Houston Journal of Mathematics
© 2021 University of Houston
Volume 47, No. 3, 2021

# BIVARIATE TRINOMIALS OVER FINITE FIELDS

MARTIN AVENDANO AND JORGE MARTÍN-MORALES

Communicated by J. Maurice Rojas

Abstract. We study the number of points in the family of plane curves defined by a trinomial with fixed exponents and varying coefficients over finite fields. We prove that each of these curves has an almost predictable number of points, given by a closed formula that depends on the coefficients, the exponents, and the field, with a small error term for which we provide an upper bound in terms of an analog of the genus and the size of the field. We obtain these upper bounds from some linear and quadratic identities that the error terms satisfy. These identities are, in some cases, strong enough to determine the error terms completely.

## 1. Introduction

The main goal of this paper is to study the number of points in the family of plane curves defined by a trinomial

$$\mathcal{C}(\alpha,\beta)=\{(x,y)\in\mathbb{F}_q^2\,:\,\alpha x^{a_{11}}y^{a_{12}}+\beta x^{a_{21}}y^{a_{22}}=x^{a_{31}}y^{a_{32}}\}$$

with fixed exponents (not collinear) and varying coefficients over a finite field $\mathbb{F}_q$.

We prove that each of these curves has an almost predictable number of points, given by a closed formula that depends on the coefficients, exponents, and the field, with a small error term $N(\alpha,\beta)$ that is bounded in absolute value by $2\tilde{g}q^{1/2}$, where $\tilde{g}$ is a constant that depends only on the exponents and the field. A formula for $\tilde{g}$ is provided, as well as a comparison of $\tilde{g}$ with the genus $g$ of the projective

2010 *Mathematics Subject Classification.* 11T06; 11H50; 11C08.

*Key words and phrases.* Plane curves; Finite fields.

Both authors are partially supported by MTM2016-76868-C2-2-P and CUD-2020_08. The second author is also supported by Gobierno de Aragón (Grupo de referencia "Álgebra y Geometría" E22_17R and E22_20R) cofunded by Feder 2014-2020 "Construyendo Europa desde Aragón", and FQM-333 from Junta de Andalucía.

closure of the curve over $\overline{\mathbb{F}}_q$. We also give several linear and quadratic identities for the numbers $N(\alpha, \beta)$ that are strong enough to prove the estimate above, and in some cases, to characterize them completely.

The main result in this article is inspired by Theorem 1.1 given below, proven by Gauss in his book Disquisitiones Arithmeticae [5, Theorem 358]. We have used a mildly rephrased version of the original theorem, taken from [9, p. 111], that better matches our more modern notation.

**Theorem 1.1** (Gauss). *Let $p$ be an odd prime and let $M_p$ be the number of points in the projective curve $\{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_p) : x^3 + y^3 + z^3 = 0\}$.*

(1) *If $p \not\equiv 1 \pmod 3$, then $M_p = p + 1$.*

(2) *If $p \equiv 1 \pmod 3$, then the equation $u^2 + 27\bar{v}^2 = 4p$ has a unique integer solution (up to the signs), and if $u$ is chosen such that $u \equiv 1 \pmod 3$, then $M_p = p + 1 + u$.*

In a few words, Gauss' theorem says that the number of (projective) points in the plane curve $x^3 + y^3 + z^3 \equiv 0 \pmod p$ is $p + 1$ plus a small error term $u$ (that only appears when $p \equiv 1 \pmod 3$) which is characterized by the quadratic equation $u^2 + 27\bar{v}^2 = 4p$ with integral unknowns. Our main result (Theorem 2.1) is a generalization of Gauss' theorem to any non-degenerate trinomial equation in two variables, over any finite field, where we show that the number of points is a predictable number (given by a closed formula in terms of the coefficients, exponents, and the field) plus an error term which also satisfies an explicit quadratic equation in many unknowns, all of them having a precise meaning (as opposed to Gauss' theorem, where only the variable $u$ matters). More precisely, our result gives, in the case $p \equiv 1 \pmod 3$, that $M_p = p + 1 + u$, where $u^2 + v^2 + uv = 3p$ for some $u, v \in \mathbb{Z}$. The symmetry of the curve allows one to rewrite it as $u^2 + 27\bar{v}^2 = 4p$, where $\bar{v} = \frac{2v+u}{9} \in \mathbb{Z}$ and to show that $u \equiv 1 \pmod 3$. All the details are given in Section 4.

Note that Gauss' theorem implies that the error term $u$ is bounded in absolute value by $2\sqrt{p}$. This observation was generalized by Hasse to elliptic curves over finite fields [8, Chapter 5, Theorem 1.1], then by Weil to hypersurfaces defined by an equation of the type $\alpha_0 x_0^{a_0} + \alpha_1 x_1^{a_1} + \cdots + \alpha_r x_r^{a_r} = b$ [13], which led to the statement of the famous Weil's conjectures, finally proven by Dwork [4], Grothendieck [6], and Deligne [3] for any smooth hypersurface.

Using our approach, the estimate of the error follows from a simple computation using Lagrange multipliers (see Proposition 3.4). In contrast with the results above, our proof is elementary and the estimate is valid for any trinomial (not necessarily smooth). Moreover, our estimate $2\tilde{g}q^{1/2}$ (see Corollary 2.2) is better that the bound obtained from Weil's conjectures $2gq^{1/2}$, since the genus $g$ is an invariant that only reflects the complex geometry of the curve, while our $\tilde{g}$ includes also information about the field. In Section 5, we obtain a closed formula for the genus $g$ of a trinomial plane curve (see Proposition 5.2), that can be compared term by term with the definition of $\tilde{g}$ given in (1). For instance, in the case of Gauss' theorem, the curve has genus $g = 1$, but our $\tilde{g}$ is zero when $p \not\equiv 1 \pmod 3$, hence capturing both cases of the statement in a unified way.

A bound for trinomials (of the same type studied by Weil), that closely resembles ours, was obtained by Hua and Vandiver [7]. However, their result follows from estimates using characters, while ours is a consequence of a quadratic optimization problem over $\mathbb{R}$. Some experiments show that a much better estimate could be computed if we were able to solve the optimization problem over the integers (see Example 3).

In [12], Wang, Wen, and Cao give formulas for the number of points in a family of hypersurfaces related to the curves $\mathcal{C}(\alpha, \beta)$. However, while they work in arbitrary dimension, their formulas have more stringent assumption than ours on the exponent vectors.

In [10], Wan approaches a bigger problem than ours (the computation of the zeta functions and $L$-functions for arbitrary hypersurfaces). In Section 2, he gives a method to do this computations in the case of diagonal hypersurfaces. While it might be possible to rederive our formulas from his framework, our approach has the advantage of being more direct, explicit, and entirely self-contained.

In [11], Wan gives an algorithm that can be used to compute the number of points in the curves $\mathcal{C}(\alpha, \beta)$ modulo $p^b$ with complexity $O(24^{(n+b)p})$, where $q = p^n$. We do not provide any algorithm in this paper, however, in the case where $\tilde{g} = 0$, the formula in Theorem 2.1 becomes a closed formula since $N_{ij} = 0$ for all $i, j$.

## 2. Statement of the results

Let $p$ be a prime and $q = p^n$ for some $n \geq 1$. Let $\rho$ be a generator of the cyclic group $\mathbb{F}_q^*$. Consider the curve

$$\mathcal{C}_{ij} = \mathcal{C}(\rho^i, \rho^j) = \{(x, y) \in \mathbb{F}_q^2 \,:\, \rho^i x^{a_{11}} y^{a_{12}} + \rho^j x^{a_{21}} y^{a_{22}} = x^{a_{31}} y^{a_{32}}\},$$

and let $\mathcal{C}_{ij}^* = \mathcal{C}_{ij} \cap (\mathbb{F}_q^*)^2$.

To avoid a degenerate case, we assume that the exponents vectors $(a_{11}, a_{12})$, $(a_{21}, a_{22})$, $(a_{31}, a_{32})$ are not collinear, i.e. the matrix

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} := \begin{bmatrix} a_{11} - a_{31} & a_{12} - a_{32} \\ a_{21} - a_{31} & a_{22} - a_{32} \end{bmatrix}$$

is invertible. We need the following constants derived from $B$:

$$\begin{aligned}
d &= \gcd(b_{11}, b_{12}, q-1),\\
e &= \gcd(b_{21}, b_{22}, q-1),\\
f &= \gcd(b_{11}-b_{21}, b_{12}-b_{22}, q-1),\\
k &= \gcd((q-1)\gcd(d,e,f), \det(B)),\\
w &= \begin{cases} 0 & q \text{ even},\\ \frac{q-1}{2} & q \text{ odd},\end{cases}\\
\tilde{g} &= \frac{1}{2}(k-d-e-f+2).
\end{aligned} \tag{1}$$

The value $k$ corresponds to $|\mathrm{coker}(B)|$, where $B$ is regarded as a group homomorphism $B : \mathbb{Z}_{q-1}^2 \to \mathbb{Z}_{q-1}^2$ given by the multiplication $v \mapsto Bv$ (see Lemma 3.3).

Our goal is to estimate the number of points $|\mathcal{C}_{ij}|$ and $|\mathcal{C}_{ij}^*|$ for all $i, j$. Since $\rho^{q-1} = 1$, the indices $i$ and $j$ can be regarded modulo $q-1$.

**Definition 1.** $D_\ell(i) = \begin{cases} \ell & \text{if } \ell \mid i,\\ 0 & \text{otherwise.}\end{cases}$

Note that $|\mathcal{C}_{ij}| = |\mathcal{C}_{ij}^*| + |\mathcal{C}_{ij} \cap \{x=0, y\neq 0\}| + |\mathcal{C}_{ij} \cap \{y=0, x\neq 0\}| + |\mathcal{C}_{ij} \cap \{x=y=0\}|$, and that the points in $\mathcal{C}_{ij} \cap \{x=0, y\neq 0\}$ and $\mathcal{C}_{ij} \cap \{y=0, x\neq 0\}$ correspond to the solutions in $\mathbb{F}_q^*$ of a univariate equation with at most two nonzero terms. Therefore, $|\mathcal{C}_{ij} \cap \{x=0, y\neq 0\}|$ and $|\mathcal{C}_{ij} \cap \{y=0, x\neq 0\}|$ can be computed exactly with a closed formula in terms of $i$, $j$, $q$, and the exponents (see Lemma 3.2). Moreover, $|\mathcal{C}_{ij} \cap \{x=y=0\}|$ is either 1 or 0, depending on whether $a_{11}+a_{12}$, $a_{21}+a_{22}$, and $a_{31}+a_{32}$ are all positive or not. This means that $|\mathcal{C}_{ij}|$ and $|\mathcal{C}_{ij}^*|$ can be easily derived from each other. For this reason, and to avoid discussing several cases depending on the configuration of the exponents, we present our results only for $|\mathcal{C}_{ij}^*|$, which can be done with a more uniform notation.

**Theorem 2.1.** *With the notation given above, we have*

$$|\mathcal{C}_{ij}^*| = q + 1 - D_d(i) - D_e(j) - D_f(i-j+w) + N_{ij} \tag{2}$$

*for some integers $N_{ij}$ that satisfy:*

(1) $\displaystyle\sum_{j=0}^{q-2} N_{ij} = 0$ *for all $i$,*

(2) $\displaystyle\sum_{i=0}^{q-2} N_{ij} = 0$ *for all $j$,*

(3) $\sum_{i-j=r} N_{ij} = 0$ *for all* $r$,

(4) $N_{i+b_{11},j+b_{21}} = N_{ij} = N_{i+b_{12},j+b_{22}}$ *for all* $i, j$,

(5) $\sum_{i=0}^{q-2}\sum_{j=0}^{q-2} N_{ij}^2 = 2\tilde{g}(q-1)^2q = (q-1)^2q(k-d-e-f+2)$.

Using (4), the sum of Theorem 2.1(5) can be rewritten taking only one representative of each $(i,j)$ modulo the subgroup $\langle(b_{11},b_{12}),(b_{21},b_{22})\rangle \subseteq \mathbb{Z}_{q-1}^2$,

$$\sum_{\overline{(i,j)}\in\operatorname{coker}(B)} N_{ij}^2 = 2\tilde{g}kq = kq(k-d-e-f+2) \leq k^2q. \tag{3}$$

We immediately obtain the upper bound $|N_{ij}| \leq k\sqrt{q}$ for all $i,j$. Using a similar approach, but taking advantage of (1), (2), and (3), it is possible to obtain a stronger upper bound.

**Corollary 2.2.** $|N_{ij}| \leq 2\tilde{g}\sqrt{q}$ *for all* $i, j$.

## 3. Proof of the main results

**Lemma 3.1.** *For any* $r \geq 1$,

$$\sum_{i=0}^{q-2} D_\ell(i)^r = \ell^{r-1}(q-1).$$

Proof. By definition of $D_\ell$ we have:

$$\sum_{i=0}^{q-2} D_\ell(i)^r = \sum_{\ell|i} \ell^r = \ell^r \cdot \frac{q-1}{\ell} = \ell^{r-1}(q-1),$$

since the number of indices $0 \leq i < q-1$ that are divisible by $\ell$ is exactly $\frac{q-1}{\ell}$. □

**Lemma 3.2.** *For any* $a_1, \dots, a_m \in \mathbb{Z}$,

$$\left|\left\{(x_1,\dots,x_m) \in (\mathbb{F}_q^*)^m \;:\; \rho^i x_1^{a_1}\cdots x_m^{a_m} = 1\right\}\right| = (q-1)^{m-1}D_\ell(i),$$

*where* $\ell = \gcd(a_1,\dots,a_m,q-1)$.

Proof. Consider the group homomorphism $\varphi : (\mathbb{F}_q^*)^m \to \mathbb{F}_q^*$ given by

$$(x_1,\dots,x_m) \longmapsto x_1^{a_1}\cdots x_m^{a_m}.$$

The image of $\varphi$ is generated by $\rho^{a_1},\dots,\rho^{a_m}$, which is also generated by $\rho^\ell$ since the group $\mathbb{F}_q^*$ is cyclic, and in particular $|\operatorname{im}(\varphi)| = \frac{q-1}{\ell}$. When $\rho^{-i} \notin \langle\rho^\ell\rangle$, i.e. $\ell \nmid i$, the left-hand side and the right-hand side of the equation in the statement are both clearly zero. Otherwise, when $\ell \,|\, i$, the number of solutions is equal to $|\mathrm{coker}(\varphi)| = (q-1)^m/|\mathrm{im}(\varphi)| = (q-1)^{m-1}\ell = (q-1)^{m-1}D_\ell(i)$. □

**Lemma 3.3.** *We have*

(1) $|\mathrm{coker}(B)| = k$.
(2) *The subgroups* $\langle\overline{(1,0)}\rangle$, $\langle\overline{(0,1)}\rangle$, $\langle\overline{(1,1)}\rangle$ *of* $\mathrm{coker}(B)$ *have orders* $\frac{k}{e}$, $\frac{k}{d}$, $\frac{k}{f}$, *respectively.*

Proof. (1) Define the matrix $L = \begin{bmatrix} b_{11} & b_{12} & q-1 & 0 \\ b_{21} & b_{22} & 0 & q-1 \end{bmatrix} \in \mathbb{Z}^{2\times 4}$, which can be regarded as a linear map $L : \mathbb{Z}^4 \to \mathbb{Z}^2$, whose cokernel is

$$\mathrm{coker}(B) = \mathbb{Z}^2_{q-1}/\langle (b_{11}, b_{12}), (b_{21}, b_{22})\rangle \cong \mathbb{Z}^2/\mathrm{im}(L).$$

Note that $|\mathbb{Z}^2/\mathrm{im}(L)|$ is invariant under elementary row or column operations (on $L$). Therefore, we can substitute $L$ by its Smith Normal form, and in particular $|\mathbb{Z}^2/\mathrm{im}(L)|$ is equal to the greatest common divisor of the determinants of the $2\times 2$ minors of $L$, i.e.

$$|\mathrm{coker}(B)| = |\mathbb{Z}^2/\mathrm{im}(L)| = \gcd(\det(B), (q-1)d, (q-1)e) = k.$$

(2) It is enough to show that $|\langle\overline{(1,0)}\rangle| = k/e$, since the other two are analogous. By definition, the order of $\overline{(1,0)}$ is

$$\min\{r \geq 1 \,:\, (r,0) \in \mathrm{im}(L)\} = \min\left\{r \geq 1 \,:\, |\mathrm{coker}(L)| = |\mathrm{coker}([L|\,{}^{r}_{0}])|\right\}.$$

The greatest common divisor of the determinant of the $2\times 2$ minors of the extended matrix $[L|\,{}^{r}_{0}]$ that do not appear in $L$ is $\gcd(r(q-1), rb_{21}, rb_{22}) = re$. Therefore, $|\langle\overline{(1,0)}\rangle| = \min\{r \geq 1 \,:\, k = \gcd(k, re)\} = k/e$. □

Proof of Theorem 2.1. We prove (1), since the proofs of (2) and (3) are analogous. Note that the sets $\mathcal{C}^*_{ij}$ for $j = 0, \ldots, q-2$ are disjoint, thus

$$\begin{aligned}\sum_{j=0}^{q-2} |\mathcal{C}^*_{ij}| = \left|\bigcup_{j=0}^{q-2} \mathcal{C}^*_{ij}\right| &= |\{(x,y) \in (\mathbb{F}^*_q)^2 \,:\, \rho^i x^{a_{11}-a_{31}} y^{a_{12}-a_{32}} \neq 1\}| \\ &= (q-1)^2 - D_d(i)(q-1).\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{j=0}^{q-2} N_{ij} &= \sum_{j=0}^{q-2} \left(|\mathcal{C}_{ij}^*| + D_d(i) + D_e(j) + D_f(i-j+w) - (q+1)\right) \\ &= (q-1)^2 - D_d(i)(q-1) + D_d(i)(q-1) + \sum_{j=0}^{q-2} D_e(j) \\ &\quad + \sum_{j=0}^{q-2} D_f(i-j+w) - (q+1)(q-1)\end{aligned}$$

which is equal to zero by Lemma 3.1.

To prove (4), note that the map $\mathcal{C}_{i+b_{11},j+b_{21}}^* \to \mathcal{C}_{ij}^*$ given by $(x,y) \mapsto (\rho x, y)$ is a bijection, so $|\mathcal{C}_{i+b_{11},j+b_{21}}^*| = |\mathcal{C}_{ij}^*|$. Moreover, $D_d(i+b_{11}) = D_d(i)$, $D_e(j+b_{21}) = D_e(j)$, and $D_f(i-j+b_{11}-b_{21}+w) = D_f(i-j+w)$ since $d \mid b_{11}$, $e \mid b_{21}$, and $f \mid b_{11} - b_{21}$ by definition. This implies that $N_{i+b_{11},j+b_{21}} = N_{ij}$. The proof of $N_{i+b_{12},j+b_{22}} = N_{ij}$ is analogous.

Now we prove (5),

$$\begin{aligned}&\sum_{i,j} |\mathcal{C}_{ij}^*|^2 = \sum_{i,j} \left(N_{ij} - D_d(i) - D_e(j) - D_f(i-j+w) + q + 1\right)^2 \\ &= \sum_{i,j} N_{ij}^2 + \sum_{i,j} D_d(i)^2 + \sum_{i,j} D_e(j)^2 + \sum_{i,j} D_f(i-j+w)^2 + (q+1)^2(q-1)^2 \\ &\quad - 2\sum_{i,j} N_{ij}D_d(i) - 2\sum_{i,j} N_{ij}D_e(j) - 2\sum_{i,j} N_{ij}D_f(i-j+w) + 2(q+1)\sum_{i,j} N_{ij} \\ &\quad + 2\sum_{i,j} D_d(i)D_e(j) + 2\sum_{i,j} D_d(i)D_f(i-j+w) + 2\sum_{i,j} D_e(j)D_f(i-j+w) \\ &\quad - 2(q+1)\sum_{i,j} D_d(i) - 2(q+1)\sum_{i,j} D_e(j) - 2(q+1)\sum_{i,j} D_f(i-j+w).\end{aligned}$$

By (1), (2), and (3) the sixth, seventh, eighth, and ninth terms vanish. The other terms can be calculated by Lemma 3.1, thus

$$\sum_{i,j} |\mathcal{C}_{ij}^*|^2 = \sum_{i,j} N_{ij}^2 + (q-1)^2(q^2 - 4q + 1 + d + e + f). \tag{4}$$

Note that $|\mathcal{C}_{ij}^*|^2 = |\mathcal{C}_{ij}^* \times \mathcal{C}_{ij}^*|$,

$$\mathcal{C}_{ij}^* \times \mathcal{C}_{ij}^* = \left\{ (x_1, y_1, x_2, y_2) \in (\mathbb{F}_q^*)^4 \ : \ \begin{array}{c} \rho^i x_1^{b_{11}} y_1^{b_{12}} + \rho^j x_1^{b_{21}} y_1^{b_{22}} = 1 \\ \rho^i x_2^{b_{11}} y_2^{b_{12}} + \rho^j x_2^{b_{21}} y_2^{b_{22}} = 1 \end{array} \right\}.$$

Les us define

$$\Delta = \det \begin{bmatrix} x_1^{b_{11}} y_1^{b_{12}} & x_1^{b_{21}} y_1^{b_{22}} \\ x_2^{b_{11}} y_2^{b_{12}} & x_2^{b_{21}} y_2^{b_{22}} \end{bmatrix}.$$

The set $\mathcal{C}_{ij}^* \times \mathcal{C}_{ij}^*$ can be written as the disjoint union $\mathcal{D}_{ij} \cup \mathcal{E}_{ij}$, where $\mathcal{D}_{ij} = (\mathcal{C}_{ij}^* \times \mathcal{C}_{ij}^*) \cap \{(x_1, y_1, x_2, y_2) \in (\mathbb{F}_q^*)^4 \,:\, \Delta \neq 0\}$ and $\mathcal{E}_{ij} = (\mathcal{C}_{ij}^* \times \mathcal{C}_{ij}^*) \cap \{(x_1, y_1, x_2, y_2) \in (\mathbb{F}_q^*)^4 \,:\, \Delta = 0\}$.

By Cramer's rule,

$$\mathcal{D}_{ij} = \left\{ (x_1, y_1, x_2, y_2) \in (\mathbb{F}_q^*)^4 \,:\, \Delta \neq 0, \begin{array}{c} \rho^i = (-x_1^{b_{21}} y_1^{b_{22}} + x_2^{b_{21}} y_2^{b_{22}})/\Delta \\ \rho^j = (x_1^{b_{11}} y_1^{b_{12}} - x_2^{b_{11}} y_2^{b_{12}})/\Delta \end{array} \right\},$$

which imply that the $\mathcal{D}_{ij}$ are disjoint and their union is

$$\bigcup_{i,j} \mathcal{D}_{ij} = \left\{ (x_1, y_1, x_2, y_2) \in (\mathbb{F}_q^*)^4 \,:\, \Delta \neq 0, \begin{array}{c} x_1^{b_{21}} y_1^{b_{22}} \neq x_2^{b_{21}} y_2^{b_{22}} \\ x_1^{b_{11}} y_1^{b_{12}} \neq x_2^{b_{11}} y_2^{b_{12}} \end{array} \right\}.$$

Introducing the change of variables $x = x_1/x_2$ and $y = y_1/y_2$, we get

$$\sum_{ij} |\mathcal{D}_{ij}| = \left| \bigcup_{i,j} \mathcal{D}_{ij} \right| = (q-1)^2 \left| \left\{ (x, y) \in (\mathbb{F}_q^*)^2 \,:\, \begin{array}{c} x^{b_{11}} y^{b_{12}} \neq 1 \\ x^{b_{21}} y^{b_{22}} \neq 1 \\ x^{b_{11}} y^{b_{12}} \neq x^{b_{21}} y^{b_{22}} \end{array} \right\} \right| =$$

$$(q-1)^2 \left( (q-1)^2 - \Big| \underbrace{\{x^{b_{11}} y^{b_{12}} = 1\}}_{S_1} \cup \underbrace{\{x^{b_{21}} y^{b_{22}} = 1\}}_{S_2} \cup \underbrace{\{x^{b_{11}-b_{21}} y^{b_{12}-b_{22}} = 1\}}_{S_3} \Big| \right).$$

Note that $S_1 \cap S_2 = S_1 \cap S_3 = S_2 \cap S_3 = S_1 \cap S_2 \cap S_3$, thus

$$|S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - 2|S_1 \cap S_2|.$$

By Lemma 3.2, $|S_1| = (q-1)d$, $|S_2| = (q-1)e$, and $|S_3| = (q-1)f$. Moreover, $|S_1 \cap S_2| = |\mathrm{coker}(B)| = k$. All together, we get

$$\sum_{i,j} |\mathcal{D}_{ij}| = (q-1)^2 \Big[ (q-1)^2 - (q-1)(d+e+f) + 2k \Big].$$

Observe that

$$\mathcal{E}_{ij} = \left\{ (x_1, y_1, x_2, y_2) \in (\mathbb{F}_q^*)^4 \,:\, \begin{array}{c} x_1^{b_{11}} y_1^{b_{12}} = x_2^{b_{11}} y_2^{b_{12}} \\ x_1^{b_{21}} y_1^{b_{22}} = x_2^{b_{21}} y_2^{b_{22}} \\ \rho^i x_1^{b_{11}} y_1^{b_{12}} + \rho^j x_1^{b_{21}} y_1^{b_{22}} = 1 \end{array} \right\}.$$

Then $\sum_{i,j} |\mathcal{E}_{ij}|$ equals

$$\left|\left\{ (i,j,x_1,y_1,x_2,y_2) \in \mathbb{Z}_{q-1}^2 \times (\mathbb{F}_q^*)^4 \ : \ \begin{array}{c} x_1^{b_{11}} y_1^{b_{12}} = x_2^{b_{11}} y_2^{b_{12}} \\ x_1^{b_{21}} y_1^{b_{22}} = x_2^{b_{21}} y_2^{b_{22}} \\ \rho^i x_1^{b_{11}} y_1^{b_{12}} + \rho^j x_1^{b_{21}} y_1^{b_{22}} = 1 \end{array} \right\}\right|$$

$$= (q-2) \left|\left\{ (x_1,y_1,x_2,y_2) \in (\mathbb{F}_q^*)^4 \ : \ \begin{array}{c} x_1^{b_{11}} y_1^{b_{12}} = x_2^{b_{11}} y_2^{b_{12}} \\ x_1^{b_{21}} y_1^{b_{22}} = x_2^{b_{21}} y_2^{b_{22}} \end{array} \right\}\right|$$

$$= (q-2)(q-1)^2 \left|\left\{ (x,y) \in (\mathbb{F}_q^*)^2 \ : \ \begin{array}{c} x^{b_{11}} y^{b_{12}} = 1 \\ x^{b_{21}} y^{b_{22}} = 1 \end{array} \right\}\right|$$

$$= (q-2)(q-1)^2 k.$$

Now we have

$$\sum_{i,j} |\mathcal{C}_{ij}^*|^2 = \sum_{ij} |\mathcal{D}_{ij}| + \sum_{ij} |\mathcal{E}_{ij}| = (q-1)^2 \Big[ (q-1)^2 - (q-1)(d+e+f) + qk \Big].$$

Finally, using Equation (4), we get $\sum_{i,j} N_{ij}^2 = (q-1)^2 q(k-d-e-f+2)$. □

**Proposition 3.4.** *Let $G$ be an abelian group and let $g_1, g_2, g_3 \in G$ such that $G = \langle g_1, g_2 \rangle = \langle g_1, g_3 \rangle = \langle g_2, g_3 \rangle$. Let $K \geq 0$ and let $N : G \to \mathbb{R}$ be a function $a \mapsto N_a := N(a)$ such that*

(1) $\displaystyle\sum_{a \in g + \langle g_1 \rangle} N_a = 0$ *for all* $g \in G$,

(2) $\displaystyle\sum_{a \in g + \langle g_2 \rangle} N_a = 0$ *for all* $g \in G$,

(3) $\displaystyle\sum_{a \in g + \langle g_3 \rangle} N_a = 0$ *for all* $g \in G$,

(4) $\displaystyle\sum_{a \in G} N_a^2 = K$.

*Then*

$$|N_g| \leq \sqrt{K \left( 1 + \frac{2}{|G|} - \frac{1}{n_1} - \frac{1}{n_2} - \frac{1}{n_3} \right)},$$

*for all $g \in G$, where $n_1$, $n_2$, and $n_3$ are the orders of the elements $g_1$, $g_2$, and $g_3$, respectively.*

Proof. Let $n_{12} = |\langle g_1 \rangle \cap \langle g_2 \rangle|$. The isomorphism

$$G/\langle g_1 \rangle \cong \langle g_2 \rangle / \langle g_1 \rangle \cap \langle g_2 \rangle$$

implies that $n_{12} = \frac{n_1 n_2}{|G|}$. Similarly, we define $n_{13}$ and $n_{23}$.

We study first the case when $1 + \frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$. Assuming without loss of generality that $n_1 \leq n_2 \leq n_3$, the previous equality implies that $n_1 < 3$. The case $n_1 = 1$ can only happen when $g_1$ is the neutral element of $G$, and then (1) reduces to $N_g = 0$ for all $g \in G$. In the case $n_1 = 2$, we have $|G| = |\langle g_1, g_2 \rangle| \leq 2n_2$, hence

$$\frac{1}{2} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{|G|} \geq 1 + \frac{1}{n_2},$$

and in particular $n_3 \leq 2$. Therefore $n_1 = n_2 = n_3 = 2$ and $G$ is a group of order $|G| = 4$. The elements $g_1, g_2, g_3$ are pairwise distinct, since each pair of them generates the group, so $G = \{0, g_1, g_2, g_3\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Items (1), (2), (3) yield the following identities:

$$\begin{aligned} N_0 + N_{g_1} =& N_{g_2} + N_{g_3} = 0 \\ N_0 + N_{g_2} =& N_{g_1} + N_{g_3} = 0 \\ N_0 + N_{g_3} =& N_{g_1} + N_{g_2} = 0, \end{aligned}$$

which imply $N_g = 0$ for all $g \in G$, and the claim follows.

Now we assume that $1 + \frac{2}{|G|} \neq \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$. We use Lagrange multipliers to get the desired upper bound for $N_g$. By the symmetry of the problem, we can restrict to the case $N_0$. Define the auxiliary function

$$\begin{aligned} F = N_0 &+ \sum_{\bar{g} \in G/\langle g_1 \rangle} \lambda_{\bar{g}} \left( \sum_{a \in g + \langle g_1 \rangle} N_a \right) + \sum_{\bar{g} \in G/\langle g_2 \rangle} \mu_{\bar{g}} \left( \sum_{a \in g + \langle g_2 \rangle} N_a \right) \\ &+ \sum_{\bar{g} \in G/\langle g_3 \rangle} \varepsilon_{\bar{g}} \left( \sum_{a \in g + \langle g_3 \rangle} N_a \right) + \gamma \left( -K + \sum_{a \in G} N_a^2 \right) \end{aligned}$$

with $N_a$, $\lambda_{\bar{g}}$, $\mu_{\bar{g}}$, $\varepsilon_{\bar{g}}$, and $\gamma$ as independent variables. The critical points of $F$ correspond with the local extrema of $N_0$ subject to the restrictions stated in the theorem.

Now, we calculate the partial derivatives of $F$ with respect to each variable. With respect to $\lambda_{\bar{g}}$, $\mu_{\bar{g}}$, $\varepsilon_{\bar{g}}$, and $\gamma$, we get the assumptions of the proposition. With respect to $N_a$, we get

$$\frac{\partial F}{\partial N_a} = \delta_{a,0} + \lambda_{\bar{a}} + \mu_{\bar{a}} + \varepsilon_{\bar{a}} + 2\gamma N_a = 0 \tag{5}$$

for all $a \in G$, where $\delta_{a,0}$ stands for the Kronecker delta.

For any element $g \in G$, we have

$$\sum_{a \in g+\langle g_1\rangle} \Big(\delta_{a,0} + \lambda_{\bar a} + \mu_{\bar a} + \varepsilon_{\bar a} + 2\gamma N_a\Big)$$
$$= \chi_{\langle g_1\rangle}(g) + n_1\lambda_{\bar g} + \sum_{a \in g+\langle g_1\rangle} \mu_{\bar a} + \sum_{a \in g+\langle g_1\rangle} \varepsilon_{\bar a}$$
$$= \chi_{\langle g_1\rangle}(g) + n_1\lambda_{\bar g} + n_{12}\sum_{\bar a \in G/\langle g_2\rangle} \mu_{\bar a} + n_{13}\sum_{\bar a \in G/\langle g_3\rangle} \varepsilon_{\bar a} = 0.$$

Define

$$\lambda = -\frac{n_{12}}{n_1}\sum_{\bar a \in G/\langle g_2\rangle} \mu_{\bar a} - \frac{n_{13}}{n_1}\sum_{\bar a \in G/\langle g_3\rangle} \varepsilon_{\bar a}.$$

The previous identity shows that $\lambda_{\bar 0} = \lambda - \frac{1}{n_1}$ and $\lambda_{\bar g} = \lambda$ for all $\bar g \neq \bar 0$. Similarly, we define

$$\mu = -\frac{n_{12}}{n_2}\sum_{\bar a \in G/\langle g_1\rangle} \lambda_{\bar a} - \frac{n_{23}}{n_2}\sum_{\bar a \in G/\langle g_3\rangle} \varepsilon_{\bar a},$$

and then $\mu_{\bar 0} = \mu - \frac{1}{n_2}$ and $\mu_{\bar g} = \mu$ for all $\bar g \neq \bar 0$. Analogously, we define

$$\varepsilon = -\frac{n_{13}}{n_3}\sum_{\bar a \in G/\langle g_1\rangle} \lambda_{\bar a} - \frac{n_{23}}{n_3}\sum_{\bar a \in G/\langle g_2\rangle} \mu_{\bar a},$$

and then $\varepsilon_{\bar 0} = \varepsilon - \frac{1}{n_3}$ and $\varepsilon_{\bar g} = \varepsilon$ for all $\bar g \neq \bar 0$.

By construction of $\varepsilon$, we have

$$\varepsilon = -\frac{n_{13}}{n_3}\sum_{\bar a \in G/\langle g_1\rangle} \lambda_{\bar a} - \frac{n_{23}}{n_3}\sum_{\bar a \in G/\langle g_2\rangle} \mu_{\bar a}$$
$$= -\frac{n_{13}}{n_3}\left(\frac{|G|}{n_1}\lambda - \frac{1}{n_1}\right) - \frac{n_{23}}{n_3}\left(\frac{|G|}{n_2}\mu - \frac{1}{n_2}\right).$$

Therefore $\lambda + \mu + \varepsilon = \frac{2}{|G|}$, and Equation (5) can be rewritten as follows:

$$2\gamma N_a = -\delta_{a,0} - \frac{2}{|G|} + \frac{\chi_{\langle g_1\rangle}(a)}{n_1} + \frac{\chi_{\langle g_2\rangle}(a)}{n_2} + \frac{\chi_{\langle g_3\rangle}(a)}{n_3}. \tag{6}$$

Squaring the previous equation and summing over all $a \in G$, we get

$$4\gamma^2 \sum_{a \in G} N_a^2 = 1 + \frac{2}{|G|} - \frac{1}{n_1} - \frac{1}{n_2} - \frac{1}{n_3} \neq 0.$$

This allows us to get $\gamma \neq 0$, and together with Equation (6) for $a = 0$, concludes the proof. □

Proof of Corollary 2.2. Consider $G = \mathbb{Z}_{q-1}^2/\langle (b_{11}, b_{12}), (b_{21}, b_{22})\rangle$ which is equal to coker$(B)$. By Theorem 2.1(4), the map $N : G \to \mathbb{R}$ such that $\overline{(i,j)} \mapsto N_{ij}$ is well defined. Let $g_1 = \overline{(1,0)} \in G$, $g_2 = \overline{(0,1)} \in G$, and $g_3 = \overline{(1,1)} \in G$. With this notation, the hypotheses of Proposition 3.4 with $K = kq(k-d-e-f+2)$ follow from Theorem 2.1 and Equation (3). By Lemma 3.3, we have $n_1 = k/e$, $n_2 = k/d$, and $n_3 = k/f$. The only thing left to do is to substitute these values in Proposition 3.4 and a suitable rearrangement of the terms. □

## 4. Gauss' theorem

We devote this section entirely to showing how to derive Theorem 1.1 as a consequence of Theorem 2.1. We consider the family of curves

$$\mathcal{C}_{ij} = \{(x,y) \in \mathbb{F}_p^2 \,:\, \rho^i x^3 + \rho^j y^3 = 1\}$$

for $0 \le i, j < p-1$. Removing the extra points on the lines $x = 0$, $y = 0$, $z = 0$, Gauss' curve corresponds to $\{(x,y) \in (\mathbb{F}_p^*)^2 \,:\, x^3 + y^3 = -1\}$ that has the same number of points as $\mathcal{C}_{00}^*$. The number of points on each of those lines is equal to the number of cubic roots of the unity in $\mathbb{F}_p$, which is equal to $\gcd(3, p-1)$ by Lemma 3.2. Therefore, $M_p = |\mathcal{C}_{00}^*| + 3\gcd(3,p-1)$. By Theorem 2.1, we get

$$M_p = p + 1 - D_d(0) - D_e(0) - D_f(w) + N_{00} + 3\gcd(3, p-1),$$

where $d = e = f = \gcd(3, p-1)$ and $w = \frac{p-1}{2}$. Then $M_p = p + 1 + N_{00}$.

Case $p \not\equiv 1 \pmod 3$: Here we have $d = e = f = 1$, $k = \gcd(p-1, 9) = 1$, then $\tilde{g} = 0$ and $N_{ij} = 0$ for all $0 \le i, j < p-1$ by Theorem 2.1(5). In particular $N_{00} = 0$ and $M_p = p + 1$, as expected.

Case $p \equiv 1 \pmod 3$: Here we have $d = e = f = 3$, $k = \gcd(3(p-1), 9) = 9$ and $\tilde{g} = \frac{1}{2}(k - d - e - f + 2) = 1$. The cokernel of the matrix $B = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$ is $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, so the numbers $N_{ij}$ reduce to only nine possibilities

$$A = \begin{bmatrix} N_{00} & N_{01} & N_{02} \\ N_{10} & N_{11} & N_{12} \\ N_{20} & N_{21} & N_{22} \end{bmatrix}$$

depending on the class of $(i,j)$ in coker$(B)$ by Theorem 2.1(4). Due to Theorem 2.1(1)(2)(3), each of the rows, columns and diagonals of the matrix $A$ above adds up to zero. This proves that

$$A = \begin{bmatrix} u & v & -u-v \\ v & -u-v & u \\ -u-v & u & v \end{bmatrix}$$

for some $u, v \in \mathbb{Z}$. Moreover, by Equation (3), the sum of the squares of the entries of $A$ is $3(u^2 + v^2 + (u+v)^2) = 18p$, so

$$u^2 + v^2 + uv = 3p. \tag{7}$$

Let $\xi_3 \in \mathbb{F}_p$ be a cubic root of the unity. Note that $|\mathcal{C}_{ij}^*|$ is divisible by 9, since for each point $(x, y) \in \mathcal{C}_{ij}^*$, its conjugates $(\xi_3^r x, \xi_3^s y)$ are also in $\mathcal{C}_{ij}^*$ for any $0 \leq r, s < 3$. By Equation (2),

$$u = N_{00} = |\mathcal{C}_{00}^*| - (p+1) + D_3(0) + D_3(0) + D_3(w) = |\mathcal{C}_{00}^*| - p + 8,$$
$$v = N_{01} = |\mathcal{C}_{01}^*| - (p+1) + D_3(0) + D_3(1) + D_3(w-1) = |\mathcal{C}_{01}^*| - p + 2.$$

Therefore $2v+v = 2|\mathcal{C}_{01}^*|+|\mathcal{C}_{00}^*|-3(p-4)$ is divisible by 9. Denoting $\bar{v} = \frac{2v+u}{9} \in \mathbb{Z}$, Equation (7) becomes $u^2 + 27\bar{v}^2 = 4p$. Moreover, $u = |\mathcal{C}_{00}^*| - p + 8 \equiv 1 \pmod 3$. The uniqueness of the solution of $u^2+27\bar{v}^2 = 4p$ with $u \equiv 1 \pmod 3$ follows from the fact that $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ is a UFD.

## 5. Genus of a trinomial curve

The aim of this section is to calculate the genus of the projective closure $\overline{\mathcal{C}_{ij}}$ of the curve $\mathcal{C}_{ij}$ in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ in the irreducible case. In order to do so, we use the standard formula that relates the genus of a curve with the delta invariant $\delta_P$ at each of its singularities, see formula (8) below. The delta invariants are computed using the techniques shown in [1, Chapter 3 and 6]. The final formula obtained in Proposition 5.2 should be compared term by term to the definition of $\tilde{g}$ given in Equation (1).

**Lemma 5.1.** *Let $\mathcal{C} \subseteq \mathbb{P}^2(\overline{\mathbb{F}}_q)$ be a curve such that its local equation at $P$ is given by $\alpha x^r + \beta y^s + \gamma x^u y^v = 0$ with $\alpha\beta \neq 0$ and $r, s \geq 1$. If either $\gamma = 0$ or $(u, v)$ is above the segment that joins $(r, 0)$ and $(0, s)$, then*

$$\delta_P = \frac{1}{2}\Big(rs - r - s + \gcd(r, s)\Big).$$

*If $\gamma \neq 0$ and $(u, v)$ is below the segment, then*

$$\delta_P = \frac{1}{2}\Big(rv + su - r - s + \gcd(u, s-v) + \gcd(v, r-u)\Big).$$

*The formula of the first case is valid even if $r = 0$ or $s = 0$. Also, the formula of the second case is valid when either $r = u = 0$ or $s = v = 0$. In both situations, the point $P$ does not belong to the curve and $\delta_P = 0$.*

Proof. In the first case, the term $\gamma x^u y^v$ can be removed from the local equation without changing the topology (since the point is above the Newton polygon). It is clear that the Milnor number at $P$ is $\mu_P = (r-1)(s-1)$ and that the number of local branches at $P$ is $r_P = \gcd(r,s)$. Therefore $2\delta_P = \mu_P + r_P - 1 = rs - r - s + \gcd(r,s)$.

In the other case, the local equation can be changed by $\alpha x^r + \beta y^s + \gamma x^u y^v + \frac{\alpha\beta}{\gamma} x^{r-u} y^{s-v}$, since the extra term is above the Newton polygon. Doing so, we get an expression that factorizes as $(\alpha x^u + \frac{\alpha\beta}{\gamma} y^{s-v})(x^{r-u} + \frac{\gamma}{\alpha} y^v)$. Applying the formula of the $\delta$-invariant of a product, we get:

$$\begin{aligned}\delta_P(\alpha x^r + \beta y^s + \gamma x^u y^v) &= \delta_P(\alpha x^u + \frac{\alpha\beta}{\gamma} y^{s-v}) + \delta_P(x^{r-u} + \frac{\gamma}{\alpha} y^v)\\ &\quad + i_P(\alpha x^u + \frac{\alpha\beta}{\gamma} y^{s-v}, x^{r-u} + \frac{\gamma}{\alpha} y^v),\end{aligned}$$

where $i_P$ denotes the intersection multiplicity at $P$. The values of $\delta_P$ of each factor can be computed as in the first case. Using Noether's formula (see [2, p. 3568]), the intersection multiplicity is $uv$. We conclude by simply adding these three values. □

**Proposition 5.2.** *If the projective closure $\overline{\mathcal{C}_{ij}}$ of the curve $\mathcal{C}_{ij}$ is irreducible in $\mathbb{P}^2(\overline{\mathbb{F}}_q)$, the genus of $\overline{\mathcal{C}_{ij}}$ is*

$$\frac{1}{2}\Big(|\det(B)| - \gcd(b_{11}, b_{12}) - \gcd(b_{21}, b_{22}) - \gcd(b_{11} - b_{21}, b_{12} - b_{22}) + 2\Big).$$

Proof. By using the irreducibility of the curve, we can reduce the proof to the case $a_{12} = a_{21} = 0$ and $a_{11} \geq a_{22}$. In this case, the genus can be computed using the following formula:

$$g(\overline{\mathcal{C}_{ij}}) = \frac{(m-1)(m-2)}{2} - \sum_P \delta_P, \tag{8}$$

where $m$ is the degree of the curve, $P$ ranges over all singular points of $\overline{\mathcal{C}_{ij}}$, and $\delta_P$ is the $\delta$-invariant of $\overline{\mathcal{C}_{ij}}$ at $P$. Since we are assuming $\det(B) \neq 0$, the set of singular points is contained in $\{[1:0:0], [0:1:0], [0:0:1]\}$.

We have to consider two cases: (1) $m = a_{11} > a_{31} + a_{32}$, (2) $m = a_{31} + a_{32} \geq a_{11}$.

Case (1): The projective closure of $\mathcal{C}_{ij}$ is given by the homogeneous polynomial

$$F(x,y,z) = \rho^i x^{a_{11}} + \rho^j y^{a_{22}} z^{a_{11} - a_{22}} - x^{a_{31}} y^{a_{32}} z^{a_{11} - a_{31} - a_{32}}.$$

We can further assume without loss of generality that the point $(a_{31}, a_{32})$ is below the line that connects the points $(a_{11}, 0)$ and $(0, a_{22})$, i.e. the Newton polygon of $F$ has two edges. Otherwise, we would simply exchange $y$ by $z$ and start over. Note that in the exceptional case when $a_{11} = 0$ ($a_{22} = 0$), we should also have $a_{31} = 0$ ($a_{32} = 0$), respectively. The singular points are $[0 : 1 : 0]$ and $[0 : 0 : 1]$, and the local equations of $\overline{\mathcal{C}_{ij}}$ at those points are $\rho^i x^{a_{11}} + \rho^j z^{a_{11}-a_{22}} - x^{a_{31}} z^{a_{11}-a_{31}-a_{32}}$ and $\rho^i x^{a_{11}} + \rho^j y^{a_{22}} - x^{a_{31}} y^{a_{32}}$, respectively. By Lemma 5.1, we have

$$\delta_{[0:1:0]} = \frac{1}{2}\Big(a_{11}(a_{11} - a_{22}) - a_{11} - (a_{11} - a_{22}) + \gcd(a_{11}, a_{11} - a_{22})\Big)$$

and

$$\delta_{[0:0:1]} = \frac{1}{2}\Big(a_{11}a_{32} + a_{22}a_{31} - a_{11} - a_{22} + \gcd(a_{31}, a_{22} - a_{32}) \\ + \gcd(a_{32}, a_{11} - a_{31})\Big).$$

Finally, using (8), we get the desired formula.

Case (2): The projective closure of $\mathcal{C}_{ij}$ is given by the homogeneous polynomial

$$F(x, y, z) = \rho^i x^{a_{11}} z^{a_{31}+a_{32}-a_{11}} + \rho^j y^{a_{22}} z^{a_{31}+a_{32}-a_{22}} - x^{a_{31}} y^{a_{32}}.$$

The local equations of $\overline{\mathcal{C}_{ij}}$ at $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$ are $\rho^i z^{a_{31}+a_{32}-a_{11}} + \rho^j y^{a_{22}} z^{a_{31}+a_{32}-a_{22}} - y^{a_{32}}$, $\rho^i x^{a_{11}} z^{a_{31}+a_{32}-a_{11}} + \rho^j z^{a_{31}+a_{32}-a_{22}} - x^{a_{31}}$, and $\rho^i x^{a_{11}} + \rho^j y^{a_{22}} - x^{a_{31}} y^{a_{32}}$, respectively. By Lemma 5.1,

$$\delta_{[1:0:0]} = \frac{1}{2}\left(a_{32}(a_{31} + a_{32} - a_{11}) - a_{32} - (a_{31} + a_{32} - a_{11}) + \gcd(a_{32}, a_{31} - a_{11})\right),$$
$$\delta_{[0:1:0]} = \frac{1}{2}\left(a_{31}(a_{31} + a_{32} - a_{22}) - a_{31} - (a_{31} + a_{32} - a_{22}) + \gcd(a_{31}, a_{32} - a_{22})\right),$$
$$\delta_{[0:0:1]} = \frac{1}{2}\left(a_{11}a_{22} - a_{11} - a_{22} + \gcd(a_{11}, a_{22})\right).$$

The conclusion follows from formula (8). □

## 6. Examples

We study some particular cases of Theorem 2.1 and Corollary 2.2 which have special significance by themselves.

**Example 1** (Diagonal case). *The curve* $\mathcal{C}_{ij} = \{(x, y) \in (\mathbb{F}_q^*)^2 : \rho^i x^{a_{11}} + \rho^j y^{a_{22}} = 1\}$ *has* $d = \gcd(a_{11}, q - 1)$, $e = \gcd(a_{22}, q - 1)$, $f = \gcd(d, e)$, *and* $w = (q - 1)/2$ *for* $q$ *odd, and* $w = 0$ *otherwise. Moreover,*

$$\operatorname{coker}(B) = \mathbb{Z}_{q-1}^2 / \langle (a_{11}, 0), (0, a_{22}) \rangle \cong \mathbb{Z}_d \oplus \mathbb{Z}_e,$$

*hence* $k = |\mathrm{coker}(B)| = de$. *By Theorem 2.1*(4), *we have* $N_{i+d,j} = N_{ij} = N_{i,j+e}$, *so the matrix* $[N_{ij}]_{0\leq i,j<q-1}$ *has its upper-left block of size* $d\times e$ *repeated* $(q-1)^2/de$ *times. As multisets, we can write:*

$$\{N_{ij}\,:\,0\leq i,j<q-1\} = \frac{(q-1)^2}{de}\cdot\{N_{ij}\,:\,0\leq i<d,\,0\leq j<e\}.$$

*Moreover, the sum in Theorem 2.1*(1) *can be taken from* $j=0$ *to* $j=e-1$. *Similarly, the sum* (2) *can be taken from* $i=0$ *to* $i=d-1$.

**Example 2.** *We consider the subcase of Example 1 when* $a_{11}$ *is odd,* $a_{22}=2$, *and* $q$ *is odd. The constants* $d$, $e$, $f$, $k$, $w$ *reduce to* $d=\gcd(a_{11},q-1)$, $e=2$, $f=1$, $k=2d$, $w=(q-1)/2$, *and the upper-left block is of size* $d\times 2$. *Since the second column of this block is the additive inverse of the first one, we have, as multisets:*

$$\{N_{ij}\,:\,0\leq i,j<q-1\} = \frac{(q-1)^2}{2d}\cdot\{\pm\alpha_0,\pm\alpha_1,\ldots,\pm\alpha_{d-1}\}$$

*where* $\alpha_i = N_{i0}$. *Moreover,*

$$\alpha_0+\alpha_1+\cdots+\alpha_{d-1}=0,$$
$$\alpha_0^2+\alpha_1^2+\cdots+\alpha_{d-1}^2=d(d-1)q.$$

*The vector* $(\alpha_0,\ldots,\alpha_{d-1})$ *is in the intersection of a sphere and a hyperplane in* $\mathbb{R}^d$, *i.e. the vector* $(\alpha_1,\ldots,\alpha_{d-1})$ *belongs to a conic in* $\mathbb{R}^{d-1}$. *Of course, when* $d=1$, *the sphere reduces to a point.*

**Example 3.** *Now, we consider the curves* $\mathcal{C}_{ij} = \{(x,y)\in(\mathbb{F}_q^*)^2\,:\,\rho^i x^3+\rho^j y^2 = 1\}$, *which is a particular case of the previous example. Clearly, when* $q\not\equiv 1 \pmod 3$, *we have* $d=1$ *and all the* $N_{ij}$ *are zero. For this reason, we only consider* $q\equiv 1 \pmod 3$, *in which case* $d=3$*:*

$$\{N_{ij}\,:\,0\leq i,j<q-1\} = \frac{(q-1)^2}{6}\cdot\{\pm\alpha_0,\pm\alpha_1,\pm\alpha_2\},$$

*where* $\alpha_0+\alpha_1+\alpha_2=0$ *and* $\alpha_0^2+\alpha_1^2+\alpha_2^2=6q$.

- *If* $q=p^{2n}$ *for some* $p\equiv 2 \pmod 3$, *then* $\alpha_0=p^n\beta_0$, $\alpha_1=p^n\beta_1$, *and* $\alpha_2=p^n\beta_2$, *for some* $\beta_0,\beta_1,\beta_2\in\mathbb{Z}$ *such that* $\beta_0+\beta_1+\beta_2=0$ *and* $\beta_0^2+\beta_1^2+\beta_2^2=6$. *This implies that, as multisets:*

  $$\{N_{ij}\,:\,0\leq i,j<q-1\} = \frac{(q-1)^2}{6}\cdot\{\pm p^n,\pm p^n,\mp 2p^n\}.$$

  *In particular,* $N_{ij}\neq 0$ *for all* $i,j$ *and the upper bound of Theorem 2.1 is sharp for this family.*

- *In constrast, for $p \equiv 1 \pmod 3$, the upper bound is not sharp. For instance, when $q = p = 997$, we have $\alpha_0 = 10$, $\alpha_1 = 49$, $\alpha_2 = -59$, but the integer part of the upper bound is $\lfloor (k - d - e - f + 2)\sqrt{q} \rfloor = 63$. Note, however, that*

$$\max \left\{ x : \begin{array}{c} x, y, z \in \mathbb{Z} \\ x + y + z = 0 \\ x^2 + y^2 + z^2 = 6q \end{array} \right\} = 59, \tag{9}$$

  *so one may think that the largest $N_{ij}$ can be obtained always by solving optimization problem in Proposition 3.4 for a function $f : G \to \mathbb{Z}$.*

- *In the case $q = 7^2$, we have $\{N_{ij} : 0 \leq i, j < 48\} = 384 \cdot \{\mp 2, \mp 11, \pm 13\}$, so the largest $N_{ij}$ is 13. However, the integer optimization problem (9) gives 14. This highlights the fact that the relations given in Theorem 2.1 are not always enough to characterize the maximum $N_{ij}$.*

**Example 4.** *When $a_{22} = 2$, $q$ is odd, and $a_{11}$ is even, the situation is similar, but $f = 2$, and item (3) of Theorem 2.1, gives the additional relation $\alpha_0 - \alpha_1 + \cdots + \alpha_{d-2} - \alpha_{d-1} = 0$. All together this gives*

$$\begin{aligned} \alpha_0 + \alpha_2 + \cdots + \alpha_{d-2} &= 0, \\ \alpha_1 + \alpha_3 + \cdots + \alpha_{d-1} &= 0, \\ \alpha_0^2 + \alpha_1^2 + \cdots + \alpha_{d-1}^2 &= d(d-2)q. \end{aligned}$$

**Example 5.** *The curve $\mathcal{C}_{ij} = \{(x, y) \in (\mathbb{F}_q^*)^2 : \rho^i x^3 + \rho^j y^2 = x\}$ with odd $q$, has $d = 2$, $e = f = 1$, $k = \gcd(q-1, 4)$, and $w = (q-1)/2$. When $q \equiv 3 \pmod 4$, we have $k = 2$, so $k - d - e - f + 2 = 0$, and in particular $N_{ij} = 0$ for all $i, j$. The other case, i.e. $q \equiv 1 \pmod 4$, is more interesting. Here $k = 4$, and*

$$\operatorname{coker}(B) = \mathbb{Z}_{q-1}^2 / \langle (2,0), (-1,2) \rangle = \{\overline{(0,0)}, \overline{(1,0)}, \overline{(0,1)}, \overline{(1,1)}\}.$$

*By Theorem 2.1(4), $N_{i+2,j} = N_{ij} = N_{i-1,j+2}$, so as multisets*

$$\{N_{ij} : 0 \leq i, j < q-1\} = \frac{(q-1)^2}{4} \cdot \{\pm\alpha, \pm\beta\},$$

*where $\alpha = N_{00}$, $\beta = N_{01}$, and $\alpha^2 + \beta^2 = 4q$. If, we also have $p \equiv 3 \pmod 4$, then $q = p^{2n}$ and the multiset is $\frac{(q-1)^2}{4} \cdot \{\pm 2p^n, 0\}$.*

## References

[1] Eduardo Casas-Alvero, *Singularities of plane curves*, London Mathematical Society Lecture Note Series, vol. 276, Cambridge University Press, Cambridge, 2000. MR 1782072

[2] José Ignacio Cogolludo-Agustín, Jorge Martín-Morales, and Jorge Ortigas-Galindo, *Local invariants on quotient singularities and a genus formula for weighted plane curves*, Int. Math. Res. Not. IMRN (2014), no. 13, 3559–3581. MR 3229762

[3] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. MR 340258

[4] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR 140494

[5] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn.-London, 1966. MR 0197380

[6] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 279, 41–55. MR 1608788

[7] Loo-Keng Hua and H. S. Vandiver, *On the number of solutions of some trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 477–481. MR 32679

[8] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 817210

[9] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR 1171452

[10] Daqing Wan, *Variation of p-adic Newton polygons for L-functions of exponential sums*, Asian J. Math. **8** (2004), no. 3, 427–471. MR 2129244

[11] ———, *Modular counting of rational points over finite fields*, Found. Comput. Math. **8** (2008), no. 5, 597–605. MR 2443090

[12] Ruyun Wang, Binbin Wen, and Wei Cao, *Degree matrices and enumeration of rational points of some hypersurfaces over finite fields*, J. Number Theory **177** (2017), 91–99. MR 3629235

[13] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR 29393

(Martin Avendano) Centro Universitario de la Defensa, Academia General Militar, Ctra. de Huesca s/n., 50090, Zaragoza, Spain
*Email address*: avendano@unizar.es

(Jorge Martín-Morales) Centro Universitario de la Defensa, Academia General Militar, Ctra. de Huesca s/n., 50090, Zaragoza, Spain
*Email address*: jorge@unizar.es