RATIONAL POINTS OF LOW DEGREE ON FERMAT CURVES THROUGH THE JACOBIAN VARIETY

Submitted by
Juanita Duque-Rosero
Department of Mathematics

In partial fulfillment of the requirements
For the Degree of Master of Science
Colorado State University
Fort Collins, Colorado
Fall 2018

Master's Committee:

Advisor: Rachel Pries

Jeff Achter

Renzo Cavalieri

Jorge Ramírez

Contents

Introduction

The Jacobian variety of a curve X is an Abelian variety $\mathrm{Jac}(X)$, such that X embeds into $\mathrm{Jac}(X)$. This embedding turns out to be a very useful property in understanding the Abelian structure of the Jacobian and, with that, recovering some information about the curve. For Mumford (1999), the importance of the Jacobian is the following.

> The Jacobian has always been the corner-stone in the analysis of algebraic curves and compact Riemann surfaces. Its power lies in the fact that it abelianizes the curve and is a reification of H_1,(...) Weil's construction (of the Jacobian) was the basis of his epoch-making proof of the Riemann Hypothesis for curves over finite fields, which really put characteristic p algebraic geometry on its feet [Mum99].

Additionally, the Jacobian variety is isomorphic to the Picard group, which gives a tool to understand the divisors of X.

The problem of finding rational points on curves has been studied by many mathematicians over time. Fermat's Last Theorem is an example of a problem in this area. Around 1637, Pierre de Fermat, wrote in the margin of his copy of *Arithmetica*, "It is impossible to write a cube as sum of two cubes, a fourth power as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers." That is, the solutions with rational coefficients for the equation

$$x^n + y^n = z^n,$$

with $n \geq 3$ are just the trivial ones, meaning that at least one of the values x, y, z has to be zero.

This problem remained unsolved for about 350 years, until Andrew Wiles finished a proof in 1994. With the theorem proved, there are some related questions that still need to be answered. One such question which we study in this document is, "what are the solutions of the Fermat equations defined over number fields?". For these fields, we get nontrivial solutions, but it is not known how to characterize all of them.

In this paper, we study some methods that give partial answers to this problem. Our approach is to consider the Jacobian variety of Fermat curves. In order to do that, we must first define the Jacobian variety for a compact Riemann surface, of which Fermat curves are one example. Next, we define the Fermat curves and explicitly construct a basis for the space of one-forms. That is relevant for this work because we can use one-forms to decompose the Jacobian of the Fermat curve as a product of the Jacobians of quotients of the curve. With this decomposition, we give some explicit examples for the rational points of the Jacobian of some Fermat curves.

Finally, we explain how to use the rational points in the Jacobian variety of the Fermat curves of degree 5 or 7 to find rational points on the curves defined over number fields of degrees at most 3 and 5, respectively. For the Fermat curve of degree 5, the reader will find a new proof of the set of solutions over those fields being a set consisting of five specific points.

1 Preliminaries

To start, let X be a smooth compact Riemann surface. To construct the Jacobian variety of X, we need some facts about the topological structure of X, namely its CW-complex structure and its first homology group.

Let g be the genus of X. It is possible to give X a CW-complex structure consisting of one 0-cell, $2g$ 1-cells and one 2-cell in the following way. Construct a polygon of $2g$ sides labeled in order a_i, b_i, a_i', b_i' for $1 \leq i \leq g$, the sides a_i and b_i oriented clockwise and the sides a_i' and b_i' oriented counterclockwise. Then, attach a 2-cell identifying the sides a_i and a_i' and also the sides b_i and b_i'. An important fact about this construction is that X can be triangulated. With this CW-complex structure, the first homology group of X, denoted by $H_1(X, \mathbb{Z})$, is isomorphic to $\mathbb{Z}^{2g}$.

Define $\Omega^1(X)$ as the set of holomorphic 1-forms on X. For a compact Riemann surface of genus g, the space of holomorphic 1-forms has dimension g over $\mathbb{C}$ and $\Omega^1(X) \cong \mathbb{C}^g$ [Nar92, Theorem 5.1.1].

A *divisor* of X is an element of the free abelian group generated by the points of X. Denote this set as $\mathrm{Div}(X)$. Note that this definition is the same as taking finite integer linear combinations of the points of X. Given a divisor $D = \sum_{P \in X} n_P P$, we define the *degree* of D as $\sum_{P \in X} n_P$. For a divisor of the same form, we define

$$\mathrm{ord}_P(D) := n_P.$$

Note that $\mathrm{ord}_P(D)$ is zero for all but finitely many $P \in X$.

Given two divisors, $D_1 = \sum_{P \in X} n_P P$ and $D_2 = \sum_{P \in X} m_P P$, we say that $D_1 \leq D_2$ if and only if $n_P \leq m_P$ for all $P \in X$, which induces a partial ordering on the set of divisors. We say that a divisor D is *effective* if $D \geq 0$.

For a meromorphic function $f : X \to \mathbb{C}$, we can compute the order of f at a point P in X as

$$\mathrm{ord}_P(f) = \begin{cases} k & \text{in } f \text{ has a zero of order } k \text{ at } P \\ -k & \text{in } f \text{ has a pole of order } k \text{ at } P \\ 0 & \text{otherwise.} \end{cases}$$

Since the set of points in which a nonzero function has a zero or a pole is finite, we can define the divisor $\mathrm{Div}(f)$ as $\sum_{P \in X} \mathrm{ord}_P(f) P$. For D a divisor, we define the vector space

$$\mathscr{L}(D) := \{f \mid f \text{ is meromorphic and } \mathrm{Div}(f) + D \geq 0\}.$$

That is, $\mathscr{L}(D)$ is the space of meromorphic functions with poles bounded by D. Let $l(D)$ be the dimension of $\mathscr{L}(D)$ as a complex vector space. Finally, define $|D|$ as the set of all effective divisors linearly equivalent to D, which means

$$|D| = \{D' \mid D - D' = \mathrm{Div}(f),\ f \text{ is a meromorphic function, } D' \text{ is effective}\}.$$

2 Jacobian varieties

We now focus on the construction of the Jacobian variety in the case where we have a smooth compact Riemann surface. First, we present an analytic definition using the space of one-forms of X followed by another construction using divisors.

2.1 Analytic definition

The Jacobian variety for a compact Riemann surface X can be constructed as a quotient of the dual space of holomorphic one-forms of X. This way of defining the Jacobian ensures we get an Abelian variety because the dual space of the holomorphic one-forms is an Abelian group with geometric structure. Also, it explains how the Jacobian can be thought of as a quotient of $\mathbb{C}^g$, with g the genus of the surface. In this section we show that construction.

Recall Stokes Theorem [Mir95, Theorem VII.3.16], which states that if B is a triangulable closed set on X and ω is a $\mathcal{C}^\infty$ one-form on X, then

$$\int_{\partial B} \omega = \iint_B \partial\omega.$$

Let $[c]$ be an element of $H_1(X, \mathbb{Z})$. For all 1-cycle d such that $[d] = [c]$, we have that $d = c + \partial b$ for some 2-chain b. Using Stokes Theorem with $D = b$, we have that for all closed, C^∞ one-forms ω,

$$\int_d \omega = \int_c \omega + \int_{\partial b} \omega = \int_c \omega + \iint_b \partial\omega = \int_c \omega + \iint_b 0 = \int_c \omega.$$

In particular, if ω is an holomorphic one-form, it is also closed [Mir95, Lemma IV.2.4] which implies that the following map is well defined.

$$\begin{array}{rccc} \int_{[c]} & : & \Omega^1(X) & \to & \mathbb{C} \\ & & \omega & \mapsto & \int_c \omega \end{array}$$

where $[c] \in H_1(X, \mathbb{Z})$.

We say that a linear functional $\lambda : \Omega^1(X) \to \mathbb{C}$ is a *period* if it is $\int_{[c]}$ for some $[c] \in H_1(X, \mathbb{Z})$. The set of periods is a subgroup of $\Omega^1(X)^*$. Indeed, given $[c], [d] \in H_1(X, \mathbb{Z})$,

$$\int_{[c]} \omega + \int_{[d]} \omega = \int_{[c]+[d]} \omega = \int_{[c+d]} \omega,$$

where $c + d$ denotes concatenation of the path c with the path d. We denote the set of periods as Λ, and because it is a subgroup of $\Omega^1(X)^*$, we can consider the quotient $\Omega^1(X)^*/\Lambda$.

Definition 2.1. The *Jacobian of a compact Riemann surface* X is the quotient of linear functionals of holomorphic one-forms of X by the set of periods, that is,

$$\mathrm{Jac}(X) := \frac{\Omega^1(X)^*}{\Lambda}.$$

Remark. Because $\Omega^1(X)^*$ is an Abelian group, $\mathrm{Jac}(X)$ is also Abelian. Moreover, since X is a compact Riemann surface of genus g, $\Omega^1(X)$ has a basis $\omega_1, \ldots, \omega_g$. Every $\lambda \in \Omega^1(X)^*$ is completely determined by $v_\lambda = (\lambda\omega_1, \ldots, \lambda\omega_g)$. This implies $\Omega^1(X)^*$ is isomorphic to $\mathbb{C}^g$ by identifying λ and v_λ. Under this map, Λ is isomorphic to the set of elements of the form $(\int_c \omega_1, \ldots, \int_c \omega_g)$ with $[c] \in H_1(X, \mathbb{Z})$.

Example 2.2. If $X = \mathbb{C}_\infty$, the genus of X is 0, which implies the space of holomorphic forms is 0, hence $\mathrm{Jac}(X) = 0$.

Example 2.3. If X is the complex torus $\mathbb{C}/L$, then $\mathrm{Jac}(X) \cong X$. As proof, note that the genus of the torus is 1, thus $\Omega^1(X) \cong \langle dz \rangle \cong \mathbb{C}$, which implies $\Omega^1(X)^* \cong \mathbb{C}$. Therefore, to show the congruence it is enough to show that $\Lambda \cong L$.

Assume $L = z_1\mathbb{Z} \oplus z_2\mathbb{Z}$ and that $\pi : \mathbb{C} \to \mathbb{C}/L$ is the quotient map. Also, define the paths

$$\begin{array}{rccc} \gamma_1 & : & [0,1] & \to & \mathbb{C} \\ & & t & \mapsto & t \cdot z_1 \end{array} \qquad \begin{array}{rccc} \gamma_2 & : & [0,1] & \to & \mathbb{C} \\ & & t & \mapsto & t \cdot z_2 \end{array}$$

Note that the compositions $\pi\gamma_1$ and $\pi\gamma_2$ are loops in X based at 0. We know that one of them is not a multiple of the other because z_1 and z_2 are linearly independent over $\mathbb{R}$. It is well known that $H_1(X, \mathbb{Z}) \cong \mathbb{Z} \oplus \mathbb{Z}$ which leads us to conclude that $\pi\gamma_1$ and $\pi\gamma_2$ generate $H_1(X, \mathbb{Z})$. Therefore, Λ is a lattice. In addition, we can compute

$$\int_{\pi\gamma_1} \pi^*(dz) = \int_{\gamma_1} dz = \int_0^1 z_1 dt = z_1$$

$$\int_{\pi\gamma_2} \pi^*(dz) = \int_{\gamma_2} dz = \int_0^1 z_2 dt = z_2.$$

This implies that the integrals are linearly independent over $\mathbb{R}$ and that we have the equality $\Lambda \cong z_1\mathbb{Z} \oplus z_2\mathbb{Z}$, which leads us to conclude $X \cong \mathrm{Jac}(X)$.

2.2 The Abel-Jacobi map

An important property of the Jacobian of a smooth compact Riemann surface X, is that X can be embedded into $\mathrm{Jac}(X)$. In this section, we study the map that provides this embedding, which is called the Abel-Jacobi map. Also, we give the generalization of the Abel-Jacobi map to a function that has the set of divisors of X as its domain. Finally, we state the Abel-Jacobi Theorem, an important result which characterizes the Jacobian in a different way.

First, let X be a compact Riemann surface. Pick $p_0 \in X$ and for each $p \in X$, let γ_p be a path from p_0 to p. We would like to define a function

$$\begin{array}{ccc} X & \to & \Omega^1(X)^* \\ p & \mapsto & \int_{\gamma_p} . \end{array} \tag{2.1}$$

However, this map is not well defined because it depends on the chosen path. If γ_p' is another path from p_0 to p, note that

$$\int_{\gamma_p} \omega = \int_{\gamma_p'} \omega + \int_{\gamma_p - \gamma_p'} \omega.$$

We see that $\gamma_p - \gamma_p'$ is a closed loop based at p_0, which implies it is a closed chain and therefore that $\int_{\gamma_p - \gamma_p'}$ is a period. This implies the function of Equation 2.1 is well defined modulo the set of periods of X.

Definition 2.4. The *Abel-Jacobi map* of X is defined as the map

$$A \ : \ X \ \to \ \mathrm{Jac}(X)$$

such that $A(p) = \int_{\gamma_p} \pmod{\Lambda}$.

This definition depends on the base point p_0. To define a map independent from the choosing of p_0, it is necessary to extend the definition to the set of divisors of degree 0 of X.

Definition 2.5. The *Abel-Jacobi map* of $\mathrm{Div}(X)$ is the function

$$\begin{array}{rcccc} A_D & : & \mathrm{Div}(X) & \to & \mathrm{Jac}(X) \\ & & \sum n_i P_i & \mapsto & \sum n_i A(P_i) \end{array}$$

If we restrict A_D to divisors of degree 0 then we get $A_0 : \mathrm{Div}_0(X) \to \mathrm{Jac}(X)$, which is independent of the base point by the following lemma.

Lemma 2.6. *The map $A_0 : \mathrm{Div}_0(X) \to \mathrm{Jac}(X)$ defined as $A_0\left(\sum n_i P_i\right) = \sum n_i A(P_i)$ is independent of the selection of a base point to compute A.*

Proof. Assume p_0 and p_0' are two distinct base points and let γ be a path from p_0' to p_0. Consider $p \in X$ and γ_p a path from p_0 to p. We can define A with base point p_0 as

$$A(p) = \left(\int_{\gamma_p} \omega_1, \ldots, \int_{\gamma_p} \omega_g \right) + \Lambda$$

or with base point p_0' as

$$A(p) = \left(\int_{\gamma+\gamma_p} \omega_1, \ldots, \int_{\gamma+\gamma_p} \omega_g \right) + \Lambda = \left(\int_{\gamma_p} \omega_1, \ldots, \int_{\gamma_p} \omega_g \right) + \left(\int_{\gamma} \omega_1, \ldots, \int_{\gamma} \omega_g \right) + \Lambda.$$

Define $j := \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right)$. The previous equation shows that if we change the base-point, we get a factor of j in $A(p)$. Then, for divisors of degree zero, $A_0(\sum n_i P_i)$ changes by a factor of $\sum n_i j = j \sum n_i = 0$, since $\sum n_i = 0$. □

Theorem 2.7 (Abel-Jacobi Theorem)**.** *The Abel-Jacobi map is surjective with kernel the principal divisors of X. That is,*

$$\frac{\mathrm{Div}_0(X)}{\mathrm{PDiv}(X)} \cong \mathrm{Jac}(X).$$

We explain a proof of the theorem in the next section. Before, we present a corollary which proves that the Abel-Jacobi map defines an embedding of X into its Jacobian.

Corollary 2.8. *If X is a smooth compact Riemann surface of genus $g \geq 1$, the Abel-Jacobi map $A : X \to \mathrm{Jac}(X)$ is injective.*

Proof. Assume towards a contradiction that $A(p) = A(q)$ for $p \neq q$, points in X. Hence, $A_0(p-q) = 0$ and Abel's Theorem implies $p-q$ is a principal divisor. Therefore, there is a meromorphic function f on X with only one zero at p and one pole at q. Using f, it is possible to define the holomorphic map $F : X \to \mathbb{C}_\infty$ as

$$F(x) = \begin{cases} f(x) & \text{if } x \text{ is not a pole of } f \\ \infty & \text{if } x \text{ is a pole of } f. \end{cases}$$

The function F is non-constant because $f(x)$ has one zero and one pole. Also, $F(x)$ has degree one since the only zero of $f(x)$ is at p. Therefore, F defines an isomorphism. However, the genus of the Riemann sphere is 0, whereas $g \geq 1$, a contradiction. □

2.3 Abel-Jacobi Theorem

We present a sketch of a proof of the Abel-Jacobi Theorem, stated in Theorem 2.7. The proof consists on two theorems, that show that the Abel-Jacobi map is injective and surjective, respectively.

Theorem 2.9 (Abel's Theorem)**.** *A divisor of degree 0 is principal if and only if its image under the Abel-Jacobi map is zero.*

Proof (sketch). For the forward direction, let f be a meromorphic function and let D be its divisor. Define $F : X \to \mathbb{C}_\infty$ as the corresponding map, which is the same map defined in Corollary 2.8. Let γ be a path from ∞ to 0 in $\mathbb{C}_\infty$ not passing through branched points of F. Note that $F^*\gamma = \sum_{i=1}^{d} \gamma_i$, where each γ_i is a path from a pole to a zero of f. Define $p_i = \gamma_i(1)$ and $q_i = \gamma_i(0)$. Then we can write

$$D = \sum_{i=1}^{d} (p_i - q_i).$$

Now, choose a base point $p_0 \in X$, a path α_i from p_0 to p_i and β_i from p_0 to q_i. If $\{\omega_1, \ldots, \omega_g\}$ is a basis for $\Omega^1(X)$, then we have

$$A_0(D) = \sum_{i=1}^{d} \left(\int_{\alpha_i} \omega_1, \ldots, \int_{\alpha_i} \omega_g \right) - \left(\int_{\beta_i} \omega_1, \ldots, \int_{\beta_i} \omega_g \right) + \Lambda.$$

If η_i is the path $\alpha_i - \gamma_i - \beta_i$, the vector $\left(\int_{\eta_i} \omega_1, \ldots, \int_{\eta_i} \omega_g \right)$ is a period for all $i \in \{1, \ldots, d\}$. Hence, we can substract those vectors from $A_0(D)$ and get the same equivalence class, i.e.

$$\begin{aligned} A_0(D) &= \sum_{i=1}^{d} \left(\int_{\alpha_i} \omega_1, \ldots, \int_{\alpha_i} \omega_g \right) - \left(\int_{\beta_i} \omega_1, \ldots, \int_{\beta_i} \omega_g \right) - \left(\int_{\eta_i} \omega_1, \ldots, \int_{\eta_i} \omega_g \right) + \Lambda. \\ &= \left(\sum_{i=1}^{d} \int_{\gamma_i} \omega_1, \ldots, \sum_{i=1}^{d} \int_{\gamma_i} \omega_g \right) + \Lambda \\ &= \left(\int_{F^*\gamma} \omega_1, \ldots, \int_{F^*\gamma} \omega_g \right) + \Lambda. \end{aligned}$$

In addition, $\int_{F^*\gamma} \omega_i = \int_\gamma \mathrm{Tr}(\omega_j)$ [Mir95, Lemma VIII.3.4], where $\mathrm{Tr}(\omega_j)$ is holomorphic because ω_j is holomorphic as well [Mir95, VIII.3]. However, the only holomorphic one-form of $\mathbb{C}_\infty$ is 0 since its genus is zero, which implies $A_0(D) = 0$.

Conversely, let $D \in \mathrm{Div}_0(X)$ be in the kernel of A_0. By [Mir95, Lemma VIII.4.6], there is a meromorphic one-form ω such that:

- ω has simple poles at the points where $D(p) \neq 0$, and has no other poles;
- $\mathrm{Res}_p(\omega) = D(p)$ for each $p \in X$, where $D(p)$ is the coefficient of p in the formal sum D;
- The $a-$ and $b-$periods of ω are integral multiples of $2\pi i$.

Here, the $a-$periods and $b-$periods are defined using the CW complex of X with 1-cells $\{a_i, b_i\}_{i=1}^{g}$. For any one-form σ we can define

$$A_i(\sigma) := \int_{a_i} \sigma \qquad \text{and} \qquad B_i(\sigma) := \int_{b_i} \sigma.$$

The $a-$periods for σ are the numbers $A_i(\sigma)$ and the $b-$periods are the numbers $B_i(\sigma)$.

We can fix a point $p_0 \in X$ and define a map $f : X \to \mathbb{C}$ as

$$f(p) = \exp\left(\int_{p_0}^{p} \omega\right).$$

The map is holomorphic where ω is holomorphic, that is, in the set of points with coefficient 0 in D. Also, because the periods are multiples of $2\pi i$ and the residues of ω are integers ($D(p) \in \mathbb{Z}$), we have that f does not depend on the path chosen from p to p_0. Our goal is to show that f is meromorphic and $\mathrm{Div}(f) = D$.

Assume $p \in X$ with $\mathrm{ord}_P(D) = n \neq 0$. By the construction of ω, this implies that in a neighborhood of p, we can write

$$\omega = \frac{n}{z} + g(z),$$

where $g(z)$ is holomorphic with no zeros at p. For z in that neighborhood,

$$f(z) = \exp\left(\int_{p_0}^{z} \omega\right) = \exp\left(\int_{p_0}^{z} \frac{n}{z} + g(z)\right) = \exp(n\ln(z) + h(z)) = z^n e^{h(z)},$$

with $h(z)$ a holomorphic function. This implies $f(z)$ is meromorphic in a neighborhood of p and $\mathrm{ord}_p(f) = n$. In conclusion, $\mathrm{Div}(f) = D$. □

Theorem 2.10 (Jacobi Inversion Theorem)**.** *The Abel-Jacobi map from divisors of degree zero to the Jacobian is surjective.*

Proof. Choose a base point p_0 and define the map $\varphi : X^g \to \mathrm{Jac}(X)$ as

$$\varphi(p_1, \ldots, p_g) = \left(\sum_{i=1}^{g} \int_{p_0}^{p_i} \omega_1, \ldots, \sum_{i=1}^{g} \int_{p_0}^{p_i} \omega_g\right),$$

where $\{\omega_1, \ldots, \omega_g\}$ is a basis of $\Omega^1(X)$. One can show that there is a tuple $p = (p_1, \ldots, p_g)$ such that the Jacobian determinant of φ is not zero [Nar92, Lemma 15.1.]. The implicit function theorem implies there is an open neighborhood of p for which φ maps bijectively into a neighborhood V of $\varphi(p)$.

Consider $\lambda = (\lambda_1, \ldots, \lambda_g)$ in $\Omega^1(X)^* \cong \mathbb{C}^g$. Because V is open, there is an n such that

$$\varphi(p) + \frac{\lambda}{n} \in V.$$

Since φ is bijective in V, there is a $q = (q_1, \ldots, q_g) \in X^g$ such that

$$\varphi(q) = \varphi(p) + \frac{\lambda}{n}. \tag{2.2}$$

Now, define the divisor

$$D' = n\sum_{i=1}^{g} q_i - n\sum_{i=1}^{g} p_i + gp_0.$$

The degree of D' is g and by the Riemann-Roch Theorem,

$$h^0(D') = 1 + h^0(K - D') \geq 1$$

for K the divisor of a meromorphic one-form. That implies D' is linearly equivalent to a divisor $D = \sum_{i=1}^{g} r_i$. Hence,

$$A_0(D' - gp_0) = A_0(D - gp_0).$$

By the definition of φ,

$$A_0(D - p_0) = A_0\left(\sum_{i=1}^{g}(r_i - p_0)\right) = \varphi(r_1, \ldots, r_g).$$

In addition,

$$\begin{aligned} A_0(D' - gp_0) &= nA_D\left(\sum_{i=1}^{g}(q_i - z_i) - \sum_{i=1}^{g}(p_i - p_0)\right) \\ &= n(\varphi(q) - \varphi(p)) \\ &= \lambda. \end{aligned}$$

Therefore, by equation 2.2 we have $A_0(D' - gp_0) = \lambda$, hence A_0 is surjective. □

Remark. After proving that $\mathrm{Jac}(X) \cong (\mathrm{Div}_0(X))/(\mathrm{PDiv}(X))$, it is also common to name the Abel-Jacobi map as the function

$$\begin{array}{ccc} X^{(d)} & \to & \mathrm{Jac}(X) \\ (P_1, \ldots, P_d) & \mapsto & \left[\sum_{i=1}^{d}(P_i - P_0)\right] \end{array}$$

where P_0 is a fixed point in X and $X^{(d)}$ is the symmetric product variety of X, $d \geq 1$.

3 Fermat Curves

For every positive integer N, the *Fermat curve of degree* N is the smooth plane curve with projective equation

$$F(N) = \{[X : Y : Z] \in \mathbb{P}^2(\bar{\mathbb{Q}}) \mid X^N + Y^N = Z^N\}.$$

Because the curves are smooth, we can apply Plücker's formula to get that the genus of $F(N)$ is $(N-1)(N-2)/2$ [Mir95, Proposition 3.2.6].

It is well known that Fermat's Last Theorem, proved by Andrew Wiles, states that the only rational points in $F(N)$ for $N \geq 3$ are the points (x, y, z) such that $xyz = 0$. This result is no longer true when we consider points defined over larger fields. In figure 1, we have graphs of the real points on Fermat curves from degree 2 to 7. In this document, we concentrate on number fields. There are many methods to find rational points defined over number fields on Fermat curves. We will use rational points of the Jacobian variety of Fermat curves to understand the rational points over the curves. Specifically, we focus on the case in which N is a prime number. In this case, we can find quotients of Fermat curves that are very useful in describing their Jacobians. This construction is based on [Mur93, Chapter 8] and [Lan82, Chapter 2].

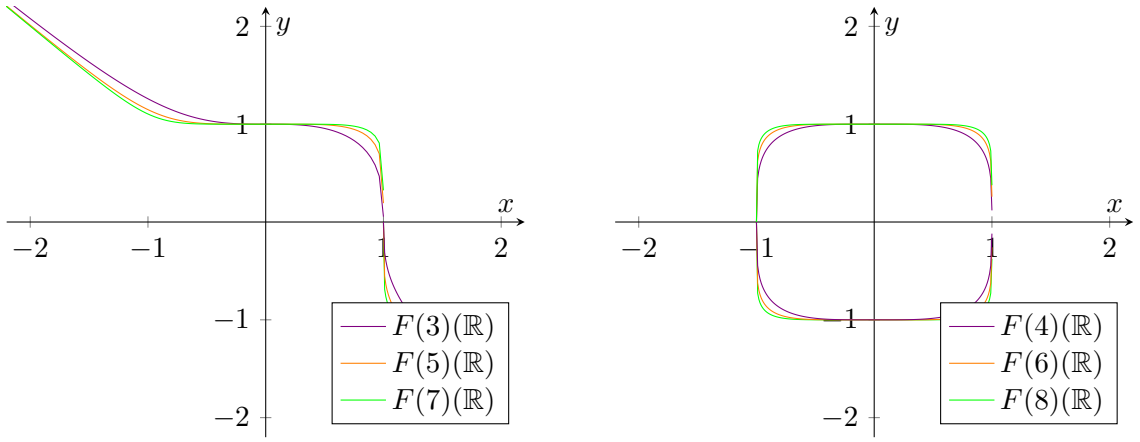

Figure 1: Real points on $x^N + y^N = 1$

3.1 The space of one-forms

In this section we consider the case where N is an odd prime number. We define the meromorphic functions on $F(N)$ given by $x = X/Z$ and $y = Y/Z$. For all r, s integers greater than 0, we define the one-form:

$$\omega_{r,s} = x^{r-1} y^{s-1} \frac{dx}{y^{n-1}}.$$

We claim that $\omega_{r,s}$ is holomorphic for all r, $s \geq 1$ such that $r + s \leq N - 1$. As proof, note that x is a uniformizer unless $y = 0$. If $y = 0$, then y is a uniformizer and the equation

$$x^N + y^N = 1$$

implies $x \neq 0$ and

$$\frac{dx}{y^{N-1}} = -\frac{dy}{x^{N-1}}.$$

Therefore, $\omega_{r,s}$ is holomorphic when $y = 0$ and $x \neq 0$. Finally, if x has a pole P, this implies Z is a simple pole and $\mathrm{ord}_P(x) = \mathrm{ord}_P(y) = -1$. We can take $t = 1/x$ to get

$$\omega_{r,s} = x^{r-1}y^{s-1}\left(\frac{1}{y^{N-1}}\right)\left(-\frac{1}{t^2}dt\right),$$

which implies

$$\mathrm{ord}_P(\omega_{r,s}) = -(r-1) - (s-1) + (N-1) - 2 = (N-1) - (r+s) \geq 0,$$

concluding the proof of our claim.

Proposition 3.1. *The set $\beta = \{\omega_{r,s} \,|\, r, s \geq 1, r+s \leq N-1\}$ is a basis for the holomorphic one-forms.*

Proof. First note that there are $\frac{1}{2}(N-1)(N-2)$ many forms in β, exactly the genus of $F(N)$. Therefore, it is enough to prove β is linearly independent over $\mathbb{C}$. In order to do that, consider A and B, the automorphisms of $F(N)$ given by

$$A[X:Y:Z] = [\zeta X:Y:Z] \qquad \text{and} \qquad B[X:Y:Z] = [X:\zeta Y:Z], \tag{3.1}$$

where ζ is the primitive $N-$th root of unity $\exp(2\pi i/N)$. It is clear that A and B generate a subgroup G of the automorphisms of $F(N)$, where $G \cong (\mathbb{Z}/N\mathbb{Z})^2$. This subgroup also acts on the set $\{\omega_{r,s}\}$ by

$$\begin{aligned} A^iB^j(\omega_{r,s}) &= \zeta^{(r-1)i+(s-1)j+i-(N-1)j}x^{r-1}y^{s-1}\frac{dx}{y^N-1} \\ &= \zeta^{ir+js}\omega_{r,s}. \end{aligned}$$

Hence, we can define a character $\chi_{r,s}$ of G such that $\chi_{r,s}(A^iB^j) = \zeta^{ir+js}$, which for all $g \in G$, implies that $g(\omega_{r,s}) = \chi_{r,s}(g)\omega_{r,s}$. Under this definition, note that for two pairs (r,s), (r',s') such that

$$r,\, s,\, r',\, s' \leq 1, \qquad r+s \leq N-1, \qquad \text{and} \qquad r'+s' \leq N-1,$$

if $\chi_{r,s} = \chi_{r',s'}$, then $(r,s) = (r',s')$. Therefore, the characters are linearly independent over $\mathbb{C}$ which implies the elements $\omega_{r,s}$ are linearly independent too. □

3.2 Quotients of the Fermat curve

To describe the Jacobian variety of $F(N)$, for N an odd prime, it is necessary to consider some quotients of $F(N)$ and their Jacobian varieties. In this section, we will define the quotients and compute their genus.

The rational function field of $F(N)$ is $K = \mathbb{C}(x,y)$, where $x^N + y^N = 1$. Here, we have the group G and the automorphisms A and B as in the previous section. The subfield of K fixed by G is $\mathbb{C}(x^N)$. Let $G_{r,s}$ be the subgroup of G given by the kernel of $\chi_{r,s}$ and let $K_{r,s}$ be the subfield of K fixed by $G_{r,s}$.

If $A^iB^j \in G_{r,s}$, then $ri + sj \equiv 0 \pmod N$ and

$$A^iB^j(x^ry^s) = \zeta^{ri+js}x^ry^s = x^ry^s.$$

This implies $x^r y^s \in K_{r,s}$. Now, assume $1 \leq r$, s and $r + s \leq N - 1$. At a pole of x, the order of any rational function of x^N is a multiple of N. Then, $x^r y^s$ is not a rational function of x^N because $r + s \leq N - 1$. In addition, $A^i B^j$ fixes $x^r y^s$ if and only if $\zeta^{ri+sj} = 1$, which happens if and only if $A^i B^j \in \ker \chi_{r,s}$. Therefore, $\mathrm{Gal}(K/\mathbb{C}(x^N, x^r y^s)) = G_{r,s}$, hence $K_{r,s} = \mathbb{C}(x^N, x^r y^s)$.

Define

$$u = x^N, \qquad\qquad v = x^r y^s.$$

Thus, u and v are related by

$$v^N = u^r (1 - u)^s.$$

However, the curve given by this equation is not normal. To get around this, we define $F_{r,s}$ as the normalization of the above curve, which turns out to have $K_{r,s}$ as the quotient field of its ring of fractions.

We are interested in finding the genus of each curve $F_{r,s}$. Towards this end, we find a basis for the space of holomorphic one-forms on $F_{r,s}$ and recall that its dimension corresponds to the genus.

Proposition 3.2. *[Mur93, Proposition 8.8] A basis for the holomorphic one-forms on $F_{r,s}$ is given by*

$$\{\omega_{\langle mr\rangle,\langle ms\rangle} \,:\, 1 \leq m \leq N,\, 1 \leq \langle mr\rangle,\, \langle ms\rangle,\, \langle ms\rangle + \langle ms\rangle \leq N - 1\},$$

where $\langle a\rangle$ is the number such that $0 \leq \langle a\rangle < N$ and $a \equiv \langle a\rangle \pmod N$.

Proof. To begin, we have that for all $r, s \leq 1$ such that $r + s \leq N - 1$,

$$\chi_{\langle mr\rangle,\langle ms\rangle}(A^i B^j) = \zeta^{\langle mr\rangle i + \langle ms\rangle j} = \zeta^{(ri+sj)m} = \zeta^{mri+msj} = \zeta^{(ri+sj)m} = \chi^m_{r,s}.$$

Hence, $x^{\langle mr\rangle} y^{\langle ms\rangle}$ is in $K_{r,s}$ and $\omega_{\langle mr\rangle,\langle ms\rangle}$ is a one-form on $F_{r,s}$. Also, consider a holomorphic one-form ω on $F_{r,s}$ such that

$$\omega = \sum c_{q,t}\omega_{q,t}.$$

If $c_{q,t} \neq 0$, $\chi_{q,t}(g) = 1$ for all $g \in G_{r,s}$. However, since the characters are independent and non-trivial, it must be true that $\ker \chi_{q,t} = \ker \chi_{r,s}$, which implies

$$\chi_{q,t} = \chi^m_{r,s} = \chi_{\langle mr\rangle,\langle ms\rangle}.$$

Thus, $q = \langle mr\rangle$ and $t = \langle ms\rangle$. This concludes the proof because the forms $\omega_{q,t}$ are linearly independent. □

Corollary 3.3. *$F_{r,s}$ has genus $\frac{1}{2}(N - 1)$ where $r, s \geq 1$ and $r + s \leq N - 1$.*

Remark. $K_{r,k} = K_{q,t}$ if and only if $q = \langle mr\rangle$ and $t = \langle mk\rangle$ for some m. Therefore, we can consider $m = r^{-1}$ and we get that $K_{r,k} = K_{1,k}$.

From the previous remark, we can simply consider the fields $K_{1,k}$ for $1 \leq k \leq N - 2$. We define the corresponding curve $F_{1,k}$ as F_k, which plays an important role in next section.

3.3 Jacobian of the Fermat curves

In this section, we present an isogeny that gives another way of describing the Jacobians of Fermat curves. We also give examples of how this result can be used to describe the Jacobian of $F(5)$ and $F(7)$.

Let J_N be the Jacobian of the Fermat curve $F(N)$. Considering the definition of F_k given in the previous section, we construct the map

$$\begin{array}{rccc} f_k & : & F(N) & \to & F_k \\ & & (x,y) & \mapsto & (x^N, xy^k). \end{array}$$

This map induces

$$f_{k,*} \quad : \quad J_N \quad \to \quad \mathrm{Jac}(F_k), \tag{3.2}$$

where, for points, $f_{k,*}(P) = f_k(P)$ and, for divisors, the map is extended linearly.

Similarly, we can define the pullback

$$f_k^* \quad : \quad \mathrm{Jac}(F_k) \quad \to \quad J_N, \tag{3.3}$$

where, given a point $P \in F_k$, we consider $Q_1, \ldots, Q_r$ as the distinct points of $F(N)$ lying above P (under f_k) with multiplicities $e_1, \ldots, e_r$. Then, $f_k^*(P) = \sum_{i=1}^r e_i Q_i$ and we linearly extend this definition.

Here A and B are as defined in Equation 3.1.

Proposition 3.4. *The following equation holds*

$$f_k^* \circ f_{k,*} \quad = \quad \sum_{j=0}^{N-1} (A^{-k}B)^j. \tag{3.4}$$

as a map $F(N) \to F(N)$.

Proof. For all $(x,y) \in f_k$,

$$f_k^* \circ f_{k,*}(x,y) \quad = \quad f_k^*(x^N, xy^k).$$

Also, the points lying above (x^N, xy^k) are the points $(\tilde{x}, \tilde{y})$ such that

$$(\tilde{x}^N, \tilde{x}\tilde{y}^k) = (x^N, xy^k).$$

The equality implies, $\tilde{x} = \zeta^i x$, for ζ the chosen $N-$th primitive root of unity and $0 \le i \le N-1$. Since (x,y) is a point in $F(N)$, it is also true that $\tilde{y} = \zeta^j y$ for some j with $0 \le j \le N-1$. The fact that $xy^k = \tilde{x}\tilde{y}^k$ implies $\zeta^i \zeta^{jk} = 1$ and for that $i = -jk$. Hence, $(\tilde{x}, \tilde{y}) = (A^{-k}B)^j(x,y)$ for some $0 \le j \le N-1$. This proves the claim. □

After those preliminaries, we are ready to state the most important theorem of this section.

Theorem 3.5. *[Mur93, Proposition 8.10] There is an isogeny*

$$J_N \sim_{\mathbb{C}} \prod_{k=1}^{N-2} \mathrm{Jac}(F_k).$$

Proof. We will define a map that is multiplication by N. This is enough to show we have an isogeny because the dimension as complex vector spaces coincide:

$$\frac{1}{2}(N-1)(N-2) = \sum_{k=1}^{N-1} \frac{1}{2}(N-1).$$

In order to obtain this map, define

$$f_* : \bigoplus_{k=1}^{N-2} f_{k,*} : J_N \to \bigoplus_{k=1}^{N-2} \mathrm{Jac}(F_k),$$

$$f^* : \bigoplus_{k=1}^{N-2} \mathrm{Jac}(F_k) \to J_N,$$

using the functions described in Equations 3.2 and 3.3. Then, Equation 3.4 implies

$$f^* \circ f_* = \sum_{k=1}^{N-2} \sum_{j=0}^{N-1} (A^{-k}B)^j. \tag{3.5}$$

To show this map is multiplication by N in divisor classes, it is enough to prove it for differentials of the first kind [Lan82, Theorem IV.5.6]. When we use Equation 3.5 with the basis $\{\omega_{r,s}\}$ of the dual space, we get

$$f^* \circ f_*(\omega_{r,s}) = \sum_{k=1}^{N-2} \sum_{j=0}^{N-1} \zeta^{-krj+sj} w_{r,s}.$$

Now, if $-kr + s \not\equiv 0 \pmod{N}$, then

$$\sum_{j=0}^{N-1} \zeta^{-krj+sj} = \sum_{j=0}^{N-1} \zeta^j = 0.$$

Similarly, if $-kr + s \equiv 0 \pmod{N}$, we have

$$\sum_{j=0}^{N-1} \zeta^{-krj+sj} = \sum_{j=0}^{N-1} 1 = N.$$

In addition, there is a unique k such that the last condition holds and for this,

$$f^* \circ f_*(\omega_{r,s}) = N w_{r,s}.$$

□

The previous theorem can be used to compute explicitly the rational points of the Jacobian of some Fermat curves. We will explain this method in the next chapter, where we need the explicit structure of $J_5(\mathbb{Q})$ and $J_7(\mathbb{Q})$.

Example 3.6. $J_5(\mathbb{Q})_{\mathrm{tor}} \cong (\mathbb{Z}/5\mathbb{Z})^r$ for some r.

Proof. From the proof of Theorem 3.5, we know that there is an isogeny given by multiplication by 5 between J_5 and the product of $\mathrm{Jac}(F_k)$ for $1 \leq k \leq 3$. Hence, for all prime $\ell \neq 5$,

$$J_5[\ell^\infty](\mathbb{Q}) = \prod_{k=1}^{3} \mathrm{Jac}(F_k)[\ell^\infty](\mathbb{Q}).$$

However, by [GR78, Theorem 1.1], the torsion of $\mathrm{Jac}(F_k)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$, for which the $\ell-$primary part is trivial and thus, the $\ell-$primary part of $J_5(\mathbb{Q})$ is trivial too. □

Remark. One can prove that $J_5(\mathbb{Q})_{\mathrm{tor}} \cong (\mathbb{Z}/5\mathbb{Z})^2$. For details, see [KT97, Theorem 2].

Example 3.7. $J_7(\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/7\mathbb{Z})^2$.

Proof. In [Tze98, Theorem 2], Tzemias concludes that the following is true:

(i) For a prime $\ell \neq 2, 7$, the group $J_7[\ell^\infty](\mathbb{Q})$ is trivial.

(ii) The group $J_7[7^\infty](\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ and is generated by

$$[(0,-1,1)-(-1,1,0)] \quad \text{and} \quad [(-1,0,1)-(-1,1,0)].$$

To find the $2-$primary part, we use the same idea as the case $N = 5$. By the isogeny of Theorem 3.5, it is enough to find the $2-$primary part of each J_k. To do so, we use the result of Gross and Rohrlich given in [GR78, Theorem 1.1] which states

$$\mathrm{Jac}(F_k)(\mathbb{Q})_{\mathrm{tor}} \cong \begin{cases} \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } 1 \equiv k^3 \equiv (6-k)^3 \pmod 7 \\ \mathbb{Z}/7\mathbb{Z} & \text{otherwise.} \end{cases}$$

The only $k \leq 5$ such that $1 \equiv k^3 \equiv (6-k)^3 \pmod 7$ are $k = 2$ or $k = 4$, which gives two copies of $\mathbb{Z}/2\mathbb{Z}$ and thus

$$J_7[2^\infty](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

□

4 Rational points of low degree

In this chapter our goal is to describe the points on the Fermat curves which are defined over number fields of low degree (depending on N). We define Γ_d as the union of all number fields of degree at most d. The following theorem is a result from Debarre and Klassen that gives a corollary about Fermat curves.

Theorem 4.1. *[DK94, Theorem 1] Let C be a smooth projective plane curve defined by an equation of degree $d \geq 7$ with rational coefficients. Then C has only finitely many points whose field of definition has degree $\leq d-2$ over $\mathbb{Q}$.*

Corollary 4.2. *For all prime N greater than 5, $F(N)(\Gamma_{N-2})$ is a finite set.*

The result is also true for the Fermat curve of degree 3 since the only solutions defined over $\mathbb{Q}$ are the trivial ones. In the following section, we prove the result for $N = 5$. Then we can conclude that for all $N \geq 3$, $F(N)(\Gamma_{N-2})$ is a finite set.

4.1 The Fermat quintic

In this section, we study the rational points of degree at most 6 on $F(5)$ by using its Jacobian variety. Fermat's Last Theorem gives that the only $\mathbb{Q}-$rational points on $F(5)$ are

$$a = (0, 1, 1), \qquad b = (1, 0, 1), \qquad c = (-1, 1, 0).$$

We also consider the points of degree two

$$P = (\eta, \overline{\eta}, 1), \qquad \overline{P} = (\overline{\eta}, \eta, 1),$$

with η a primitive $6-$th root of unity and $\overline{\eta}$ its conjugate such that $\eta + \overline{\eta} = 1$. The minimal polynomial of η is $x^2 - x + 1$ and P and $\overline{P}$ are points on $F(5)$. In [GR78, Theorem 5.1], Gross and Rohrlich showed

$$F(5)(\Gamma_2) = \{a, b, c, P, \overline{P}\}. \tag{4.1}$$

In addition, we will show there are no points of degree three in the Fermat quintic. We will follow the method used in [Tze98] for the Fermat curve of degree seven. To prove this fact, we first need to find the rational points in the Jacobian of $F(5)$.

To start, let K be the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive 5th root of unity. In addition, define ϵ as a $10-$th root of unity such that $\epsilon^2 = \zeta$.

Definition 4.3. The *points at infinity* are the following K-rational points on F_5:

$$a_j = (0, \zeta^j, 1), \qquad b_j = (\zeta^j, 0, 1), \qquad c_j = (\epsilon\zeta^j, 1, 0),$$

where $0 \leq j \leq 4$.

Remark. With the above definition, $a = a_0$, $b = b_0$ and $c = c_2$.

Theorem 4.4. *[KT97, Theorem 2] The group $J_5(\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$. The divisor classes $[c-a]$ and $[c-b]$ form a basis for $J_5(\mathbb{Q})$ as a $\mathbb{Z}/5\mathbb{Z}$-vector space.*

Using the structure of the rational points in the Jacobian, we will be able to show our main result after proving the following lemmas.

Lemma 4.5. *$\mathscr{L}(11c)$ is a vector space of dimension six with a basis given by the functions*

$$1, \quad \frac{1}{x+y}, \quad \frac{x}{x+y}, \quad \frac{1}{(x+y)^2}, \quad \frac{x}{(x+y)^2}, \quad \frac{x^2}{(x+y)^2}. \tag{4.2}$$

Proof. In [Roh77], it is shown that

$$\begin{aligned} \mathrm{Div}(x) &= (a_0 + \cdots + a_4) - (c_0 + \cdots + c_4) \\ \mathrm{Div}(x+y) &= 4c - (c_0 + c_1 + c_3 + c_4). \end{aligned} \tag{4.3}$$

Therefore, all the functions in Equation 4.2 are in $\mathscr{L}(11c)$. They are also linearly independent so it suffices to prove that $l(11c) = 6$. To find the dimension of $\mathscr{L}(11c)$, we use the inequalities

$$l(kc) \leq l((k+1)c) \leq l(kc) + 1.$$

We have an equality on the left if and only if $k+1$ is a Weierstrass gap sequence of c. The Weiestrass gap sequence of c is 1, 2, 3, 6, 7, 11, ... [ACGH85, Exercise E-11]. Thus, given that $l(c) = 1$, we get $l(kc) = 1$ for $1 \leq k \leq 3$, $l(4c) = 2$, $l(kc) = 3$ for $5 \leq k \leq 7$, $l(8c) = 4$, $l(9c) = 5$ and $l(kc) = 6$ with $10 \leq k \leq 11$. □

Lemma 4.6. *Let L_a, L_b and L_c be the lines tangent to $F(5)$ at a, b and c respectively, then*

(i) L_a, L_b and L_c have contact of order 5 with the points a, b and c respectively.

(ii) If C is a plane conic with contact of order 3 with a, b or c, then C is reducible and contains L_a, L_b or L_c respectively.

Proof. For the first fact, an affine open set where a lies is $z \neq 0$. Thus, the line tangent to $F(5)$ at a is $y = 1$. However, the only point of intersection of $y = 1$ and $x^5 + y^5 = 1$ is a, which implies the tangent line at a has contact of order 5 at a. Using the same idea, it is possible to prove the result for b and c. For the second , it is necessary to use that if F, H and G are plane curves such that F is irreducible and is not a component of G or H, then

$$\min\{\mathrm{ord}_P(F \cap G), \mathrm{ord}_P(F \cap H)\} \leq \mathrm{ord}_P(G \cap H),$$

with P any non-singular point of F [Nam79, Theorem 2.3.2]. If we take $F \in \{L_a, L_b, L_c\}$, $G = F(5)$ and $H = C$, where C is a plane conic, we get the desired result for (ii). □

With this result, we can prove the following theorem. Although the theorem is known, we are presenting a new proof that is suggested in [Tze98] but which has not been found in the literature.

Theorem 4.7. *$F(5)(\Gamma_3) = \{a, b, c, P, \overline{P}\}$. In particular, there are no elements of degree three on $F(5)$.*

Proof. By Equality 4.1, it is enough to show there is no point of degree three on $F(5)$. Assume towards a contradiction that there exists a point R_1 on $F(5)$ of degree three over $\mathbb{Q}$ and let R_2 and R_3 be its Galois conjugates. In particular, R_1, R_2 and R_3 are not elements in $F(5)(\Gamma_2)$.

Now, consider the divisor of degree zero $R_1 + R_2 + R_3 - 3c$. Such a divisor is rational because it is invariant under any automorphism of $\overline{\mathbb{Q}}$ fixing $\mathbb{Q}$. By Theorem 4.4, there are integers $0 \leq d, e \leq 4$ such that

$$D := R_1 + R_2 + R_3 - 3c - d(c-a) - e(c-b)$$

is a principal divisor, thus $D = 0$ in $J_5(\mathbb{Q})$. Hence, the coefficient of c is between -11 and -3 and thus, the divisor is in $\mathscr{L}(11c)$. By Lemma 4.5, there is a polynomial $f(x, y)$ of degree two such that

$$\mathrm{Div}\left(\frac{f(x,y)}{(x+y)^2}\right) = R_1 + R_2 + R_3 + da + eb - (3 + d + e)c.$$

Using equation 4.3,

$$\mathrm{Div}((x+y)^2) = 10c - 2(c_0 + c_1 + c_2 + c_3 + c_4).$$

This implies

$$\mathrm{Div}(f(x,y)) = R_1 + R_2 + R_3 + da + eb + (7 - d - e)c - 2(c_0 + c_1 + c_2 + c_3 + c_4).$$

Note that $f(x, y)$ is a quotient of a homogeneous quadratic polynomial g by Z^2. Let C be the curve given by $g = 0$. Since $F(5)$ is a smooth plane curve,

$$\mathrm{Div}(f(x,y)) = C \cap F_5 - 2(c_0 + c_1 + c_2 + c_3 + c_4).$$

Combining the previous equations,

$$C \cap F_5 = R_1 + R_2 + R_3 + da + eb + (7 - d - e)c.$$

If $d \geq 3$, Lemma 4.6 implies that C is reducible and contains L_a. The lemma also shows that L_a has contact of order 5 with a. However, $d \leq 4$ and none of the points R_i is a by hypothesis, a contradiction. Hence, $d < 3$ and similarly, $e < 3$. Therefore $3 \leq 7 - d - e \leq 7$. By the same argument, $3 \leq 7 - d - e \leq 4$ is impossible. Then we get $5 \leq 7 - d - e \leq 7$, which, by Lemma 4.6 implies that C is reducible and contains L_c. Hence, there is a line L such that

$$L \cap F_5 = R_1 + R_2 + R_3 + da + eb + (2 - d - e)c$$

Any combination of $0 \leq d, e \leq 2$ implies the line L has two points in common with the lines L_a, L_b, L_c or $X + Y = Z$ (possible with multiplicities). However, L can not be L_a, L_b or L_c because its divisor does not have coefficient greater than 4 for a, b or c. Furthermore, L cannot be $X + Y = Z$ because this line contains P and $\overline{P}$ and, by hypothesis, none of the points R_i is P or $\overline{P}$. Therefore, L can not exist, a contradiction. We conclude that there are no points of degree three on $F(5)$. □

A special corollary of the theorem describes more geometrically the points of degree less than 4 on $F(5)$. We will show the same result for $F(7)$ and it has been conjectured that this is the case for all primes. For details see [KT97].

Corollary 4.8. *All the points in $F(5)(\Gamma_3)$ lie on the line $X + Y = Z$.*

It is also possible to describe geometrically all the points in $F(5)(\Gamma_6)$. We will show a characterization given by Klassen and Tzermias in [KT97].

Definition 4.9. Consider a point $R \in F(5)(\bar{\mathbb{Q}})$ of degree d over $\mathbb{Q}$, with $4 \leq d \leq 6$, and let $R_2, \ldots, R_d$ be its Galois conjugates. Also, let

- L' be a plane $\mathbb{Q}-$rational line;
- P' be one of the points $\{a, b, c\}$;
- C' be a plane $\mathbb{Q}-$rational conic with contact of order 2 with $F(5)$ at each point in one of the pairs (a, b), (b, c), (a, b) or $(P, \overline{P})$;

- $t(C')$ be the divisor $2a+2b$, $2b+2c$, $2a+2b$ or $2P+2\overline{P}$, depending on the pair chosen before.

Then R is called a *trivial point* if one of the following holds

(a) $R + R_2 + \cdots + R_d = F_5 \cap L' - P'$;

(b) $R + R_2 + \cdots + R_d = F_5 \cap L'$;

(c) or $R + R_2 + \cdots + R_d = F_5 \cap C' - t(C')$;

Remark. By Bezout's Theorem [Mir95, Theorem V.2.13], the degrees of the trivial points of types (a), (b) and (c) are 4, 5 and 6, respectively.

We can now state the result which completely describes the elements in $F(5)(\Gamma_6)$.

Theorem 4.10. *[KT97, Theorem 1] $F(5)(\Gamma_6)$ consists of $F(5)(\Gamma_2)$ and the trivial points.*

This theorem also gives us a good tool to describe the points of certain degree algebraically. For example, in [Kra17, Theorem 2], Kraus proves the following theorem by using Theorem 4.10.

Theorem 4.11. *Suppose that $F(5)(K)$ has a non-trivial point of degree 4. One of the following conditions is satisfied:*

1. *the Galois closure of K is a dihedral extension of $\mathbb{Q}$ of degree 8.*
2. *One has $K = \mathbb{Q}(\alpha)$ with*

$$31\alpha^4 - 36\alpha^3 + 26\alpha^2 - 36\alpha + 31 = 0.$$

The extension $K/\mathbb{Q}$ is cyclic. Up to Galois conjugation and permutation, $(2, 2\alpha, -\alpha - 1)$ is the only non-trivial point in $F(5)(K)$.

To prove Theorem 4.10, we need some results involving the Jacobian of $F(5)$ and the Abel-Jacobi map. Let C be a smooth plane quintic which, by Plücker's formula, has genus 6. We can describe the classes of divisors of degree 6 over C as the fibers of the Abel-Jacobi map

$$f^{(6)} : C^{(6)} \to \mathrm{Jac}(C).$$

For all $x \in \mathrm{Jac}(C)$, we define f_x as $(f^{(6)})^{-1}(x)$, that is, as a set of divisors of degree 6. Let D be a divisor in f_x. Then, there are several possibilities:

(i) $f_x = \{D\}$, $l(D) = 1$;

(ii) $f_x = |D|$, $l(D) = 2$, and D contains 4 collinear points;

(iii) $f_x = |D|$ and D contains 5 collinear points;

(iv) $f_x = |D|$ and D consists of 6 points on a conic.

Lemma 4.12. *[KT97, Lemma 1] If C is a smooth plane quintic, then the fibers of the Abel-Jacobi map are completely described by the cases $(i) - (iv)$ above.*

Proof. Let D be an effective divisor of degree 6 in C. We show that if $l(D) > 1$, then D falls into one of the cases $(ii) - (iv)$. Therefore, we need the version of the Riemann-Roch Theorem which states

$$(l(D) - 1) - i(D) = \deg(D) - g,$$

where $i(D)$ is the dimension of the vector space of effective meromorphic one-forms such that $(\omega) \geq D$ [Mir95, Theorem VI.3.11]. In our case, the theorem implies

$$l(D) - 1 = i(D). \tag{4.4}$$

By Clifford's theorem [ACGH85, Section III.1], we know that $l(D) - 1 \leq 2$. Finally, if D is constructed as before and $l(D) > 1$, then the points of D lie on a conic.

If the conic is irreducible, then it must be the only conic containing the six points of D and we are in case (iv).

Similarly, if the conic consists of two lines, we have at maximum 3, 4 or 5 collinear points. Having 6 collinear points is not possible because the points are in C, a plane quintic. If we have 3 points on each line, the lines are unique and the conic is the only one that passes through those points. By the same argument as in the irreducible conic, this is case (iv). Finally, if we have 4 points on the same line, D is in case (ii) and for 5 points, D is in case (iii). □

Lemma 4.13. *Let L' be a plane line and C' be a plane conic. Consider an effective $\mathbb{Q}-$rational divisor D on $F(5)$ of degree 4, 5 or 6 such that $D < F(5) \cap L'$, $D = F(5) \cap L'$ or $D < F(5) \cap C'$, respectively. Then the corresponding line L' or conic C' is $\mathbb{Q}-$rational.*

Proof. Consider $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. If $D = F(5) \cap L' - E$, with E an effective divisor of degree 1, then $D = D^\sigma = F(5) \cap L'^\sigma - E^\sigma$. Therefore, L' and L'^σ have at least 3 points in common. Since L' and L'^σ are lines, $L' = L'^\sigma$ and L' is $\mathbb{Q}-$rational. Following the same idea, we can prove the analogous result for the divisors of degree 5 and 6. □

Proof. (Theorem 4.10), sketch. Using Lemma 4.12, one can find explicitly the 25 divisor classes for $J_5(\mathbb{Q})$, call them $D_1, \ldots, D_{25}$. Since $J_5(\mathbb{Q})$ is generated by $[a - c]$ and $[b - c]$, we get that

$$J_5(\mathbb{Q}) = \{[D - 6c] : D = D_1, \ldots, D_{25}\}.$$

It is important to note that we can place each divisor into one of the cases of Lemma 4.12.

Consider a point R on $F(5)$ of degree $k = 4$, $k = 5$ or $k = 6$ and let $R_2, \ldots, R_k$ be its Galois conjugates. For each case, define the divisor D as follows

$$D = R + R_2, + \cdots + R_k + (6 - k)c.$$

The poof of the theorem is done by degree. We want to use the fact that D is in one of the cases $(i) - (iv)$ of Lemma 4.12 thus that either R has a lower degree than the assumed one or that R is a trivial point. Lemma 4.13 ensures that R is a trivial point because we get $\mathbb{Q}-$rational lines or conics. □

4.2 The Fermat curve of degree seven

To describe points of low degree over the Fermat curve of degree 7, we use Example 3.7. This method is similar to the one used in Section 4.1. By [GR78, Theorem 5.1], there are exactly five points in $F(7)(\Gamma_3)$ given by

$$\begin{gathered} a = (0,1,1), \qquad b = (1,0,1), \qquad c = (-1,1,0). \\ P = (\eta, \overline{\eta}, 1), \qquad \overline{P} = (\overline{\eta}, \eta, 1), \end{gathered} \tag{4.5}$$

with η a primitive $6-$th root of unity and $\overline{\eta}$ its complex conjugate. The main result is the following theorem.

Theorem 4.14. *[Tze98, Theorem 1] For all number fields K such that $[K : \mathbb{Q}] \leq 5$, we have $F(7)(K) \subseteq \{a, b, c, P, \overline{P}\}$.*

The proof uses the same idea as the proof of Theorem 4.7 in combination with Example 3.7. For details, see [Tze98].

4.3 Further cases

The methods described in sections 4.1 and 4.2 to find rational points on Fermat curves using the rational points in the corresponding Jacobians do not work when $N \geq 11$ because $J(N)(\mathbb{Q})$ is infinite. This was proven by Gross and Rohrlich in [GR78, Theorem 2.1], by finding a point of infinite order on $\mathrm{Jac}(F_k)(\mathbb{Q})$ for $k \neq 1$.

A weaker, but similar result to the ones obtained before is given for $N = 11$ by the same authors, in [GR78, Theorem 5.1]. It states that

$$F(11)(\Gamma_5) = \{a, b, c, P, \bar{P}\},$$

where the elements of the set above are defined as in Equation 4.5.

As remarked in Corollary 4.2, the strongest result that we have for all prime $N > 11$ is due to Debarre and Klassen and states that $F(N)(\Gamma_{N-2})$ is finite.

Finally, there are several known results for an analogy of Fermat's Last Theorem in some number fields. Jarris and Meekin proved in 2004 that for $N \geq 4$, the only points on the curve $x^N + y^N = z^N$, defined over $\mathbb{Q}(\sqrt{2})$, are those where $xyz = 0$ [JM04, Theorem 1.3]. Later, in 2014, Freitas and Siksek extended this result for quadratic real fields $\mathbb{Q}(\sqrt{d})$ with $d \in \{3, 6, 7, 10, 11, 13, 14, 15, 19, 21, 22, 23\}$ [FS15b, Theorem 1]. The main result in answering the question is related to the asymptotic Fermat's Last Theorem.

For K a field, the asymptotic Fermat's Last Theorem over K states: there is a constant B_K such that for any prime exponent $p > B_K$, the only solutions to the Fermat equation

$$a^p + b^p + c^p = 0, \qquad a, b, c \in K$$

are the trivial ones satisfying $abc = 0$. Freitas and Siksek proved in 2015 that for real quadratic fields, there is a set of fields of density 5/6 such that the asymptotic Fermat's Last Theorem holds [FS15a, Theorem 4.].

References

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[AKM+01] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, and Alexander R. Perlis. Jacobians of genus one curves. *J. Number Theory*, 90(2):304–315, 2001.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[DK94] Olivier Debarre and Matthew J. Klassen. Points of low degree on smooth plane curves. *J. Reine Angew. Math.*, 446:81–87, 1994.

[FS15a] Nuno Freitas and Samir Siksek. The asymptotic Fermat's last theorem for five-sixths of real quadratic fields. *Compos. Math.*, 151(8):1395–1415, 2015.

[FS15b] Nuno Freitas and Samir Siksek. Fermat's last theorem over some small real quadratic fields. *Algebra Number Theory*, 9(4):875–895, 2015.

[GR78] Benedict H. Gross and David E. Rohrlich. Some results on the Mordell-Weil group of the Jacobian of the Fermat curve. *Invent. Math.*, 44(3):201–224, 1978.

[JM04] Frazer Jarvis and Paul Meekin. The Fermat equation over $\mathbb{Q}(\sqrt{2})$. *J. Number Theory*, 109(1):182–196, 2004.

[Kra17] A. Kraus. Quartic points on the Fermat quintic. *ArXiv e-prints*, June 2017.

[KT97] Matthew Klassen and Pavlos Tzermias. Algebraic points of low degree on the Fermat quintic. *Acta Arith.*, 82(4):393–401, 1997.

[Lan82] Serge Lang. *Introduction to algebraic and abelian functions*, volume 89 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, second edition, 1982.

[Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[Mum99] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, expanded edition, 1999. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.

[Mur93] V. Kumar Murty. *Introduction to abelian varieties*, volume 3 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 1993.

[Nam79] Makoto Namba. *Families of meromorphic functions on compact Riemann surfaces*, volume 767 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979.

[Nar92] Raghavan Narasimhan. *Compact Riemann surfaces*. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1992.

[Roh77] David E. Rohrlich. Points at infinity on the Fermat curves. *Invent. Math.*, 39(2):95–127, 1977.

[Tze98] Pavlos Tzermias. Algebraic points of low degree on the Fermat curve of degree seven. *Manuscripta Math.*, 97(4):483–488, 1998.