DESCENT METHODS FOR STUDYING INTEGER POINTS ON
\[ y^n = f(x)g(x), \quad n \geq 2 \]

Abstract. We study the integer points on superelliptic and hyperelliptic curves of the form \( y^n = f(x)g(x), \ n \geq 2, \deg f + \deg g \geq 4 \).

1. Introduction

The practical solution of integer points on hyperelliptic curves, \( C : y^2 = F(x) \) for \( F \in \mathbb{Z}[x] \ (\deg F \geq 3) \) not a square, is a well studied problem. For instance if \( F(x) \) is monic and quartic, we have very sharp (upper) bounds for \( \max\{|x|, |y|\} \) or explicit methods to solve them [11]. For \( \deg F \) even, again we have polynomial bounds (but not very sharp), which in some cases we can just enumerate its integer points [27]. What is more, in this case we have specific algorithm to solve them, see [26]. If \( F(x) \) is of odd degree, the problem is harder. One reason for this, it is that the even degree can be treated with the so called Runge’s method [11, Appendix]. The same if \( F(x) \) is not monic (even for even degree), the problem is more difficult. In general, the case where \( F(x) \) is irreducible and \( \deg F \in \{3, 4\} \) leads to an elliptic curve, in which case we have a very good knowledge to practically solve it, for instance see [29]. The case where \( F \) is irreducible and \( \deg F \geq 5 \), was studied in [5], where two assumptions must be satisfied so that their method be successful. They need a rational point on \( C \) and a basis for the jacobian of \( C \) over the rationals.

Another method for \( y^2 = F(x) \) and \( \deg F \) odd is the so called quadratic Chabauty [1]. In [1] they combined Mordell-Weil sieve and \( p \)-adic approximations techniques to attack the problem.

Now, let \( F(x) \) be a reducible polynomial over the rationals. In this paper we address this case. The quadratic Chabauty method of [1] is still valid. Now there is also another method, the so called descent method. For instance in [9], they use covers of \( C \) (in their paper they call such covers, heterogeneous spaces) in order to find rational points on curves of genus 2, where \( F(x) \) is factorized in \( \mathbb{Q} \) as \( f(x)g(x) \). In [10] we used such covers to study the integer points on families of elliptic curves \( y^2 = x(x^2 \pm p) \) (\( p \) prime). This method is used in the current work to study hyperelliptic equations. We study the integer points on the hyperelliptic curve
\[ y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4), \]
which it was also studied in [1, Section 9] (using the quadratic Chabauty method).

It was proved that the integer solutions \((x, y)\) with \( y > 0 \), are
\[ \Sigma = \{(-1, 2), (0, 2), (-2, 12), (3, 62)\}. \]

It is easy to show that the set of integer solutions is indeed \( \Sigma \) using descent method, without the heavy computations on jacobian varieties.

2010 Mathematics Subject Classification. 11Y50, 11D41, 11D45, 11Y16.

Key words and phrases. Number Theory, Diophantine Equations, hyperelliptic curves, superelliptic curves, Chevalley-Weil Theorem, elliptic curves, jacobian varieties.
We provide a more general framework, where superelliptic curves \( M : y^p = f(x)g(x) \), also fits. For instance, in [10, Section 8] we tried this method in \( y^3 = x^4 + kx \). In the present paper we study \( y^p = (\alpha x^p + \beta)g(x) \) (\( p \) prime). Therefore, in part, we generalize the results of [10, Section 8].

In the bibliography, for superelliptic curves we have the following method (see [23, Chapter IV, Section 4]), which we call it reduction to \( S \)-unit equations. Under some conditions it may be practical. It is based on factorization over a number field. Say, \( y^n = f(x) \), \( n \geq 3 \), \( d = \deg f \geq 2 \) and \( \alpha, \beta \) are simple roots of \( f(x) \). If \( (x, y) \) is an integer point with \( y \neq 0 \), then, \( x - \alpha = \kappa \xi^n \) where it is proved that \( \kappa \) belongs to a finite set of integral elements of the number field \( K = \mathbb{Q}(\alpha) \), for the proof of this see [23, Lemma 4B]. Similar if \( \beta \) is another simple root we get an equation of the form \( x - \beta = \kappa' \xi'^n \). If \( d \geq 3 \), then we end up with finitely many Thue equations \( \kappa \xi^n - \kappa' \xi'^n = \beta - \alpha \) in \( \mathbb{Q}(\alpha, \beta) \) with unknowns \( \xi, \xi' \). If it occurs \( \alpha, \beta, \xi, \xi', \kappa, \kappa' \) be rational integers, we can solve the Thue equations over the integers.

For further information on descent method see [9], [14, Section 2.3], [16, Section 1.3], [20, Section 5.5] and their references.

1.1. Our Contribution. We study the following families of superelliptic curves \( y^p = (\alpha x^p + \beta)g(x) \) for \( g \in \mathbb{Z}[x] \). We provide an implementation for solving such Diophantine equations. In Corollary 2.2 we bound the number of integer points on the curve \( y^p = (\alpha x^p \pm 1)(\gamma x^m + \beta) \).

Furthermore, we study hyperelliptic curves of the form \( y^2 = f(x)g(x) \), where \( y^2 = f(x) \) defines an elliptic curve. We provide an implementation and we present many examples. What is more, we study the following families \( y^2 = (x^4 \pm 1)g(x) \). For instance, we prove that \( y^2 = (x^4 + 1)(x^4 - 1) \) has only the trivial integer solutions, for all \( n \neq 0 \) (mod 4).

Roadmap. In section 2 we study the curve \( y^p = f(x)g(x) \), for \( p \) prime. In section 3, we study the hyperelliptic curve \( y^2 = f(x)g(x) \). In the final section, we summarize our results and provide some concluding remarks. Also, there is an appendix where we provide pseudocode for solving the Diophantine equations \( y^2 = (x^4 - 1)g(x) \) and we provide tables for the solutions of the families \( y^2 = (x^4 - 1)g(x) \) for \( g(x) \in \{x^2 + kx + 1, x^3 + kx^2 + 1, x^3 + kx + 1\} \).

2. The case \( y^p = f(x)g(x) \), \( p \) odd prime

Let
\[
(2.1) \quad C : y^p = f(x)g(x)
\]
where \( g(x), f(x) \) do not have common roots over the algebraic closure \( \overline{\mathbb{Q}} \). Let \( V \subset \mathbb{A}^4(\overline{\mathbb{Q}}) \) be the algebraic curve defined by the equations
\[
u^p = f(x), v^p = g(x), y = uv.
\]
We consider the projection
\[
\Psi : V \to C, \quad \Psi(x, y, u, v) = (x, y).
\]
\( \Psi \) is a finite unramified map of degree \( p \). It is finite, since it is a projection and also unramified, since \( Z(f, g) = \emptyset \). Indeed, if we fix \( (x, y) \) then the system
\[
u^p = f(x), v^p = g(x), uv = y
\]
\[
^1\text{With } \mathbb{A}^n(K) \text{ we denote the } n \text{-th dimensional affine space over the field } K.
\]
\[
^2\text{With } Z(f, g) \text{ we denote the set of common zeros of } f(x), g(x) \text{ in } \overline{\mathbb{Q}}
\]
has exactly $p-$ solutions in $\mathbb{Q}$. To see this, it is enough to enumerate the distinct pairs $(\zeta_i, \zeta_j)$ ($\zeta_i^p = \zeta_j^p = 1$), such that $\zeta_i \zeta_j = 1$. Now, from Chevalley-Weil Theorem \cite{6, 12, 13}, \cite[Section 4.2, p. 50]{24} we get finitely many number fields $K = \mathbb{Q}(u, v)$ with degree at most $p$ over $\mathbb{Q}$. Since $p$ is a prime then $K = \mathbb{Q}$ or is of degree exactly $p$. This provides the following constraints in $(u, v)$. If we fix $(x, y) = (a, b) \in \mathbb{Z}^2$ then necessarily,

\begin{equation}
(2.2) \quad f(a) = d_1X^p, g(a) = d_2Y^p, d_1d_2 = Z^p,
\end{equation}

for some $X, Y, Z$ integers, $d_1, d_2$ $p-$free\footnote{3$d_1, d_2$ do not have any prime power of the form $q^p$ in their primitive factorization} non zero integers, and $i \in \{0, 1, ..., p-1\}$. Assume that $|d_1| \neq 1$ and let $\{p_1, ..., p_k\}$ be the prime divisors of $d_1$. Say, $d_1 = p_1^{a_1} \cdots p_k^{a_k}$, where $1 \leq a_i \leq p - 1$. Then, from the third equation of (2.2) we get $d_2 = p_1^{p-a_1} \cdots p_k^{p-a_k}$. Note that $\text{rad}(d_1) = \text{rad}(d_2)$, where $\text{rad}(k)$ is the largest square free divisor of $k$. We set $d = \text{rad}(d_1)$. If $d_1 = 1$, then also $d_2 = 1$ and similar if $d_1 = -1$. So again $\text{rad}(d_1) = \text{rad}(d_2) = d$. We shall prove the following Proposition.

**Proposition 2.1.** If $R(u, v) = \text{res}_x(u^p - f(x), v^p - g(x))$ ($p \geq 3$) and $c = R(0, 0)$, then, $d|c$, where $d = \text{rad}(d_1) = \text{rad}(d_2)$.

Proof. We note that $R(u, v) = R_0(u^p, v^p)$, for some $R_0 \in \mathbb{Z}[X, Y]$. Let $(a, b)$ be an integer point of $C : y^p = f(x)g(x)$. Let $(u_0, v_0)$ such that $u_0^p = f(a)$, $v_0^p = g(a)$. Thus (as in (2.2)) we get,

\begin{align*}
u_0^p &= d_1X^p, \quad v_0^p = d_2Y^p, \quad d_1d_2 = Z^p.
\end{align*}

But, $R(u_0, v_0) = 0$. Therefore, $R_0(u_0^p, v_0^p) = R_0(d_1X^p, d_2Y^p) = 0$. So we get

\begin{align*}
R_0(d_1X^p, d_2Y^p) &= dR_1(X^p, Y^p) + c = 0,
\end{align*}

for some $R_1 \in \mathbb{Z}[X, Y]$ and integer $c = R(0, 0) \neq 0$. We remark that $c = \text{res}_x(f, g)$ (up to sign), so $c \neq 0$, since $f, g$ do not have common roots. We conclude that $d|c$. \qed

The previous is a basic result for what follows. More general results, similar to Proposition 2.1 were given in \cite[Lemma 4B]{23} and \cite[Lemma 2.2.1]{3}.

Having the previous Proposition, for $(a, b) \in C(\mathbb{Z})$, we get an integer $z$ such that $dz^p = f(z)$, for some $d$ belonging to the set,

\begin{equation}
S_{f, g, p} = \{k \in \mathbb{Z} : (p - \text{free}) : k|c, c = \text{res}_x(u^p - f, v^p - g)|_{(u=0, v=0)}\}.
\end{equation}

In general, the Diophantine equation $dx^p = f(x)$ is not easier than the initial $y^p = f(x)g(x)$, thus it may be hard to solve it. However, in some cases is more easy. For instance, if $C : y^p = (Ax^p + B)g(x)$, $A, B \in \mathbb{Z} - \{0\}$ and $g(x)$ does not have common roots with $Ax^p + B$, then we reduce the study of $C$ to finitely many binomial Thue equations. Since Thue equations can be solved practically for moderate degree, for instance using Pari \cite{19} or Magma \cite{2}, the same is true for $C$.

Also, we get the following result.

**Corollary 2.2.** Let $m, p$ be positive integers with $p \geq 3$ prime, $m \geq 2$ and $\alpha, \beta, \gamma$ non zero integers. Then, the number of integer solutions of the Diophantine equation

\begin{equation}
y^p = (\alpha x^p \pm 1)(\gamma x^m + \beta)
\end{equation}

is at most $2\tau(c)$, where $c = -\alpha^m\beta^p \mp \gamma^p$ and $\tau(k)$ is the number of positive divisors of integer $k$. 


Proof. We consider the Diophantine equation
\[ y^p = (\alpha x^p + 1)(\gamma x^m + \beta), \]
where \( p \geq 3 \), and \( m \geq 2 \).

Set \( f(x) = \alpha x^p + 1 \), \( g(x) = \gamma x^m + \beta \), then \( c = R(0, 0) = -\alpha^m \beta^p \mp \gamma^p \), where \( R(u, v) = \text{res}_x(u^p - f(x), v^p - g(x)) \). From Proposition 2.1, we have to solve equations of the form
\[ dz^p = \alpha x^p + 1, \; d|c \; (d \text{ is } p\text{-free}). \]
These are (binomial) Thue equations and they have been already studied. These equations have at most one integer solution, see [15, Chapter 3, Lemma 3.3]. So, overall the number of integer solutions of (2.4) is at most \(|\{d \in \mathbb{Z} : d|c, \; d \text{ is } p\text{-free}\}| \leq 2\tau(c). \]

2.1. The Algorithm. Now, we easily get the following pseudocode\(^4\).

**Input:** \( p \) odd prime, \( f(x) = Ax^p + B \) and \( g(x) \in \mathbb{Z}[x] \) (\( f, g \) do not have common roots).

**Output:** The integer solutions of \( y^p = f(x)g(x) \).

1. \( L, M \) two empty lists
2. \( R \leftarrow \text{res}_x(u^p - f(x), v^p - g(x)) \)
3. \( R_0 \leftarrow R(0, 0) \)
4. \( PF \leftarrow \{d \in \mathbb{Z} : d|R_0, \; d \text{ is } p\text{-free integer}\} \)
5. for \( d \) in \( PF \)
6. \( \text{Solve Thue equation } T_d : \pm dy^p - Ax^p = B \)
7. append \( L \) with \( x = a \) where \( (x, y) = (a, b) \in T_d(\mathbb{Z}) \)
8. for \( z \) in \( L \)
9. \( \text{if } f(z)g(z) \text{ is pth power} \)
10. \( \text{Append list } M \text{ with } (z, \sqrt[2p]{f(z)g(z)}) \)
11. return \( M \)

2.2. Examples. (i). Let the curve \( y^3 = (x^3 + 691)(x^2 - 17) \). Executing the previous algorithm we get only one point \((13, 76)\).

(ii). The curve \( y^3 = (x^3 + 625)(x + 1) \) has the integer solutions
\[ \{(-10, 15), (-1, 0), (15, 40)\}. \]

(iii). The curve \( y^5 = (x^5 - 724)(x + 2) \) has the integer solutions
\[ \{(-2, 0), (5, 7)\}. \]

3. The case \( y^2 = f(x)g(x) \) where \( y^2 = f(x) \) defines an elliptic curve

Let
\[ C : y^2 = f(x)g(x), \]
with \( f(x) \) a cubic or quartic polynomial and \( g(x) \), \( f(x) \) do not have common root over the algebraic closure \( \overline{\mathbb{Q}} \). We remark that if \( \deg g + \deg f \) is even and the leading coefficient of \( f(x)g(x) \) is one, then \( C \) is of Runge type and in this case there are

\(^4\) for an implementation in Sagemath see, https://github.com/drazioti/hyper_super_elliptic/blob/main/superelliptic.sage
uniform upper bounds (for instance see [11, Introduction]). As in the superelliptic case, let \( V \subset \mathbb{A}^4(\mathbb{Q}) \) be the algebraic curve defined by the equations:

\[
\begin{align*}
u^2 &= f(x), v^2 = g(x), y = uv.
\end{align*}
\]

We consider the projection

\[
P : V \to C, P(x, y, u, v) = (x, y).
\]

\( P \) is a finite unramified map of degree 2. Indeed, if we fix \((x, y)\) then the system

\[
u^2 = f(x), v^2 = g(x), uv = y
\]

has exactly two solutions in \( \overline{\mathbb{Q}} \). Now, from Chevalley-Weil Theorem we get that the number field \( \mathbb{Q}(u, v) \) is at most of degree two. This provides the following constraints in integer solutions. If we fix \((x, y)\) then necessarily,

\[
(3.2) \quad u_0^2 = f(a) = dX^2, v_0^2 = g(a) = dY^2,
\]

so,

\[
(u_0, v_0) = (\sqrt{d}|X|, \sqrt{d}|Y|),
\]

for some \( X, Y \) integers and \( d \) square free, non zero integer.

**Proposition 3.1.** Set \( R(u, v) = \text{res}_x(u^2 - f(x), v^2 - g(x)) \) and \( c = R(0, 0) \). Then \( d|c \).

**Proof.** First we remark that, \( \text{res}_x(u^2 - f(x), v^2 - g(x)) \) at \((u, v) = (0, 0)\) equals to \( R_0 = \varepsilon \cdot \text{res}_x(f(x), g(x)), \varepsilon \in \{-1, 1\} \). Let \((a, b)\) such that \( b^2 = f(a)g(a) \). Let also \( u_0^2 = f(a), v_0^2 = g(a) \). We note that \( R(u, v) = R_0(u^2, v^2) \), for some \( R_0 \in \mathbb{Z}[X, Y] \).

We set \( u = u_0, v = v_0 \), as in (3.2), then

\[
R_0(u_0^2, v_0^2) = R_0(dX^2, dY^2) = dR_1(u_0^2, v_0^2) + c = 0,
\]

for some \( R_1 \in \mathbb{Z}[X, Y] \), thus, \( d|c \). \( \square \)

**Remark 3.2.** The set where \( d \) belongs, is in fact \( S_{f, g, 2} \) given in (2.3).

**Corollary 3.3.** If \( f(x) = (x-a_1)(x-a_2)(x-a_3) \) \((a_1, a_2, a_3, \text{ are distinct integers})\), then \( d|g(a_1)g(a_2)g(a_3) \).

**Proof.** This is immediate, since the resultant of two polynomials \( f(x), g(x) \) can be expressed as

\[
\text{res}_x(f(x), g(x)) = \prod_{i=1}^{\deg(f)} g(\lambda_i) \text{ (up to sign)},
\]

where \( \{\lambda_i\}_i \) are the roots of \( f(x) \). \( \square \)

Assume that \( f(x) = x^3 + Ax^2 + Bx + C \). Let \((a, b) \in C(\mathbb{Z}) \), then there exists integer \( b' \) such that \((a, b')\) belongs to the curve\(^5\)

\[
(3.3) \quad C'_d : dy^2 = f(x).
\]

Let

\[
\Psi_d : C'_d \to \mathcal{E}_d, \Psi_d(x, y) = (dx, d^2y)
\]

where,

\[
\mathcal{E}_d : y^2 = x^3 + Adx^2 + Bd^2x + d^3C
\]

\(^5\)In the bibliography \( C'_d \) is also called heterogeneous space or twist.
and in the case where \( f(x) \) has three integer roots \( a_1, a_2, a_3 \), then
\[
\mathcal{E}_d : y^2 = (x - da_1)(x - da_2)(x - da_3).
\]
We have \( \Psi_d(C'_d(\mathbb{Z})) \subset \mathcal{E}_d(\mathbb{Z}) \), so in order to compute the integer points of \( C'_d \) it is enough to compute the integer points of \( \mathcal{E}_d \).

**Proposition 3.4.** Let \( f(x) = x^3 + Ax^2 + Bx + C \in \mathbb{Z}[x] \) and \( C : y^2 = f(x)g(x) \). We set \( N = R(0,0) \), where \( R(u,v) = \text{res}_x(u^2 - f(x), v^2 - g(x)) \). Let also, \( \Sigma_N = \{d \in \mathbb{Z} : d \text{ squarefree, } d|N\} \), and
\[
\mathcal{M}_N(f) = \left\{ \frac{a}{d} : d \in \Sigma_N, \text{there is } b \in \mathbb{Z}, \text{with } d^2|b \text{ and } b^2 = a^3 + Ada^2 + Bd^2a + d^3C \right\}.
\]

Then, the set \( C(\mathbb{Z}) = \{(A,B) \in \mathbb{Z}^2 : A \in \mathcal{M}_N(f), B^2 = f(A)g(A)\} \)

This Proposition provides the reduction of the study of \( y^2 = f(x)g(x) \) to the elliptic curve
\[
y^2 = a^3 + Ada^2 + Bd^2a + d^3C.
\]
If \( f(x) = (x - a_1)(x - a_2)(x - a_3) \), then we get the following.

**Corollary 3.5.** Let \( C : y^2 = (x - a_1)(x - a_2)(x - a_3)g(x) \). We set
\[
N = g(a_1)g(a_2)g(a_3), \quad \Sigma_N = \{d \in \mathbb{Z} : d \text{ squarefree, } d|N\},
\]
and
\[
\mathcal{M}_N(f) = \left\{ \frac{a}{d} : d \in \Sigma_N, \text{there is } b \in \mathbb{Z}, \text{with } d^2|b \text{ and } b^2 = \prod_{i=1}^3(a - da_i) \right\}.
\]

Then, the set \( C(\mathbb{Z}) = \{(A,B) \in \mathbb{Z}^2 : A \in \mathcal{M}_N(f), B^2 = f(A)g(A)\} \)

### 3.1. The algorithm.

**Input:** \( f(x) = x^3 + Ax^2 + Bx + C \in \mathbb{Z}[x] \) (with non zero discriminant) and \( g(x) \in \mathbb{Z}[x] \) \( \{f,g \text{ do not have common roots}\} \).

**Output:** The integer solutions of \( y^2 = f(x)g(x) \) \( (y > 0) \).

01. \( L, M \) two empty lists
02. \( R_0 \leftarrow \text{res}_x(f,g) \)
03. \( SF \leftarrow \{d \in \mathbb{Z} : d|R_0, \ d \text{ is square free}\} \)
04. for \( d \) in \( SF \)
05. \( \text{Solve } \mathcal{E}_d : y^2 = x^3 + Adx^2 + Bd^2x + Cd^3 \)
06. \( \text{append } L \text{ with } a \text{ where } (a,b) \in \mathcal{E}_d(\mathbb{Z}) \)
07. for \( z \) in \( L \)
08. if \( f(z)g(z) \) is square
09. Append list \( M \) with \( (z, \sqrt{f(z)g(z)}) \)
10. return \( M \)

**Remark 3.6.** If
\[
C : Dy^2 = f(x)g(x), \quad D \in \mathbb{Z} \setminus \{0\}
\]
then we can reduce this case to the previous, by considering the curve
\[
C' : y^2 = f(x)G(x)
\]

---

\( ^6 \)for an implementation in Sagemath see
https://github.com/drazioti/hyper_super_elliptic/blob/main/hyperelliptic.sage
where \( y' = Dy \) and \( G(x) = Dg(x) \).

**Remark 3.7.** Let \( \theta(N) \), where \( N = R(0,0) \), be the number of square free divisors of \( N \). Then, the number of equations \( \{E_d\}_{d \in \Sigma_N} \) is \( 2\theta(N) \). But, \( \theta(N) = 2^{\omega(N)} \), where \( \omega(N) = |\{p : p \text{ prime}, p|N\}| \). So the number of equations \( E_d \) is \( 2^{\omega(N)+1} \).

**Remark 3.8.** In magma [2], the command \texttt{SIntegralLjunggrenPoints([D,A,B,C],[]} provides the integral points on the curve \( C : D y^2 = A x^4 + B x^2 + C \), provided that \( C \) is nonsingular. Furthermore, \texttt{IntegralQuarticPoints([a,b,c,d,e])} provides the integral points on the curve \( C : y^2 = ax^4 + bx^3 + cx^2 + dx + e \).

### 3.2. Examples.

We assume that functions for computing integer points in elliptic curves given by Sagemath and magma do not miss any integer point.

(i). \( f(x) = x^3 + x + 1 \) and \( g(x) = x^4 + 2x^3 - 3x^2 + 4x + 4 \). This is example 9.2 from [1, Section 9] which was solved using the heavy machinery of jacobian varieties. It was proved that the integer points of curve

\[
y^2 = (x^3 + x + 1)(x^4 + 2x^3 - 3x^2 + 4x + 4)
\]

with \( y > 0 \), are

\[
\Sigma = \{(-1, 2), (0, 2), (-2, 12), (3, 62)\}.
\]

This specific curve has genus 3 and the rank of its jacobian is again 3 so the method of [1] can, in principal, be applied. Of course, our method can be also considered heavy, since we use elliptic logarithm method for computing the integer points of many elliptic curves (here only 4). In our opinion, our method is more simple and practical since we already have efficient implementations (for instance in Magma and Sagemath) for calculating integer points on elliptic curves. Since \( dy^2 = f(x) \) and \( dy^2 = g(x) \) both define elliptic curves, we work with the cubic polynomial, \( dy^2 = f(x) \).

In Sagemath, we compute in some seconds that indeed the set of integer points of \( y^2 = f(x)g(x) \) is the set \( \Sigma \).

(ii). The following example is from [4, example 8.1], where they studied its rational points. Let

\[
C : y^2 = 2x^6 + x^4 + 3x^2 - 2.
\]

This can be rewritten as \( y^2 = (x^4 + x^2 + 2)(2x^2 - 1) \). We set \( f(x) = x^4 + x^2 + 2 \) and \( g(x) = 2x^2 - 1 \). We work with the curve \( C'_d \) (see, 3.3). Executing in magma \texttt{SIntegralLjunggrenPoints([d,1,1,2],[]} for \( d \in \{\pm 1, \pm 11\} \), we get only for \( d = 1 \) the integer points \((\pm 1, 2)\) (restricting \( y \) to positive integers). Substituting to \( f(x)g(x) \) we get the points \((\pm 1, 4)\). So,

\[
C(Z) = \{\pm 1, \pm 4\}.
\]

(iii). \( C : y^2 = x(x^2 - 1)(x^2 - 1600) \). We set \( f(x) = x(x^2 - 1600) \) and \( g(x) = x^2 - 1 \). Then, the integer solutions with \( y > 0 \), are

\[
\{(-25, 3900)\}.
\]

(iv). \( C : y^2 = x(x^2 - 1)(x - 4)(x - 5) \). We set \( f(x) = x(x - 1)(x - 4) \) and \( g(x) = (x + 1)(x - 4) \). Then, the integer solutions with \( y > 0 \), are

\[
\{(2, 6), (9, 120)\}.
\]

(v). \( f(x) = x(x - 1)(x - 2) \) and \( g(x) = (x + 40)(x + 4)(x - 4)(x - 7) \). Then the solutions of \( y^2 = f(x)g(x) \) with \( y > 0 \), are

\[
\{(-7, 2772), (16, 20160)\}.
\]
3.3. The Diophantine equations \( y^2 = (x^4 \pm 1)g(x) \). We start our study with \( y^2 = (x^4 - 1)g(x) \).

**Proposition 3.9.** Let \( C : y^2 = (x^4 - 1)g(x) \) for \( g(x) \in \mathbb{Z}[x] \) with \( g(\pm 1) \) and \( g(\pm i) \) not zero. Set \( C_+(\mathbb{Z}) = \{(a, b) \in C(\mathbb{Z}) : b > 0\} \). Then,
\[
|\mathcal{C}_+(\mathbb{Z})| \leq 2^{\omega(N)+2},
\]
where \( N = g(1)g(-1)g(i)g(-i) \) and \( \omega(N) \) is the number of prime divisors of \( N \).

**Proof.** Set \( f(x) = x^4 - 1 \). The twists here are of the form \( dy^2 = x^4 - 1 \), where \( d \mid R_0 \), \( R_0 = \text{res}_x(f(x), g(x)) \). It is easy to see that \( R_0 = N \). From [17] (also see [7]) the Diophantine equation \( dy^2 = x^4 - 1 \) has at most two solutions in positive integers for \( d \geq 2 \). Also, from [22, Lemma 1.1], for \( d = 2 \) we have only the trivial solution \((\pm 1, 0)\). For \( d = 1 \) and \( d < 0 \) we have \( y = 0 \). Since we are interested in positive \( y \), we ignore the cases \( d \leq 1 \). Now, each solution \((a, b)\) (we have at most two) of \( dy^2 = x^4 - 1 \), \( d \geq 2 \), it might provide a solution on \( C \) for the two possible signs of \( a \). I.e. we have to check if \((a^4 - 1)g(a)\) or \((a^4 - 1)g(-a)\) is square. Thus, \( |\mathcal{C}_+(\mathbb{Z})| \) is bounded above by the number of equations \( dy^2 = x^4 - 1 \), \( d \geq 2 \), squarefree divisor of \( N \), and the result is multiplied by 4. So, \( |\mathcal{C}_+(\mathbb{Z})| < 4 \cdot 2^{\omega(n)} \). The result follows.

**Remark 3.10.** Since, for large \( N \) we have \( \omega(N) \sim \frac{\log N}{\log \log N} \), we get that for every \( \varepsilon > 0 \), \( 2^{\omega(N)} \ll_{\varepsilon} N^{\varepsilon} \) thus,
\[
|\mathcal{C}_+(\mathbb{Z})| \ll_{\varepsilon} N^{\varepsilon}.
\]

With \( \ll_{\varepsilon} N^{\varepsilon} \) we mean that there is a constant depending on \( \varepsilon \), say \( c(\varepsilon) \), such that \( < c(\varepsilon)N^{\varepsilon} \).

Furthermore, it is easy to compute all the integer solutions of \( y^2 = (x^4 - 1)g(x) \) using [7]. First, we compute \( N = g(1)g(-1)g(i)g(-i) \) and we construct the set \( \Sigma_N = \{d \in \mathbb{Z}_{>0} : d \mid N \text{ and } d \text{ is squarefree}\} \). For every integer \( d \in \Sigma_N \) we compute the fundamental solution of the Pell equation \( X^2 - dy^2 = 1 \) say \( u + v\sqrt{d} \). Then we compute \( a = \sqrt{u} \) and \( a = \sqrt{2u^2 - 1} \), (only for \( d = 1785 \) both the square roots are integers). If it occurs \( a \) to be integer, then we check if \((a^4 - 1)g(\pm a)\) is a square. If it is, then we found an integer solution \((a, \sqrt{(a^4 - 1)g(a)})\) or \((a, \sqrt{(a^4 - 1)g(-a)})\).

In appendix we provide a pseudocode and we compute the integer points of the three families
\[
y^2 = (x^4 - 1)(x^2 + kx + 1), \quad y^2 = (x^4 - 1)(x^3 + kx^2 + 1), \quad y^2 = (x^4 - 1)(x^3 + kx + 1)
\]
for various values of \( k \).

We can also study the symmetric Diophantine equation \( y^2 = (x^4 + 1)g(x) \). Set \( \zeta_j = \frac{1}{2^{1/4}}(\pm 1 \pm i) \), \( j = 1, 2, 3, 4 \) the quartic roots of \(-1\) (take all the possible signs, and it is not important here how you pick \( \zeta_j \)'s). Now the analogous Proposition of 3.9 is the following.

**Proposition 3.11.** Let \( W : y^2 = (x^4 + 1)g(x) \) for \( g(x) \in \mathbb{Z}[x] \) with \( g(\zeta_j) \neq 0 \) \( (j = 1, 2, 3, 4) \). Set \( W_+(\mathbb{Z}) = \{(a, b) \in W(\mathbb{Z}) : b > 0\} \). Then,
\[
|W_+(\mathbb{Z})| \leq 2^{\omega(N)+1},
\]
where \( N = \prod_{j=1}^4 g(\zeta_j) \) and \( \omega(N) \) the number of prime divisors of \( N \).
Proof. Set $f(x) = x^4 - 1$. The twists here are of the form $dy^2 = x^4 + 1$, where $d|R_0$ with $R_0 = res_s(f(x), g(x))$. It is easy to see that $R_0 = N$. From [18] (see also [8]), the Diophantine equation $dy^2 = x^4 + 1$ has at most one solution in positive integers for $d \geq 2$. For $d = 1$ we have $x = 0$ and for $d < 0$ we do not have any integer solution. Now, each solution $(a, b)$ (we have at most one) of $dy^2 = x^4 + 1$ it might provide a solution on $W$ for the two possible signs of $a$. I.e. we have to check if $(a^4 + 1)g(a)$ or $(a^4 + 1)g(-a)$ is square. Thus,

$$|W_+(\mathbb{Z})| \leq 2\{d \in \mathbb{Z}_{>0} : d|N, \ d \text{ squarefree}\} = 2\cdot 2^{\omega(N)}.$$  

So the result follows. \hfill $\square$

Remark 3.12. As in Remark 3.10, for every $\varepsilon > 0,$

$$|W_+(\mathbb{Z})| \ll \varepsilon N^\varepsilon.$$  

In order to solve the Diophantine equation $dy^2 = x^4 + 1$ we use Cohn’s algorithm in [8]. To apply this algorithm, we first compute a fundamental solution of $V^2 - dU^2 = -1$ (if it exists, see the remark below), say $(v_0, u_0)$. Also, say $A$ be the square free part of $v_0$. We set, $\mu = v_0 + u_0\sqrt{d}$ and $\lambda = v_0 - u_0\sqrt{d}$ and $s_n = \frac{\mu^n + \lambda^n}{2}$. Finally, compute $s_A$. Then, $x = \pm \sqrt{s_A}$.  

Remark 3.13. The negative Pell equation $Y^2 - NX^2 = -1$ is solvable if and only if the period of the continued fraction of $\sqrt{N}$ is odd (see [25, Chapter 8, Section 5, Theorem 9]).

Corollary 3.14. Let $C_n : y^2 = (x^4 + 1)(x^n + 1)$, then

$$C_n(\mathbb{Z}) \subset \{(-1,0), (\pm 1, \pm 2), (0, \pm 1)\},$$  

for all $n \neq 0$ (mod 4).

Proof. Suppose that $x \neq 0$. Straightforward calculations show that $N$ is a power of 2. In fact $res_s(f, g) = 2^i, i \in \{1,2\}$, the exponent $i = 2$ appears when $i = 2$ (mod 4). So all the squarefree divisors of $N$ are $\{-2,2,-1,1\}$. The negative Pell equation for $d = 2$ provides the fundamental solution $(1,1)$, and so $x = \pm 1$. For $d \in \{1,-1,-2\}$, the corresponding twists do not provide any non trivial integer solution. The result follows. \hfill $\square$

4. Conclusion

Let

$$y^2 = F(x), \ F \in \mathbb{Z}[x], \ \deg F > 3.$$  

We assume that the polynomial $F(x)$ in (4.1) is reducible polynomial with one irreducible component a cubic polynomial or quartic polynomial. For instance, if $F(x)$ has three integer roots the previous constraint is satisfied. We reduced the study of Diophantine hyperelliptic equations, with the previous constraint, to the study of integer points on elliptic curves. Since, the integer points of elliptic curves have been studied very thoroughly, it is easy to find the integer points of (4.1).

As far as the superellipitic equations $S : y^p = f(x)g(x), p \geq 3$ prime, we provide also an unramified map $\Phi : Y_d \to S$ for known $d$’s such that

$$S(\mathbb{Z}) \subset \Phi\left(\bigcup_{d|N} Y_d(\mathbb{Z})\right),$$  

where

$$d \in \mathbb{Z}_{>0} : d|N, \ d \text{ squarefree}.$$
where $N$ is $p$–free integer equal to the resultant of $f, g$. Following similar ideas as in the hyperelliptic case we study curves of the form $y^p = (Ax^p + B)g(x)$.

REFERENCES

[1] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller, Computing integral points on hyperelliptic curves using quadratic Chabauty. Math. Comp. 86 (2017), no. 305, p. 1403–1434 (for the preprint version https://arxiv.org/pdf/1504.07040.pdf).
[2] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24, p. 235–265, 1997.
[3] N. Bruin, On Generalized Fermat Equations. PhD Dissertation, Leiden, 1999.
[4] N. Bruin and M. Stoll, Two-cover descent on hyperelliptic curves. Math. Comp. 78 (2009), no. 268, p. 2347–2370 (preprint version: https://arxiv.org/pdf/0803.2052.pdf).
[5] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and Sz. Tengely, Integral Points on Hyperelliptic Curves, Algebra and Number Theory, Vol. 2 (2008), No. 8, p. 859–885, Mathematical Sciences Publishers (preprint version https://arxiv.org/pdf/0801.4459.pdf).
[6] C. Chevalley, Un théorème d’arithmétique sur les courbes algébriques. C. R. Acad. Sci. Paris (1932).
[7] J. H. E. Cohn, The Diophantine equation $x^4 - Dy^2 = 1$. II. Acta Arith. 78 (1997), no. 4, p. 401–403.
[8] J. H. E. Cohn, The Diophantine equation $x^4 + 1 = Dy^2$. Math. Comp. 66 (1997), no. 219, p. 1347–1351.
[9] K. R. Coombes and D. R. Grant, On heterogeneous spaces, J. London. Math.Soc (2) 40 (1989), no. 3, p. 385-397.
[10] K. A. Draziotis, Integer points on the curve $Y^2 = X^3 ± pX$. Math. Comp. 75 (2006), no. 255, p. 1493–1505.
[11] K. A. Draziotis, Practical solution of some families of quartic diophantine hyperelliptic equations, arxiv:2207.10754 https://arxiv.org/pdf/2207.10754.pdf.
[12] K. A. Draziotis and D. Poulakis, Explicit Chevalley-Weil Theorem for affine plane Curves. Rocky Mountain Journal of Mathematics, Vol.39, no.1, Pages 49-70, Rocky Mountain Mathematics Consortium (2009).
[13] S. Duquesne, Points rationnels et méthode de Chabauty elliptique. (French) [Rational points and the elliptic Chabauty method] Les XXIèmes Journées Arithmetiques (Lille, 2001). J. Théor. Nombres Bordeaux 15 (2003), no. 1, p. 99–113.
[14] I. Gaal, Diophantine Equations and Power Integral Bases: New Computational Methods (2nd ed.), 2019, Springer.
[15] Stevan Gajović, Curves with sharp Chabauty-Coleman bound. Arithmetic geometry, number theory, and computation, p. 461–484, Simons Symp., Springer, Cham, 2021.
[16] W. Ljunggren, Über die Gleichung $x^4 - Dy^2 = 1$, Arch. Math. Naturv. 45 (5) (1942), p.61–70.
[17] W. Ljunggren, Einige Sätze über unbestimmte Gleichungen von der Form $Ax^4 + Bz^2 + C = Dy^2$, Vid-Akad. Skr. Norske Oslo 1942 No. 9.
[18] The PARI Group, PARI/GP version 2.13.4, Univ. Bordeaux, 2012, http://pari.math.u-bordeaux.fr/.
[19] Bjorn Poonen, Computing rational points on curves, https://math.mit.edu/~poonen/papers/millennial.pdf.
[20] SageMath, the Sage Mathematics Software System (Version 8.1). The Sage Developers, 2018, https://www.sagemath.org.
[21] P. Samuel, Resultats élémentaires sur certaines équations diophantiennes. J. Theor. Nombres Bordeaux 14 (2002), no. 2, p.629–646. https://jtnb.centre-mersenne.org/item/10.5802/jtnb.379.pdf
[22] W. M. Schmidt, Diophantine approximations and Diophantine equations. Lecture Notes in Mathematics, 1467. Springer-Verlag, Berlin, 1991.
[23] J. P. Serre, Lectures on the Mordell-Weil theorem. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig (1989).
[24] W. Sierpinski, Elementary Theory of Numbers. Polish Scientific Publishers, Warszawa (1987).
DESCENT METHODS FOR STUDYING INTEGER POINTS ON $y^n = F(x)G(x)$

[26] L. Szalay, Superelliptic equations of the form $y^n = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, Bull. Greek Math. Soc., 46, p. 23–33, 2002.
[27] S. Tengely, Effective Methods for Diophantine Equations, PhD Thesis, Thomas Stieltjes Institute for Mathematics, 2005, https://www.math.leidenuniv.nl/~tijdeman/tengely.pdf.
[28] A. Thue, Uber Annaherungswerte algebraischer Zahlen, J. Reine Angew. Math. 135 (1909), p. 284–305.
[29] Nikos Tzanakis, Elliptic Diophantine Equations, De Gruyter 2013.

APPENDIX

A. Pseudocode for the diophantine equation $y^2 = (x^4 - 1)g(x)$.

Now, we easily get the following pseudocode$^7$.

Input: $g(x) \in \mathbb{Z}[x]$ ($g(\pm 1) \neq 0$, $g(\pm i) \neq 0$)
Output: The integer solutions $(x, y)$ of $y^2 = (x^4 - 1)g(x)$ ($y > 0$).

01. $L$ an empty list
02. $N \leftarrow g(1)g(-1)g(i)g(-i)$
03. $SF \leftarrow \{d \in \mathbb{Z}_{>0} : d \mid N, d \text{ is square free}\}$
04. for $d$ in $SF$
05. Compute the fundamental solution $u + v\sqrt{d}$ of $X^2 - dY^2 = 1$
06. if $a = \sqrt{u}$ is integer
07. if $g(a)(a^4 - 1)$ is square say $b^2$ ($b > 0$)
08. Append list $L$ with $(a, b)$
09. if $g(-a)(a^4 - 1)$ is square say $b^2$ ($b > 0$)
10. Append list $L$ with $(-a, b)$
11. if $a = \sqrt{2u^2 - 1}$ is integer
12. if $g(a)(a^4 - 1)$ is square say $b^2$ ($b > 0$)
13. Append list $L$ with $(a, b)$
14. if $g(-a)(a^4 - 1)$ is square say $b^2$ ($b > 0$)
15. Append list $L$ with $(-a, b)$
16. return $L$

$y^2 = (x^4 - 1)(x^2 + kx + 1), 1 < k \leq 1000$

| $k$ | Integer points $(x, y)$, $y > 0$ |
|-----|--------------------------------|
| 5   | (2, 15)                        |
| 26  | (5, 312)                       |
| 65  | (2, 45), (5, 468)              |
| 101 | (10, 3333)                     |
| 185 | (2, 75)                        |
| 290 | (17, 20880)                    |
| 365 | (2, 105)                       |
| 377 | (5, 1092)                      |
| 494 | (5, 1248)                      |
| 605 | (2, 135)                       |
| 677 | (26, 91395)                    |
| 905 | (2, 165)                       |

$^7$ for an implementation in SageMath see
https://github.com/drazioti/hyper_super_elliptic/blob/main/special_case_hyperelliptic_1.sage
12 DESCENT METHODS FOR STUDYING INTEGER POINTS ON $Y^N = F(X)G(X)$

\[
y^2 = (x^4 - 1)(x^3 + kx^2 + 1), \, 1 < k \leq 500
\]

| $k$  | Integer points $(x, y)$, $y > 0$ |
|------|----------------------------------|
| 9    | (5, 468)                         |
| 19   | (-5, 468)                        |

For the second Table, for some values of $k$, for instance $k = 421$, the algorithm is memory expensive. I.e. the fundamental solution of Pell equation is very large. So, you may need enough memory to construct the second table. You will need enough hours for all $k$’s.

\[
y^2 = (x^4 - 1)(x^3 + kx + 1), \, 1 < k \leq 200
\]

| $k$  | Integer points $(x, y)$, $y > 0$ |
|------|----------------------------------|
| 3    | (2, 15)                          |
| 6    | (5, 312)                         |
| 11   | (10, 3333)                       |
| 18   | (17, 20880)                      |
| 27   | (21, 91395)                      |
| 38   | (37, 312360)                     |
| 45   | (5, 468)                         |
| 51   | (50, 892857)                     |
| 63   | (2, 45)                          |
| 66   | (65, 2231328)                    |
| 83   | (82, 5023575)                    |
| 102  | (82, 5023575)                    |
| 123  | (122, 20139405)                  |
| 146  | (145, 36837552)                  |
| 168  | (41, 462840)                     |
| 171  | (170, 64246923)                  |
| 183  | (2, 75)                          |
| 197  | (197, 107581320)                 |

We remark that, if $k = n^2 + 2$, then we always have the solution \((n^2 + 1, (n^4 + 2n^2 + 2)(n^2 + 2)n)\).

K. A. Draziotis, Department of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

Email address: drazioti@csd.auth.gr