \qquad 5Q_0 \xleftarrow{T_{3Q_0}\circ[2]}$$

$$-4Q_0 \xleftarrow{[2]} (-1,1) = -2Q_0 \longleftarrow (-1,\pm 1) \qquad 4Q_0 \xleftarrow{[2]} (-1,-1) = 2Q_0 \longleftarrow (-1,\pm 1)$$
$$-Q_0 \xleftarrow{T_{3Q_0}\circ[2]} \qquad 7Q_0 \xleftarrow{T_{3Q_0}\circ[2]}$$

$$6Q_0 \xleftarrow{[2]} (0,1) = 3Q_0 \longleftarrow (0,\pm 1) \qquad -6Q_0 \xleftarrow{[2]} (0,-1) = -3Q_0 \longleftarrow (0,\pm 1)$$
$$9Q_0 \xleftarrow{T_{3Q_0}\circ[2]} \qquad -3Q_0 \xleftarrow{T_{3Q_0}\circ[2]}$$

Hence, combining them with the first two cases $\pi(x) = O$ or $3Q_0$, the point $\pi(x)$ is in the set

$$S = \{O, \pm Q_0, \pm 2Q_0, \pm 3Q_0, \pm 4Q_0, 5Q_0, \pm 6Q_0, 7Q_0, 9Q_0\}.$$

By direct calculation, we conclude that

$$X_4(\mathbb{Q}) = \pi^{-1}(S) \cap X_4(\mathbb{Q}) = \{P_i \mid 1 \le i \le 10\},$$

where P_i's are the points listed in 2.4 (ii). □

4. Proof of main results for $d \ge 3$

We prove 1.3 (ii) by reducing the problem to the following theorem.

Theorem 4.1 ([DM97, Main Theorem 2.])**.** *The equation*

$$x^n + y^n = z^2 \tag{4.1}$$

has no non-trivial primitive solution when $n \ge 4$.

Note that a solution (x,y,z) of the equations in 4.1 is said to be primitive if x, y, z are integers and $\gcd(x,y,z) = 1$ holds, and to be trivial if $xyz = 0$ or ± 1. Since the Shimura–Taniyama Conjecture, the modularity of every elliptic curve over $\mathbb{Q}$, is proved by Wiles, Taylor, Breuil, Conrad, and Diamond in [Wil95], [TW95], [CDT99], and finally [BCDT99], the conclusion of 4.1 is now unconditionally valid.

For the case $d = 3$ or 4, we use the following proposition on the Mordell–Weil group of specific elliptic curves.

Proposition 4.2.

(i) *The Mordell–Weil group of the elliptic curve defined by*

$$y^2 = x^3 - 1.$$

is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and consists of $[0,1,0]$ and $[1,0,1]$ in the homogeneous coordinate.

(ii) *The Mordell–Weil group of the elliptic curve defined by*

$$y^2 = x^3 + 1.$$

is isomorphic to $\mathbb{Z}/6\mathbb{Z}$*, and consists of the points*

$$[0,1,0], [2,\pm 3,1], [0,\pm 1,1], \text{ and } [-1,0,1]$$

in the homogeneous coordinate.

Proof. See the entry in the LMFDB [BMS+19, Elliptic Curve 144.a3 and 36.a4]. One can prove the assertion by using elementary number theory or Magma. □

Proof of 1.3(ii). Suppose $c \neq 0, -1$. Assume that we have $z_2 \in f_{d,c}^{-2}(0)(\mathbb{Q})$, and put $z_1 = f_{d,c}(z_2)$. Then, we have

$$c = -z_1^d \neq 0$$

by $f_{d,c}(z_1) = 0$. By the definition of z_1, we have

$$\left(\frac{z_2}{z_1}\right)^d = \left(\frac{1}{z_1}\right)^{d-1} + 1. \tag{4.2}$$

If $d = 3$, the point $(z_2/z_1, 1/z_1)$ is a rational point of the elliptic curve defined by

$$y^2 = x^3 - 1.$$

Thus, the point $(z_2/z_1, 1/z_1)$ equals $[0,1,0]$ or $[1,0,1]$ by 4.2(i). However, this is impossible since we are assuming $-z_1^d = c \neq 0$.

If $d = 4$, the point $(1/z_1, (z_2/z_1)^2)$ is a rational point of the elliptic curve defined by

$$y^2 = x^3 + 1.$$

Thus, the point $(1/z_1, (z_2/z_1)^2)$ equals either

$$[0,1,0], \ [2,\pm 3,1], \ [0,\pm 1,1], \text{ or } [-1,0,1]$$

by 4.2(ii). However, this is impossible since ± 3 are not squares of rationals, and we are assuming $-z_1^d = c \neq 0$.

Let $d \geq 5$. By comparing the valuations of both sides of (4.2) over all prime numbers, we can see that there are non-zero integers A, B, C with $(A, B) = (B, C) = 1$ such that

$$\frac{z_2}{z_1} = \frac{A}{B^{d-1}}, \quad \frac{1}{z_1} = \frac{C}{B^d}.$$

These A, B, C satisfies the equality

$$A^d = C^{d-1} + B^{d(d-1)}.$$

If $d \geq 5$ is even, the point $(C, B^d, A^{d/2})$ is a non-trivial primitive solution of (4.1) for $n = d - 1$. If $d \geq 5$ is odd, the point $(A, -B^{d-1}, C^{(d-1)/2})$ is a non-trivial primitive solution of (4.1) for $n = d$. They are contradictions. □

Proof of 1.4. Suppose that $d \geq 3$ is even. If $c = 0$, rational iterated preimages of 0 are only 0. If $c = -1$, we have

$$f_{d,-1}^{-1}(0)(\mathbb{Q}) = \{1, -1\},$$
$$f_{d,-1}^{-1}(1)(\mathbb{Q}) = \emptyset, \text{ and}$$
$$f_{d,-1}^{-1}(-1)(\mathbb{Q}) = \{0\}.$$

If $c = -r^d$ for some rational number $r \neq 0, \pm 1$, we have

$$f_{d,c}^{-1}(0)(\mathbb{Q}) = \{\pm r\}.$$

By 1.3(ii), there are no second rational preimages of 0 under $f_{d,c}$. For the remaining case that c is not of the form $-r^d$ with a rational number r, the set $f_{d,c}^{-1}(0)(\mathbb{Q})$ is empty. The assertion for even d follows from these observations.

Suppose that $d \geq 3$ is odd. If $c = 0$, the rational iterated preimages of 0 are only 0. If $c = -r^d$ for some rational number $r \neq 0$, we have

$$f_{d,c}^{-1}(0)(\mathbb{Q}) = \{r\}.$$

By 1.3 (ii), there are no rational second iterated preimages of 0 under $f_{d,c}$. If c is not of the form $-r^d$ with a rational number r, the set $f_{d,c}^{-2}(0)(\mathbb{Q})$ is empty. The assertion for odd d follows from these observations. □

Appendix A. Magma code for the elliptic Chabauty method

We write the code of Magma to determine the K-rational points of C_{D_B} whose image under ξ is in $\mathbb{P}^1(\mathbb{Q})$. We used it in the proof of 1.5.

```
Q := Rationals();
Qt<t> := PolynomialRing(Q);
P1 := ProjectiveSpace(Q,1);
K<a> := ext<Q | t^3 - t + 1>;
Kx<x> := PolynomialRing(K);

// list up primes to saturate
primes_to_saturate := [2,3];

// set n = 0..3
n := 0;
C<X,Y,Z> := HyperellipticCurve((-a)^n*x^4 - 1/4*(3*a^2 - 4));
P := RationalPoints(C : Bound := 10)[1];
E, phi := EllipticCurve(C, P);

T, piT := TorsionSubgroup(E);
IT := Invariants(T);
MWR := MordellWeilRank(E);

// collecting candidates by 2-descent
Covers, maps := TwoDescent(E);
pts := [];
for i in [1..#Covers] do
    PtsCi := Points(Covers[i] : Bound := 1);
    if #PtsCi gt 0 then
        _, phiCi := AssociatedEllipticCurve(Covers[i] : E := E);
        for Q in PtsCi do
            Append(~pts, phiCi(Q));
        end for;
    end if;
end for;

// picking up independent elements
S := [];
if #pts gt 0 then
    _ := IsLinearlyIndependent(pts);
    S := ReducedBasis(pts);

    // saturation for each p
    for p in primes_to_saturate do
        S := Saturation(S, p : TorsionFree := true);
    end for;
end if;

// found free rank and the flag
r_found := #S;
flag_fullrank := (r_found eq MWR);
```

```
// construction of A, imgs, phi
A := AbelianGroup([0 : i in [1..r_found]] cat IT);
imgs := S cat [ piT(g) : g in Generators(T) ];
m := hom< A -> E | a :-> &+[ Eltseq(a)[i]*imgs[i] : i in [1..#imgs] ]>;
if not flag_fullrank then;
    print "need more independence elements";
end if;

if flag_fullrank then;
    // definition of function Ecov
    xi := map<C->P1 | [Y - a/2*Z^2, Z^2]>;
    Ecov := phi^(-1)*xi;

    // run Chabauty method
    Chab, I := Chabauty(m, Ecov: IndexBound:=6);

    // wanted points in C_DB
    print "n = ", n;
    print "K-rational points of C_DB with rational image of xi";
    for c in Chab do;
        print (m*phi^(-1))(c);
    end for;
end if
```

Listing 1. Magma code for the elliptic Chabauty method

References

[BCDT99] Christophe Breuil, Brian Conrad, Fred Diamond, and Ross Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 12:521–567, 1999.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system, i: The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997.

[BMS+19] John W. Bosman, Nathan Mascot, Jeroen Sijsling, John Voight, and et al. The L-functions and Modular Forms Database. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Series*, pages 377–395. Mathematical Sciences Publishers, 2019.

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. *Forum of Mathematics, Sigma*, 4:e6, 2016.

[Bru03] Nils Bruin. Chabauty methods using elliptic curves. *Journal für die reine und angewandte Mathematik*, 2003(562):27–49, 2003.

[BS09] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Mathematics of Computation*, 78(268):2347–2370, 2009.

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor. Modularity of Certain Potentially Barsotti-Tate Galois Representations. *Journal of the American Mathematical Society*, 12:521–567, 1999.

[Cre13] Brendan Creutz. Explicit descent in the picard group of a cyclic cover of the projective line. In *Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X)*, volume 1 of *Open Book Series*, pages 295–315. Mathematical Sciences Publishers, 2013.

[DM97] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's Last Theorem. *J. Reine Angew. Math.*, 1997(490–491):81–100, 1997.

[FHI+09] Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve. Uniform bounds on pre-images under quadratic dynamical systems. *Math. Res. Lett.*, 16(1):87–101, 2009.

[FHS11] Xander Faber, Benjamin Hutz, and Michael Stoll. On the number of rational iterated preimages of the origin under quadratic dynamical systems. *Int. J. Number Theory*, 07(07):1781–1806, 2011.

[HHK11] Benjamin Hutz, Trevor Hyde, and Benjamin Krause. Preimages of quadratic dynamical systems. *Involve*, 4(4):343–363, 2011.

[Jon13] Rafe Jones. Galois representations from pre-image trees: an arboreal survey. *Publications mathématiques de Besançon. Algèbre et théorie des nombres*, pages 107–136, 2013.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné.

[Mou12] Michael Mourão. Descent on superelliptic curves. *arXiv, preprint*, 2012.

[NS24] Maryam Nowroozi and Samir Siksek. Perfect powers in elliptic divisibility sequences. *Bulletin of the London Mathematical Society*, 56(11):3331–3345, 2024.

[Odo85] Robert W. K. Odoni. The Galois Theory of Iterates and Composites of Polynomials. *Proceedings of the London Mathematical Society*, s3-51(3):385–414, 1985.

[Poo17] Bjorn Poonen. *Rational Points on Varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[PS97] Bjorn Poonen and Edward F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *Journal für die reine und angewandte Mathematik*, 488:141–188, 1997.

[Rey12] Jonathan Reynolds. Perfect powers in elliptic divisibility sequences. *Journal of Number Theory*, 132(5):998–1015, 2012.

[Sch95] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51:219–232, 1995.

[Sta18] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2018.

[Sto01] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arithmetica*, 98(3):245–277, 2001.

[TW95] Richard Taylor and Andrew Wiles. Ring-Theoretic Properties of Certain Hecke Algebras. *Ann. of Math.*, 141(3):53–72, 1995.

[Wil95] Andrew Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Ann. of Math.*, 141(3):443–551, 1995.

NTT Institute for Fundamental Mathematics, NTT Communication Science Laboratories, NTT, Inc., 2-4, Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0237, Japan

Email address: `kaoru.sano@ntt.com`