

Polar Curves

Abramo Hefez*

Departamento de Matemática Aplicada, Universidade Federal Fluminense, R. São Paulo s/n-Campus do Valonguinho, 24020-005 Niterói, RJ-Brazil

Metadata, citation and similar papers at core.ac.uk

Neuza Nakuta

Departamento de Matemática-IBILCE, UNESP, R. Cristovão Colombo 2265 J. Nazareth, 15054-000 S. Jose do Rio Preto, SP-Brazil

Communicated by Walter Feit

Received January 31, 1995

1. INTRODUCTION

Polar curves of plane algebraic curves in characteristic zero have been studied extensively by several people and appear in the classical literature related to Plücker's formulas (see for example [2, 8, or 10]).

This study however has not been carried out in depth for curves defined over fields of positive characteristic, and the aim of this work is to contribute to filling this gap. It turns out, as we will see, that the theory in positive characteristic is quite different from the characteristic zero case and establishes interesting interplays between geometry and number theory.

Our motivation comes from [5] where, making a new use of polar curves in positive characteristic, we improved on the known upper bounds for the number of points of Fermat curves over finite fields. After the study we make in the present paper, it will be possible to apply the methods of [5] to other families of curves as well.

The paper is organized as follows. Let Z be a projective plane curve of degree d and let λ be an integer between 1 and d . We denote by $\Delta_p^\lambda Z$ the

* Partially supported by CNPq-Brazil.

polar λ -ic of Z at P . In Section 2 we show that the intersection multiplicity of Z and $\Delta_P^\lambda Z$ at P is an upper semi-continuous function in P on Z . The minimum value of this function, achieved on an open dense Zariski subset of Z , will be denoted by $\eta_{Z,\lambda}$. It is shown in Theorem 2.5 that there exists an arithmetical function $\eta(d,\lambda)$ such that for any curve Z of degree d we have $\eta_{Z,\lambda} \geq \eta(d,\lambda)$, with equality holding for the general curve of degree d . In Section 3 we characterize the non-general curves Z , that is, the curves for which $\eta_{Z,\lambda} > \eta(d,\lambda)$, in terms of the vanishing of certain derivatives of the defining polynomial of Z , assuming some mild behaviour on the singularities of the curve. In Section 4 we show how to get in some cases the shape of the equation of a non-general curve. In Section 5 we totally describe the arithmetical function $\eta(d,\lambda)$. In Section 6 we give an enumerative formula for the stationary points on a suitably general curve with respect to its associated family of polar λ -ics. More precisely, we count the number of points P on Z at which Z and $\Delta_P^\lambda Z$ have intersection multiplicity greater than $\eta_{Z,\lambda}$. This result contains in particular the usual Plücker's formula for the number of flexes of a non-singular plane projective curve. In Section 7 we introduce the polar morphisms of plane curves, which generalize the Gauss map, and prove a formula that generalizes Plücker's formula relating the degree of a curve, the degree of its Gauss map, and the degree of its dual curve.

2. GENERAL THEORY

Let K be an algebraically closed field, of characteristic $p \geq 0$, fixed once and for all. Let $F \in K[X_0, X_1, X_2]$ be a homogeneous polynomial of degree d and let Q be an element of K^3 . We consider, for $\lambda = 1, \dots, d$, the homogeneous polynomials

$$(\Delta_Q^\lambda F)(X_0, X_1, X_2) = \sum_{i_0+i_1+i_2=\lambda} (D_{i_0, i_1, i_2} F)(Q) X_0^{i_0} X_1^{i_1} X_2^{i_2},$$

where D_{i_0, i_1, i_2} denotes the mixed partial Hasse differential operator, of order i_ν with respect to the indeterminate X_ν , for $\nu = 0, 1, 2$. We will also denote $D_{i_0, 0, 0}$, $D_{0, i_1, 0}$, and $D_{0, 0, i_2}$ respectively by $D_{X_0}^{i_0}$, $D_{X_1}^{i_1}$, and $D_{X_2}^{i_2}$. For the properties of these operators needed here we refer the reader to [3].

From the definition of the Hasse operators, we have, for $P, Q \in K^3$ and indeterminates t_0 and t_1 , the identity

$$\begin{aligned} F(t_0 P + t_1 Q) &= t_0^d F(P) + t_0^{d-1} t_1 (\Delta_P^1 F)(Q) + \dots \\ &\quad + t_0 t_1^{d-1} (\Delta_P^{d-1} F)(Q) + t_1^d F(Q) \end{aligned} \quad (1)$$

The above identity gives many relations involving the polynomials $\Delta_Q^\lambda F$, of which we use only a few.

LEMMA 2.1. *We have the relations*

$$(i) \quad (\Delta_P^\lambda F)(Q) = (\Delta_Q^{d-\lambda} F)(P).$$

$$(ii) \quad (\Delta_P^\lambda F)(P) = \binom{d}{\lambda} F(P).$$

(iii) *Let T be a linear automorphism of K^3 . For any polynomial G in $K[X_0, X_1, X_2]$ and any Q in K^3 , we denote $G(T(Q))$ by $G^T(Q)$. Then we have*

$$(\Delta_P^\lambda F)^T = (\Delta_{T^{-1}(P)}^\lambda F^T).$$

Proof. (i) is obtained by comparing the corresponding identity for $F(t_1 Q + t_0 P)$ with (1). (ii) follows easily from identity (1) when we put $P = Q$. (iii) follows replacing Q by $T(Q)$ in both members of (1) and then developing the first member using again formula (1).

Note that Lemma 2.1 (ii) is a generalization of Euler's relation, which applied to the monomial $X_0^{n_0} X_1^{n_1} X_2^{n_2}$, with $n_0 + n_1 + n_2 = d$, gives in particular the well known relation, still called *Euler's relation*,

$$\sum_{i_0+i_1+i_2=\lambda} \binom{n_0}{i_0} \binom{n_1}{i_1} \binom{n_2}{i_2} \equiv \binom{d}{\lambda}.$$

Note also that what we established for polynomials in three indeterminates is valid in any number of indeterminates; in particular, also in the above Euler's relation.

DEFINITION. If Z is a projective plane curve defined by $F = 0$, and if some of the derivatives of F of order λ evaluated at P is nonzero, then the curve $\Delta_P^\lambda Z$ defined by $\Delta_P^\lambda F = 0$ is called the *polar λ -ic curve* of Z at P .

In particular, we have for $\lambda = 1$ the polar line at P (which is, for $P \in Z$, the tangent line at P), for $\lambda = 2$ we have the polar conic at P , and for $\lambda = 3$ the polar cubic at P .

It is clear from Lemma 2.1 (i) that our indices for polars are reversed with respect to the classical use, that is, our definition of Δ_P^λ is the classical $\Delta^{d-\lambda}$ (as defined for example in [2] or in [8]). We also have from this formula that $P \in \Delta_Q^\lambda Z$ if and only if $Q \in \Delta_P^{d-\lambda} Z$. It follows from Lemma 2.1(ii) that if $P \in Z$, then $P \in \Delta_P^\lambda Z$ for all λ . Lemma 2.1(iii) says that the polar λ -ic is a well defined projective object.

In order to study the behavior of the intersection multiplicity function of Z with its polar curves, we establish the following result.

PROPOSITION 2.2. *Let $Z: F = 0$ be an integral projective plane curve and let $\tilde{Z} \xrightarrow{\pi} Z$ be the normalization map of Z . Let λ be an integer such that $1 \leq \lambda < d$, and some mixed derivative of F of order λ is not identically zero. Then the integer-valued function on \tilde{Z} defined by the formula*

$$\tilde{P} \mapsto \text{ord}_{\tilde{P}}(\Delta_{\pi(\tilde{P})}^{\lambda} F)$$

is upper semi-continuous.

Proof. Let $Q \in \tilde{Z}$ and suppose without loss of generality that $\pi(Q) = (1; a; b)$. Choose a rational function $s \in K(\tilde{Z})$ such that its image in the local ring $\mathcal{O}_{\tilde{Z}, Q}$ is a uniformizing parameter. If \tilde{U} is the open set of \tilde{Z} of all points \tilde{P} for which $t = s - s(\tilde{P})$ is an uniformizing parameter of $\mathcal{O}_{\tilde{Z}, \tilde{P}}$ and $\pi(\tilde{P}) \notin \{X_0 = 0\}$, then we have that

$$(\Delta_{\pi(\tilde{P})}^{\lambda} F)(1, x, y) = \sum_{i_0+i_1+i_2=\lambda} (D_{i_0, i_1, i_2} F)(\pi(\tilde{P})) x^{i_1} y^{i_2}.$$

Consider the powers series $\sum_{i \geq 0} D_s^i(x \circ \pi) t^i$ and $\sum_{i \geq 0} D_s^i(y \circ \pi) t^i$ in $K[\tilde{U}][[t]]$. These powers series with their coefficients evaluated at $\tilde{P} \in \tilde{U}$ represent the expansions of the functions $x \circ \pi$ and $y \circ \pi$ in the completion of the local ring $\mathcal{O}_{\tilde{Z}, \tilde{P}}$. Consider now the expansion

$$(\Delta_{\pi(\tilde{P})}^{\lambda} F) \left(1, \sum_{i \geq 0} D_s^i(x \circ \pi)(\tilde{P}) t^i, \sum_{i \geq 0} D_s^i(y \circ \pi)(\tilde{P}) t^i \right) = \sum_{i \geq 0} h_i(\tilde{P}) t^i,$$

where each h_i is a regular function on \tilde{U} . Let η be the first index i for which $h_i \neq 0$ (such an index exists because some derivative of F of order λ is nonzero), then $\text{ord}_{\tilde{P}}(\Delta_{\pi(\tilde{P})}^{\lambda} F)$ is equal to η for \tilde{P} in the open dense set $\{\tilde{P} \in \tilde{U} | h_i(\tilde{P}) \neq 0\}$ and is greater than η at the other points of \tilde{U} , so the function under consideration is upper semi-continuous on \tilde{U} , hence on \tilde{Z} .

We will denote by $I(P, F, G)$ the intersection multiplicity of the curves $F = 0$ and $G = 0$ at the point P .

COROLLARY 2.3. *If F is an irreducible polynomial of degree d in $K[X_0, X_1, X_2]$, then for every $\lambda = 1, \dots, d - 1$ such that some derivative of order λ of F is nonzero, the function $P \mapsto I(P, F, \Delta_P^{\lambda} F)$ is upper semi-continuous on $Z: F = 0$.*

The upper semi-continuity of the above intersection multiplicity implies that its minimum value is achieved in a non-empty Zariski open set of Z .

DEFINITION. We define $\eta_{Z, \lambda}$ as being the minimum value of the above intersection multiplicity function.

The number $\eta_{Z, 1}$ is well known and it is the last order ε_2 of the order sequence of the curve in the projective plane, that is, it is the intersection multiplicity at a general point P of Z with its tangent line at P (see for example [6] or [9]).

In order to compute the value of $\eta_{Z, \lambda}$, we will give the expansion of the polynomial $\Delta_Q^\lambda F$ at a point P .

Let $f(x, y)$ be a polynomial in $K[x, y]$. If $P' = (a, b)$ is a point in the affine plane, and r is an integer such that $0 \leq r \leq \deg(f)$, we define

$$f_{r, P'}(x, y) = \sum_{i+j=r} D_{i,j} f(P')(x-a)^i (y-b)^j,$$

where $D_{i,j}$ means the Hasse differential operator of order i with respect to x and of order j with respect to y . It is clear that we have

$$f(x, y) = \sum_{r=0}^{\deg(f)} f_{r, P'}(x, y).$$

In the following we will denote by P the point (a_0, a_1, a_2) , with $a_0 \neq 0$, in K^3 and by P' the point $(a, b) = (a_1/a_0, a_2/a_0)$ in K^2 .

LEMMA 2.4. Let $F(X_0, X_1, X_2)$ be a homogeneous polynomial of degree d in $K[X_0, X_1, X_2]$, and let $P = (a_0, a_1, a_2) \in K^3$, with $a_0 \neq 0$, and λ an integer such that $1 \leq \lambda \leq d$.

(i) If $Q \in K^3$, then

$$(\Delta_Q^\lambda F)(1, x, y) = \sum_{i+j=0}^{\lambda} a_0^{i+j-\lambda} (\Delta_P^{d-\lambda} D_{0,i,j} F)(Q)(x-a)^i (y-b)^j.$$

(ii) If $f(x, y)$ denotes the polynomial $F(1, x, y)$, then

$$\begin{aligned} (\Delta_P^\lambda F)(1, x, y) &= \sum_{r=0}^{\lambda} a_0^{r-\lambda} \binom{d-r}{\lambda-r} \sum_{i+j=r} D_{0,i,j} F(P)(x-a)^i (y-b)^j \\ &= a_0^{d-\lambda} \sum_{r=0}^{\lambda} \binom{d-r}{\lambda-r} f_{r, P'}(x, y). \end{aligned}$$

Proof. (i) If $I = (i_0, i_1, i_2)$, and $|I| = i_0 + i_1 + i_2$, we have

$$\begin{aligned} (\Delta_Q^\lambda F)(1, x, y) &= \sum_{|I|=\lambda} D_I F(Q) (x-a+a)^{i_1} (y-b+b)^{i_2} \\ &= \sum_{|I|=\lambda} \sum_{i+j=0}^\lambda \binom{i_1}{i} \binom{i_2}{j} \\ &\quad \times D_I F(Q) \left(\frac{a_1}{a_0}\right)^{i_1-i} \left(\frac{a_2}{a_0}\right)^{i_2-j} (x-a)^i (y-b)^j \quad (2) \end{aligned}$$

$$\begin{aligned} &= \sum_{|I|=\lambda} \sum_{i+j=0}^\lambda a_0^{i+j-\lambda} (D_{i_0, i_1-i, i_2-j} \circ D_{0, i, j} F)(Q) \\ &\quad \times a_0^{i_0} a_1^{i_1-i} a_2^{i_2-j} (x-a)^i (y-b)^j \quad (3) \end{aligned}$$

$$= \sum_{i+j=0}^\lambda a_0^{i+j-\lambda} (\Delta_Q^{\lambda-(i+j)} D_{0, i, j} F)(P) (x-a)^i (y-b)^j$$

$$= \sum_{i+j=0}^\lambda a_0^{i+j-\lambda} (\Delta_P^{d-\lambda} D_{0, i, j} F)(Q) (x-a)^i (y-b)^j, \quad (4)$$

where equality (2) is obtained from the binomial expansion, equality (3) is a consequence of the composition law for the Hasse differential operators, and equality (4) follows from Lemma 2.1(i).

(ii) This formula follows from (i) and from Lemma 2.1(ii).

It follows from part (ii) of the above lemma that

$$I(P, Z, \Delta_P^\lambda Z) \geq 2, \quad \forall P \in Z.$$

DEFINITION. Let d and λ be two integers such that $1 \leq \lambda < d$. We define

$$\eta(d, \lambda) = \min \left\{ s \left| \binom{d-1}{\lambda-1} \not\equiv \binom{d-s}{\lambda-s} \pmod{p} \right. \right\}.$$

It is clear that

$$2 \leq \eta(d, \lambda) \leq \lambda + 1 \leq d.$$

In particular, for any $d > 1$ we have $\eta(d, 1) = 2$. We also have that if $p = 0$, then $\eta(d, \lambda)$ is always equal to 2.

DEFINITION. If $d = d_0 + d_1p + \cdots + d_n p^n$ is the p -adic expansion of d , then $\lambda = d_0 + \cdots + d_m p^m$, for $m < n$, is called the *truncation of d at order m* , or simply a *truncation of d* .

Remark 1. When $p > 0$ and $\lambda \neq 0$ is a truncation of d , then $\binom{d-1}{\lambda-1} \equiv 1 \pmod{p}$, and

$$\eta(d, \lambda) = \lambda + 1.$$

The above equality follows from the following well known congruence, which we will refer to as the *fundamental congruence*,

$$\begin{pmatrix} a_0 + a_1p + a_2p^2 + \cdots \\ b_0 + b_1p + b_2p^2 + \cdots \end{pmatrix} \equiv \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \cdots \pmod{p}.$$

The following result will illustrate the importance of this arithmetical function.

THEOREM 2.5. Let $Z: F = 0$ be an irreducible projective plane curve of degree $d \geq 2$, and let λ be an integer such that $1 \leq \lambda < d$. Then we have

- (i) $\eta_{Z, \lambda} \geq \eta(d, \lambda)$,
- (ii) $\eta_{Z, \lambda} > \eta(d, \lambda)$, if and only if,

$$\sum_{r=0}^{\eta(d, \lambda)} \left(D_{X_i}^r \circ D_{X_j}^{\eta(d, \lambda) - r} F \right) (-F_{X_i})^{\eta(d, \lambda) - r} (F_{X_j})^r \equiv 0 \pmod{F}, \quad (5)$$

for some $i, j = 0, 1, 2$, with $i \neq j$.

- (iii) If Z is a general curve of degree d , then $\eta_{Z, \lambda} = \eta(d, \lambda)$.

Proof. (i) Let $P = (1; a; b)$ be a general point of Z , and let $P' = (a, b)$. If $f(x, y) = F(1, x, y) = \sum_{r \geq 0} f_{r, P'}(x, y)$, and $(\Delta_{P'}^\lambda f)(x, y) = \sum_{r \geq 0} \binom{d-r}{\lambda-r} f_{r, P'}(x, y)$, then we have from Lemma 2.4(ii) that

$$I(P, F \cdot \Delta_P^\lambda F) = I(P', f \cdot \Delta_{P'}^\lambda f).$$

Now, since

$$I(P', f \cdot \Delta_{P'}^\lambda f) = I\left(P', f \cdot \left(\Delta_{P'}^\lambda f - \binom{d-1}{\lambda-2} f \right)\right)$$

and

$$\Delta_{P'}^\lambda f - \binom{d-1}{\lambda-1} f = \sum_{r \geq \eta(d, \lambda)} \left[\binom{d-r}{\lambda-r} - \binom{d-1}{\lambda-1} \right] f_{r, P'}(x, y), \quad (6)$$

we have that

$$I(P, F, \Delta_P^\lambda F) \geq \eta(d, \lambda).$$

(ii) Remark that (5) is always true if $i = j$. We keep the notation of (i) and assume that $f_y(x, y) \not\equiv 0$ (because if $f_y(x, y) \equiv 0$, then we have $f_x(x, y) \not\equiv 0$, and the argument is similar). We may then choose a parametrization of Z at P as follows:

$$P(t) = (1; a + t; b + b_1 t + b_2 t^2 + \dots). \quad (7)$$

This implies, for $\eta = \eta(d, \lambda)$, that

$$\begin{aligned} & \left[\Delta_{P'}^\lambda f - \binom{d-1}{\lambda-1} f \right] (P(t)) \\ &= \left[\binom{d-\eta}{\lambda-\eta} - \binom{d-1}{\lambda-1} \right] \sum_{r=0}^{\eta} b_1^{\eta-r} (D_{r, \eta-r} f)(P') t^\eta \\ & \quad + \text{higher powers of } t. \end{aligned} \quad (8)$$

Since $\binom{d-\eta}{\lambda-\eta} \not\equiv \binom{d-1}{\lambda-1} \pmod{p}$, we have that $I(P, F, \Delta_P^\lambda F) > \eta$ if and only if

$$\sum_{r=0}^{\eta} b_1^{\eta-r} (D_{r, \eta-r} f)(P') = 0$$

Now, since $b_1 = -f_x(a, b)/f_y(a, b) = -F_{X_1}(1, a, b)/F_{X_2}(1, a, b)$, it follows that $I(P, F, \Delta_P^\lambda F) > \eta$ if and only if

$$\sum_{r=0}^{\eta} (D_{0, r, \eta-r} F)(P) (F_{X_2}(P))^r (-F_{X_1}(P))^{\eta-r} = 0, \quad (9)$$

and since P is general, this is equivalent to (5) for $i = 1$ and $j = 2$. The other cases are proved taking $P = (a; 1; b)$ or $P = (a; b; 1)$.

(iii) Part (ii) shows that $\eta_{Z, \lambda} = \eta(d, \lambda)$ is an open condition in the open subset of irreducible curves in the space of all curves of degree d , so the only thing we have to show is that this condition is not empty, which amounts to produce any polynomial F such that (5) is not satisfied.

Given d and λ as above, let

$$F(X_0, X_1, X_2) = X_0^\eta X_2^{d-\eta} + X_1 X_2^{d-1},$$

where $\eta = \eta(d, \lambda)$. In this case the left-hand side of the congruence in (5), for $i = 1, j = 2$, is $X_2^{d+\eta(d-2)}$, which is clearly not divisible by F .

DEFINITION. An irreducible curve Z of degree d will be called (d, λ) -general if $\eta_{Z, \lambda} = \eta(d, \lambda)$.

In particular, a $(d, 1)$ -general curve is a curve with $\eta_{Z, 1} = \eta(d, 1) = 2$. Thus if $\text{char } K \neq 2$, then $(d, 1)$ -generality is equivalent to reflexivity.

Remark 2. The proof of Theorem 2.5(ii) shows that if (5) is true for some $i, j = 0, 1, 2$, with $i \neq j$, then it is true for all $i, j = 0, 1, 2$.

COROLLARY 2.6. Let $\eta = \eta(d, \lambda)$. If for some i and j , with $i \neq j$, we have $D_{X_i}^r \circ D_{X_j}^{\eta-r} F = 0$, for all $r = 0, \dots, \eta$, then the curve $F = 0$ is not (d, λ) -general.

EXAMPLE 1. We give here an example of a family of non-general curves.

Let d and λ be such that $d \equiv \eta(d, \lambda) - 1 \pmod{p^s}$ with $\eta(d, \lambda) < p^s$, for some positive integer s . If F is of the form

$$F = \sum_{i_0+i_1+i_2=\eta(d, \lambda)-1} P_{i_0, i_1, i_2}(X_0^{p^s}, X_1^{p^s}, X_2^{p^s}) X_0^{i_0} X_1^{i_1} X_2^{i_2},$$

for some homogeneous polynomials P_{i_0, i_1, i_2} , then the curve $Z: F = 0$ is not (d, λ) -general.

Indeed, for all non-negative integers j_0, j_1 , and j_2 such that $j_0 + j_1 + j_2 = \eta(d, \lambda)$, we have that

$$D_{j_0, j_1, j_2} F = 0,$$

and the result follows from the above corollary.

COROLLARY 2.7. Let Z be a projective irreducible curve of degree $d \geq 2$ defined over a field K of characteristic $p \neq 2$. Let λ be an integer such that $1 \leq \lambda < d$. Then $\eta_{Z, \lambda} > 2$ if and only if either Z is non-reflexive or

$$\binom{d-1}{\lambda-1} \equiv \binom{d-2}{\lambda-2} \pmod{p}.$$

Proof. Since $\eta_{Z, \lambda} \geq \eta(d, \lambda) \geq 2$, it follows from Theorem 2.5 that $\eta_{Z, \lambda} = 2$ if and only if $\eta(d, \lambda) = 2$ and for some $i, j = 0, 1, 2, i \neq j$,

$$\sum_{r=0}^2 \left(D_{X_i}^r \circ D_{X_j}^{2-r} F \right) (-F_{X_i})^{2-r} (F_{X_j})^r \not\equiv 0 \pmod{F},$$

which, according to [3, Proposition 4.12], is equivalent to reflexivity.

Remark 3. The above collary tells us that in characteristic zero we always have $\eta_{Z,\lambda} = 2$, and since $\eta(d, \lambda) = 2$, we always have (d, λ) -generality in this case.

Remark 4. In general, the polar λ -ic curve does not coincide with the osculating curve of degree λ , since for a general curve Z these curves have different intersection multiplicities with Z at a general point.

3. NON-GENERAL CURVES

In order to characterize the non-general curves in terms of their defining equations we have to make some restrictions on the singularities of the curve.

DEFINITION. We will say that a curve Z of degree d has *mild singularities* with respect to the pair (d, λ) if the following inequality holds;

$$\sum_{P \in Z} e_P < d(\eta(d, \lambda) - 1),$$

where e_P is the multiplicity of the Jacobian ideal of Z at P .

Note that all non-singular curves satisfy the above condition.

PROPOSITION 3.1. *Let $Z : F = 0$ be an irreducible curve of degree d with mild singularities with respect to (d, λ) . Suppose that for some $\rho \geq \eta(d, \lambda)$ and for all $i, j = 0, 1, 2$, we have*

$$\sum_{r=0}^{\rho} (D_{X_i}^r \circ D_{X_j}^{\rho-r} F)(-F_{X_i})^{\rho-r} (F_{X_j})^r \equiv 0 \pmod{F}, \tag{10}$$

then for all $i, j = 0, 1, 2$, and all $r = 0, 1, \dots, \rho$, we have

$$D_{X_i}^r \circ D_{X_j}^{\rho-r} F = 0.$$

Proof. We may choose coordinates in \mathbb{P}_K^2 in such a way that for every singular point Q of Z we have for all $i = 0, 1, 2$ that

$$e_Q = I(Q, F.F_{X_i}),$$

and such that no partial derivative of F of the first order vanishes at the smooth points of Z located on any of the coordinates axes. In particular, $F_{X_i} \neq 0$, for all $i = 0, 1, 2$.

Now, from (10) we get, for all $i, j = 0, 1, 2$, that

$$(D_{X_j}^\rho F)(F_{X_i})^\rho \equiv F_{X_j} \cdot G \pmod{F} \quad (11)$$

for some polynomial G .

Suppose by reductio ad absurdum that $D_{X_j}^\rho F \neq 0$ for some j . From (11) it follows, for all $i = 0, 1, 2$ and for all $P \in Z$, that

$$I(P, F \cdot D_{X_j}^\rho F) + \rho I(P, F \cdot F_{X_i}) \geq I(P, F \cdot F_{X_i}). \quad (12)$$

If P is a regular point of Z , then for some $k = 0, 1, 2$ we have

$$I(P, F \cdot F_{X_k}) = e_P = 0,$$

therefore from (12) taking $i = k$, we get that

$$I(P, F \cdot D_{X_j}^\rho F) \geq I(P, F \cdot F_{X_j}),$$

hence

$$I(P, F \cdot D_{X_j}^\rho F) + e_P \geq I(P, F \cdot F_{X_j}). \quad (13)$$

If P is any singular point of Z , we have clearly that

$$I(P, F \cdot D_{X_j}^\rho F) + e_P \geq e_P = I(P, F \cdot F_{X_j}). \quad (14)$$

Summing (13) over all regular points of Z , with (14) over all singular points of Z , we have

$$\sum_{P \in Z} I(P, F \cdot D_{X_j}^\rho F) + \sum_{P \in Z} e_P \geq \sum_{P \in Z} I(P, F \cdot F_{X_j}),$$

which together with Bézout's Theorem yields (recall that $D_{X_j}^\rho F, F_{X_j} \neq 0$)

$$d(d - \rho) + \sum_{P \in Z} e_P \geq d(d - 1).$$

It then follows that

$$\sum_{P \in Z} e_P \geq d(\rho - 1) \geq d(\eta - 1),$$

contradicting the assumption that Z has mild singularities with respect to the pair (d, λ) , hence

$$D_{X_j}^\rho F = 0, \quad \forall j = 0, 1, 2.$$

We will analyze now the vanishing of $D_{X_i}^1 \circ D_{X_j}^{\rho-1}F$. If $i = j$, we have

$$D_{X_i}^1 \circ D_{X_j}^{\rho-1}F = (\rho - 1)D_{X_i}^{\rho}F = 0.$$

So we may assume $i \neq j$ and, again by reductio ad absurdum, assume that $D_{X_i}^1 \circ D_{X_j}^{\rho-1}F \neq 0$. Since $D_{X_j}^{\rho}F = 0$, from (10) we have that there is a polynomial G' such that

$$(D_{X_i}^1 \circ D_{X_j}^{\rho-1}F)(-F_{X_i})^{\rho-1} \equiv F_{X_j} \cdot G' \pmod{F},$$

and consequently we have for any $P \in Z$ that

$$I(P, F \cdot D_{X_i}^1 \circ D_{X_j}^{\rho-1}F) + (\rho - 1)I(P, F \cdot F_{X_i}) \geq I(P, F \cdot F_{X_j}). \tag{15}$$

Let now P be a regular point of Z . If $F_{X_i}(P) \neq 0$, then we have from (15) that

$$I(P, F \cdot D_{X_i}^1 \circ D_{X_j}^{\rho-1}F) \geq I(P, F \cdot F_{X_j}). \tag{16}$$

If $F_{X_i}(P) = 0$, then from Euler's relation we get, for $k \neq i$ and $k \neq j$, that

$$P_j F_{X_j}(P) + P_k F_{X_k}(P) = 0,$$

and since our coordinates have been chosen in order that the point P is not on any of the coordinate axes, we must have $F_{X_j}(P) \neq 0$. This implies that (16) is also true in this case. Therefore we have for all regular points P of Z that

$$I(P, F \cdot D_{X_i}^1 \circ D_{X_j}^{\rho-1}F) + e_P \geq I(P, F \cdot F_{X_j}).$$

If P is any singular point, then we have an equation analogous to (14) with $D_{X_i}^1 \circ D_{X_j}^{\rho-1}F$ in place of $D_{X_j}^{\rho}F$, and the proof proceeds exactly as above to show that $D_{X_i}^1 \circ D_{X_j}^{\rho-1}F = 0$.

The same argument can now be used to show that $D_{X_i}^2 \circ D_{X_j}^{\rho-2}F = 0$, and so on.

Let d and λ be positive integers with $\lambda < d$, and p a prime number. Consider the following open statements on integers ν :

$$R(\nu) : \binom{d - \nu}{\lambda - \nu} \not\equiv \binom{d - 1}{\lambda - 1}$$

and

$$S(\nu) : \exists i, j = 0, 1, 2, \exists r = 0, \dots, \nu; D_{X_i}^r \circ D_{X_j}^{\nu-r}F \neq 0.$$

THEOREM 3.2. *Let $Z: F = 0$ be an irreducible projective plane curve of degree d with mild singularities with respect to a pair (d, λ) . We have that $\eta_{Z, \lambda}$ is the smallest integer in the set*

$$\{\eta(d, \lambda) \leq \nu \leq \lambda |R(\nu) \text{ and } S(\nu)\} \cup \{\nu > \lambda |S(\nu)\}.$$

Proof. Let ρ be the smallest integer in the above set. Let $P = (1; a; b)$ be a general point of Z , then we have a formula like (6) with ρ instead of $\eta(d, \lambda)$. This expression evaluated at a parametrization of Z at P like (7) yields a formula like (8) with ρ instead of η , hence $\eta_{Z, \lambda} = I(P, F, \Delta_p^\lambda F) \geq \rho$. Also, $\eta_{Z, \lambda} > \rho$ implies a formula like (9) with ρ instead of η . The same argument will show that if $\eta_{Z, \lambda} > \rho$, then (10) holds for all $i, j = 0, 1, 2$ with $i \neq j$, therefore from Proposition 3.1 it follows that for all $i, j = 0, 1, 2$ and all $r = 0, \dots, \rho$,

$$D_{X_i}^r \circ D_{X_j}^{\rho-r} F = 0,$$

which contradicts the definition of ρ . So $\eta_{Z, \lambda} = \rho$.

Remark 5. If $\lambda \neq 0$ is a truncation of d and Z has mild singularities, then we have that

$$\eta_{Z, \lambda} = \min\{\nu > \lambda |S(\nu)\}$$

The following result is a generalization for all λ of [7, Theorem 2.1; 3, Theorem 5.1; and 1, Theorem 3], all established for $\lambda = 1$.

COROLLARY 3.3. *Let $Z: F = 0$ be an irreducible curve of degree d with mild singularities with respect to (d, λ) . The curve Z is not (d, λ) -general if and only if for all $i, j = 0, 1, 2$, and all integers m and n such that $m + n = \eta(d, \lambda)$, we have*

$$D_{X_i}^m \circ D_{X_j}^n F = 0.$$

EXAMPLE 2. Let $p = 5$ and $d = 38$. If

$$F = X_0^{17} X_1^{21} + X_1^9 X_2^{29} + X_0^{38} + X_2^{38},$$

then the curve $Z: F = 0$ is smooth of degree 38 over the algebraic closure of \mathbb{F}_5 . So we may apply to it Theorem 3.2 and the above corollary.

For $\lambda = 3$, the curve Z is (d, λ) -general because, as it is easy to verify, we have $\eta(d, \lambda) = 4$, and $D_{X_1}^4 F = X_1^5 X_2^{29} \neq 0$.

For $\lambda = 13$, the curve Z is not (d, λ) -general, because we have in this case $\eta(d, \lambda) = 14$, and for all $i, j = 0, 1, 2$, and all m, n with $n + m = 14$, that

$$D_{X_i}^n D_{X_j}^m F = 0.$$

Now since we have $D_{X_0}^{15} F = 2 X_0^2 X_1^{21} \neq 0$, it follows that $\eta_{Z, \lambda} = 15$.

PROPOSITION 3.4. *Let $Z : F = 0$ be an irreducible projective plane curve of degree d with mild singularities with respect to a pair (d, λ) .*

(i) *We have $\eta_{Z, \lambda} < d$.*

If moreover λ is a truncation of d , then

(ii) $\forall \lambda', \eta(d, \lambda') \geq \eta(d, \lambda) \Rightarrow \eta_{Z, \lambda'} \geq \eta_{Z, \lambda}$.

(iii) *If $P, Q \in \mathbb{P}_K^2$ and $P \in Z \cap \Delta_Q^{d-\lambda}Z$, then*

$$I(P, Z \cap \Delta_Q^{d-\lambda}Z) \geq \eta_{Z, \lambda} - \lambda.$$

Proof. (i) and (ii) follow immediately from Theorem 3.2, while (iii) is proved also using Lemma 2.4 (i), replacing λ by $d - \lambda$.

COROLLARY 3.5. *With the same hypotheses as in Proposition 3.4 (iii), and assuming that $\Delta_Q^{d-\lambda}F \neq 0$, we have*

$$\#(Z \cap \Delta_Q^{d-\lambda}Z) \leq \frac{d(d - \lambda)}{\eta_{Z, \lambda} - \lambda}.$$

4. THE EQUATION OF A NON-GENERAL CURVE

In order to give explicitly the shape of the equation of a curve which is not (d, λ) -general, we will need the following two lemmas:

LEMMA 4.1. *Let non-negative integers n_0, n_1, n_2, η , and p be given such that p is prime, $2 \leq \eta < p$, and $\eta - 1 \equiv n_0 + n_1 + n_2 \pmod p$. If for all non-negative integers α and β with $\alpha + \beta = \eta$, and for all $i, j = 0, 1, 2$, we have*

$$\binom{n_i}{\alpha} \binom{n_j}{\beta} \equiv 0 \pmod p,$$

then for all non-negative integers i_0, i_1 , and i_2 with $i_0 + i_1 + i_2 = \eta$, we have

$$\binom{n_0}{i_0} \binom{n_1}{i_1} \binom{n_2}{i_2} \equiv 0 \pmod p.$$

Proof. Write the p -adic expansion of n_i as

$$n_i = n_{i,0} + n_{i,1}p + \dots.$$

Since $\alpha + \beta = \eta < p$, we have from the hypotheses and from the fundamental congruence that

$$0 \equiv \binom{n_i}{\alpha} \binom{n_j}{\beta} \equiv \binom{n_{i,0}}{\alpha} \binom{n_{j,0}}{\beta}.$$

It then follows that

$$n_{i,0} + n_{j,0} \leq \eta - 1, \quad \forall i, j = 0, 1, 2,$$

hence

$$2(n_{0,0} + n_{1,0} + n_{2,0}) \leq 3(\eta - 1). \quad (17)$$

Since $n_0 + n_1 + n_2 \equiv \eta - 1 \pmod{p}$, we have, for some $r \in \{0, 1, 2\}$, that

$$n_{0,0} + n_{1,0} + n_{2,0} = \eta - 1 + rp. \quad (18)$$

From (17) and (18) it follows that $2rp \leq \eta - 1 < p$. So $r = 0$ and

$$n_{0,0} + n_{1,0} + n_{2,0} = \eta - 1.$$

So for all (i_0, i_1, i_2) with $i_0 + i_1 + i_2 = \eta$, we have

$$\binom{n_0}{i_0} \binom{n_1}{i_1} \binom{n_2}{i_2} \equiv \binom{n_{0,0}}{i_0} \binom{n_{1,0}}{i_1} \binom{n_{2,0}}{i_2} \equiv 0 \pmod{p}.$$

PROPOSITION 4.2. *Let d , η , and p be integers such that p is prime, $2 \leq \eta < p$, and $d \equiv \eta - 1 \pmod{p}$. If $F \in K[X_0, X_1, X_2]$ is homogeneous of degree d , where $\text{char } K = p$, and*

$$D_{X_i}^\alpha D_{X_j}^\beta F = 0 \quad \forall i, j = 0, 1, 2, \forall \alpha, \beta; \alpha + \beta = \eta,$$

then

$$D_{i_0, i_1, i_2} F = 0 \quad \forall i_0, i_1, i_2; i_0 + i_1 + i_2 = \eta.$$

Proof. It is sufficient to prove the assertion for monomials

$$X_0^{n_0} X_1^{n_1} X_2^{n_2}; \quad n_0 + n_1 + n_2 = d,$$

and in this case the result follows from Lemma 4.1.

The assertion in Proposition 4.2 may fail if the hypotheses are not satisfied, as one can see in the following example.

EXAMPLE 3. Put $p = 5$ and let

$$F = X_0^2 X_1^2 X_2^3.$$

It is easy to verify for all $i, j = 0, 1, 2$ that

$$D_{X_i}^\alpha D_{X_j}^\beta F = 0 \quad \forall \alpha, \beta; \alpha + \beta = 6,$$

but $D_{X_0}^2 D_{X_1}^2 D_{X_2}^2 F \neq 0$. This does not contradict Proposition 4.2, since $\eta = 6 > p = 5$.

Given a multi-index $I = (i_0, i_1, \dots, i_n)$, we will use the notation

$$|I| = i_0 + i_1 + \dots + i_n.$$

We will also use the notation $a \leq_p b$ to mean that a is less than or equal to b with respect to the p -adic ordering, that is, $a_i \leq b_i$, for all i , where a_i and b_i are respectively the coefficients of the p -adic expansions of a and b .

It follows immediately from the fundamental congruence that

$$\binom{a}{b} \not\equiv 0 \pmod p \Leftrightarrow b \leq_p a.$$

LEMMA 4.3. *Given non-negative integers μ and ρ such that $\rho \leq_p \mu$ and given $J = (j_0, \dots, j_n)$ such that $|J| = \mu$, then there exists $I = (i_0, i_1, \dots, i_n)$ with $|I| = \rho$ such that*

$$i_0 \leq_p j_0, \dots, i_n \leq_p j_n.$$

Proof. Suppose by reductio ad absurdum that for all I such that $|I| = \rho$, there exists an integer $s(I)$ such that $0 \leq s(I) \leq n$ and $i_{s(I)} \not\leq_p j_{s(I)}$. It then follows that for all such I there exists $s(I)$ such that

$$\binom{j_{s(I)}}{i_{s(I)}} \equiv 0 \pmod p.$$

From Euler's relation we get that

$$\binom{\mu}{\rho} = \sum_{|I|=\rho} \binom{j_0}{i_0} \dots \binom{j_{s(I)}}{i_{s(I)}} \dots \binom{j_n}{i_n} \equiv 0 \pmod p,$$

whence $\rho \not\leq_p \mu$, a contradiction.

PROPOSITION 4.4. *Suppose that D_{i_0, \dots, i_n} are Hasse differential operators acting on a function space. Assume that for some function f all derivatives of some order ρ are zero, that is,*

$$D_{i_0, \dots, i_n} f = 0, \quad \forall I = (i_0, \dots, i_n); |I| = \rho,$$

then all derivatives of order μ of f are zero if $\mu \geq_p \rho$.

Proof. Suppose that $J = (j_0, \dots, j_n)$ is such that $|J| = \mu$. From Lemma 4.3 there exists $I = (i_0, \dots, i_n)$ with $|I| = \rho$ such that $i_0 \leq_p j_0, \dots, i_n \leq_p j_n$. Since

$$0 = D_{j_0 - i_0, \dots, j_n - i_n} \circ D_{i_0, \dots, i_n} f = \binom{j_0}{i_0} \cdots \binom{j_n}{i_n} D_{j_0, \dots, j_n} f,$$

and $\binom{j_0}{i_0} \cdots \binom{j_n}{i_n} \neq 0$, it follows that $D_{j_0, \dots, j_n} f = 0$.

THEOREM 4.5. *Let $Z: F = 0$ be a projective plane curve of degree d with mild singularities with respect to the pair (d, λ) . If $1 \leq \lambda < p - 1$ and $d \equiv \lambda \pmod{p}$, then the following assertions are equivalent:*

- (i) Z is (d, λ) -non-general
- (ii) $\eta_{Z, \lambda} = p^\alpha$ for some integer $\alpha \geq 1$.
- (iii) There exist homogeneous polynomials $Q_{i_0, i_1, i_2} \in K[X_0, X_1, X_2]$ such that F is of the form

$$F = \sum_{i_0 + i_1 + i_2 = \lambda} X_0^{i_0} X_1^{i_1} X_2^{i_2} Q_{i_0, i_1, i_2}^p.$$

Proof. Since $1 \leq \lambda < p - 1$ and $d \equiv \lambda \pmod{p}$, it follows that λ is a truncation of d , hence from Remark 1 we have that $\eta(d, \lambda) = \lambda + 1 < p$.

(i) \Rightarrow (ii): Since Z is (d, λ) -non-general with mild singularities then from Corollary 3.3 we have, for all $i, j = 0, 1, 2$ and all integers m and n such that $m + n = \lambda + 1$, that

$$D_{X_i}^m \circ D_{X_j}^n F = 0.$$

It follows from Proposition 4.4 that for all $i, j = 0, 1, 2$,

$$D_{X_i}^m \circ D_{X_j}^n F = 0, \quad \forall m, n; m + n \geq_p \lambda + 1.$$

Now, since $\lambda + 1 < p$, we have that the least possible value for $m + n$ with $m + n > \lambda + 1$ such that $D_{X_i}^m \circ D_{X_j}^n F \neq 0$ is p^α for some $\alpha \geq 1$. Hence from Theorem 3.2 we have $\eta_{Z, \lambda} = p^\alpha$.

(ii) \Rightarrow (iii): If $\eta_{Z, \lambda} = p^\alpha$ for some $\alpha \geq 1$, then from Theorem 3.2 we have for all $i, j = 0, 1, 2$,

$$D_{X_i}^m \circ D_{X_j}^n F = 0, \quad \forall m, n; m + n = \lambda + 1.$$

So from Proposition 4.2 we have

$$D_{i_0, i_1, i_2} F = 0, \quad \forall i_0, i_1, i_2; i_0 + i_1 + i_2 = \lambda + 1.$$

Hence for all i_0, i_1, i_2 such that $i_0 + i_1 + i_2 = \lambda$, and for all $i = 0, 1, 2$, we have

$$D_{X_i}^1(D_{i_0, i_1, i_2} F) = 0.$$

So $D_{i_0, i_1, i_2} F$, with $i_0 + i_1 + i_2 = \lambda$, is of the form Q_{i_0, i_1, i_2}^p . Now from the generalized Euler's relation we get that

$$F = \sum_{i_0+i_1+i_2=\lambda} (D_{i_0, i_1, i_2} F) X_0^{i_0} X_1^{i_1} X_2^{i_2} = \sum_{i_0+i_1+i_2=\lambda} Q_{i_0, i_1, i_2}^p X_0^{i_0} X_1^{i_1} X_2^{i_2}.$$

(iii) \Rightarrow (i): From Theorem 3.2 we have that (iii) implies that $\eta_{Z, \lambda} \geq p$. Then

$$\eta_{Z, \lambda} \geq p > \lambda + 1 = \eta(d, \lambda),$$

so Z is (d, λ) -non-general.

Remark 6. Example 2 shows us that (i) may not imply (ii) if $\eta(d, \lambda) \geq p$.

5. THE FUNCTION $\eta(d, \lambda)$

DEFINITION. We define the integral function $\mu(d, \lambda)$ as

$$\mu(d, \lambda) = \max \left\{ \mu \left| \binom{d-1}{\lambda-1} \equiv \binom{d-r}{\lambda-r} \pmod p, \forall r, 1 \leq r \leq \mu \right. \right\}.$$

It is clear that we have

$$\eta(d, \lambda) = \mu(d, \lambda) + 1.$$

In this section we will study the function $\mu(d, \lambda)$, and consequently the function $\eta(d, \lambda)$. We introduce the notation $a^{(l)}$ to denote the truncation of the p -adic expansion of $a = a_0 + a_1 p + \dots$ up to order l , that is,

$$a^{(l)} = a_0 + a_1 p + \dots + a_l p^l.$$

LEMMA 5.1. *Let a, b, α, β , and γ be positive integers.*

(i) *If $a \leq p^\gamma$ and $b \leq p^\gamma$, then*

$$\begin{pmatrix} \alpha p^\gamma - a \\ \beta p^\gamma - b \end{pmatrix} \equiv (-1)^{b-a} \begin{pmatrix} \alpha - 1 \\ \beta - 1 \end{pmatrix} \begin{pmatrix} b - 1 \\ a - 1 \end{pmatrix} \pmod p$$

(ii) $\mu(\alpha p^\gamma, \beta p^\gamma) = p^\gamma \mu(\alpha, \beta)$.

Proof. (i) First note that it is easy to prove by induction on a , observing that the case $a = 1$ is Wilson's Theorem, that

$$(p-1)!(a-1)! \equiv (-1)^a \pmod{p}.$$

Using this and proceeding by induction on γ , the case $\alpha = \beta = 1$ is proved. The general statement follows from observing that from the fundamental congruence we have

$$\begin{pmatrix} \alpha p^\gamma - a \\ \beta p^\gamma - b \end{pmatrix} \equiv \begin{pmatrix} (\alpha-1)p^\gamma + p^\gamma - a \\ (\beta-1)p^\gamma + p^\gamma - b \end{pmatrix} \equiv \begin{pmatrix} \alpha-1 \\ \beta-1 \end{pmatrix} \begin{pmatrix} p^\gamma - a \\ p^\gamma - b \end{pmatrix}.$$

(ii) This follows from (i) and from the fundamental congruence.

From now on, d and λ will be integers such that $1 \leq \lambda < d$, and p^s (respectively p^t) will be the highest power of p that divides λ (respectively d).

Remark 7. It is easy to verify that the condition

$$\begin{pmatrix} d-1 \\ \lambda-1 \end{pmatrix} \not\equiv 0 \pmod{p} \tag{19}$$

is equivalent to

- (a) $s < t$, $\lambda_i < d_i$, and $\lambda_i \leq d_i$, $\forall i \geq t+1$, or
- (b) $s = t$ and $\lambda_i \leq d_i$, $\forall i \geq t$.

Note that when $d_0 \neq 0$, then $t = 0$ and necessarily we are in case (b), hence in such case we have that condition (19) is equivalent to $\lambda \leq_p d$.

PROPOSITION 5.2. *Let d and λ be integers such that $1 \leq \lambda < d$, and suppose that $\binom{d-1}{\lambda-1} \not\equiv 0 \pmod{p}$. Then we have*

- (i) *If $\mu(d, \lambda) > 1$ then $d \equiv \lambda \pmod{p}$.*
- (ii) *Suppose that $d \equiv \lambda \pmod{p}$. If $l = \max\{i \mid d^{(i)} = \lambda^{(i)}\}$, then we have*

$$\mu(d, \lambda) = \begin{cases} d^{(l)} & \text{if } d^{(l)} \neq 0 \\ p^{l+1} & \text{if } d^{(l)} = 0. \end{cases}$$

Proof. (i) Remark that $\mu(d, \lambda) > 1$ is equivalent to $\binom{d-1}{\lambda-1} \equiv \binom{d-2}{\lambda-2} \pmod{p}$, which in turn is equivalent to $\binom{d-2}{\lambda-1} \equiv 0 \pmod{p}$.

Case $d_0 = 0$. If $\lambda_0 \geq 1$, then we have

$$\binom{d-2}{\lambda-1} \equiv \binom{p-2}{\lambda_0-1} \binom{p-1}{\lambda_1} \cdots \binom{p-1}{\lambda_{t-1}} \binom{d_t-1}{\lambda_t} \binom{d_{t+1}}{\lambda_{t+1}} \cdots$$

which is not congruent to zero mod p in view of Remark 7. So $\lambda_0 = d_0$.

Case $d_0 \neq 0$. From Remark 7 we have that $\lambda_0 \neq 0$ and $\lambda \leq_p d$, hence $0 < \lambda_0 \leq d_0$. So if $d_0 = 1$, we have that $\lambda_0 = 1$. If $d_0 \geq 2$, then $d_0 - 2 < \lambda_0 - 1$, hence $d_0 < \lambda_0 + 1$, and therefore $d_0 = \lambda_0$.

(ii) Suppose that $d \equiv \lambda \pmod p$, and write $d = d^{(l)} + \alpha p^{l+1}$ and $\lambda = \lambda^{(l)} + \beta p^{l+1}$.

Case $d^{(l)} = \lambda^{(l)} \neq 0$. From Lemma 5.1(i) and from the fundamental congruence we have, for all r with $1 \leq r \leq d^{(l)}$, that

$$\binom{d-r}{\lambda-r} \equiv \binom{\alpha}{\beta} \binom{\lambda^{(l)}-r}{d^{(l)}-r} = \binom{\alpha}{\beta}.$$

Now, since from Remark 7 we have that $\lambda_i \leq d_i$, for all $i \geq l + 1$, then from the definition of l it follows that $\lambda_{l+1} < d_{l+1}$ and hence

$$\binom{\alpha-1}{\beta} = \binom{(d_{l+1}-1) + pd_{l+2} + \cdots}{\lambda_{l+1} + p\lambda_{l+2} + \cdots} \not\equiv 0 \pmod p.$$

It then follows from Stifel's relation and from Lemma 5.1(i) that

$$\binom{d-d^{(l)}-1}{\lambda-d^{(l)}-1} \equiv \binom{\alpha-1}{\beta-1} \not\equiv \binom{\alpha}{\beta} \equiv \binom{d-d^{(l)}}{\lambda-d^{(l)}} \pmod p,$$

hence $\mu(d, l) = d^{(l)}$.

Case $d^{(l)} = \lambda^{(l)} = 0$. From Lemma 5.1(ii) we have that

$$\mu(d, \lambda) = \mu(\alpha p^{l+1}, \beta p^{l+1}) = p^{l+1} \mu(\alpha, \beta).$$

Since $\binom{d-1}{\lambda-1} \not\equiv 0$, it follows from Lemma 5.1(i) that $\binom{\alpha-1}{\beta-1} \not\equiv 0$, and from the definition of l we have that $\alpha \not\equiv \beta \pmod p$, so from (i) we have that $\mu(\alpha, \beta) = 1$, from which the result follows.

PROPOSITION 5.3. *Let d and λ be integers such that $1 \leq \lambda < d$, and $\binom{d-1}{\lambda-1} \equiv 0 \pmod p$. Then we have*

$$\mu(d, \lambda) = \begin{cases} d^{(m)}, & \text{if } \lambda \not\leq_p d \\ d^{(s-1)}, & \text{if } \lambda \leq_p d \end{cases}$$

with $m = \max\{i | d^{(i)} < \lambda^{(i)}\}$, and p^s the highest power of p that divides λ .

Proof. Case $\lambda \not\equiv_p d$. Writing $d = d^{(m)} + \alpha p^{m+1}$ and $\lambda = \lambda^{(m)} + \beta p^{m+1}$, it follows from the definition of m that $d^{(m)} < \lambda^{(m)}$, $d_{m+1} > \lambda_{m+1}$, and $\alpha \geq_p \beta$.

First of all let us observe that $d^{(m)} \neq 0$. This is so because otherwise we would have as a consequence of $d_{m+1} > \lambda_{m+1}$ that

$$\begin{pmatrix} d-1 \\ \lambda-1 \end{pmatrix} \equiv \begin{pmatrix} p^{m+1}-1 \\ \lambda^{(m)}-1 \end{pmatrix} \begin{pmatrix} \alpha-1 \\ \beta \end{pmatrix} \neq 0.$$

Now, for all r such that $1 \leq r \leq d^{(m)}$, since $d^{(m)} < \lambda^{(m)}$, it follows that

$$\begin{pmatrix} d-r \\ \lambda-r \end{pmatrix} \equiv \begin{pmatrix} d^{(m)}-r \\ \lambda^{(m)}-r \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv 0.$$

On the other hand,

$$\begin{pmatrix} d-(d^{(m)}+1) \\ \lambda-(d^{(m)}+1) \end{pmatrix} \equiv \begin{pmatrix} p^{m+1}-1 \\ \lambda^{(m)}-d^{(m)}-1 \end{pmatrix} \begin{pmatrix} \alpha-1 \\ \beta \end{pmatrix} \neq 0,$$

hence in this case we have $\mu(d, \lambda) = d^{(m)}$.

Case $\lambda \leq_p d$. In this case the hypotheses imply that $s > t \geq 0$, hence $d^{(s-1)} \neq 0$. Write $d = d^{(s-1)} + \alpha p^s$ and $\lambda = \beta p^s$.

Now, since $d^{(d-1)} < p^s$, we have for all r , such that $1 \leq r \leq d^{(s-1)}$, that

$$\begin{pmatrix} d-r \\ \lambda-r \end{pmatrix} \equiv \begin{pmatrix} d^{(s-1)}-r \\ p^s-r \end{pmatrix} \begin{pmatrix} \alpha \\ \beta-1 \end{pmatrix} \equiv 0.$$

On the other hand,

$$\begin{pmatrix} d-(d^{(s-1)}+1) \\ \lambda-(d^{(s-1)}+1) \end{pmatrix} \equiv \begin{pmatrix} p^s-1 \\ p^s-d^{(s-1)}-1 \end{pmatrix} \begin{pmatrix} \alpha-1 \\ \beta-1 \end{pmatrix} \neq 0,$$

hence in this case we have $\mu(d, \lambda) = d^{(s-1)}$.

COROLLARY 5.4. For any pair (d, λ) of positive integers with $1 \leq \lambda < d$, we have that

$$\mu(d, \mu(d, \lambda)) = \mu(d, \lambda).$$

Proof. This follows from Propositions 5.2 and 5.3 by a direct verification.

PROPOSITION 5.5. For any pair (d, λ) of positive integers with $1 \leq \lambda < d$, we have that

$$\mu(d, d-\lambda) = \mu(d, \lambda).$$

Proof. The proof of this result is elementary and may be done using the definition of $\mu(d, \lambda)$ and twice Stifel’s relation. Alternatively, this can be proved using Propositions 5.2 and 5.3.

COROLLARY 5.6. *Let Z be a plane projective curve of degree d and let λ be an integer such that $1 \leq \lambda < d$. Then*

- (i) Z is (d, λ) -general if and only if Z is $(d, d - \lambda)$ -general.
- (ii) If Z has mild singularities, and λ is a truncation of d , then

$$\eta_{Z, d-\lambda} \geq \eta_{Z, \lambda}.$$

Proof. (i) is a consequence of Theorem 2.5 and Proposition 5.5, while (ii) is a consequence of Corollary 3.4(ii) and of Proposition 5.5.

6. STATIONARY POINTS

Let $Z : F = 0$ be a projective irreducible plane curve of degree d . Let λ be an integer such that $1 \leq \lambda < d$ and some mixed derivative of F of order λ is nonzero.

DEFINITION. A point $P \in Z$ will be called λ -stationary if

$$I(P, Z, \Delta_P^\lambda Z) > \eta_{Z, \lambda}.$$

By the very definition of $\eta_{Z, \lambda}$ we have that there are finitely many such points, and the aim of this section is to determine their number. We will compute this number when either Z is (d, λ) -general, or when λ is a truncation of d , and Z has mild singularities with respect to the pair (d, λ) . We will make this assumption from now on in this section.

For any integer ρ and distinct integers, $i, j, k = 0, 1, 2$, we define for $i < j$,

$$\mathcal{S}_k^{(\rho)} = \sum_{r=0}^{\rho} (D_{X_i}^r \circ D_{X_j}^{\rho-r} F)(F_{X_j})^r (-F_{X_i})^{\rho-r}.$$

Note that from the arguments we used in the proof of Theorem 2.5, and from Remark 5 and Proposition 3.1, we have that $P \in Z$ is a λ -stationary point if and only if $\mathcal{S}_k^{(\eta_{Z, \lambda})}(P) = 0$, for all $k = 0, 1, 2$.

Remark that from the above definition we have that all singular points of Z are stationary points.

To establish the main result of this section, namely Theorem 6.7, we will need several auxiliary results.

LEMMA 6.1. *Let a be an integer. If b is minimal among the integers greater than a but not p -adically greater, then there exists some $r \geq 1$ such that*

$$b = a - a^{(r-1)} + p^r.$$

Proof. Let $a = a_s p^s + a_{s+1} p^{s+1} + \dots + a_n p^n$, with $a_s \neq 0$, be the p -adic expansion of a . It is clear that the first integer greater than a which is not p -adically greater than a is

$$b_0 = (a_{s+1} + 1) p^{s+1} + \dots + a_n p^n = a - a^{(s)} + p^{s+1}.$$

Now we can restrict our search to the integers which are greater than b_0 but not p -adically greater, and the result follows clearly.

PROPOSITION 6.2. *Let Z be a projective irreducible plane curve of degree d , and let $\lambda = d^{(l)}$ for some l . Suppose that Z is not (d, λ) -general and with mild singularities, then we have for some r ,*

$$\eta_{Z, \lambda} = d^{(l)} - d^{(r-1)} + p^r. \quad (20)$$

Proof. Since λ is a truncation of d , we have from Remark 5 that

$$\eta_{Z, \lambda} = \min\{\nu \geq \lambda + 1 \mid S(\nu)\}.$$

Now, in view of Proposition 4.4, $\eta_{Z, \lambda}$ must be an integer greater than $\eta(d, \lambda) = \lambda + 1$, but not p -adically greater than $\lambda + 1$, and minimal with respect to the p -adic ordering. So from Lemma 6.1 we have that

$$\eta_{Z, \lambda} = (\lambda + 1) - (\lambda + 1)^{(r-1)} + p^r$$

for some r , and the proposition follows.

COROLLARY 6.3. *Let $Z:F = 0$ be a plane projective irreducible curve of degree d and $\lambda = d^{(l)}$ for some l . If Z is not (d, λ) -general, with mild singularities, then $\eta_{Z, \lambda} \equiv 0 \pmod{p}$.*

LEMMA 6.4. *If (d, λ) is a pair of integers such that $1 \leq \lambda < d$, then we have*

$$\binom{d-s}{\eta(d, \lambda) - s} \equiv 0 \pmod{p} \quad \forall s; s = 2, \dots, \eta(d, \lambda) - 1.$$

Proof. From Stifel's relation we have that

$$\binom{d-s}{\eta(d, \lambda) - s} + \binom{d-s}{\mu(d, \lambda) - s} = \binom{d - (s-1)}{\mu(d, \lambda) - (s-1)}. \quad (21)$$

Now, from Corollary 5.4 it follows that

$$\binom{d-1}{\mu(d, \lambda) - 1} \equiv \binom{d-2}{\mu(d, \lambda) - 2} \equiv \dots \equiv \binom{d - \mu(d, \lambda)}{\mu(d, \lambda) - \mu(d, \lambda)}.$$

From this and from (21), we get that

$$\binom{d-s}{\eta(d, \lambda) - s} \equiv 0 \pmod p, \quad s = 2, \dots, \eta(d, \lambda) - 1.$$

LEMMA 6.5. *Let d and λ be integers such that $1 \leq \lambda < d$. If λ is a truncation of d , and $\eta_{Z, \lambda}$ is as in (20), then*

$$\binom{d-s}{\eta_{Z, \lambda} - s} \equiv 0 \pmod p, \quad s = 2, \dots, \lambda.$$

Proof. Suppose that $\lambda = d^{(l)}$ for some $l \geq 0$, and let $\eta_{Z, \lambda} = d^{(l)} - d^{(r-1)} + p^r$, for some r with $1 \leq r \leq l + 1$. We will initially suppose that $r < l + 1$. From the fundamental congruence we get, for all $s = 0, \dots, d^{(l)}$, that

$$\binom{d-s}{\eta_{Z, \lambda} - s} = \binom{d^{(l)} + \alpha p^{l+1} - s}{d^{(l)} - d^{(r-1)} + p^r - s} \equiv \binom{d^{(l)} - s}{d^{(l)} - d^{(r-1)} + p^r - s} \equiv 0.$$

Suppose now that $r = l + 1$, then $\eta_{Z, \lambda} = p^r$, and from the fundamental congruence we have for $s \geq 1$ that

$$\binom{d-s}{p^r - s} = \binom{d^{(r-1)} + \beta p^r - s}{p^r - s} \equiv \binom{d^{(r-1)} - s}{p^r - s} = 0.$$

PROPOSITION 6.6. *Let $Z : F = 0$ be a projective irreducible plane curve of degree d and let λ be an integer such that $1 \leq \lambda < d$. Suppose that either Z is (d, λ) -general, or Z has mild singularities and λ is a truncation of d , then we have for $\eta = \eta_{Z, \lambda}$, and for all integers $i, j = 0, 1, 2$, that*

$$X_j^\eta \mathcal{S}_i^{(\eta)} \equiv X_i^\eta \mathcal{S}_j^{(\eta)} \pmod F.$$

Proof. If $i = j$, there is nothing to prove. We will only prove the case $j = 0$ and $i = 2$, since the other cases are similar.

Let $P = (a_0, a_1, a_2) \in K^3$. From Lemma 2.4(ii) we have

$$\begin{aligned} X_0^\eta(\Delta_P^\eta F) & \left(1, \frac{X_1}{X_0}, \frac{X_2}{X_0}\right) \\ &= a_0^{-\eta} \sum_{r=0}^{\eta} X_0^{\eta-r} \binom{d-r}{\eta-r} \\ & \quad \times \sum_{\alpha+\beta=r} (D_{0,\alpha,\beta} F)(P) (a_0 X_1 - a_1 X_0)^\alpha (a_0 X_2 - a_2 X_0)^\beta, \end{aligned}$$

and

$$\begin{aligned} X_2^\eta(\Delta_P^\eta F) & \left(\frac{X_0}{X_2}, \frac{X_1}{X_2}, 1\right) \\ &= a_2^{-\eta} \sum_{s=0}^{\eta} X_2^{\eta-s} \binom{d-s}{\eta-s} \\ & \quad \times \sum_{\gamma+\delta=s} (D_{\gamma,\delta,0} F)(P) (a_2 X_0 - a_0 X_2)^\gamma (a_2 X_1 - a_1 X_2)^\delta. \end{aligned}$$

Now, since obviously

$$X_0^\eta(\Delta_P^\eta F) \left(1, \frac{X_1}{X_0}, \frac{X_2}{X_0}\right) = X_2^\eta(\Delta_P^\eta F) \left(\frac{X_0}{X_2}, \frac{X_1}{X_2}, 1\right),$$

we get by comparing the coefficients of $X_1^t X_2^{\eta-t}$ of both expressions that

$$\begin{aligned} D_{0,t,\eta-t} F(P) &= a_2^{-\eta} \sum_{s=0}^{\eta} \binom{d-s}{\eta-s} \\ & \quad \times \sum_{\gamma+\delta=s} (D_{\gamma,\delta,0} F)(P) (-a_0)^\gamma \binom{\delta}{t} a_2^t (-a_1)^{\delta-t}. \end{aligned}$$

Now, from the above expression, Lemmas 6.4 and 6.5, and Theorem 3.2, we have that

$$\begin{aligned} X_2^\eta D_{0,t,\eta-t} F &= \binom{d}{\eta} \binom{0}{t} X_2^t (-X_0)^{-t} F + \binom{d-1}{\eta-1} \\ & \quad \times \left[\binom{0}{t} (-X_0) (-X_1)^{-t} X_2^t F_{X_0} + \binom{1}{t} (-X_1)^{1-t} X_2^t F_{X_1} \right] \\ & \quad + \sum_{\gamma+\delta=\eta} \binom{\delta}{t} (D_{\gamma,\delta,0} F) (-X_0)^\gamma X_2^t (-X_1)^{\delta-t}. \end{aligned}$$

Using Euler’s identity and the above one, we get the following equalities and congruences mod F ,

$$\begin{aligned}
 X_0^\eta \mathcal{S}_2^{(\eta)} &= \sum_{\gamma+\delta=\eta} (D_{X_0}^\gamma \circ D_{X_1}^\delta F) X_0^\gamma (-X_0 F_{X_0})^\delta (F_{X_1})^\gamma \\
 &\equiv \sum_{\gamma+\delta=\eta} (D_{X_0}^\gamma \circ D_{X_1}^\delta F) X_0^\gamma (X_1 F_{X_1} + X_2 F_{X_2})^\delta (F_{X_1})^\gamma \\
 &= \sum_{\gamma+\delta=\eta} \sum_{t=0}^\eta \binom{\delta}{t} (D_{\gamma, \delta, 0} F) (-X_0)^\gamma (-X_1)^{\delta-t} \\
 &\quad \times X_2^t (-F_{X_1})^{\eta-t} (F_{X_2})^t \\
 &\equiv \sum_{t=0}^\eta (X_2^\eta D_{0,t,\eta-t} F) (-F_{X_1})^{\eta-t} (F_{X_2})^t - \binom{d-1}{\eta-1} \\
 &\quad \times \left[(-X_0) F_{X_0} (-F_{X_1})^\eta + (-X_1) F_{X_1} (-F_{X_1})^\eta \right. \\
 &\quad \quad \left. + X_2 F_{X_1} (-F_{X_1})^{\eta-1} F_{X_2} \right] \\
 &\equiv X_2^\eta \sum_{t=0}^\eta (D_{X_1}^t \circ D_{X_2}^{\eta-t} F) (-F_{X_1})^{\eta-t} (F_{X_2})^t = X_2^\eta \mathcal{S}_0^{(\eta)}.
 \end{aligned}$$

Remark 8. The above proposition tells us that the data

$$\left\{ \left(U_\alpha, \frac{\mathcal{S}_\alpha^{(\eta)}}{X_\alpha^\eta} \right) \right\}_{\alpha=0,1,2},$$

where $U_\alpha = \{(X_0; X_1; X_2) | X_\alpha \neq 0\}$, define a section of the fiber bundle $\mathcal{O}_Z(d(\eta + 1) - 3\eta)$, whose zeros are the stationary points of Z with respect to (d, λ) .

DEFINITION. We define the λ -weight of P as being the order of vanishing $w(P)$ at P of the above section. So $P \in Z$ is a λ -stationary point if and only if $w(P) > 0$.

THEOREM 6.7. Let $Z : F = 0$ be a projective irreducible plane curve of degree d and let λ be an integer such that $1 \leq \lambda < d$. Suppose that either Z is (d, λ) -general, or Z has mild singularities and λ is a truncation of d ; then we have, for $\eta = \eta_{Z, \lambda}$, that

$$\sum_{P \in Z} w(P) = d[d(\eta + 1) - 3\eta].$$

Proof. This follows immediately from the above remark, and from the definition of $w(P)$.

Remark 9. The method of proof of the above theorem is inspired from [4], where the result is proved for $\lambda = 1$. Observe that if a curve Z of degree d is reflexive, then it is $(d, 1)$ -general. And if Z is smooth and $(d, 1)$ -non-general, then $d \equiv 1 \pmod{p}$ (see for example [3] or [7]), then 1 is a truncation of d , so that Theorem 6.7 gives us the classical formula for the weighted number of flexes of a non-singular plane curve Z of degree d . Namely,

$$f = d[d(\varepsilon_2 + 1) - 3\varepsilon_2],$$

where ε_2 is the intersection multiplicity of the curve with its tangent line at a general point, or alternatively, the inseparable degree of the dual map of the curve. (see for example [10] and [6] or [9]).

Remark also that in characteristic zero, a point is λ -stationary if and only if it is a flex, so in this case we are just counting the flexes.

7. POLAR MORPHISMS

Let $Z : F = 0$ be an irreducible smooth plane curve of degree d , and let λ be an integer such that $1 \leq \lambda < d$, and suppose that some mixed derivative of F of order λ is nonzero. Let $N_\lambda = \lambda(\lambda + 3)/2$.

DEFINITION. The λ th polar morphism is the morphism defined by

$$\begin{aligned} p_\lambda : Z &\rightarrow \mathbb{P}_K^{N_\lambda} \\ P &\mapsto (D_{i_0, i_1, i_2} F(P); i_0 + i_1 + i_2 = \lambda) \end{aligned}$$

We will denote the image of p_λ by Z_λ .

So for $\lambda = 1$, we have that p_λ is the Gauss map and Z_λ is the dual curve of Z .

We will also denote by v_λ the Veronese λ -uple embedding,

$$\begin{aligned} v_\lambda : \mathbb{P}_K^2 &\rightarrow (\mathbb{P}_K^{N_\lambda})^* \\ Q &\mapsto (Q_0^{i_0} Q_1^{i_1} Q_2^{i_2}; i_0 + i_1 + i_2 = \lambda). \end{aligned}$$

THEOREM 7.1. Let Z be a smooth curve of degree d , and let λ be an integer such that $1 \leq \lambda < d$. Then we have

$$\deg(p_\lambda) \deg(Z_\lambda) = d(d - \lambda).$$

Proof. We will denote by $\deg_s(p_\lambda)$ (respectively, $\deg_i(p_\lambda)$) the separable (respectively, inseparable) degree of p_λ .

Let $P_1, \dots, P_r \in Z$ be the points such that

$$U = Z_\lambda \setminus \{p_\lambda(P_1), \dots, p_\lambda(P_r)\}$$

is the open set of points R for which

$$\#p_\lambda^{-1}(R) = \deg_s(p_\lambda).$$

Let Q be a point of \mathbb{P}_K^2 , and consider the hyperplane H_Q in $\mathbb{P}_K^{N_\lambda}$ whose coefficients are the coordinates of the point $v_\lambda(Q) \in (\mathbb{P}_K^{N_\lambda})^*$. So

$$H_Q: \sum_{i_0+i_1+i_2=\lambda} Q_0^{i_0} Q_1^{i_1} Q_2^{i_2} Z_{i_0, i_1, i_2} = 0,$$

where Z_{i_0, i_1, i_2} are the coordinate functions of $\mathbb{P}_K^{N_\lambda}$.

For Q general in \mathbb{P}_K^2 we have that

$$H_Q \cap Z_\lambda \subset U,$$

because the above condition means that the general point Q of \mathbb{P}_K^2 is not a zero of any of the nonzero polynomials $\Delta_{P_i}^\lambda F$, for $i = 1, \dots, r$.

Now, from standard ramification theory and from Lemma 2.1(i) we have that

$$\deg_i(p_\lambda) I(p_\lambda(P), H_Q \cap Z_\lambda) = I(P, Z \cap \Delta_-^\lambda F(Q)) = I(P, Z \cap \Delta_Q^{d-\lambda} Z),$$

where

$$\Delta_-^\lambda F(Q) = \sum_{i_0+i_1+i_2=\lambda} Q_0^{i_0} Q_1^{i_1} Q_2^{i_2} D_{i_0, i_1, i_2} F(X_0, X_1, X_2).$$

Now, from Bézout's Theorem we have

$$\begin{aligned} d(d-\lambda) &= \sum_{P \in Z} I(P, Z \cap \Delta_Q^{d-\lambda} Z) = \deg_i(p_\lambda) \sum_{P \in Z} I(p_\lambda(P), H_Q \cap Z_\lambda) \\ &= \deg_i(p_\lambda) \deg_s(p_\lambda) \sum_{R \in Z_\lambda} I(R, H_Q \cap Z_\lambda) = \deg(p_\lambda) \deg(Z_\lambda). \end{aligned}$$

The above theorem is a generalization of Plücker's formula, which was known for $\lambda = 1$, relating the degree of a curve with that of the Gauss map and of the dual curve.

REFERENCES

1. E. Ballico and A. Hefez, Non-reflexive projective curves of low degree, *Manuscripta Math.* **70** (1991), 385–396.

2. J. L. Coolidge, "A Treatise on Algebraic Plane Curves," 1931; Dover, New York, 1959.
3. A. Hefez, Non-reflexive curves, *Compositio Math.* **69** (1989), 3–35.
4. A. Hefez, "Introdução à geometria projetiva," Monografias de Matemática, Vol. 46, IMPA, 1991.
5. A. Hefez and N. Kakuta, New bounds for Fermat curves over finite fields, in "Proc. Zeuthen Symp.," Contemporary Math., Vol. 123, pp. 89–97, Amer. Math. Soc., Providence, RI, 1991.
6. D. Laksov, Wronskians and Plücker formulas for linear systems on curves, *Ann. Sci. Écol. Norm. Sup.* **17** (1984), 45–66.
7. R. Pardini, Some remarks on plane curves over fields of finite characteristic, *Compositio Math.* **60** (1986), 3–17.
8. G. Salmon, "A Treatise on the Higher Plane Curves," 3rd ed., Chelsea, New York.
9. K. O. Stöhr, and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* (3) **52** (1986), 1–19.
10. R. Walker, "Algebraic Curves," Princeton Univ. Press, Princeton, NJ, 1950.