

On Probabilities regarding Poncelet Polygons over Finite Fields

Ruzzel Dizon Ragas

Supervisor: Milena Radnović

A thesis submitted in fulfillment of
the requirements for the degree of
Master of Philosophy

School of Mathematics and Statistics
Faculty of Science
The University of Sydney

Statement of Originality

I certify that the intellectual content of this thesis is the product of my own work and that all the assistance received in preparing this thesis and sources have been acknowledged. This thesis has not been submitted for any degree or other purposes. No generative AI tools were used in the preparation of this thesis.

Ruzzel Ragas

Authorship Attribution Statement

Chapter 5 of this thesis is accepted for publication in *Finite Fields and Their Applications*, and is available at <https://doi.org/10.1016/j.ffa.2026.102815>. This is a joint authorship with Milena Radnović.

In addition to the statements above, in cases where I am not the corresponding author of a published item, permission to include the published material has been granted by the corresponding author.

Ruzzel Ragas

As supervisor for the candidature upon which this thesis is based, I can confirm that the authorship attribution statements above are correct.

Milena Radnović

Abstract

An n -sided polygon that is inscribed in a conic \mathcal{A} and circumscribed about a conic \mathcal{B} is called a Poncelet polygon, and we call the pair of conics $(\mathcal{A}, \mathcal{B})$ an n -Poncelet pair. In the projective plane over a finite field of characteristic not equal to 2, we study Poncelet polygons and n -Poncelet pairs, with emphasis on the cases $n = 3$ and $n = 4$. In particular, we discuss the construction of Poncelet polygons and derive results regarding degenerate Poncelet polygons. Moreover, we provide in-depth results regarding the construction of Poncelet triangles. For our main result, we compute the probability of obtaining a 3-Poncelet pair or a 4-Poncelet pair when we randomly select a pair of distinct conics $(\mathcal{A}, \mathcal{B})$, with \mathcal{A} smooth or singular and \mathcal{B} smooth, in a fixed pencil of conics. We do this for all pencils, classified up to projective automorphism, with at least one smooth conic.

Acknowledgements

I am greatly indebted to Milena Radnović for her expertise, patience, and guidance throughout my research journey.

This research would not be possible without the support I received from the university through the Faculty of Science Research Tuition Fee Scholarship and the Postgraduate Research Scholarship in Mathematics and Statistics, for which I am sincerely grateful.

I would also like to express my utmost gratitude to my family, relatives, friends, and colleagues for their support during my studies.

Above all, I thank the Almighty for providing me the opportunity and strength to accomplish this research.

Contents

1	Introduction	3
2	Preliminaries	6
2.1	Finite field	6
2.2	Projective plane	10
2.3	Pencils of conics	14
2.4	Poncelet's theorem and Cayley's condition	18
2.5	Notation	20
3	Poncelet polygons	21
3.1	Intersection of a line and a conic	21
3.2	Construction of a Poncelet polygon	23
3.3	Degenerate polygons	26
3.4	Irregular pairs	30
3.5	Results from triangle construction	31
4	Examples regarding the construction of Poncelet polygons	36
4.1	Poncelet Triangle	36
4.2	Poncelet Tetragon	45
4.3	Degenerate Poncelet polygons	46
4.4	Valid pairs in non-transversal case	48
5	Computation of probabilities	50
5.1	Computation of Cayley's condition	52
5.1.1	Pencil \mathcal{P}_3	54
5.1.2	Pencil \mathcal{P}_4	55
5.1.3	Pencil \mathcal{P}_5	56

5.1.4	Pencil \mathcal{P}_6	57
5.1.5	Pencil \mathcal{P}_8	58
5.1.6	Pencil \mathcal{P}_{14}	59
5.1.7	Pencil \mathcal{P}_{15}	60
5.1.8	Pencil \mathcal{P}_{16}	61
5.1.9	Pencil \mathcal{P}_{17}	62
5.1.10	Pencil \mathcal{P}_{18}	63
5.1.11	Pencil \mathcal{P}_{19}	65
5.1.12	Summary for all pencils	66
5.2	Probabilities for 3-Poncelet pairs	69
5.2.1	Pencils $\mathcal{P}_3, \mathcal{P}_{14}, \mathcal{P}_{16}, \mathcal{P}_{19}$	75
5.2.2	Pencil \mathcal{P}_{18}	77
5.2.3	Pencils $\mathcal{P}_4, \mathcal{P}_6, \mathcal{P}_{15}, \mathcal{P}_{17}$	81
5.2.4	Pencils $\mathcal{P}_5, \mathcal{P}_8$	81
5.2.5	Main theorem for 3-Poncelet pairs	82
5.3	Probabilities for 4-Poncelet pairs	85
5.3.1	Pencils $\mathcal{P}_3, \mathcal{P}_{16}$	86
5.3.2	Pencils $\mathcal{P}_{14}, \mathcal{P}_{19}$	88
5.3.3	Pencil \mathcal{P}_{18}	89
5.3.4	Pencils $\mathcal{P}_4, \mathcal{P}_6, \mathcal{P}_{15}, \mathcal{P}_{17}$	90
5.3.5	Pencils $\mathcal{P}_5, \mathcal{P}_8$	90
5.3.6	Main theorem for 4-Poncelet pairs	90
6	Conclusion	92
A	Representation of finite field elements	93
B	Enumeration of Poncelet triangles	95

1. Introduction

Considered as one of the most beautiful results in projective geometry, Poncelet's theorem states that if we have an n -sided polygon that is inscribed in a conic \mathcal{A} and circumscribed about another conic \mathcal{B} , then we can construct another n -sided polygon that is inscribed and circumscribed about the same pair of conics starting from any point in \mathcal{A} as a vertex [12, 20]. In this context, we call such polygon a Poncelet n -gon and say that $(\mathcal{A}, \mathcal{B})$ is an n -Poncelet pair. To complement Poncelet's theorem, given conics \mathcal{A}, \mathcal{B} and a fixed n , Cayley developed an algebraic condition to determine if a Poncelet n -gon inscribed in \mathcal{A} and circumscribed about \mathcal{B} exists [2, 13]. Poncelet's theorem, Cayley's condition, and their extensive connections to other areas of mathematics are discussed in detail, for example, in [8, 10].

Poncelet's theorem holds for a projective plane over any field of characteristic not equal to 2 [1, 17]. The reason for avoiding a projective plane over a field of characteristic 2 is the existence of a point where all the tangents to a smooth conic meet [17, 19], which creates a problem in constructing our Poncelet polygon. Taking these into account, it is meaningful to examine n -Poncelet pairs in a projective plane over a finite field of characteristic not equal to 2. In this setting, we consider a collection of conics called a pencil of conics, which Dickson [5] classified up to projective automorphism in the projective plane over a finite field. Using this, [3] derived bounds for the probability of obtaining a 3-Poncelet pair among the pairs of smooth conics, for each pencil of conics with elements that intersect transversally; that is, at four distinct points. Following this work, [23] computed exact probabilities of obtaining 3-Poncelet pairs and derived bounds for the probabilities of obtaining 4-Poncelet pairs for the same pencils.

This thesis aims to build on these previous works by extending the discussion to a larger collection of conic pairs in the projective plane over a finite field of characteristic not equal to 2, which we refer to as valid pairs. In this collection, we allow the conic in which we inscribe the Poncelet polygon to be smooth or singular while retaining the smoothness condition for the

conic about which we circumscribe the Poncelet polygon. Moreover, we allow valid pairs to intersect non-transversally. With this, our main objective is to answer the following:

In the projective plane over a finite field of characteristic not equal to 2, among the valid pairs for each pencil of conics having at least one smooth conic:

1. What is the probability of obtaining a 3-Poncelet pair?
2. What is the probability of obtaining a 4-Poncelet pair?

In this thesis, we provide exact probabilities for 3-Poncelet pairs and 4-Poncelet pairs while considering a larger collection of pairs of conics that includes non-transversally intersecting conics. Moreover, we discuss in detail the probabilities for 3-Poncelet pairs when the characteristic of the finite field is 3, which are not addressed thoroughly in previous works.

The rest of this thesis is organized in this manner:

- In Chapter 2, we review preliminary concepts and propositions regarding finite fields and projective planes. We also state the two major theorems we use in this thesis, namely, Poncelet's theorem and Cayley's condition.
- In Chapter 3, we outline how to construct a Poncelet polygon in a projective plane. Using this, we prove results on the construction of a Poncelet polygon in a projective plane over a finite field, with additional results on the construction of a Poncelet triangle. We also prove results regarding degenerate Poncelet polygons and pairs of conics that will yield a problematic construction.
- In Chapter 4, we provide sample constructions of Poncelet triangles, a Poncelet tetragon inscribed in a singular conic, degenerate Poncelet polygons, and several other scenarios.
- In Chapter 5, we derive Cayley's condition for each pencil of conics considered in this study. We then derive the probability of obtaining a 3-Poncelet pair or 4-Poncelet pair for each of these pencils.

- In Chapter 6, we conclude by discussing future research directions and observations on n -Poncelet pairs in finite fields of small order.

The contents of Chapters 3, 4, and 5 are original contributions of this thesis.

2. Preliminaries

In this chapter, we present definitions and background necessary to understand and answer our research problem. The setting of our problem will be $\mathbf{P}^2(\mathbb{F}_q)$, the projective plane over a finite field of order q , where the characteristic of the finite field is not equal to 2. To gain insight about our setting, we review the concept of a finite field and a projective plane. We then consider a particular family of conics, which we call a pencil of conics. Finally, we state Poncelet's theorem and Cayley's condition, the two main theorems utilized in this thesis.

2.1 Finite field

In this section, we review essential concepts and results regarding finite fields. For a more detailed discussion, see, for example, [9].

We start this section by defining the concept of a field, which abstracts the usual way of performing arithmetic into an algebraic structure.

Definition 2.1.1. *A field \mathbb{F} is a set together with two binary operations addition (+) and multiplication (\bullet), such that:*

1. $(\mathbb{F}, +)$ is an abelian group with identity element 0,
2. $(\mathbb{F} \setminus \{0\}, \bullet)$ is an abelian group with identity element 1,
3. For all $x, y, z \in \mathbb{F}$, $x \bullet (y + z) = (x \bullet y) + (x \bullet z)$.

Example 2.1.2. *The real numbers \mathbb{R} , together with the usual addition and multiplication of real numbers, is a field.*

Example 2.1.3. *The complex numbers \mathbb{C} , together with the usual addition and multiplication of complex numbers, is a field.*

Example 2.1.4. For prime p , the set $\{0, 1, \dots, p-1\}$, together with the operations addition and multiplication modulo p , is a field.

Example 2.1.4 illustrates a finite field.

Definition 2.1.5. Let \mathbb{F} be a field where the cardinality of the set \mathbb{F} is a finite number q . Then, we call \mathbb{F} a finite field of order q .

One property of a field that we are interested in is its characteristic.

Definition 2.1.6. The characteristic of a field \mathbb{F} , denoted by $\text{char } \mathbb{F}$, is the smallest positive integer c such that $\underbrace{1 + \dots + 1}_{c \text{ terms}} = 0$. If no such c exists, then $\text{char } \mathbb{F} = 0$.

We state properties of finite fields needed for this study.

Theorem 2.1.7 ([9]). Let \mathbb{F}_q be a finite field of order q .

- If \mathbb{K} is another finite field of order q , then \mathbb{F}_q and \mathbb{K} are isomorphic.
- The order must be of the form $q = p^k$ for some prime p and $k \in \mathbb{Z}^+$. In this case, $\text{char } \mathbb{F}_q = p$.

Henceforth, we denote by \mathbb{F}_q any finite field of order q . From Example 2.1.4, we know that for prime order p , \mathbb{F}_p can be represented as the set $\{0, 1, \dots, p-1\}$ equipped with modulo arithmetic, and all fields of prime order will have this structure by Theorem 2.1.7. Now, we discuss how to obtain a representation for a finite field with a non-prime order. To do this, we need the concept of a ring, which generalizes that of a field.

Definition 2.1.8. A ring R is a set together with two binary operations addition (+) and multiplication (\bullet), such that:

1. $(R, +)$ is an abelian group,
2. \bullet is associative,
3. For all $x, y, z \in R$, $x \bullet (y + z) = (x \bullet y) + (x \bullet z)$.

Remark 2.1.9. All fields are rings.

Example 2.1.10. The integers \mathbb{Z} , together with the usual addition and multiplication of integers, is a ring but not a field.

Example 2.1.11. Let R be a ring. The set of polynomials in x with coefficients in R , together with addition and multiplication of polynomials, is a ring called the polynomial ring in x over R , denoted by $R[x]$.

Definition 2.1.12. A polynomial in $R[x]$ is irreducible if it is not a product of lower-degree polynomials.

Now, we construct a field of non-prime order.

Example 2.1.13. Let $q = p^k$ where p is prime and $k > 1$ is an integer. Let g be an irreducible polynomial of degree k in $\mathbb{F}_p[x]$. Then, the quotient of $\mathbb{F}_p[x]$ by the ideal generated by g is a finite field with order q . This can be seen as the collection of polynomials in $\mathbb{F}_p[x]$ where we impose the condition that $g(x) = 0$. With this, every polynomial of degree greater than or equal to k can be reduced to a polynomial of degree less than k and thus, elements of \mathbb{F}_q can be represented as $a_{k-1}\alpha^{k-1} + a_{k-2}\alpha^{k-2} + \dots + a_1\alpha + a_0$, where α is a root of g and $a_i \in \mathbb{F}_p$ for all i .

It is always possible to find an irreducible polynomial described in Example 2.1.13. In this study, we use the Conway polynomial $C_{p,k}(x)$ as our irreducible polynomial of degree k in $\mathbb{F}_p[x]$. See Appendix A for more details.

Theorem 2.1.14 ([9]). Let \mathbb{F}_q be a finite field of order q . Then, there exist an element $\alpha \in \mathbb{F}_q$, called a primitive element, that generates the multiplicative group $(\mathbb{F}_q \setminus \{0\}, \bullet)$.

One reason to consider Conway polynomials is that their roots act as a primitive element of our field. This means that for a fixed α that satisfies $C_{p,k}(\alpha) = 0$, every non-zero element of \mathbb{F}_q with $q = p^k$ can be written as α^j , for some j . From this, we have two ways to represent elements of our finite field.

Definition 2.1.15. Let \mathbb{F}_q be a finite field of order $q = p^k$ and α a primitive element of \mathbb{F}_q . The elements of \mathbb{F}_q can be represented as follows:

- Polynomial representation: $a_{k-1}\alpha^{k-1} + a_{k-2}\alpha^{k-2} + \dots + a_1\alpha + a_0$, where $a_i \in \mathbb{F}_p$, $i = 0, 1, \dots, k-1$.

- *Power representation: 0 and α^j , where $j = 1, \dots, q - 1$.*

In all the representations that will be used in this study, we fix a primitive element α , which is a root of our Conway polynomial.

Now, we define the square root of $x \in \mathbb{F}_q$ as a value y such that $y^2 = x$. Notice that if $x = 0$, then $y = 0$ is the only possible value of the square root, and if y is a square root of x , then $-y$ will also be a square root of x . Using the power representation and a primitive element α , we see that square elements of our field are either 0 or of the form α^k where k is even. We formalize this in the definition below and define the principal square root, which is the value of the square root that we will use whenever we encounter a square root in our computations.

Definition 2.1.16. *Let α be a primitive element of \mathbb{F}_q . The principal square root of x , denoted by \sqrt{x} is defined as*

$$\sqrt{x} = \begin{cases} 0 & , x = 0 \\ \alpha^{k/2} & , x = \alpha^k \text{ where } k \text{ is even.} \end{cases}$$

If $x = \alpha^k$ where k is odd, then \sqrt{x} is not defined in \mathbb{F}_q .

The existence of some square roots not being defined in \mathbb{F}_q is due to this field not being algebraically closed.

Definition 2.1.17. *A field \mathbb{K} is said to be algebraically closed if every nonconstant polynomial in $\mathbb{K}[x]$ has a root in \mathbb{K} .*

Theorem 2.1.18 ([9]). *For any field \mathbb{F} , there exists an algebraically closed field extension of \mathbb{F} called its algebraic closure, denoted by $\overline{\mathbb{F}}$.*

Example 2.1.19. *The field \mathbb{R} is not algebraically closed. Its algebraic closure is given by $\overline{\mathbb{R}} = \mathbb{C}$.*

In our case, computing square roots is equivalent to finding roots of a quadratic equation. Thus, all square roots of elements in \mathbb{F}_q will exist in $\overline{\mathbb{F}_q}$. For more details and sample computations regarding the representation of finite fields and the calculation of principal square roots, the reader is referred to Appendix A.

We end this section by discussing the concept of discriminants, which relates to square elements in \mathbb{F}_q . This will be one of our main tools for computing probabilities in Chapter 5.

Definition 2.1.20. *The discriminant of a polynomial $f \in \mathbb{F}_q[x]$ with roots $\mu_i, i = 1, 2, \dots, d$ in $\overline{\mathbb{F}_q}$ is given by*

$$D(f) = \prod_{i < j}^d (\mu_i - \mu_j)^2.$$

For a quadratic polynomial in $\mathbb{F}_q[x]$, its discriminant characterizes the number of roots that it has in \mathbb{F}_q .

Lemma 2.1.21 ([9]). *Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial in $\mathbb{F}_q[x]$ where $a \neq 0$. Then*

$$D(f) = b^2 - 4ac.$$

Moreover,

- *f has two distinct roots in \mathbb{F}_q if and only if $D(f)$ is a non-zero square in \mathbb{F}_q .*
- *f has one root in \mathbb{F}_q if and only if $D(f) = 0$.*
- *f has no roots in \mathbb{F}_q if and only if $D(f)$ is non-square in \mathbb{F}_q .*

Finally, we also have a result for cubic polynomials.

Lemma 2.1.22 ([4]). *Let $f(x) = x^3 + bx^2 + cx + d$ be a cubic polynomial in $\mathbb{F}_q[x]$. Then*

$$D(f) = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd.$$

Moreover, if f is an irreducible polynomial in $\mathbb{F}_q[x]$, then $D(f)$ is a non-zero square in \mathbb{F}_q .

2.2 Projective plane

In this section, we review the concept of a projective plane and the geometric elements that we can define in it, including points, lines, and conics. An extensive discussion of projective geometry is available, for example, in [21] and [10].

First, we define a general projective space over a field.

Definition 2.2.1. Let \mathbb{F} be a field and \mathbb{F}^n be the vector space of n -tuples having entries in \mathbb{F} . The n -dimensional projective space over a field \mathbb{F} , denoted by $\mathbf{P}^n(\mathbb{F})$, is the set of equivalence classes in $\mathbb{F}^{n+1} \setminus \{\mathbf{0}\}$ under the equivalence relation \sim where

$$a \sim b \text{ if there exists } \lambda \in \mathbb{F} \setminus \{0\} \text{ such that } a = \lambda b.$$

Elements of $\mathbf{P}^n(\mathbb{F})$ are called points. The point containing $(x_1, x_2, \dots, x_{n+1})$ will be denoted by its homogeneous coordinates $[x_1 : x_2 : \dots : x_{n+1}]$.

The one-dimensional projective space $\mathbf{P}^1(\mathbb{F})$, called the projective line, is bijective to $\mathbb{F} \cup \{\infty\}$, where the additional element ∞ is called a point at infinity. To see this, notice that elements of $\mathbf{P}^1(\mathbb{F})$ can be standardized, utilizing the invariance of homogeneous coordinates to multiplication of non-zero scalars, in the form

$$[x : y] = \begin{cases} \left[\frac{x}{y} : 1 \right] & , y \neq 0 \\ [1 : 0] & , y = 0. \end{cases}$$

With this, we see that $[1 : 0]$ can be mapped to ∞ and $[x : 1]$ with $x \in \mathbb{F}$.

The setting of our study is the two-dimensional projective space $\mathbf{P}^2(\mathbb{F})$, called the projective plane. Using the same arguments above, elements of the projective plane can be standardized as follows

$$[x : y : z] = \begin{cases} \left[\frac{x}{z} : \frac{y}{z} : 1 \right] & , z \neq 0 \\ \left[\frac{x}{y} : 1 : 0 \right] & , z = 0 \text{ and } y \neq 0 \\ [1 : 0 : 0] & , z = 0 \text{ and } y = 0. \end{cases}$$

One can show that $\mathbf{P}^2(\mathbb{F})$ is bijective to $\mathbb{F}^2 \cup \mathbf{P}^1(\mathbb{F})$ and in this context, the projective line component is called a line at infinity. Using this standardization, we can map $[x : y : 1]$ to $(x, y) \in \mathbb{F}^2$. This is equivalent to choosing the affine chart $z = 1$ as the viewing plane, with points of the form $[x : y : 0]$ lying on the line at infinity.

Another geometric object that we can define is a line in the projective plane.

Definition 2.2.2. *A line in $\mathbf{P}^2(\mathbb{F})$, represented by homogeneous coordinates in the dual plane, is the collection of points*

$$[u : v : w] = \{[x : y : z] \in \mathbf{P}^2(\mathbb{F}_q) \mid ux + vy + wz = 0\}.$$

Remark 2.2.3. *The dual plane is an isomorphic copy of the plane $\mathbf{P}^2(\mathbb{F})$, where the elements are lines. This provides a correspondence between the points and lines in the projective plane.*

In projective geometry, it is useful to treat $[x : y : z]$ as the column vector $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$.

For example, if we denote p^T as the transpose of p , then the line condition in Definition 2.2.2 reduces to $a^T b = 0$ where $a = [u : v : w]$ and $b = [x : y : z]$.

With this, we define a conic in the context of a projective plane.

Definition 2.2.4. *Let A be a 3×3 nonzero, symmetric matrix. We define the conic \mathcal{A} as*

$$\mathcal{A} = \{p \in \mathbf{P}^2(\mathbb{F}) \mid p^T A p = 0\}.$$

Here, we call A a matrix representation of conic \mathcal{A} .

Since we are in the projective plane, a matrix representation is unique up to non-zero scalar multiplication.

Now, we define the concept of a line tangent to a conic.

Definition 2.2.5. *A line τ is tangent to a conic \mathcal{A} if τ and \mathcal{A} have exactly one common point.*

Remark 2.2.6. *In a projective plane over an algebraically closed field, a line and a conic intersect at two points, since this is equivalent to solving a quadratic equation. A line is tangent to a conic when the two intersection points coincide, and we call the point of tangency an intersection point of multiplicity 2.*

Theorem 2.2.7 ([21]). *Let \mathcal{A} be a conic with matrix representation A . Then:*

- \mathcal{A} is a smooth conic; that is, for every point $p \in \mathcal{A}$, there exist a line tangent to \mathcal{A} at p if and only if $\text{rank } A = 3$.
- \mathcal{A} is a union of two distinct lines if and only if $\text{rank } A = 2$.
- \mathcal{A} is a double line if and only if $\text{rank } A = 1$.

A smooth conic \mathcal{B} with matrix representation B can be used to induce a map from the points to the lines in the projective plane. We call this map a polarity.

Definition 2.2.8. *Let \mathcal{B} be a smooth conic with matrix representation B . The polarity induced by \mathcal{B} is the map that sends a point p in the projective plane to the line Bp , which we call the polar line to \mathcal{B} with respect to p .*

The usefulness of the polar line is summarized in the statement below.

Theorem 2.2.9 ([21]). *Let \mathcal{B} be a smooth conic with matrix representation B . Let $\ell = Bp$ be the polar line to \mathcal{B} with respect to $p \in \mathbf{P}^2(\mathbb{F})$.*

- ℓ intersects \mathcal{B} at the points of tangency of the tangent lines to \mathcal{B} that pass through p .
- If $p \in \mathcal{B}$, then ℓ is the tangent line to \mathcal{B} at point p .

In fact, the second statement in Theorem 2.2.9 coincides with the method of obtaining the tangent line via formal derivatives. To see this, note that a smooth conic \mathcal{B} with matrix representation

$$B = \begin{bmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{bmatrix}$$

has an underlying conic equation $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$, which is an algebraic curve. We can perform formal derivatives and obtain the equation of the tangent line at point $p = [x_0 : y_0 : z_0]$ to be $(2ax_0 + by_0 + dz_0)x + (bx_0 + 2cy_0 + ez_0)y + (dx_0 + ey_0 + 2fz_0)z = 0$, which is exactly the polar line Bp .

Finally, we give a brief discussion about projective automorphism.

Definition 2.2.10. *Let \mathbb{F} be a field.*

- *The projective linear group, $\text{PGL}(n, \mathbb{F}) = \text{GL}(n, \mathbb{F})/\{cI_n \mid c \in \mathbb{F}\}$, is the multiplicative group of $n \times n$ matrices with entries in \mathbb{F} and determinant 1.*
- *The map $T : \mathbf{P}^2(\mathbb{F}) \rightarrow \mathbf{P}^2(\mathbb{F})$ defined by $T(p) = Cp$ where $C \in \text{PGL}(3, \mathbb{F})$ is called a projective automorphism over $\mathbf{P}^2(\mathbb{F})$.*

We list important properties of projective automorphisms that we need for this study.

Theorem 2.2.11 ([10]). *Let T be a projective automorphism over $\mathbf{P}^2(\mathbb{F})$.*

- *T maps lines to lines, and maps smooth conics to smooth conics.*
- *If ℓ is a line tangent to conic \mathcal{B} , then $T(\ell)$ is a line tangent to conic $T(\mathcal{B})$.*
- *If p is an intersection point with multiplicity m of conics \mathcal{A} and \mathcal{B} , then $T(p)$ is an intersection point with multiplicity m of conics $T(\mathcal{A})$ and $T(\mathcal{B})$.*

2.3 Pencils of conics

In this section, we introduce pencils of conics, which are collections of conics that we will consider as sample spaces for the computation of probabilities in Chapter 5. In particular, we consider pencils in $\mathbf{P}^2(\mathbb{F}_q)$ that are unique up to projective automorphism. A more detailed discussion about these is available, for example, in [10].

Definition 2.3.1. *Let \mathcal{A} and \mathcal{B} be two distinct conics in $\mathbf{P}^2(\mathbb{F})$ with matrix representation A and B , respectively. The collection of conics with matrix representation in $\{\eta A + B : \eta \in \mathbf{P}^1(\mathbb{F})\}$ is called the pencil of conics generated by \mathcal{A} and \mathcal{B} .*

Now, we state a version of Bézout's theorem for the intersection of two conics

Theorem 2.3.2 (Bézout's [10, 18]). *Let \mathcal{A} and \mathcal{B} be two conics defined in a projective plane over an algebraically closed field. If \mathcal{A} and \mathcal{B} do not have a common component, then \mathcal{A} and \mathcal{B} intersect at four points, counting multiplicity.*

Definition 2.3.3. Let $\mathcal{A} = \{p \in \mathbf{P}^2(\mathbb{F}) \mid p^T A p = 0\}$ be a conic in $\mathbf{P}^2(\mathbb{F})$.

- $\mathbf{P}^2(\overline{\mathbb{F}})$ is called the extended plane, where $\overline{\mathbb{F}}$ is the algebraic closure of \mathbb{F} .
- $\overline{\mathcal{A}} = \{p \in \mathbf{P}^2(\overline{\mathbb{F}}) \mid p^T A p = 0\}$ is the conic in the extended plane defined by the same conic equation as \mathcal{A} .

Using these, we define the base points of a pencil.

Definition 2.3.4. The base points of the pencil generated by \mathcal{A} and \mathcal{B} are the points in $\overline{\mathcal{A}} \cap \overline{\mathcal{B}}$.

We follow the approach in [3] by considering pencils of conics in $\mathbf{P}^2(\mathbb{F}_q)$ up to projective automorphisms using the classification provided by Dickson [5], which we give in Table 2.3.1; see also Table 7.7 on page 175 of [14].

The configuration of the base points for each pencil is described in the second column. Aside from pencils \mathcal{P}_1 and \mathcal{P}_2 , the rest of the pencils have generators with no common components and must have four base points, counting multiplicity, in $\mathbf{P}^2(\overline{\mathbb{F}_q})$ by Bézout's theorem. The configuration $(1, 1, 1, 1)1$ represents four base points in \mathbb{F}_q , each of intersection multiplicity 1. Now, $(m)1$ represents a base point in \mathbb{F}_q with intersection multiplicity m , and $(1)h$ represents h base points in \mathbb{F}_{q^h} obtained by solving an irreducible degree h polynomial in $\mathbb{F}_q[T]$.

The number of each type of conic for each pencil is described in the third column. Note that in the projective plane $\mathbf{P}^2(\mathbb{F}_q)$, there are four types of conics: a smooth conic, the union of two distinct lines, a single line, and a point. Here, a conic which coincides with a line is treated as a double line, while a conic coinciding with a point will in fact be, in the projective plane over the algebraic closure $\overline{\mathbb{F}_q}$, the union of two conjugate lines which intersect at that point.

For any pencil \mathcal{P}_j from Table 2.3.1, each $\eta \in \mathbf{P}^1(\mathbb{F}_q)$ correspond to the conic with matrix representation $C_j(\eta) = \eta A_j + B_j$ where A_j and B_j are the matrix representations of the generators \mathcal{A}_j and \mathcal{B}_j , with the convention that $C_j(\infty) = A_j$.

Table 2.3.1: Pencils of conics in $P^2(\mathbb{F}_q)$, up to projective automorphism [5, 14]

\mathcal{P}_j	Base Points	Count per Type of Conic				Generators	
		Smooth	Two Lines	Point	Line	\mathcal{A}_j	\mathcal{B}_j
\mathcal{P}_1		0	q	0	1	x^2	xy
\mathcal{P}_2		0	$q + 1$	0	0	xy	xz
\mathcal{P}_3	(1, 1, 1, 1)1	$q - 2$	3	0	0	xy	$xz + yz + z^2$
\mathcal{P}_4	(1, 1, 2)1	$q - 1$	2	0	0	xy	$xz + z^2$
\mathcal{P}_5	(1, 3)1	q	1	0	0	xy	$xz + y^2$
\mathcal{P}_6	(2, 2)1	$q - 1$	1	0	1	xy	z^2
\mathcal{P}_7^{**}	(4)1	0	0	0	$q + 1$	x^2	y^2
\mathcal{P}_8	(4)1	q	0	0	1	x^2	$xy + z^2$
\mathcal{P}_9^{**}	(4)1	0	$q/2$	$q/2$	1	x^2	$xy + y^2$
$\mathcal{P}_{10}^\#$	(4)1	0	$(q - 1)/2$	$(q - 1)/2$	2	xy	$x^2 - y^2$
$\mathcal{P}_{11}^\#$	(4)1	0	$(q + 1)/2$	$(q + 1)/2$	0	xy	$x^2 - \nu y^{2^\dagger}$
$\mathcal{P}_{12}^{##}$	(4)1	0	$(q - 1)/2$	$(q - 1)/2$	2	xy	$x^2 + y^2$
$\mathcal{P}_{13}^{##}$	(4)1	0	$(q + 1)/2$	$(q + 1)/2$	0	xy	$x^2 - y^2$
\mathcal{P}_{14}	(1, 1)1, (1)2	q	1	0	0	xy	$xz + y^2 + yz + ez^{2^\ddagger}$
\mathcal{P}_{15}	(2)1, (1)2	$q - 1$	1	1	0	xy	$y^2 + yz + ez^{2^\ddagger}$
\mathcal{P}_{16}	(1, 1)2	$q - 2$	1	2	0	xy	$ex^2 + xz + dy^2 + yz + z^{2^\ddagger}$
\mathcal{P}_{17}	(2)2	$q - 1$	0	1	1	x^2	$y^2 + yz + ez^{2^\ddagger}$
\mathcal{P}_{18}	(1)1, (1)3	$q + 1$	0	0	0	$-xz + y^2$	$x^2 + cxy + by^2 + yz^\ddagger$
\mathcal{P}_{19}^*	(1)4	q	0	1	0	$x^2 - \nu y^{2^\dagger}$	$2\sigma xy - \rho y^2 + z^{2^\dagger}$
\mathcal{P}_{20}^{**}	(1)4	q	0	1	0	$x^2 + xy + ey^{2^\ddagger}$	$fxz + y^2 + z^{2^\ddagger}$

$^\dagger \nu$ and $\rho^2 - 4\nu\sigma^2$ are non-squares. $^\ddagger T^3 + bT^2 + cT + 1, T^2 + T + d, T^2 + T + e,$ and $T^2 + ef^2T + f^2$ are irreducible in $\mathbb{F}_q[T]$.

* q must be odd. ** q must be even. # $q \equiv 1 \pmod{4}$. ## $q \equiv -1 \pmod{4}$.

For pencils considered in this study, we derived the homogeneous coordinates of the base points together with the index $\eta \in \mathbf{P}^1(\mathbb{F}_q)$ corresponding to singular elements in that pencil. These are summarized in Table 2.3.2.

Table 2.3.2: Singular elements and base points of each pencil

\mathcal{P}_j^*	Singular η^{**}	Base Points (Intersection Multiplicity)
\mathcal{P}_3	$0, 1, \infty$	$[-1 : 0 : 1], [0 : -1 : 1], [0 : 1 : 0], [1 : 0 : 0]$
\mathcal{P}_4	$0, \infty$	$[-1 : 0 : 1], [1 : 0 : 0], [0 : 1 : 0](2)$
\mathcal{P}_5	∞	$[1 : 0 : 0], [0 : 0 : 1](3)$
\mathcal{P}_6	$0, \infty$	$[0 : 1 : 0](2), [1 : 0 : 0](2)$
\mathcal{P}_8	∞	$[0 : 1 : 0](4)$
\mathcal{P}_{14}	∞	$[-e : 0 : 1], [1 : 0 : 0], [0 : \mu_1^\dagger : 1], [0 : \mu_2^\dagger : 1]$
\mathcal{P}_{15}	$0, \infty$	$[1 : 0 : 0](2), [0 : \mu_1^\dagger : 1], [0 : \mu_2^\dagger : 1]$
\mathcal{P}_{16}	η_+, η_-, ∞	$[0 : 1 : \mu_3^\ddagger], [0 : 1 : \mu_4^\ddagger], [1 : 0 : \mu_1^\dagger], [1 : 0 : \mu_2^\dagger]$
\mathcal{P}_{17}	$0, \infty$	$[0 : \mu_1^\dagger : 1](2), [0 : \mu_2^\dagger : 1](2)$
\mathcal{P}_{18}	None	$[0 : 0 : 1], [1 : \mu_5^\# : \mu_5^{2\#}], [1 : \mu_6^\# : \mu_6^{2\#}], [1 : \mu_7^\# : \mu_7^{2\#}]$
\mathcal{P}_{19}	∞	$[-\sqrt{v} : 1 : \zeta_1^{\#\#}], [-\sqrt{v} : 1 : -\zeta_1^{\#\#}], [\sqrt{v} : 1 : \zeta_2^{\#\#}], [\sqrt{v} : 1 : -\zeta_2^{\#\#}]$

* See Table 2.3.1

** η that correspond to singular conics in \mathcal{P}_j ; $\eta_+ = \frac{1 + \sqrt{(1-4d)(1-4e)}}{2}, \eta_- = \frac{1 - \sqrt{(1-4d)(1-4e)}}{2}$

† μ_1, μ_2 are roots of $T^2 + T + e$ in $\overline{\mathbb{F}_q}$ ‡ μ_3, μ_4 are roots of $T^2 + T + d$ in $\overline{\mathbb{F}_q}$

μ_5, μ_6, μ_7 are roots of $T^3 + bT + cT + 1$ in $\overline{\mathbb{F}_q}$ ## $\zeta_1 = \sqrt{\rho + 2\sigma\sqrt{v}}, \zeta_2 = \sqrt{\rho - 2\sigma\sqrt{v}}$

Definition 2.3.5. *Two conics in $\mathbf{P}^2(\mathbb{F})$ intersect transversally if they intersect at four distinct points in $\mathbf{P}^2(\overline{\mathbb{F}})$; that is, each base point must have intersection multiplicity 1.*

Remark 2.3.6. *Pencils with transversally intersecting elements refers to $\mathcal{P}_3, \mathcal{P}_{14}, \mathcal{P}_{16}, \mathcal{P}_{18}$ and \mathcal{P}_{19} , which are the pencils considered in [3]. In this study, we consider all pencils with at least one smooth conic; that is, we also consider pencils with non-transversally intersecting elements, which refers to $\mathcal{P}_4, \mathcal{P}_5, \mathcal{P}_6, \mathcal{P}_8, \mathcal{P}_{15}$ and \mathcal{P}_{17} .*

2.4 Poncelet's theorem and Cayley's condition

In this section, we present the two theorems that play a central role in this study.

First, we state Poncelet's theorem as used in our setting.

Theorem 2.4.1 (Poncelet [1, 17, 20]). *Let $(\mathcal{A}, \mathcal{B})$ be a pair of conics in $\mathbf{P}^2(\mathbb{F}_q)$. If there exists an n -sided polygon that is inscribed in \mathcal{A} and circumscribed about \mathcal{B} , then every point in \mathcal{A} is a vertex of an n -sided polygon that is inscribed in \mathcal{A} and circumscribed about \mathcal{B} .*

This tells us that the number of sides of our Poncelet polygon is only dependent on the pair $(\mathcal{A}, \mathcal{B})$, which leads us to define the following.

Definition 2.4.2. *Let $(\mathcal{A}, \mathcal{B})$ be a pair of conics in $\mathbf{P}^2(\mathbb{F}_q)$ such that an n -sided polygon is inscribed in \mathcal{A} and circumscribed about \mathcal{B} .*

- *We call such n -sided polygon a Poncelet n -gon.*
- *We call the pair $(\mathcal{A}, \mathcal{B})$ an n -Poncelet pair.*

Remark 2.4.3. *As a consequence of Theorem 2.2.11, if T is a projective automorphism and $(\mathcal{A}, \mathcal{B})$ is an n -Poncelet pair, then $(T(\mathcal{A}), T(\mathcal{B}))$ is an n -Poncelet pair. Moreover, we can use a projective automorphism to map any pencil with at least one smooth conic to a pencil in Table 2.3.2. In effect, considering the pencils in Table 2.3.2 takes into account every possible pencil in $\mathbf{P}^2(\mathbb{F}_q)$ with at least one smooth conic.*

With this, we can consider an ordered pair $(\mathcal{A}, \mathcal{B})$ of conics from \mathcal{P}_j and ask whether it is an n -Poncelet pair. We can answer this using Cayley's condition.

Theorem 2.4.4 (Cayley [2, 6, 13]). *Consider the formal series expansion*

$$\sqrt{\det(tA + B)} = H_0 + H_1t + H_2t^2 + H_3t^3 + \dots,$$

where A and B are the matrix representations for conics \mathcal{A} and \mathcal{B} , respectively.

Then, $(\mathcal{A}, \mathcal{B})$ is an n -Poncelet pair if and only if

$$\begin{vmatrix} H_2 & \cdots & H_{m+1} \\ \vdots & \ddots & \vdots \\ H_{m+1} & \cdots & H_{2m} \end{vmatrix} = 0; n = 2m + 1, m \geq 1,$$

$$\begin{vmatrix} H_3 & \cdots & H_{m+1} \\ \vdots & \ddots & \vdots \\ H_{m+1} & \cdots & H_{2m-1} \end{vmatrix} = 0; n = 2m, m \geq 2.$$

Remark 2.4.5. *Utilizing Cayley's condition:*

- $(\mathcal{A}, \mathcal{B})$ is a 3-Poncelet pair if and only if $H_2 = 0$.
- $(\mathcal{A}, \mathcal{B})$ is a 4-Poncelet pair if and only if $H_3 = 0$.

More precisely, our statement of Poncelet's theorem and Cayley's condition works for $(\overline{\mathcal{A}}, \overline{\mathcal{B}})$ in $\mathbf{P}^2(\overline{\mathbb{F}}_q)$. In this study, since our condition only depends on the matrix representations A and B , we say that $(\mathcal{A}, \mathcal{B})$ is an n -Poncelet pair in $\mathbf{P}^2(\mathbb{F}_q)$ if the induced pair $(\overline{\mathcal{A}}, \overline{\mathcal{B}})$ in $\mathbf{P}^2(\overline{\mathbb{F}}_q)$ is an n -Poncelet pair. Geometrically, this is equivalent to having at least one of the vertices of our Poncelet n -gon in \mathcal{A} .

2.5 Notation

In this study, we always work in $\mathbf{P}^2(\mathbb{F}_q)$ where $\text{char } \mathbb{F}_q \neq 2$. In representing \mathbb{F}_q where $q = p^k$ with $k > 1$, we fix a primitive element α which is a root of the Conway polynomial $C_{p,k}(x)$.

Conics will be denoted by capital script letters \mathcal{A} and \mathcal{B} and their respective matrix representation by A and B . In constructing a Poncelet polygon, \mathcal{A} will be the conic in which we inscribe the polygon, while \mathcal{B} will be the conic about which we circumscribe it.

When referring to pairs of conics in pencil \mathcal{P}_j , we associate $(r, s) \in \mathbf{P}^1(\mathbb{F}_q) \times \mathbf{P}^1(\mathbb{F}_q)$ to the pair $(\mathcal{A}, \mathcal{B})$ where $A = C_j(r)$ and $B = C_j(s)$.

3. Poncelet polygons

In this chapter, we discuss the construction of Poncelet polygons in the projective plane. First, we examine a method of computing the intersection of a line and a conic in the projective plane and use this to provide the steps for construction. We also discuss constructions in the scenario where we need to consider the extended plane and degenerate cases. Moreover, we mention pairs of conics that create a problem in our construction. We conclude this section by presenting results on Poncelet triangle construction in $\mathbf{P}^2(\mathbb{F}_q)$.

3.1 Intersection of a line and a conic

In this section, we describe a method of computing intersection points of a line and a conic in the projective plane from [21]. This method handles this computation by making use of the conic's matrix representation together with the homogeneous coordinates of the line. This also naturally accounts for intersections that may occur at points at infinity. From this, we derive our own method of computing the intersection points when one of them is given.

Algorithm 3.1.1 (Intersection of line and conic [21]). *Let $[\lambda : \mu : \tau]$ be the homogeneous coordinates of our line ℓ and A be the matrix representation of conic \mathcal{A} .*

1. Construct $\mathcal{M}_\ell = \begin{bmatrix} 0 & \tau & -\mu \\ -\tau & 0 & \lambda \\ \mu & -\lambda & 0 \end{bmatrix}$.
2. Compute $V_{\mathcal{A},\ell} = \mathcal{M}_\ell^T A \mathcal{M}_\ell = [V_{i,j}]$.
3. Compute $k_{\mathcal{A},\ell} = \begin{cases} \lambda^{-1} \sqrt{V_{2,3}^2 - V_{2,2}V_{3,3}}, & \text{if } \lambda \neq 0 \\ \mu^{-1} \sqrt{V_{1,3}^2 - V_{1,1}V_{3,3}}, & \text{if } \mu \neq 0 \\ \tau^{-1} \sqrt{V_{1,2}^2 - V_{1,1}V_{2,2}}, & \text{if } \tau \neq 0. \end{cases}$

4. $V_{A,\ell} + k_{A,\ell}\mathcal{M}_\ell$ is a rank 1 matrix proportional to pq^T , where p and q are the points of intersection of ℓ and \mathcal{A} .

That is, any nonzero column and row of $V_{A,\ell} + k_{A,\ell}\mathcal{M}_\ell$ serves as homogeneous coordinates of $p = [p_1 : p_2 : p_3]$ and $q = [q_1 : q_2 : q_3]$.

It was also shown in [21] that $V_{A,\ell}$ is proportional to $pq^T + qp^T$. We use this fact to modify this method if one of the points of intersection, say p , is already given. Choose a coordinate system such that $V_{A,\ell} = [V_{i,j}] = pq^T + qp^T$. With this, we need to solve the overdetermined system

$$\begin{bmatrix} V_{1,1} \\ V_{2,2} \\ V_{3,3} \\ V_{1,2} \\ V_{1,3} \\ V_{2,3} \end{bmatrix} = \underbrace{\begin{bmatrix} 2p_1 & 0 & 0 \\ 0 & 2p_2 & 0 \\ 0 & 0 & 2p_3 \\ p_2 & p_1 & 0 \\ p_3 & 0 & p_1 \\ 0 & p_3 & p_2 \end{bmatrix}}_X \begin{bmatrix} q_1 \\ q_2 \\ q_3 \end{bmatrix}.$$

Since the coordinates of p cannot all be zero, X always has a full column rank and hence, $X^T X$ is invertible. We can solve for q , up to a scalar multiple, by left multiplying both sides by $(X^T X)^{-1} X^T$, the left inverse of X . We formalize this in Algorithm 3.1.2.

Algorithm 3.1.2 (Intersection of line and conic given one intersection point). *Let $[\lambda : \mu : \tau]$ be the homogeneous coordinates of our line ℓ and A be the matrix representation of conic \mathcal{A} . Suppose one of the intersection points, $p = [p_1 : p_2 : p_3]$, is given.*

$$1. \text{ Construct } \mathcal{M}_\ell = \begin{bmatrix} 0 & \tau & -\mu \\ -\tau & 0 & \lambda \\ \mu & -\lambda & 0 \end{bmatrix} \text{ and } X = \begin{bmatrix} 2p_1 & 0 & 0 \\ 0 & 2p_2 & 0 \\ 0 & 0 & 2p_3 \\ p_2 & p_1 & 0 \\ p_3 & 0 & p_1 \\ 0 & p_3 & p_2 \end{bmatrix}.$$

2. Compute $V_{A,\ell} = \mathcal{M}_\ell^T A \mathcal{M}_\ell = [V_{i,j}]$.

$$3. (X^T X)^{-1} X^T \begin{bmatrix} V_{1,1} \\ V_{2,2} \\ V_{3,3} \\ V_{1,2} \\ V_{1,3} \\ V_{2,3} \end{bmatrix} \text{ is proportional to the other point of intersection } q.$$

3.2 Construction of a Poncelet polygon

Given an n -Poncelet pair $(\mathcal{A}, \mathcal{B})$ and a point $P_1 \in \mathcal{A}$, we want to construct the Poncelet n -gon with starting vertex P_1 . In this section, we describe the steps for doing this construction.

Algorithm 3.2.1 (Constructing a Poncelet n -gon inscribed in \mathcal{A} and circumscribed about \mathcal{B}).

Let P_k be the k th vertex of our polygon.

1. Choose $P_1 \in \mathcal{A}$ as a starting vertex and set $k = 1$.
2. Construct $\ell_k = \mathbf{B}P_k$, the polar line to \mathcal{B} with respect to P_k .
3. If $k = 1$, obtain the intersection points of ℓ_k and \mathcal{B} using Algorithm 3.1.1 and assign one intersection point to R_1 . If $k > 1$, assign to R_k the other intersection point of ℓ_k and \mathcal{B} given the known intersection point R_{k-1} using Algorithm 3.1.2.
4. Construct $\tau_k = \mathbf{B}R_k$, the tangent line to \mathcal{B} at R_k .

5. Obtain the next vertex, P_{k+1} , as the other intersection point of τ_k and \mathcal{A} given the known intersection point P_k using Algorithm 3.1.2.
6. Increment k by one and repeat step 2. Stop when $k = n + 1$.

We illustrate in Figure 3.2.1 how Algorithm 3.2.1 works in the real plane. Here, we put an arrowhead on the side of our Poncelet polygon to establish the direction of our construction. This direction is arbitrary and is decided by our choice of R_1 , where the forward direction is chosen to be the path from P_1 going to the next vertex through the line τ_1 that is tangent to \mathcal{B} at R_1 . The polygon that we obtain in the end will not depend on this choice of direction; however, we make this choice to label the vertices of our Poncelet polygon consistently.

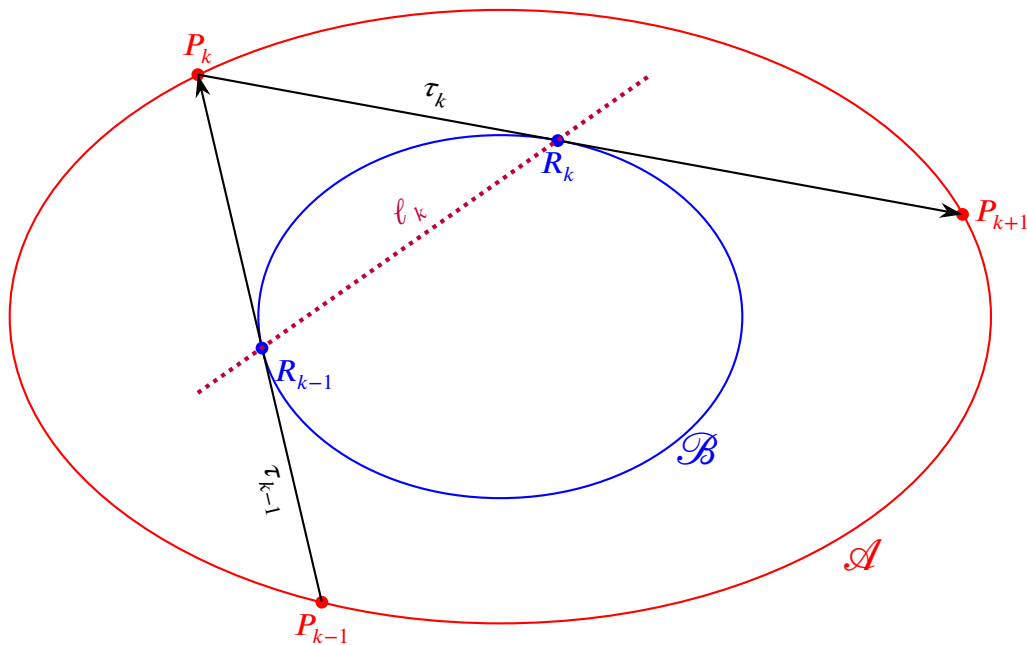


Figure 3.2.1: Construction in the real plane

Following the Poncelet polygon construction in Algorithm 3.2.1, notice that it is only for the case of $k = 1$ that we need to compute two intersection points using Algorithm 3.1.1. In effect, we only need to take one square root for the whole construction. In this study, whenever we are intersecting lines or conics in $\mathbf{P}^2(\mathbb{F}_q)$, we implicitly consider the intersection of their versions in the extended plane $\mathbf{P}^2(\overline{\mathbb{F}_q})$. The need to do our computations in the extended plane arises when the square root that we are considering is not defined in \mathbb{F}_q .

Now, we show that we don't actually need the entire extended plane in our calculations.

Lemma 3.2.2. *All elements of \mathbb{F}_q have a square root in \mathbb{F}_{q^2} .*

Proof. Consider the primitive element α_* of \mathbb{F}_{q^2} and use the fact that the multiplicative group generated by α_*^{q+1} is isomorphic to $\mathbb{F}_q \setminus \{0\}$. Hence, α_*^{q+1} can be used in lieu of α in Definition 2.1.16 and for $x = \alpha_*^{(q+1)k}$, we have $\sqrt{x} = \alpha_*^{\frac{(q+1)k}{2}}$. This is always defined since $\text{char } \mathbb{F}_q \neq 2$, which implies that $q + 1$ is even. \square

Proposition 3.2.3. *Let P_i be the vertices of a Poncelet polygon inscribed in $\overline{\mathcal{A}}$ and circumscribed about $\overline{\mathcal{B}}$, and ℓ_i be the polar line BP_i . If $P_i \in \mathbf{P}^2(\mathbb{F}_q)$ for some i , then $P_j \in \mathbf{P}^2(\mathbb{F}_{q^2})$ for all j . Moreover, if ℓ_i intersects \mathcal{B} in $\mathbf{P}^2(\mathbb{F}_q)$, then $P_j \in \mathbf{P}^2(\mathbb{F}_q)$ for all j .*

Proof. Choose P_i as the starting vertex and apply Algorithm 3.2.1. Since we use Algorithm 3.1.1 only once, we take the square root only once, and we are assured that all coordinates will be in \mathbb{F}_{q^2} by Lemma 3.2.2.

Now, suppose ℓ_i intersects \mathcal{B} in $\mathbf{P}^2(\mathbb{F}_q)$. Treating P_i as the starting vertex, this implies that the square root we obtain from Algorithm 3.1.1 is in \mathbb{F}_q . Since the rest of the vertices can now be obtained by Algorithm 3.1.2, which only involves linear operations, all coordinates are assured to be in \mathbb{F}_q . \square

Remark 3.2.4. *Proposition 3.2.3 implies that if any of the polar lines intersect \mathcal{B} in $\mathbf{P}^2(\mathbb{F}_q)$, then all our calculations can be done in $\mathbf{P}^2(\mathbb{F}_q)$.*

From a geometric point of view, it may happen that the polar line will not intersect the conic \mathcal{B} in the plane since \mathbb{F}_q is not an algebraically closed field. In this case, some of the vertices of the Poncelet polygon will not be in the plane. However, Proposition 3.2.3 states that we do not need the whole algebraic closure $\overline{\mathbb{F}_q}$ to obtain all the vertices in our construction. Using this, we define polygons that are in the extended plane.

Definition 3.2.5. *A Poncelet polygon inscribed in \mathcal{A} and circumscribed about \mathcal{B} is in the extended plane if at least one of its vertices is in $\mathbf{P}^2(\mathbb{F}_{q^2}) \setminus \mathbf{P}^2(\mathbb{F}_q)$.*

3.3 Degenerate polygons

In this section, we discuss the case when a Poncelet polygon becomes degenerate.

Definition 3.3.1. *A polygon is degenerate if at least two of its vertices coincide.*

The following lemmas enable us to characterize degenerate Poncelet polygons.

Lemma 3.3.2. *Using the notations in Algorithm 3.2.1, the following are equivalent:*

1. τ_k is a common tangent of $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$,
2. $P_k = P_{k+1}$,
3. $\tau_{k-1} = \tau_{k+1}$,
4. $R_{k-1} = R_{k+1}$.

Proof. τ_k being tangent to \mathcal{A} is equivalent to the consecutive vertices P_k and P_{k+1} coinciding with each other. $P_k = P_{k+1}$ is equivalent to having the tangent τ_{k+1} , treated as the side going from P_{k+1} to P_{k+2} , coinciding with the tangent τ_{k-1} , treated as the side going from P_{k-1} to P_k . Finally, $\tau_{k-1} = \tau_{k+1}$ if and only if they have the same point of tangency in \mathcal{B} , that is, $R_{k-1} = R_{k+1}$. \square

Lemma 3.3.3. *Using the notations in Algorithm 3.2.1, the following are equivalent:*

1. $P_k \in \overline{\mathcal{A}} \cap \overline{\mathcal{B}}$,
2. $P_k = R_{k-1} = R_k$,
3. $\ell_k = \tau_{k-1} = \tau_k$,
4. $P_{k-1} = P_{k+1}$.

Proof. P_k being an element of \mathcal{B} is equivalent to having the polar line ℓ_k coincide with the tangent line τ_k with point of tangency at P_k , that is, $P_k = R_k = R_{k-1}$. $R_k = R_{k-1}$ is equivalent to yielding the same tangent line, that is, $\tau_k = \tau_{k-1}$. Since both τ_k and τ_{k-1} contain the point

P_k , then $\tau_k = \tau_{k-1}$ is equivalent to having the other point of intersection to be the same, that is, $P_{k-1} = P_{k+1}$. □

We illustrate the scenario in the real plane when a common tangent is involved in Figure 3.3.1 and the scenario involving a base point in Figure 3.3.2.

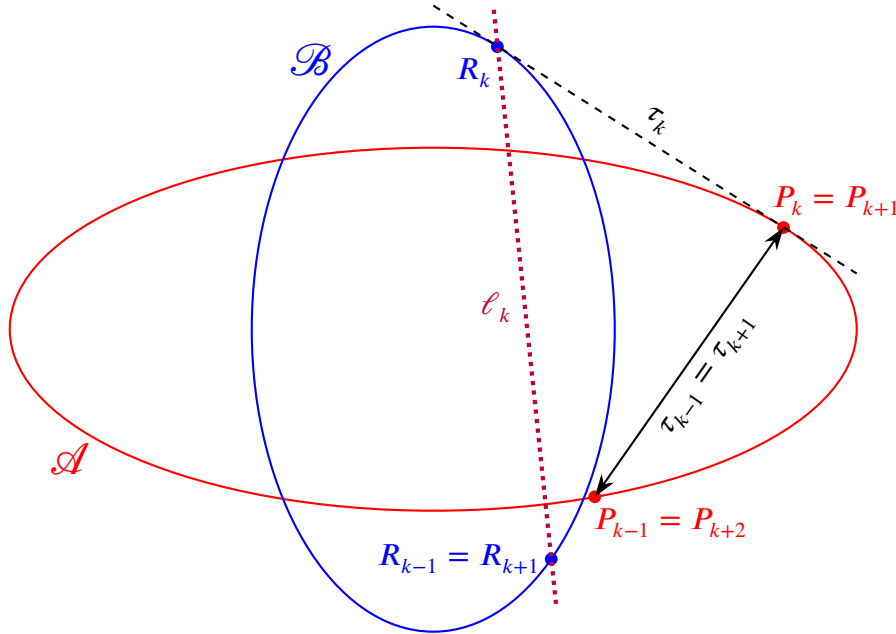


Figure 3.3.1: Degenerate Poncelet polygon when τ_k is a common tangent

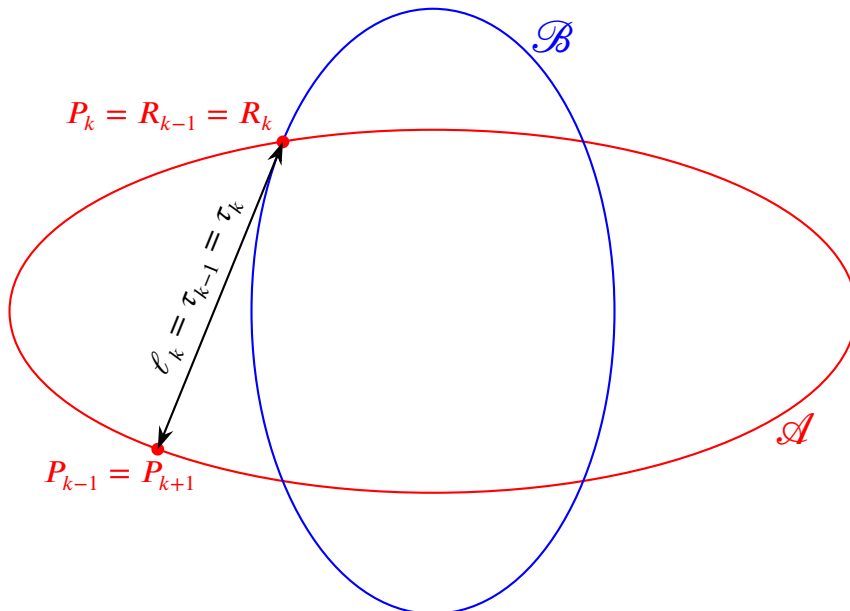


Figure 3.3.2: Degenerate Poncelet polygon when P_k is a base point

Now, we state a lemma that describes the intersection multiplicity of the base point based on the construction.

Lemma 3.3.4. *Let P_k be the k th vertex of a Poncelet n -gon inscribed in $\overline{\mathcal{A}}$ and circumscribed about $\overline{\mathcal{B}}$. Suppose P_k is an intersection point of $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$ with multiplicity m , then $m = 1$ if and only if $P_k \neq P_{k+1}$.*

Proof. Since $P_k \in \overline{\mathcal{A}} \cap \overline{\mathcal{B}}$, then we have τ_k to be tangent to $\overline{\mathcal{B}}$ at P_k by Lemma 3.3.3. Hence, P_k is a point of intersection with multiplicity greater than 1 if and only if τ_k is a common tangent of $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$, which is equivalent to having $P_k = P_{k+1}$ by Lemma 3.3.2. \square

Remark 3.3.5. *If we start the construction at vertex P_k , which is a base point of multiplicity greater than 1, then Lemma 3.3.3 and Lemma 3.3.4 imply that $P_{k-1} = P_k = P_{k+1}$. That is, the construction gets stuck at P_k because moving forward or backward in our construction returns to the same point. In this case, we get a degenerate Poncelet polygon that is a point.*

We characterize a degenerate Poncelet polygon for cases where we avoid base points of multiplicity greater than 1.

Proposition 3.3.6. *Any degenerate Poncelet n -gon with at least two distinct vertices must fall into one of these cases:*

1. *two of its vertices are base points,*
2. *two of its sides are common tangents,*
3. *one of its vertices is a base point, and one of its sides is a common tangent.*

Moreover, n is odd if and only if it belongs to the last case.

Proof. Suppose $i < j \leq n$ and P_i and P_j are two vertices of the Poncelet polygon that coincide. From the construction, we must have $P_{i+k} = P_{j-k}$ for all k such that $i+k < j-k$. Let k_* be the largest such k that satisfies this inequality. With this, we have two cases. If $(i+k_*) - (j-k_*) = 1$, then by Lemma 3.3.2, we have a common tangent inducing two consecutive vertices that are equal to each other. Otherwise, we have $(i+k_*) - (j-k_*) = 2$, which by Lemma 3.3.3 means that the vertex in between $P_{i+k_*} = P_{j-k_*}$ must be a base point. We can do the same argument in the other direction, and again, we either get a base point or a common tangent.

By Lemma 3.3.2 and Lemma 3.3.3, a common tangent will induce two vertices, base points of intersection multiplicity 1 count as one vertex, and the rest of the vertices come in pairs that coincide with each other. Thus, n is odd if and only if the degenerate polygon contains only one vertex that is a base point. \square

The remaining propositions give us a more precise description of our degenerate Poncelet polygons. Detailed examples for each of these are shown in Chapter 4 in the construction of degenerate Poncelet polygons.

Proposition 3.3.7. *For a Poncelet n -gon having two base points as vertices, if P_1 is one of these base points, then:*

- $P_{1+i} = P_{n+1-i}$, for $i = 1, \dots, \frac{n}{2} - 1$,
- $P_{\frac{n}{2}+1}$ is the other base point.

Proof. By Proposition 3.3.6, n is even in this case. By Lemma 3.3.3, we must have $P_2 = P_n$ and continuing the construction, we must have $P_{1+i} = P_{n+1-i}$, for $i = 1, \dots, \frac{n}{2} - 1$. Applying Lemma 3.3.3 once again, the vertex between $P_{1+\frac{n}{2}-1} = P_{\frac{n}{2}}$ and $P_{n+1-(\frac{n}{2}-1)} = P_{\frac{n}{2}+2}$ must be a base point and this is the vertex $P_{\frac{n}{2}+1}$. \square

Proposition 3.3.8. *For a Poncelet n -gon having two common tangents as sides, if τ_n is one of these common tangents, then:*

- $P_i = P_{n+1-i}$, for $i = 1, \dots, \frac{n}{2}$,
- $\tau_{\frac{n}{2}}$ is the other common tangent.

Proof. By Proposition 3.3.6, n is even in this case. By Lemma 3.3.2, we must have $P_1 = P_n$ and continuing the construction, we must have $P_i = P_{n+1-i}$, for $i = 1, \dots, \frac{n}{2}$. Since the vertex $P_{\frac{n}{2}}$ coincides with $P_{n+1-\frac{n}{2}} = P_{\frac{n}{2}+1}$, we have two consecutive vertices that coincide with each other and applying Lemma 3.3.2 once again, $\tau_{\frac{n}{2}}$ must be a common tangent. \square

Proposition 3.3.9. *For a Poncelet n -gon having one base point as a vertex and one common tangent as a side, if P_1 is the base point, then*

- $P_{1+i} = P_{n+1-i}$, for $i = 1, \dots, \frac{n-1}{2}$,
- $\tau_{\frac{n+1}{2}}$ is the common tangent.

Proof. By Proposition 3.3.6, n is odd in this case. By Lemma 3.3.3, we must have $P_2 = P_n$ and continuing the construction, we must have $P_{1+i} = P_{n+1-i}$, for $i = 1, \dots, \frac{n-1}{2}$. Since the vertex $P_{1+\frac{n-1}{2}} = P_{\frac{n+1}{2}}$ coincides with $P_{n+1-\frac{n-1}{2}} = P_{\frac{n+1}{2}+1}$, we have two consecutive vertices that coincide with each other and applying Lemma 3.3.2 once again, $\tau_{\frac{n+1}{2}}$ must be a common tangent. \square

3.4 Irregular pairs

In this section, we discuss the pairs of conics that cause problems when we attempt to construct a Poncelet polygon. We exclude these pairs from our study and refer to them as irregular.

Definition 3.4.1. *For a fixed pencil \mathcal{P}_j from Table 2.3.2, we call $(r, s) \in \mathbf{P}^1(\mathbb{F}_q) \times \mathbf{P}^1(\mathbb{F}_q)$ an irregular pair if it belongs to the following cases:*

Case 1: \mathcal{A} is a double line.

- for $j = 6$, $(0, \eta)$, $\eta \in \mathbb{F}_q \setminus \{0\}$,
- for $j = 8$, (∞, η) , $\eta \in \mathbb{F}_q$,
- for $j = 17$, (∞, η) , $\eta \in \mathbb{F}_q \setminus \{0\}$.

Case 2: \mathcal{A} is a union of two lines, one of which is tangent to \mathcal{B} .

- for $j \in \{4, 6, 15\}$, (∞, η) , $\eta \in \mathbb{F}_q \setminus \{0\}$,
- for $j = 5$, (∞, η) , $\eta \in \mathbb{F}_q$,
- for $j = 17$, $(0, \eta)$, $\eta \in \mathbb{F}_q \setminus \{0\}$.

Remark 3.4.2. For the case where \mathcal{A} is a double line, every Poncelet polygon inscribed in \mathcal{A} has all of its vertices equal to the chosen starting vertex. Indeed, each tangent line to \mathcal{B} passing through the starting vertex intersects \mathcal{A} only at that point, treated as an intersection of multiplicity 2.

Remark 3.4.3. Inscribing a polygon in a union of two lines will result in vertices that alternate between each line [7]. Hence, if \mathcal{A} is a union of two lines and one of which is tangent to \mathcal{B} , we eventually obtain a vertex lying in a line tangent to \mathcal{B} which coincides with one of the lines making up \mathcal{A} . In which case, our construction terminates, since the next vertex is no longer well-defined.

3.5 Results from triangle construction

For the triangle case, we have derived several results that describe its general construction. First, we have Proposition 3.5.1, which gives us a way to characterize the type of triangle that we obtain in the construction.

Proposition 3.5.1. Let $(\mathcal{A}, \mathcal{B})$ be a 3-Poncelet pair in the plane, $\mathbf{P}^2(\mathbb{F}_q)$. Let $P \in \mathcal{A}$, ℓ be the polar line to \mathcal{B} with respect to P , and define $k_{\mathcal{B},\ell}$ as in Algorithm 3.1.1, obtained from considering the intersection of line ℓ and conic \mathcal{B} . Then, point P is:

- a vertex of a non-degenerate Poncelet triangle in the plane if and only if $k_{\mathcal{B},\ell} \in \mathbb{F}_q \setminus \{0\}$,
- a vertex of a degenerate Poncelet triangle in the plane if and only if $k_{\mathcal{B},\ell} = 0$,
- a vertex of a Poncelet triangle in the extended plane if and only if $k_{\mathcal{B},\ell} \notin \mathbb{F}_q$.

Proof. We obtain a non-degenerate Poncelet triangle in the plane if the other vertices are also in the plane and distinct from each other. This is equivalent to having the polar line ℓ intersect \mathcal{B} at two points in the plane, which is the case if and only if $k_{\mathcal{B},\ell} \in \mathbb{F}_q \setminus \{0\}$.

A degenerate triangle happens when the polar line ℓ is tangent to \mathcal{B} by Lemma 3.3.3. This is equivalent to having $k_{\mathcal{B},\ell} = 0$.

Finally, $k_{B,\ell} \notin \mathbb{F}_q$ is equivalent to the polar line ℓ not intersecting \mathcal{B} in the plane, yielding a triangle in the extended plane. \square

At the pencil level, we have Proposition 3.5.2 developed from a proposition in [3]. This gives us a condition where we are assured to find a non-degenerate Poncelet triangle in the plane for transversally intersecting smooth conic pairs.

Proposition 3.5.2. *Let $(\mathcal{A}, \mathcal{B})$ be a pair of smooth, transversally intersecting conics in the plane $\mathbf{P}^2(\mathbb{F}_q)$ that is a 3-Poncelet pair. Consider the pencil π generated by \mathcal{A} and \mathcal{B} and let $b = |\mathcal{A} \cap \mathcal{B}|$, the number of base points in the plane. Then we can find a pair of conics $(\mathcal{A}, \mathcal{B})$ in π that contains a non-degenerate Poncelet triangle in the plane if and only if:*

- $q \geq 17$ for $b = 4$,
- $q \geq 7$ for $b = 2$,
- $q \geq 5$ for $b = 1$,
- $q \geq 3$ for $b = 0$.

Proof. From the proof of Proposition 3.4 in [3], we utilize Hasse-Weil bounds to obtain the condition that we can construct a non-degenerate Poncelet triangle in the plane if $\frac{1}{2}(q+1-2\sqrt{q})$ is greater than the number of common tangents of \mathcal{A} and \mathcal{B} . By duality in the projective plane, the number of common tangents in the plane is the same as the number of base points in the plane. Hence, a sufficient condition to have a non-degenerate Poncelet triangle in the plane is

$$\frac{1}{2}(q+1-2\sqrt{q}) > b \Rightarrow q > (1 + \sqrt{2b})^2.$$

The necessary condition follows from constructing all the possible Poncelet triangles for orders q that are less than that of the sufficient condition and showing that all Poncelet triangles in this case are either degenerate or in the extended plane. These calculations are presented in Appendix B. \square

Remark 3.5.3. Proposition 3.5.2 requires the existence of a 3-Poncelet pair before we can use it. For example, pencil \mathcal{P}_{16} will have $b = 0$, but there are no 3-Poncelet pairs $(\mathcal{A}, \mathcal{B})$ in this pencil if $q < 7$. Thus, we need $q \geq 7$ before we obtain a Poncelet triangle, and in this case, we are assured to find one that is non-degenerate in the plane.

The next set of propositions describes the behavior of triangles that can be constructed for particular pencils. Surprisingly, some of them lead to a simple number-theoretic result.

Proposition 3.5.4. Suppose $\text{char } \mathbb{F}_q \neq 3$ and consider the pencil \mathcal{P}_6 in Table 2.3.1. Let $(\mathcal{A}, \mathcal{B})$ be any smooth pair in the plane $\mathbf{P}^2(\mathbb{F}_q)$ in pencil \mathcal{P}_6 that is a 3-Poncelet pair. Then:

- all points of \mathcal{A} are a vertex of a Poncelet triangle in the plane if and only if -3 is a square in \mathbb{F}_q ,
- all points of \mathcal{A} not contributing to a degenerate triangle in the plane are a vertex of a triangle in the extended plane if and only if -3 is not a square in \mathbb{F}_q .

Proof. Let $\text{char } \mathbb{F}_q \neq 3$ and consider $A = C_6(r)$ and $B = C_6(s)$, which are the matrix representations of our pair of smooth conics $(\mathcal{A}, \mathcal{B})$ in \mathcal{P}_6 . By Cayley's condition, $(\mathcal{A}, \mathcal{B})$ is a 3-Poncelet pair if $r \in \mathbb{F}_q \setminus \{0\}$ and $s = 4r$. That is, we have conics

$$\mathcal{A} : rxy + z^2 = 0,$$

$$\mathcal{B} : 4rxy + z^2 = 0.$$

Let $P = [\lambda : \beta : \gamma]$ be an arbitrary point in \mathcal{A} .

Computing for the polar line to \mathcal{B} with respect to point P ,

$$\begin{bmatrix} 0 & 4r & 0 \\ 4r & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix} \begin{bmatrix} \lambda \\ \beta \\ \gamma \end{bmatrix} = \begin{bmatrix} 4\beta r \\ 4\lambda r \\ 2\gamma \end{bmatrix} = \ell.$$

By Proposition 3.5.1, $k_{B,\ell}$ determines the type of triangle that we obtain from this vertex.

Performing the computation, we have

$$V_{A,\ell} = \mathcal{M}_\ell^T A \mathcal{M}_\ell = \begin{bmatrix} 32\lambda^2 r^2 & -16r(2\lambda\beta r + \gamma^2) & 32\lambda\gamma r \\ -16r(2\lambda\beta r + \gamma^2) & 32\beta^2 r^2 & 32\beta\gamma r^2 \\ 32\lambda\gamma r & 32\beta\gamma r^2 & -128\lambda\beta r^3 \end{bmatrix},$$

which yields $k_{B,\ell} = c\sqrt{4\lambda\beta r + \gamma^2}$ for some $c \in \mathbb{F}_q \setminus \{0\}$.

Since $p = [\lambda : \beta : \gamma]$ is a point in \mathcal{A} , then it must satisfy $r\lambda\beta + \gamma^2 = 0$. Hence, we arrive at the condition that the Poncelet triangle with vertex P is in the plane if and only if $3r\lambda\beta$ is a square in \mathbb{F}_q . Since $r \neq 0$, then $3r\lambda\beta$ is zero if λ or β is zero, which corresponds to the case where P is the base point $[0 : 1 : 0]$ and $[1 : 0 : 0]$, respectively. By Proposition 3.5.1, these are degenerate triangles in the plane.

If we assume that λ and β are both non-zero, then γ should be non-zero. Otherwise, since $P \in \mathcal{A}$, then $r\lambda\beta = 0$, forcing one of the factors to be zero, which is a contradiction. In this case, we can now standardize our point $P = [\lambda : \beta : 1] \in \mathcal{A}$, which gives us the condition that $r\lambda\beta = -1$. Hence, we arrive at the final condition that P is a vertex of a non-degenerate Poncelet triangle in the plane if and only if $3r\lambda\beta = -3$ is a square in \mathbb{F}_q . This condition is independent of P and hence, all our Poncelet triangles will be in the plane if and only if -3 is a square in \mathbb{F}_q . Otherwise, if -3 is not a square in \mathbb{F}_q , by Proposition 3.5.1, all the points of \mathcal{A} will be a vertex of a triangle in the extended plane except for the base points.

□

As a corollary, we derive this simple result in number theory from a geometric argument.

Corollary 3.5.5. *Suppose $q = p^k$ where $p \notin \{2, 3\}$ is prime and k is a positive integer. -3 is a square in \mathbb{F}_q if and only if 3 divides $q - 1$. In particular, for prime $p \notin \{2, 3\}$, -3 is a quadratic residue mod p if and only if $p \equiv 1 \pmod{3}$.*

Proof. From Proposition 3.5.4, -3 is a square in \mathbb{F}_q if and only if all points of \mathcal{A} are vertices of a non-degenerate Poncelet triangle in the plane or of a degenerate triangle. Since there are $q + 1$ points on a smooth conic in \mathbb{F}_q and 2 of them will be a degenerate triangle, then $q - 1$ must be divisible by 3, the number of vertices of our non-degenerate Poncelet triangle in the plane. \square

Proposition 3.5.6. *Suppose $\text{char } \mathbb{F}_q \neq 3$ and consider the pencil \mathcal{P}_{17} in Table 2.3.1. Let $(\mathcal{A}, \mathcal{B})$ be any smooth pair in the plane $\mathbf{P}^2(\mathbb{F}_q)$ in pencil \mathcal{P}_{17} that is a 3-Poncelet pair. Then:*

- *all points of \mathcal{A} are a vertex of a non-degenerate Poncelet triangle in the plane if and only if -3 is not a square in \mathbb{F}_q ,*
- *all points of \mathcal{A} are a vertex of a triangle in the extended plane if and only if -3 is not a square in \mathbb{F}_q .*

Proof. Similar to proof of Proposition 3.5.4. Note that for this pencil, there are no degenerate triangles since there are no base points in the plane. \square

Proposition 3.5.7. *Suppose $\text{char } \mathbb{F}_q = 3$ and consider the pencil \mathcal{P}_8 in Table 2.3.1. Let $(\mathcal{A}, \mathcal{B})$ be any smooth pair in the plane $\mathbf{P}^2(\mathbb{F}_q)$ in pencil \mathcal{P}_8 with matrix representations $A = C_8(r)$ and $B = C_8(s)$. Then:*

- *all points of \mathcal{A} are a vertex of a Poncelet triangle in the plane if and only if $s - r$ is a square in \mathbb{F}_q ,*
- *all points of \mathcal{A} not contributing to a degenerate triangle in the plane are a vertex of a triangle in the extended plane if and only if $s - r$ is not a square in \mathbb{F}_q .*

Proof. Similar to proof of Proposition 3.5.4. \square

4. Examples regarding the construction of Poncelet polygons

In this chapter, we provide examples of Poncelet polygons in different scenarios. To illustrate our construction, we view our points in the affine plane $z = 1$ and associate the homogeneous coordinate $[x : y : 1]$ with the ordered pair $(x, y) \in \mathbb{F}_q^2$. Note that points on the horizon with homogeneous coordinates $[x : y : 0]$ are not visible in our illustrations.

4.1 Poncelet Triangle

For the Poncelet triangle construction, we consider pencil \mathcal{P}_4 over $\mathbf{P}^2(\mathbb{F}_{11})$. This choice allows us to provide examples of all kinds of Poncelet triangles since \mathcal{P}_4 will have base points of multiplicities 1 and 2. In particular, as shown in Section 3.3, we have a degenerate Poncelet triangle that appears as a line segment when we choose a base point of multiplicity 1 as the starting vertex. On the other hand, we get a degenerate Poncelet triangle that gets stuck at the starting vertex when we start on a base point of multiplicity 2. Moreover, the order of the finite field was chosen to be the smallest so that both a non-degenerate Poncelet triangle in the plane and a Poncelet triangle in the extended plane exist.

In this section, we consider $\mathcal{A} : xy + xz + z^2 = 0$ and $\mathcal{B} : 4xy + xz + z^2 = 0$. Their matrix representations are:

$$A = C_4(1) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix}, \text{ and } B = C_4(4) = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix}$$

This particular choice satisfies Cayley's condition for $n = 3$. We display conic \mathcal{A} in Figure 4.1.1

and conic \mathcal{B} in Figure 4.1.2. An overlaid version showing both conics is given in Figure 4.1.3.

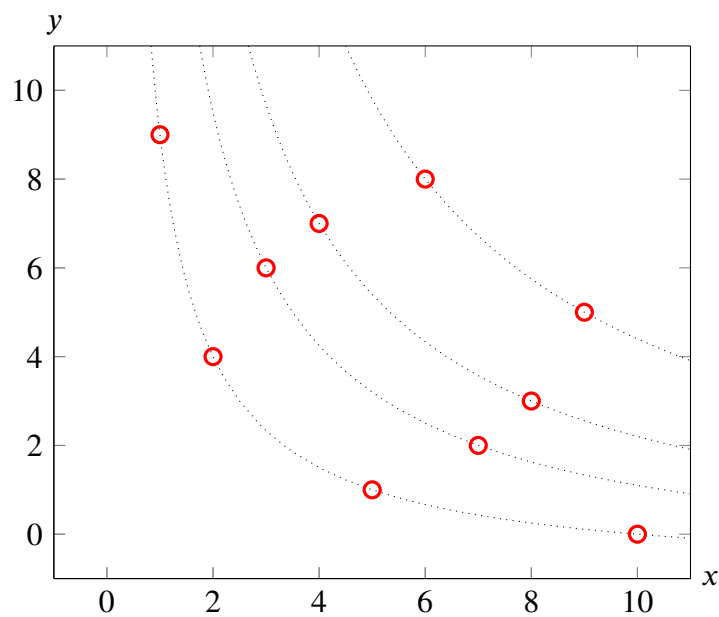


Figure 4.1.1: Conic $\mathcal{A} : xy + x + 1 = 0$ in \mathbb{F}_{11}^2

- Hollow circles are the points of conic $\mathcal{A} : xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Dotted curves represent the underlying equation of the conic, $xy + x + 1 = 11k$, $k \in \mathbb{Z}$
- Only curves that intersect at least one point in \mathbb{F}_{11}^2 are displayed

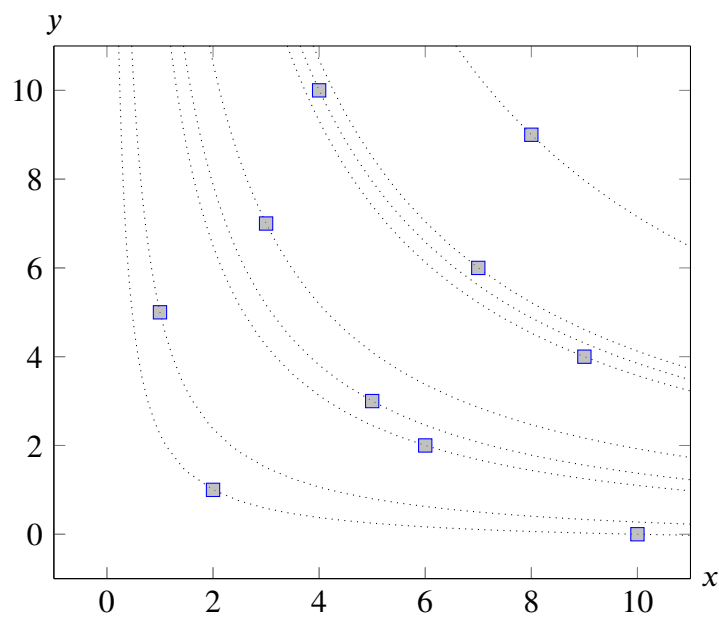


Figure 4.1.2: Conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2

- Filled squares are the points of conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Dotted curves represent the underlying equation of the conic, $4xy + x + 1 = 11k$, $k \in \mathbb{Z}$
- Only curves that intersect at least one point in \mathbb{F}_{11}^2 are displayed

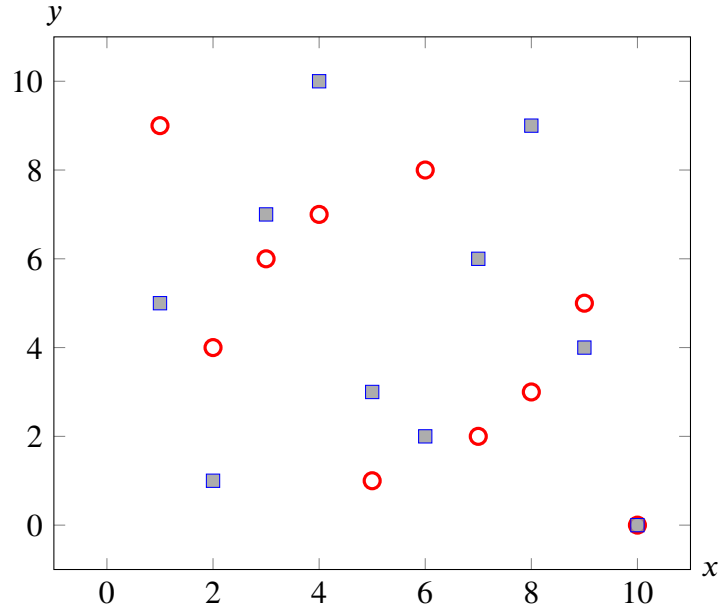


Figure 4.1.3: Conics $\mathcal{A} : xy + x + 1 = 0$ and $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2

- Hollow circles are the points of conic $\mathcal{A} : xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Filled squares are the points of conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2

Example 4.1.1. Non-degenerate Poncelet triangle in the plane:

We follow Algorithm 3.2.1 to compute the vertices of our Poncelet triangle starting with vertex $P_1 = [1 : 9 : 1]$ and summarize the calculations in Table 4.1.1.

Table 4.1.1: Non-degenerate Poncelet triangle in the plane

k	1	2	3
Vertex (P_k)	[1 : 9 : 1]	[9 : 5 : 1]	[5 : 1 : 1]
Polar Line (ℓ_k)	[5 : 5 : 1]	[7 : 1 : 0]	[7 : 6 : 1]
Point of Tangency (R_k)	[7 : 6 : 1]	[6 : 2 : 1]	[9 : 4 : 1]
Tangent Line (τ_k)	[4 : 8 : 1]	[8 : 3 : 1]	[2 : 1 : 0]

We show the calculations for obtaining P_2 starting from P_1 . Note that all arithmetic operations are done in modulo 11. The polar line to \mathcal{B} with respect to P_1 is given by

$$\ell_1 = BP_1 = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 9 \\ 1 \end{bmatrix} = \begin{bmatrix} 37 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \\ 3 \end{bmatrix}.$$

Hence, we have

$$\ell_1 = [4 : 4 : 3] = [5 : 5 : 1].$$

Now, we compute the intersection of ℓ_1 and \mathcal{B} using Algorithm 3.1.1.

$$\mathcal{M}_{\ell_1} = \begin{bmatrix} 0 & 1 & -5 \\ -1 & 0 & 5 \\ 5 & -5 & 0 \end{bmatrix},$$

$$\begin{aligned} V_{B,\ell_1} &= \mathcal{M}_{\ell_1}^T \mathbf{B} \mathcal{M}_{\ell_1} = \begin{bmatrix} 0 & -1 & 5 \\ 1 & 0 & -5 \\ -5 & 5 & 0 \end{bmatrix} \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & 1 & -5 \\ -1 & 0 & 5 \\ 5 & -5 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 50 & -49 & -5 \\ -49 & 40 & 45 \\ -5 & 45 & -200 \end{bmatrix} = \begin{bmatrix} 6 & 6 & 6 \\ 6 & 7 & 1 \\ 6 & 1 & 9 \end{bmatrix} = [V_{i,j}], \end{aligned}$$

$$k_{B,\ell_1} = \sqrt{V_{1,2}^2 - V_{1,1}V_{2,2}} = \sqrt{6^2 - (6)(7)} = \sqrt{5} = 4,$$

which, by Proposition 3.5.1, assures us that we obtain a non-degenerate Poncelet triangle in the plane.

Finally,

$$V_{B,\ell_1} + k_{B,\ell_1} \mathcal{M}_{\ell_1} = \begin{bmatrix} 6 & 6 & 6 \\ 6 & 7 & 1 \\ 6 & 1 & 9 \end{bmatrix} + 4 \begin{bmatrix} 0 & 1 & -5 \\ -1 & 0 & 5 \\ 5 & -5 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 10 & -14 \\ 2 & 7 & 21 \\ 26 & -19 & 9 \end{bmatrix} = \begin{bmatrix} 6 & 10 & 8 \\ 2 & 7 & 10 \\ 4 & 3 & 9 \end{bmatrix}.$$

Choosing the intersection point represented by the first column, we obtain

$$R_1 = [6 : 2 : 4] = [7 : 6 : 1],$$

and the other intersection point represented by the first row is given by

$$R_3 = [6 : 10 : 8] = [9 : 4 : 1].$$

We illustrate the polar line ℓ_1 intersecting conic \mathcal{B} in Figure 4.1.4.

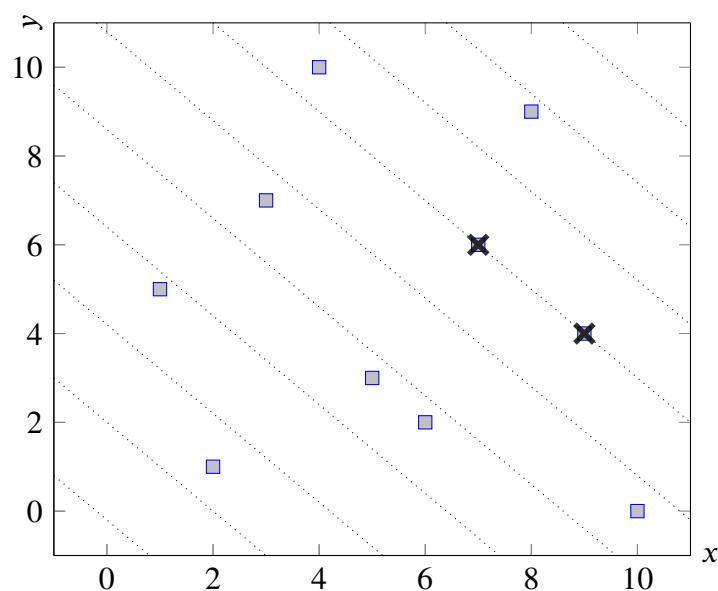


Figure 4.1.4: Polar line $\ell_1 : 5x + 5y + 1 = 0$ and conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2

- Filled squares are the points of conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Dotted lines represent the underlying equation of the polar line, $5x + 5y + 1 = 11k$, $k \in \mathbb{Z}$
- Cross marks represent the intersection points of ℓ_1 and \mathcal{B}

Note that in our case, we arbitrarily chose $R_1 = [7 : 6 : 1]$, and choosing $[9 : 4 : 1]$ as R_1 would yield the same polygon, traversed in the opposite direction.

The tangent line at R_1 is given by

$$\tau_1 = BR_1 = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 7 \\ 6 \\ 1 \end{bmatrix} = \begin{bmatrix} 25 \\ 28 \\ 9 \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \\ 9 \end{bmatrix}.$$

Hence, we have

$$\tau_1 = [3 : 6 : 9] = [4 : 8 : 1].$$

Since we know that τ_1 intersect \mathcal{A} at $P_1 = [1 : 9 : 1]$, we use Algorithm 3.1.2 to compute the other intersection point of τ_1 and \mathcal{A} which by construction, is our next vertex P_2 .

$$\mathcal{M}_{\tau_1} = \begin{bmatrix} 0 & 1 & -8 \\ -1 & 0 & 4 \\ 8 & -4 & 0 \end{bmatrix}, X = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 18 & 0 \\ 0 & 0 & 2 \\ 9 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 9 \end{bmatrix},$$

$$\begin{aligned} V_{A,\tau_1} &= \mathcal{M}_{\tau_1}^T A \mathcal{M}_{\tau_1} = \begin{bmatrix} 0 & -1 & 8 \\ 1 & 0 & -4 \\ -8 & 4 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & 1 & -8 \\ -1 & 0 & 4 \\ 8 & -4 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 128 & -57 & -56 \\ -57 & 24 & 36 \\ -56 & 36 & -64 \end{bmatrix} = \begin{bmatrix} 7 & 9 & 10 \\ 9 & 2 & 3 \\ 10 & 3 & 2 \end{bmatrix} = [V_{i,j}]. \end{aligned}$$

Note that for a 3×3 , invertible matrix A , we have $\det(A)A^{-1} = \text{adj}(A)$, where

$$\text{adj} \left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \right) = \begin{bmatrix} a_{22}a_{33} - a_{23}a_{32} & a_{13}a_{32} - a_{12}a_{33} & a_{12}a_{23} - a_{13}a_{22} \\ a_{23}a_{31} - a_{21}a_{33} & a_{11}a_{33} - a_{13}a_{31} & a_{13}a_{21} - a_{11}a_{23} \\ a_{21}a_{32} - a_{22}a_{31} & a_{12}a_{31} - a_{11}a_{32} & a_{11}a_{22} - a_{12}a_{21} \end{bmatrix}.$$

Hence, the inverse matrix is just a scalar multiple of the adjoint matrix. To simplify our calculations, we use the adjoint rather than the inverse.

$$\begin{aligned} \begin{bmatrix} V_{1,1} \\ V_{2,2} \\ V_{3,3} \\ V_{1,2} \\ V_{1,3} \\ V_{2,3} \end{bmatrix} &= \text{adj} \left(\begin{bmatrix} 9 & 9 & 1 \\ 9 & 7 & 9 \\ 1 & 9 & 9 \end{bmatrix} \right) \begin{bmatrix} 2 & 0 & 0 & 9 & 1 & 0 \\ 0 & 7 & 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 2 \\ 2 \\ 9 \\ 10 \\ 3 \end{bmatrix} \\ &= \begin{bmatrix} 4 & 5 & 8 \\ 5 & 3 & 5 \\ 8 & 5 & 4 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 8 \end{bmatrix} = \begin{bmatrix} 9 \\ 5 \\ 1 \end{bmatrix}, \end{aligned}$$

which gives us the next vertex $P_2 = [9 : 5 : 1]$.

This completes the first side of our Poncelet triangle, and we display this in Figure 4.1.5.

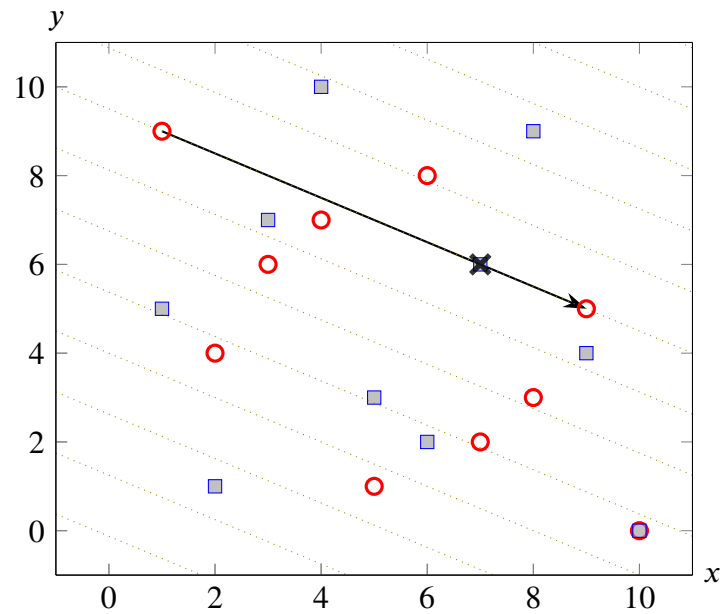


Figure 4.1.5: First side of a non-degenerate Poncelet triangle in \mathbb{F}_{11}^2

- Hollow circles are the points of conic $\mathcal{A} : xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Filled squares are the points of conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Dotted lines represent the underlying equation of the tangent line, $4x + 8y + 1 = 11k$, $k \in \mathbb{Z}$
- Cross mark represent the point of tangency to \mathcal{B}
- Arrows represent the direction we traverse the polygon

The complete figure for our constructed Poncelet triangle is given in Figure 4.1.6.

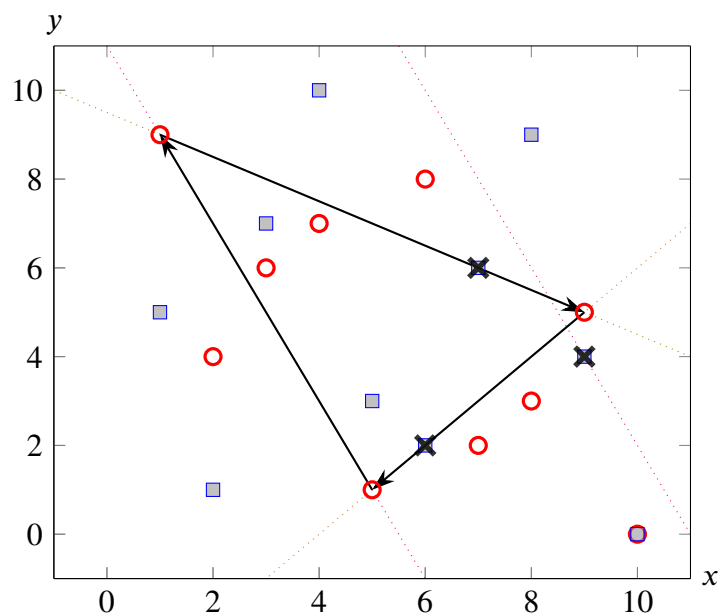


Figure 4.1.6: Non-degenerate Poncelet triangle in \mathbb{F}_{11}^2

- Hollow circles are the points of conic $\mathcal{A} : xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Filled squares are the points of conic $\mathcal{B} : 4xy + x + 1 = 0$ in \mathbb{F}_{11}^2
- Dotted lines represent the tangent lines to \mathcal{B} . Parallel lines represent the same lines via modulo arithmetic
- Cross marks represent the points of tangency to \mathcal{B}
- Arrows represent the direction we traverse the polygon

Example 4.1.2. Degenerate Poncelet triangle as a line segment:

Starting at $P_1 = [10 : 0 : 1]$, a base point of multiplicity 1, Lemma 3.3.3 states that $P_2 = P_0$, where, by our convention, P_0 is the previous vertex and hence, $P_0 = P_3$ since these are vertices of a Poncelet triangle. Moreover, by Lemma 3.3.2, since $P_2 = P_3$, we have that τ_2 is a common tangent of \mathcal{A} and \mathcal{B} . Finally, Lemma 3.3.4 assures us that $P_1 \neq P_2$ and hence, we obtain a degenerate triangle in the form of a line segment.

We summarize the calculations for this case in Table 4.1.2.

Table 4.1.2: Degenerate Poncelet triangle as a line segment in \mathbb{F}_{11}^2

k	1	2	3
Vertex (P_k)	$[10 : 0 : 1]$	$[7 : 2 : 1]$	$[7 : 2 : 1]$
Polar Line (ℓ_k)	$[1 : 7 : 1]$	$[1 : 8 : 1]$	$[1 : 8 : 1]$
Point of Tangency (R_k)	$[10 : 0 : 1]$	$[2 : 1 : 1]$	$[10 : 0 : 1]$
Tangent Line (τ_k)	$[1 : 7 : 1]$	$[4 : 2 : 1]$	$[1 : 7 : 1]$

Example 4.1.3. Degenerate Poncelet Triangle as a Point:

Starting at $P_1 = [0 : 1 : 0]$, a base point of intersection multiplicity 2, yields a degenerate Poncelet triangle that appears as a point. Performing Algorithm 3.2.1, we get $\ell_1 = [1 : 0 : 0]$ which is also the tangent τ_1 to \mathcal{B} at $P_1 = R_1 = R_0$. But τ_1 is also tangent to \mathcal{A} and so we have $P_1 = P_2$. If we choose the opposite direction through R_0 , we get the same tangent line τ_1 . Moreover, the same calculation will occur in the next iteration, leaving us stuck at the point P_1 in our construction.

Example 4.1.4. Poncelet triangle in the extended plane:

For $P = [2 : 4 : 1]$, Proposition 3.5.1 gives us $k_{B,\ell} = \sqrt{8}$ which is not an element of \mathbb{F}_{11} since 8 is not a square in \mathbb{F}_{11} . Based on our discussion in Section 2.1, we need to do the calculation in \mathbb{F}_{11^2} where the elements are represented in the form $a_1\alpha + a_0$ with $a_1, a_0 \in \mathbb{F}_{11}$ and α being the primitive element of \mathbb{F}_{11^2} given by a fixed root of the Conway polynomial $C_{11,2}(x) = x^2 + 7x + 2$.

Observe that in this representation of \mathbb{F}_{11^2} , we have $\alpha^2 = -7\alpha - 2 = 4\alpha + 9$. Hence,

$$\begin{aligned} (9\alpha + 4)^2 &= 81\alpha^2 + 72\alpha + 16 = 4\alpha^2 + 6\alpha + 5 \\ &= 4(4\alpha + 9) + 6\alpha + 5 = 22\alpha + 41 = 8 \end{aligned}$$

In effect, we have shown here that $9\alpha + 4$ is a square root of 8. In fact, this is the principal square root since $\alpha^{36} = 8$ and $\alpha^{18} = 9\alpha + 4$. Thus, $\sqrt{8} = 9\alpha + 4$.

The rest of the computations are done in the same way as shown in the case of a non-degenerate Poncelet triangle. We summarize the construction starting from $P_1 = [2 : 4 : 1]$ in Table 4.1.3.

Table 4.1.3: Poncelet triangle in the extended plane

k	1	2	3
Vertex (P_k)	$[2 : 4 : 1]$	$[5\alpha + 3 : 3\alpha + 5 : 1]$	$[6\alpha + 1 : 8\alpha + 6 : 1]$
Polar Line (ℓ_k)	$[7 : 2 : 1]$	$[\alpha + 4 : 4\alpha + 6 : 1]$	$[10\alpha + 8 : 7\alpha : 1]$
Point of Tangency (R_k)	$[9\alpha + 2 : 7\alpha + 9 : 1]$	$[4 : 10 : 1]$	$[2\alpha + 5 : 4\alpha + 4 : 1]$
Tangent Line (τ_k)	$[7\alpha + 5 : 2\alpha : 1]$	$[5 : 10 : 1]$	$[4\alpha : 9\alpha + 8 : 1]$

4.2 Poncelet Tetragon

For the tetragon case, we will show an example of a Poncelet polygon that is inscribed in a singular conic \mathcal{A} . We consider pencil \mathcal{P}_3 over $\mathbf{P}^2(\mathbb{F}_{11})$ for this construction.

In this section, we consider $\mathcal{A} : xy = 0$ and $\mathcal{B} : 6xy + xz + yz + z^2 = 0$. This particular choice will satisfy Cayley's condition for $n = 4$.

Example 4.2.1. Non-degenerate Poncelet tetragon in the plane:

The tetragon construction follows the same construction as that of the triangle case, and we summarize the calculations in Table 4.2.1. We provide the complete figure of our constructed Poncelet tetragon in Figure 4.2.1, where we used modulo arithmetic to improve visualization.

Table 4.2.1: Poncelet tetragon in \mathbb{F}_{11}^2

k	1	2	3	4
Vertex (P_k)	[0 : 5 : 1]	[7 : 0 : 1]	[0 : 1 : 1]	[6 : 0 : 1]
Polar Line (ℓ_k)	[6 : 8 : 1]	[5 : 6 : 1]	[6 : 4 : 1]	[7 : 6 : 1]
Point of Tangency (R_k)	[5 : 3 : 1]	[4 : 2 : 1]	[8 : 7 : 1]	[1 : 6 : 1]
Tangent Line (τ_k)	[3 : 2 : 1]	[3 : 10 : 1]	[9 : 10 : 1]	[9 : 2 : 1]

Remark 4.2.2. In Figure 4.2.1, we see that the vertices of our Poncelet tetragon alternate between the two lines, $x = 0$ and $y = 0$, making up our singular conic \mathcal{A} . This behavior persists for $n > 4$, and in general, we can only inscribe a Poncelet n -gon in a singular conic \mathcal{A} if n is even [7].

Example 4.2.3. Construction involving the intersection of the two lines making up \mathcal{A} :

The lines $x = 0$ and $y = 0$ meet at $[0 : 0 : 1]$. Since none of the lines making up \mathcal{A} are tangent to $\overline{\mathcal{B}}$, then every tangent line to $\overline{\mathcal{B}}$ that passes through $P_1 = [0 : 0 : 1]$ will only intersect \mathcal{A} at P_1 . That is, τ_1 is a common tangent of $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$ and by Lemma 3.3.2, we must have $P_1 = P_2$. The same argument works for the opposite direction, giving us $P_0 = P_1$. In either direction, the construction is stuck at P_1 and we obtain a degenerate Poncelet tetragon as a point.

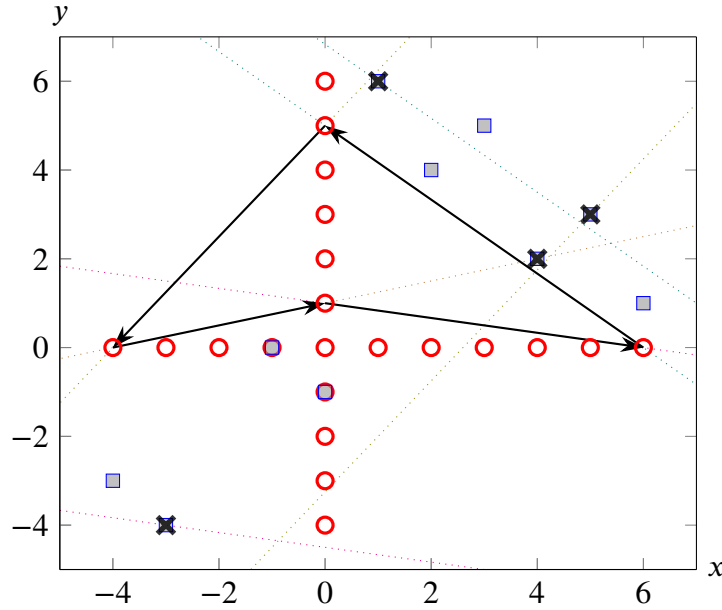


Figure 4.2.1: Poncelet Tetragon in \mathbb{F}_{11}^2

- Hollow circles are the points of conic $\mathcal{A} : xy = 0$ in \mathbb{F}_{11}^2
- Filled squares are the points of conic $\mathcal{B} : 6xy + x + y + 1 = 0$ in \mathbb{F}_{11}^2
- Dotted lines represent the tangent lines to \mathcal{B} . Parallel lines represent the same lines via modulo arithmetic
- Cross marks represent the points of tangency to \mathcal{B}
- Arrows represent the direction we traverse the polygon

4.3 Degenerate Poncelet polygons

In this section, we provide examples focusing on degenerate polygons. General statements for these examples are given in Section 3.3.

Example 4.3.1. Degenerate Poncelet polygons having two base points as vertices:

Consider pencil \mathcal{P}_{14} over $\mathbf{P}^2(\mathbb{F}_3)$ for this construction.

Let $\mathcal{A} : xy + xz + y^2 + yz + 2z^2 = 0$ and $\mathcal{B} : xz + y^2 + yz + 2z^2 = 0$. This is a 4-Poncelet pair and starting at $P_1 = [1 : 0 : 0]$, the rest of the vertices are given by:

$$P_2 = P_4 = [2 : 1 : 0], P_3 = [1 : 0 : 1].$$

Here, P_1 and P_3 are both base points.

Now, consider $\mathcal{A} : xz + y^2 + yz + 2z^2 = 0$ and $\mathcal{B} : xy + xz + y^2 + yz + 2z^2 = 0$. This is a

6-Poncelet pair and starting at $P_1 = [1 : 0 : 0]$, the rest of the vertices are given by:

$$P_2 = P_6 = [1 : 2 : 1], P_3 = P_5 = [2 : 1 : 1], P_4 = [1 : 0 : 1].$$

Here, P_1 and P_4 are both base points.

Example 4.3.2. Degenerate Poncelet polygons having two common tangents as sides:

Consider pencil \mathcal{P}_{19} over $\mathbf{P}^2(\mathbb{F}_3)$ for this construction.

Let $\mathcal{A} : 2(x^2 - 2y^2) + 2xy - y^2 + z^2 = 0$ and $\mathcal{B} : 2xy - y^2 + z^2 = 0$. This is a 4-Poncelet pair, and with τ_4 being a common tangent, the vertices are given by:

$$P_1 = P_4 = [1 : 0 : 1], P_2 = P_3 = [2 : 0 : 1].$$

Here, τ_2 and τ_4 are both common tangents.

Now, consider $\mathcal{A} : (x^2 - 2y^2) + 2xy - y^2 + z^2 = 0$ and $\mathcal{B} : 2(x^2 - 2y^2) + 2xy - y^2 + z^2 = 0$. This is a 6-Poncelet pair and with τ_6 being a common tangent, the vertices are given by:

$$P_1 = P_6 = [1 : 2 : 1], P_2 = P_5 = [1 : 1 : 0], P_3 = P_4 = [2 : 1 : 1].$$

Here, τ_3 and τ_6 are both common tangents.

Example 4.3.3. Degenerate Poncelet polygons having one base point as a vertex and one common tangent as a side:

Consider pencil \mathcal{P}_{18} over $\mathbf{P}^2(\mathbb{F}_3)$ for this construction.

Let $\mathcal{A} : 2(-xz + y^2) + x^2 + 2y^2 + yz = 0$ and $\mathcal{B} : (-xz + y^2) + x^2 + 2y^2 + yz = 0$. This is a 3-Poncelet pair, and starting with $P_1 = [0 : 0 : 1]$, the other vertices are given by:

$$P_2 = P_3 = [2 : 2 : 1].$$

Here, P_1 is a base point and τ_2 is a common tangent. In fact, this is the case when our degenerate

Poncelet triangle appears as a line segment.

Now, consider $\mathcal{A} : (-xz + y^2) + x^2 + 2y^2 + yz = 0$ and $\mathcal{B} : x^2 + 2y^2 + yz = 0$. This is a 5-Poncelet pair and starting with $P_1 = [0 : 0 : 1]$, the rest of the vertices are given by:

$$P_2 = P_5 = [1 : 0 : 1], P_3 = P_4 = [2 : 1 : 1].$$

Here, P_1 is a base point and τ_3 is a common tangent.

4.4 Valid pairs in non-transversal case

So far, we have provided samples where \mathcal{A} and \mathcal{B} intersect non-transversally, as seen in Section 4.1, and when \mathcal{A} is singular, as seen in Section 4.2. Now, we provide an example in which \mathcal{A} and \mathcal{B} intersect non-transversally, and \mathcal{A} is singular.

Taking into account our irregular pairs, the only valid pair where this can happen is when the intersection point of the two lines making up \mathcal{A} lies in the conic \mathcal{B} , acting as the intersection point of multiplicity 2. This happens when considering pairs corresponding to $(0, s)$, $s \neq 0$ in pencil \mathcal{P}_4 or \mathcal{P}_{15} .

The difference between these pencils is that in pencil \mathcal{P}_4 , both lines making up \mathcal{A} are in the plane $\mathbf{P}^2(\mathbb{F}_q)$, and in effect, the two other base points, each of multiplicity 1, are also in the plane. For pencil \mathcal{P}_{15} , the lines making up \mathcal{A} are in the extended plane, and only the intersection of these two lines is in the plane. For our sample construction, consider pencil \mathcal{P}_4 over $\mathbf{P}^2(\mathbb{F}_3)$.

In this section, we consider $\mathcal{A} : xz + z^2 = 0$ and $\mathcal{B} : xy + xz + z^2 = 0$. This is a 6-Poncelet pair where \mathcal{A} is the union of the two lines $x + z = 0$ and $z = 0$, which intersects at $[0 : 1 : 0] \in \mathcal{B}$.

Example 4.4.1. Degenerate Poncelet hexagon:

We can start at the base point $P_1 = [1 : 0 : 0]$ and the rest of the vertices are given by:

$$P_2 = P_6 = [2 : 2 : 1], P_3 = P_5 = [1 : 1 : 0], P_4 = [2 : 0 : 1].$$

and from our discussions about degenerate Poncelet polygons, $P_4 = [2 : 0 : 1]$ is the other base point of multiplicity 1.

Example 4.4.2. Non-degenerate Poncelet hexagon:

In our current case, all Poncelet hexagons in the plane are degenerate. Hence, we need to do our construction in $\mathbf{P}^2(\mathbb{F}_9)$. The Conway polynomial for this case is given by $C_{3,2}(x) = x^2 + 2x + 2$. Defining α as the primitive of \mathbb{F}_9 which is a fixed root of $C_{3,2}(x)$, an example of a non-degenerate Poncelet hexagon have vertices:

$$P_1 = [2 : 1 : 1], P_2 = [2\alpha + 2 : 1 : 0], P_3 = [2 : \alpha + 1 : 1],$$

$$P_4 = [2 : 1 : 0], P_5 = [2 : 2\alpha + 2 : 1], P_6 = [\alpha + 1 : 1 : 0].$$

5. Computation of probabilities

Now that we have a good understanding of Poncelet polygons and their construction, we are in a position to answer our main research question. In this chapter, we compute the probability of selecting a random pair of conics in a given pencil of conics in $\mathbf{P}^2(\mathbb{F}_q)$ such that a Poncelet triangle or a Poncelet tetragon can be constructed from it. To do this, we define precisely the probability spaces under consideration and compute the probabilities of obtaining a 3-Poncelet pair or a 4-Poncelet pair.

We define our valid pairs, which are the pairs we consider in this study.

Definition 5.0.1. *For a fixed pencil \mathcal{P}_j from Table 2.3.2, we call $(r, s) \in \mathbf{P}^1(\mathbb{F}_q) \times \mathbf{P}^1(\mathbb{F}_q)$ a valid pair if $r \neq s$, (r, s) is not an irregular pair, and $\det C_j(s) \neq 0$. We denote by Φ_j the set of valid pairs in pencil \mathcal{P}_j .*

To allow comparisons to the previous works of [3, 23], we also consider the subset of valid pairs (r, s) in pencil \mathcal{P}_j with the additional constraint that $\det C_j(r) \neq 0$ and call them smooth pairs in pencil \mathcal{P}_j .

Definition 5.0.2. *For a fixed pencil \mathcal{P}_j from Table 2.3.2, we call $(r, s) \in \mathbf{P}^1(\mathbb{F}_q) \times \mathbf{P}^1(\mathbb{F}_q)$ a smooth pair if (r, s) is a valid pair and $\det C_j(r) \neq 0$. We denote by Ψ_j the set of smooth pairs in pencil \mathcal{P}_j .*

For each $j \in \{3, 4, 5, 6, 8, 14, 15, 16, 17, 18, 19\}$, we compute probabilities in the sample space Φ_j , equipped with the uniform measure which gives each valid pair in \mathcal{P}_j an equal chance of being selected. Additionally, we consider the case when the sample space is restricted to Ψ_j .

Under this setup, we derive in Section 5.1 the form of H_2 and H_3 from Theorem 2.4.4 for each pencil. Then, we answer our main research questions by computing the probability of obtaining a 3-Poncelet pair in Section 5.2 and obtaining a 4-Poncelet pair in Section 5.3.

Before deriving the probabilities in the general case, we illustrate how this works for a fixed pencil and a fixed order in the following example.

Example 5.0.3. *n-Poncelet pairs for pencil \mathcal{P}_3 in $\mathbf{P}^2(\mathbb{F}_7)$.*

We summarize in Table 5.0.1 the value of n such that the valid pair (r, s) corresponds to an n -Poncelet pair. For instance, the valid pair $(0, 2)$ correspond to the 4-Poncelet pair $(\mathcal{A}, \mathcal{B})$, where $\mathcal{A} : xz + yz + z^2 = 0$ and $\mathcal{B} : 2xy + xz + yz + z^2 = 0$. With this, we get the value of 4 in the intersection of the row corresponding to 0 and the column corresponding to 2. Note that empty entries correspond to non-valid pairs, which we do not consider. Focusing on the case where $n = 3$ or 4, we highlight in Table 5.0.1 the pairs that correspond to these cases.

Table 5.0.1: *n-Poncelet pairs in $\mathbf{P}^2(\mathbb{F}_7)$*

r \ s	0 †	1 †	2	3	4	5	6	∞ †
0 †			4	8	6	8	6	
1 †			6	8	6	8	4	
2				4	4	4	4	
3			6		6	3	6	
4			4	4		4	4	
5			6	3	6		6	
6			4	4	4	4		
∞ †			6	8	4	8	6	

†: Singular Elements

From Table 5.0.1, we can see that there are 35 valid pairs: 2 of which correspond to 3-Poncelet pairs, while 15 of them correspond to 4-Poncelet pairs. Hence, for pencil \mathcal{P}_3 in $\mathbf{P}^2(\mathbb{F}_7)$, with Φ_3 as our sample space and giving each valid pair an equal chance of being selected, the probability of obtaining a 3-Poncelet pair is $\frac{2}{35}$ while the probability of obtaining a 4-Poncelet pair is $\frac{15}{35} = \frac{3}{7}$.

Restricting to the smooth pairs, by removing the rows corresponding to singular conics, we are left with 20 smooth pairs: 2 of which correspond to 3-Poncelet pairs, while 12 of them correspond to 4-Poncelet pairs. Hence, for pencil \mathcal{P}_3 in $\mathbf{P}^2(\mathbb{F}_7)$, with Ψ_3 as our sample space and giving each smooth pair an equal chance of being selected, the probability of obtaining a 3-Poncelet pair is $\frac{2}{20} = \frac{1}{10}$ while the probability of obtaining a 4-Poncelet pair is $\frac{12}{20} = \frac{3}{5}$.

5.1 Computation of Cayley's condition

In this section, we derive the form of Cayley's condition for the case where $n = 3$ or $n = 4$. Recall that for a fixed pencil \mathcal{P}_j , we assign the ordered pair $(r, s) \in \mathbf{P}^1(\mathbb{F}_q) \times \mathbf{P}^1(\mathbb{F}_q)$ to the conic pair $(\mathcal{A}, \mathcal{B})$ with matrix representation $A = C_j(r)$ and $B = C_j(s)$. With this, H_2 and H_3 in Theorem 2.4.4 will take the form of a polynomial in r and s .

To aid with our derivation of Cayley's condition, we have Lemma 5.1.1.

Lemma 5.1.1. *Let $\Delta(t) = \sqrt{\lambda t^3 + \beta t^2 + \gamma t + \epsilon}$ have a formal series expansion given by $H_0 + H_1 t + H_2 t^2 + H_3 t^3 + \dots$. Then:*

- $H_2 = \frac{4\beta\epsilon - \gamma^2}{8\epsilon\sqrt{\epsilon}},$
- $H_3 = \frac{8\lambda\epsilon^2 - 4\beta\gamma\epsilon + \gamma^3}{16\epsilon^2\sqrt{\epsilon}}.$

Proof. Define $P(t) = \lambda t^3 + \beta t^2 + \gamma t + \epsilon \in \mathbb{F}_q[t]$ and denote by $f^{(k)}$ the k th derivative of f .

Since $\Delta(t) = H_0 + H_1 t + H_2 t^2 + H_3 t^3 + \dots$, we can differentiate both sides twice and evaluate at $t = 0$ to obtain

$$\Delta^{(2)}(0) = 2H_2.$$

Similarly, differentiating thrice and evaluating at $t = 0$ yields

$$\Delta^{(3)}(0) = 6H_3.$$

Now, since $\Delta(t)^2 = P(t)$, differentiating yields

$$2\Delta(t)\Delta^{(1)}(t) = P^{(1)}(t)$$

and evaluating at $t = 0$ gives us

$$\Delta^{(1)}(0) = \frac{P^{(1)}(0)}{2\Delta(0)} = \frac{\gamma}{2\sqrt{\epsilon}}.$$

Differentiating $\Delta(t)^2 = P(t)$ twice gives us

$$2\Delta(t)\Delta^{(2)}(t) + 2(\Delta^{(1)}(t))^2 = P^{(2)}(t)$$

and evaluating at $t = 0$ gives us

$$\Delta^{(2)}(0) = \frac{P^{(2)}(0) - 2(\Delta^{(1)}(0))^2}{2\Delta(0)} = \frac{2\beta - 2\left(\frac{\gamma}{2\sqrt{\epsilon}}\right)^2}{2\sqrt{\epsilon}} = \frac{4\beta\epsilon - \gamma^2}{4\epsilon\sqrt{\epsilon}}.$$

Hence,

$$H_2 = \frac{\Delta^{(2)}(0)}{2} = \frac{4\beta\epsilon - \gamma^2}{8\epsilon\sqrt{\epsilon}}.$$

Finally, differentiating $\Delta(t)^2 = P(t)$ thrice gives us

$$2\Delta(t)\Delta^{(3)}(t) + 6\Delta^{(1)}(t)\Delta^{(2)}(t) = P^{(3)}(t)$$

and evaluating at $t = 0$ gives us

$$\Delta^{(3)}(0) = \frac{P^{(3)}(0) - 6\Delta^{(1)}(0)\Delta^{(2)}(0)}{2\Delta(0)} = \frac{6\lambda - 6\left(\frac{\gamma}{2\sqrt{\epsilon}}\right)\left(\frac{4\beta\epsilon - \gamma^2}{4\epsilon\sqrt{\epsilon}}\right)}{2\sqrt{\epsilon}} = \frac{24\lambda\epsilon^2 - 12\beta\gamma\epsilon + 3\gamma^3}{8\epsilon^2\sqrt{\epsilon}}.$$

Hence,

$$H_3 = \frac{\Delta^{(3)}(0)}{6} = \frac{8\lambda\epsilon^2 - 4\beta\gamma\epsilon + \gamma^3}{16\epsilon^2\sqrt{\epsilon}}.$$

□

Remark 5.1.2. *If we let $\Delta(t) = \det(tA + B)$, then $\Delta(0) = \det(B) \neq 0$ since we are only considering valid pairs. From Lemma 5.1.1, we have $\Delta(0) = \sqrt{\epsilon}$ which implies that the denominators of H_2 and H_3 are always non-zero. Since we are only interested in the case where H_2 and H_3 are zero, we ignore the non-zero denominator and any non-zero scalar multiple to obtain a simplified version of our Cayley's condition. In this chapter, we will use the simplified Cayley's condition in lieu of the original, noting that the equality symbol that we are using is, more precisely, a proportionality symbol.*

Now, we derive H_2 and H_3 for each pencil in Table 2.3.1. We use the notation $H_{i,j}$ to refer to the form of H_i for pencil \mathcal{P}_j . To do this, we determine the singular elements for each pencil in Table 2.3.1 and with this, for every valid pair (r, s) in pencil \mathcal{P}_j , we derive the form of $\det(tC_j(r) + C_j(s))$.

Note that once we obtain the form of $\det(tC_j(r) + C_j(s)) = \lambda t^3 + \beta t^2 + \gamma t + \epsilon$, we can use Lemma 5.1.1 to see that H_2 is proportional to $4\beta\epsilon - \gamma^2$, and H_3 is proportional to $8\lambda\epsilon^2 - 4\beta\gamma\epsilon + \gamma^3$. In this study, we use the Computer Algebra System SymPy to perform these calculations. Note that we could also use SymPy to directly obtain the formal series expansion of $\sqrt{\det(tC_j(r) + C_j(s))}$.

5.1.1 Pencil \mathcal{P}_3

Starting with pencil \mathcal{P}_3 , conics in this pencil have matrix representations:

$$C_3(\eta) = \begin{bmatrix} 0 & \eta & 1 \\ \eta & 0 & 1 \\ 1 & 1 & 2 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_3(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since $\det(C_3(\eta)) = -2\eta(\eta - 1)$ and $\det(C_3(\infty)) = 0$, the singular elements for this pencil correspond to $\eta \in \{0, 1, \infty\}$.

For $r, s \in \mathbb{F}_q$, where $r \neq s$ and $s \notin \{0, 1\}$. Let $A = C_3(r)$ and $B = C_3(s)$,

$$\det(tA + B) = \begin{vmatrix} 0 & rt + s & t + 1 \\ rt + s & 0 & t + 1 \\ t + 1 & t + 1 & 2t + 2 \end{vmatrix} = -2(t + 1)(rt + s)(rt + s - t - 1).$$

Since we are allowing A to be singular, we consider the case where $A = C_3(\infty)$ and $B = C_3(s)$ for $s \in \mathbb{F}_q \setminus \{0, 1\}$,

$$\det(tA + B) = \begin{vmatrix} 0 & t + s & 1 \\ t + s & 0 & 1 \\ 1 & 1 & 2 \end{vmatrix} = -2(t + s)(s + t - 1).$$

Note that in this case, we only have a polynomial that is quadratic in t and we obtain $H_{2,3}(\infty, s)$ as a constant that is non-zero when $\text{char } \mathbb{F}_q \neq 2$.

5.1.2 Pencil \mathcal{P}_4

Proceeding to pencil \mathcal{P}_4 , conics in this pencil have matrix representations:

$$C_4(\eta) = \begin{bmatrix} 0 & \eta & 1 \\ \eta & 0 & 0 \\ 1 & 0 & 2 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_4(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since $\det(C_4(\eta)) = -2\eta^2$ and $\det(C_4(\infty)) = 0$, the singular elements for this pencil correspond to $\eta \in \{0, \infty\}$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$ and $s \neq 0$. Let $A = C_4(r)$ and $B = C_4(s)$,

$$\det(tA + B) = \begin{vmatrix} 0 & rt + s & t + 1 \\ rt + s & 0 & 0 \\ t + 1 & 0 & 2t + 2 \end{vmatrix} = -2(t + 1)(rt + s)^2.$$

Now, consider $A = C_4(\infty)$ and $B = C_4(s)$ for $s \in \mathbb{F}_q \setminus \{0\}$. Note that these are considered irregular pairs in this study.

$$\det(tA + B) = \begin{vmatrix} 0 & t + s & 1 \\ t + s & 0 & 0 \\ 1 & 0 & 2 \end{vmatrix} = -2(t + s)^2.$$

Remark 5.1.3. *Aside from the construction problems when dealing with irregular pairs as discussed in Section 3.4, irregular pairs under Case 2 also have the problem of being zero for both H_2 and H_3 .*

5.1.3 Pencil \mathcal{P}_5

For pencil \mathcal{P}_5 , conics in this pencil have matrix representations:

$$C_5(\eta) = \begin{bmatrix} 0 & \eta & 1 \\ \eta & 2 & 0 \\ 1 & 0 & 0 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_5(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since $\det(C_5(\eta)) = -2$ and $\det(C_5(\infty)) = 0$, the singular element for this pencil correspond to $\eta = \infty$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$. Let $A = C_5(r)$ and $B = C_5(s)$,

$$\det(tA + B) = \begin{vmatrix} 0 & rt + s & t + 1 \\ rt + s & 2t + 2 & 0 \\ t + 1 & 0 & 0 \end{vmatrix} = -2(t + 1)^3.$$

Now, for $A = C_5(\infty)$ and $B = C_5(s)$ where $s \in \mathbb{F}_q$, which is an irregular pair,

$$\det(tA + B) = \begin{vmatrix} 0 & t + s & 1 \\ t + s & 2 & 0 \\ 1 & 0 & 0 \end{vmatrix} = -2.$$

5.1.4 Pencil \mathcal{P}_6

For pencil \mathcal{P}_6 , conics in this pencil have matrix representations:

$$C_6(\eta) = \begin{bmatrix} 0 & \eta & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_6(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since $\det(C_6(\eta)) = -2\eta^2$ and $\det(C_6(\infty)) = 0$, the singular elements for this pencil correspond to $\eta \in \{0, \infty\}$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$ and $s \neq 0$. Let $A = C_6(r)$ and $B = C_6(s)$,

$$\det(tA + B) = \begin{vmatrix} 0 & rt + s & 0 \\ rt + s & 0 & 0 \\ 0 & 0 & 2t + 2 \end{vmatrix} = -2(t + 1)(rt + s)^2,$$

which is the same as the case of \mathcal{P}_4 .

Now, for $A = C_6(\infty)$ and $B = C_6(s)$ where $s \in \mathbb{F}_q \setminus \{0\}$,

$$\det(tA + B) = \begin{vmatrix} 0 & t+s & 0 \\ t+s & 0 & 0 \\ 0 & 0 & 2 \end{vmatrix} = -2(t+s)^2,$$

which again yields the same results as in the case of \mathcal{P}_4 .

5.1.5 Pencil \mathcal{P}_8

For pencil \mathcal{P}_8 , conics in this pencil have matrix representations:

$$C_8(\eta) = \begin{bmatrix} 2\eta & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_8(\infty) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since $\det(C_8(\eta)) = -2$ and $\det(C_8(\infty)) = 0$, the singular element for this pencil correspond to $\eta = \infty$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$. Let $A = C_8(r)$ and $B = C_8(s)$,

$$\det(tA + B) = \begin{vmatrix} 2rt + 2s & t+1 & 0 \\ t+1 & 0 & 0 \\ 0 & 0 & 2t+2 \end{vmatrix} = -2(t+1)^3.$$

Now, for $A = C_8(\infty)$ and $B = C_8(s)$ where $s \in \mathbb{F}_q$,

$$\det(tA + B) = \begin{vmatrix} 2t + 2s & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{vmatrix} = -2.$$

These both yield the same result as \mathcal{P}_5 .

5.1.6 Pencil \mathcal{P}_{14}

For pencil \mathcal{P}_{14} , conics in this pencil have matrix representations:

$$C_{14}(\eta) = \begin{bmatrix} 0 & \eta & 1 \\ \eta & 2 & 1 \\ 1 & 1 & 2e \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_{14}(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Here, $e \in \mathbb{F}_q$ such that $T^2 + T + e \in \mathbb{F}_q[T]$ is irreducible.

For this pencil, $\det(C_{14}(\eta)) = -2(e\eta^2 - \eta + 1)$ and $\det(C_{14}(\infty)) = 0$. The discriminant of $e\eta^2 - \eta + 1$ is the same as that of $T^2 + T + e$, which is $1 - 4e$. Since $T^2 + T + e$ is irreducible, by Lemma 2.1.21, $1 - 4e$ is not a square in \mathbb{F}_q and $\det(C_{14}(\eta))$ will not have a root in \mathbb{F}_q . Hence, the singular element corresponds to $\eta = \infty$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$. Let $A = C_{14}(r)$ and $B = C_{14}(s)$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 0 & rt + s & t + 1 \\ rt + s & 2t + 2 & t + 1 \\ t + 1 & t + 1 & 2et + 2e \end{vmatrix} \\ &= -2(t + 1)[(er^2 - r + 1)t^2 + (2ers - r - s + 2)t + (es^2 - s + 1)]. \end{aligned}$$

Now, for $A = C_{14}(\infty)$ and $B = C_{14}(s)$ where $s \in \mathbb{F}_q$,

$$\det(tA + B) = \begin{vmatrix} 0 & t + s & 1 \\ t + s & 2 & 1 \\ 1 & 1 & 2e \end{vmatrix} = -2[et^2 + (2es - 1)t + (es^2 - s + 1)].$$

This will yield $H_{2,14}(\infty, s) = 1 - 4e$ which is a non-zero constant by our assumption that $1 - 4e$ is not a square in \mathbb{F}_q .

5.1.7 Pencil \mathcal{P}_{15}

For pencil \mathcal{P}_{15} , conics in this pencil have matrix representations:

$$C_{15}(\eta) = \begin{bmatrix} 0 & \eta & 0 \\ \eta & 2 & 1 \\ 0 & 1 & 2e \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_{15}(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Here, $e \in \mathbb{F}_q$ such that $T^2 + T + e \in \mathbb{F}_q[T]$ is irreducible.

Since $\det(C_{15}(\eta)) = -2e\eta^2$ and $\det(C_{15}(\infty)) = 0$, the singular elements for this pencil correspond to $\eta \in \{0, \infty\}$. Here, we invoked the fact that $e \neq 0$ since $T^2 + T = T(T + 1)$ is reducible.

For $r, s \in \mathbb{F}_q$ where $r \neq s$ and $s \neq 0$. Let $A = C_{15}(r)$ and $B = C_{15}(s)$,

$$\det(tA + B) = \begin{vmatrix} 0 & rt + s & 0 \\ rt + s & 2t + 2 & t + 1 \\ 0 & t + 1 & 2et + 2e \end{vmatrix} = -2e(t + 1)(rt + s)^2.$$

Observe that this is just the same determinant as in the case of \mathcal{P}_4 but with an extra factor of e .

Proceeding with our calculation, we obtain

$$H_{2,15}(r, s) = e^2 H_{2,4}(r, s)$$

and

$$H_{3,15}(r, s) = e^3 H_{3,4}(r, s).$$

The final simplified form will be the same as that of \mathcal{P}_4 since $e \neq 0$.

Now, for $A = C_{15}(\infty)$ and $B = C_{15}(s)$ where $s \in \mathbb{F}_q \setminus \{0\}$,

$$\det(tA + B) = \begin{vmatrix} 0 & t+s & 1 \\ t+s & 2 & 1 \\ 1 & 1 & 2e \end{vmatrix} = -2e(t+s)^2.$$

Again, this is just the same determinant as in the case of \mathcal{P}_4 but with an extra factor of e . In effect, $H_2(\infty, s)$ will get an extra factor of e^2 , and $H_3(\infty, s)$ will get an extra factor of e^3 . But the final simplified form will be the same as that of \mathcal{P}_4 .

5.1.8 Pencil \mathcal{P}_{16}

For pencil \mathcal{P}_{16} , conics in this pencil have matrix representations:

$$C_{16}(\eta) = \begin{bmatrix} 2e & \eta & 1 \\ \eta & 2d & 1 \\ 1 & 1 & 2 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_{16}(\infty) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Here, $d, e \in \mathbb{F}_q$ such that $T^2 + T + d, T^2 + T + e \in \mathbb{F}_q[T]$ are both irreducible.

For this pencil, $\det(C_{16}(\eta)) = -2[\eta^2 - \eta + (-4de + d + e)]$ and $\det(C_{16}(\infty)) = 0$. Solving for the roots of $\eta^2 - \eta + (-4de + d + e)$ yields

$$\eta_+ = \frac{1 + \sqrt{(1-4d)(1-4e)}}{2}, \eta_- = \frac{1 - \sqrt{(1-4d)(1-4e)}}{2}.$$

By Lemma 5.2.1, the discriminants $1 - 4d$ and $1 - 4e$ are both non-square and consequently, their product is a non-zero square implying that $\eta_+, \eta_- \in \mathbb{F}_q$ and $\eta_+ \neq \eta_-$. Hence, the singular elements correspond to $\eta \in \{\eta_+, \eta_-, \infty\}$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$ and $s \notin \{\eta_+, \eta_-\}$. Let $A = C_{16}(r)$ and $B = C_{16}(s)$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 2et + 2e & rt + s & t + 1 \\ rt + s & 2dt + 2d & t + 1 \\ t + 1 & t + 1 & 2t + 2 \end{vmatrix} \\ &= -2(t + 1)[(-4de + d + e + r^2 - r)t^2 + (-8de + 2d + 2e + 2rs - r - s)t \\ &\quad + (-4de + d + e + s^2 - s)]. \end{aligned}$$

Now, for $A = C_{16}(\infty)$ and $B = C_{16}(s)$ where $s \in \mathbb{F}_q \setminus \{\eta_+, \eta_-\}$,

$$\det(tA + B) = \begin{vmatrix} 2e & t + s & 1 \\ t + s & 2d & 1 \\ 1 & 1 & 2 \end{vmatrix} = -2(-4de + d + e + s^2 + 2st - s + t^2 - t).$$

This will yield $H_{2,16}(\infty, s) = (1 - 4d)(1 - 4e)$ which is non-zero since this is a product of the non-zero discriminants $1 - 4d$ and $1 - 4e$.

5.1.9 Pencil \mathcal{P}_{17}

For pencil \mathcal{P}_{17} , conics in this pencil have matrix representations:

$$C_{17}(\eta) = \begin{bmatrix} 2\eta & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2e \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_{17}(\infty) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Here, $e \in \mathbb{F}_q$ such that $T^2 + T + e \in \mathbb{F}_q[T]$ is irreducible.

For this pencil, $\det(C_{17}(\eta)) = -2(1 - 4e)\eta$ and $\det(C_{17}(\infty)) = 0$. By Lemma 5.2.1, $1 - 4e$ is not a square in \mathbb{F}_q and hence, non-zero. So, the singular elements correspond to $\eta \in \{0, \infty\}$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$ and $s \neq 0$. Let $A = C_{17}(r)$ and $B = C_{17}(s)$,

$$\det(tA + B) = \begin{vmatrix} 2rt + 2s & 0 & 0 \\ 0 & 2t + 2 & t + 1 \\ 0 & t + 1 & 2et + 2e \end{vmatrix} = -2(1 - 4e)(t + 1)^2(rt + s).$$

Now, for $A = C_{17}(\infty)$ and $B = C_{17}(s)$ where $s \in \mathbb{F}_q \setminus \{0\}$,

$$\det(tA + B) = \begin{vmatrix} 2s + 2t & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2e \end{vmatrix} = -2(1 - 4e)(t + s).$$

This will yield $H_{2,17} = -4(1 - 4e)^2$ and $H_{3,17} = -8(1 - 4e)^3$ which are both non-zero constants since $1 - 4e$ is not a square in \mathbb{F}_q and $\text{char } \mathbb{F}_q \neq 2$.

5.1.10 Pencil \mathcal{P}_{18}

For pencil \mathcal{P}_{18} , conics in this pencil have matrix representations:

$$C_{18}(\eta) = \begin{bmatrix} 2 & c & -\eta \\ c & 2\eta + 2b & 1 \\ -\eta & 1 & 0 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_{18}(\infty) = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{bmatrix}.$$

Here, $b, c \in \mathbb{F}_q$ such that $T^3 + bT^2 + cT + 1 \in \mathbb{F}_q[T]$ is irreducible.

For this pencil, $\det(C_{18}(\eta)) = -2(\eta^3 + b\eta^2 + c\eta + 1)$ and $\det(C_{18}(\infty)) = -2$. By irreducibility, $\det(C_{18}(\eta))$ will not be zero for any $\eta \in \mathbb{F}_q$. Hence, there are no singular elements in this pencil.

For $r, s \in \mathbb{F}_q$ where $r \neq s$. Let $A = C_{18}(r)$ and $B = C_{18}(s)$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 2t + 2 & ct + c & -rt - s \\ ct + c & (2b + 2r)t + 2b + 2s & t + 1 \\ -rt - s & t + 1 & 0 \end{vmatrix} \\ &= -2[(br^2 + cr + r^3 + 1)t^3 + (br^2 + 2brs + 2cr + cs + 3r^2s + 3)t^2 \\ &\quad + (2brs + bs^2 + cr + 2cs + 3rs^2 + 3)t + (bs^2 + cs + s^3 + 1)]. \end{aligned}$$

Now, for $A = C_{18}(r)$ and $B = C_{18}(\infty)$ where $r \in \mathbb{F}_q$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 2t & ct & -rt - 1 \\ ct & (2b + 2r)t + 2 & t \\ -rt + 1 & t & 0 \end{vmatrix} \\ &= -2[(br^2 + cr + r^3 + 1)t^3 + (2br + c + 3r^2)t^2 + (b + 3r)t + 1]. \end{aligned}$$

Lastly, for $A = C_{18}(\infty)$ and $B = C_{18}(s)$ where $s \in \mathbb{F}_q$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 2 & c & -t - s \\ c & 2t + (2b + 2s) & 1 \\ -t - s & 1 & 0 \end{vmatrix} \\ &= -2[t^3 + (b + 3s)t^2 + (2bs + c + 3s^2)t + (bs^2 + cs + s^3 + 1)]. \end{aligned}$$

5.1.11 Pencil \mathcal{P}_{19}

For pencil \mathcal{P}_{19} , conics in this pencil have matrix representations:

$$C_{19}(\eta) = \begin{bmatrix} 2\eta & 2\sigma & 0 \\ 2\sigma & -2v\eta - 2\rho & 0 \\ 0 & 0 & 2 \end{bmatrix}; \eta \in \mathbb{F}_q, \text{ and } C_{19}(\infty) = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -2v & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Here, $v, \rho, \sigma \in \mathbb{F}_q$ such that v and $\rho^2 - 4v\sigma^2$ are both non-squares in \mathbb{F}_q .

For this pencil, $\det(C_{19}(\eta)) = -8(v\eta^2 + \rho\eta + \sigma^2)$ and $\det(C_{19}(\infty)) = 0$. The discriminant of $v\eta^2 + \rho\eta + \sigma^2$ is $\rho^2 - 4v\sigma^2$ which is assumed to be non-square, so this will not have a root in \mathbb{F}_q by Lemma 5.2.1. Hence, the singular element correspond to $\eta = \infty$.

For $r, s \in \mathbb{F}_q$ where $r \neq s$. Let $A = C_{19}(r)$ and $B = C_{19}(s)$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 2rt + 2s & 2\sigma t + 2\sigma & 0 \\ 2\sigma t + 2\sigma & (-2vs - 2\rho)t + (-2vs - 2\rho) & 0 \\ 0 & 0 & 2t + 2 \end{vmatrix} \\ &= -8(t+1)(vr^2t^2 + 2vrst + vs^2 + r\rho t^2 + r\rho t + \rho st + \rho s + \sigma^2 t^2 + 2\sigma^2 t + \sigma^2). \end{aligned}$$

Now, for $A = C_{19}(\infty)$ and $B = C_{19}(s)$ where $s \in \mathbb{F}_q$,

$$\begin{aligned} \det(tA + B) &= \begin{vmatrix} 2t + 2s & 2\sigma & 0 \\ 2\sigma & -2vt - 2vs - 2\rho & 0 \\ 0 & 0 & 2 \end{vmatrix} \\ &= -8(vs^2 + 2vst + vt^2 + \rho s + \rho t + \sigma^2). \end{aligned}$$

This will yield $H_{2,19} = -64(\rho^2 - 4v\sigma^2)$ which is a non-zero constant since $\rho^2 - 4v\sigma^2$ is not a square in \mathbb{F}_q .

5.1.12 Summary for all pencils

From the derived forms $\det(tC_j(r) + C_j(s))$, we use the Computer Algebra System SymPy to obtain the simplified form of H_2 and H_3 where non-zero scalar multiples and denominators are ignored. We summarize all our derivations for H_2 in Table 5.1.1 and that of H_3 in Table 5.1.2.

Remark 5.1.4. *The obtained forms of H_2 and H_3 are consistent with those in [23], which provided the forms of H_2 and H_3 but only for the case of transversally intersecting and smooth conics.*

Remark 5.1.5. *Our results are consistent with the main theorem of [17], which states that all smooth conic pairs from pencils with base points of intersection multiplicity 3 and 4 are n -Poncelet pairs where $n = \text{char } \mathbb{F}_q$. This correspond to pencils \mathcal{P}_3 and \mathcal{P}_8 in our study, and we have $H_2(r, s) = 3$ for $r, s \neq \infty$, which is zero precisely when $\text{char } \mathbb{F}_q = 3$.*

Table 5.1.1: Summary of Cayley's condition for 3-Poncelet pairs

$H_{2,j}^\dagger$
$H_{2,3}(r, s) = r^2 + (-4s^3 + 6s^2 - 4s)r + s^4$
$H_{2,3}(\infty, s) = u^\ddagger$
$H_{2,4}(r, s) = 4r - s$
$H_{2,4}(\infty, s) = 0$
$H_{2,5}(r, s) = 3$
$H_{2,5}(\infty, s) = 0$
$H_{2,6}(r, s) = 4r - s$
$H_{2,6}(\infty, s) = 0$
$H_{2,8}(r, s) = 3$
$H_{2,8}(\infty, s) = 0$
$H_{2,14}(r, s) = (1 - 4e)r^2 + (-4e^2s^3 + 6es^2 + 4es - 4s + 2)r + (e^2s^4 - 6es^2 + 4s - 3)$
$H_{2,14}(\infty, s) = u^\ddagger$
$H_{2,15}(r, s) = 4r - s$
$H_{2,15}(\infty, s) = 0$
$H_{2,16}(r, s) = [(1 - 4d)(1 - 4e)]r^2$ $+ [-4s^3 + 6s^2 + (-16de + 4d + 4e - 4)s + (-8de + 2d + 2e)]r$ $+ [s^4 + (24de - 6d - 6e)s^2 + (-16de + 4d + 4e)s$ $+ (-48d^2e^2 + 24d^2e + 24de^2 - 3d^2 - 6de - 3e^2)]$
$H_{2,16}(\infty, s) = u^\ddagger$
$H_{2,17}(r, s) = r(r - 4s)$
$H_{2,17}(\infty, s) = u^\ddagger$
$H_{2,18}(r, s) = [3s^4 + 4bs^3 + 6cs^2 + 12s + (4b - c^2)]r^2$ $+ [2bs^4 + (4b^2 - 4c)s^3 + (6bc - 18)s^2 + (-4b + 4c^2)s + 2c]r$ $+ [(-b^2 + 4c)s^4 + 12s^3 + 6bs^2 + 4cs + 3]$
$H_{2,18}(r, \infty) = 3r^2 + 2br + (-b^2 + 4c)$
$H_{2,18}(\infty, s) = 3s^4 + 4bs^3 + 6cs^2 + 12s + (4b - c^2)$
$H_{2,19}(r, s) = [\rho^2 - 4v\sigma^2]r^2$ $+ [-4v^2s^3 - 6v\rho s^2 + (4v\sigma^2 - 4\rho^2)s - 2\rho\sigma^2]r$ $+ [v^2s^4 - 6v\sigma^2s^2 - 4\rho\sigma^2s - 3\sigma^4]$
$H_{2,19}(\infty, s) = u^\ddagger$

$^\dagger H_{2,j} = H_2$ from Cayley's condition for pencil \mathcal{P}_j where non-zero scalar multiples and denominators are ignored

$^\ddagger u$ is a non-zero constant for $\text{char } \mathbb{F}_q \neq 2$

Table 5.1.2: Summary of Cayley's condition for 4-Poncelet pairs

$H_{3,j}^\dagger$
$H_{3,3}(r, s) = [r - s^2][(2s - 1)r - s^2][r + (s^2 - 2s)]$
$H_{3,3}(\infty, s) = 2s - 1$
$H_{3,4}(r, s) = 2r - s$
$H_{3,4}(\infty, s) = 0$
$H_{3,5}(r, s) = u^\ddagger$
$H_{3,5}(\infty, s) = 0$
$H_{3,6}(r, s) = 2r - s$
$H_{3,6}(\infty, s) = 0$
$H_{3,8}(r, s) = u^\ddagger$
$H_{3,8}(\infty, s) = 0$
$H_{3,14}(r, s) = [(2es - 1)r + (-es^2 + 1)]$ $[(1 - 4e)r^2 + (8es - 2s)r + (-e^2s^4 + 2es^3 - 6es^2 + 2s - 1)]$
$H_{3,14}(\infty, s) = 2es - 1$
$H_{3,15}(r, s) = 2r - s$
$H_{3,15}(\infty, s) = 0$
$H_{3,16}(r, s) = [(2s - 1)r + (-s^2 - 4de + d + e)]$ $[(1 - 4d)(1 - 4e)r^2 + ((-32de + 8d + 8e - 2)s)r$ $+ (-s^4 + 2s^3 + (24de - 6d - 6e)s^2 + (-8de + 2d + 2e)s$ $+ (-16d^2e^2 + 8d^2e - d^2 + 8de^2 - 2de - e^2)]$
$H_{3,16}(\infty, s) = 2s - 1$
$H_{3,17}(r, s) = r^2(r - 2s)$
$H_{3,17}(\infty, s) = u^\ddagger$
$H_{3,18}(r, s) = [s^6 + 2bs^5 + 5cs^4 + 20s^3 + (20b - 5c^2)s^2 + (8b^2 - 2bc^2 - 4c)s + (4bc - c^3 - 8)]r^3$ $+ [bs^6 + (4b^2 - 6c)s^5 + (10bc - 45)s^4 + (-40b + 20c^2)s^3$ $+ (-20b^2 + 5bc^2 + 30c)s^2 + (-8bc + 2c^3 + 36)s + (4b - c^2)]r^2$ $+ [(-b^2 + 4c)s^6 + (2b^3 - 8bc + 36)s^5 + (5b^2c + 30b - 20c^2)s^4$ $+ (20b^2 - 40c)s^3 + (10bc - 45)s^2 + (-6b + 4c^2)s + c]r$ $+ [(-b^3 + 4bc - 8)s^6 + (-2b^2c - 4b + 8c^2)s^5$ $+ (-5b^2 + 20c)s^4 + 20s^3 + 5bs^2 + 2cs + 1]$
$H_{3,18}(r, \infty) = r^3 + br^2 + (-b^2 + 4c)r + (-b^3 + 4bc - 8)$
$H_{3,18}(\infty, s) = s^6 + 2bs^5 + 5cs^4 + 20s^3 + (20b - 5c^2)s^2 + (8b^2 - 2bc^2 - 4c)s + (4bc - c^3 - 8)$
$H_{3,19}(r, s) = [(2vs + \rho)r + (-vs^2 + \sigma^2)]$ $[(\rho^2 - 4v\sigma^2)r^2 + ((8v\sigma^2 - 2\rho^2)s)r + (-v^2s^4 - 2v\rho s^3 - 6v\sigma^2s^2 - 2\rho\sigma^2 - \sigma^4)]$
$H_{3,19}(\infty, s) = 2vs + \rho$

$^\dagger H_{3,j} = H_3$ from Cayley's condition for pencil \mathcal{P}_j where non-zero scalar multiples and denominators are ignored

$^\ddagger u$ is a non-zero constant for $\text{char } \mathbb{F}_q \neq 2$

5.2 Probabilities for 3-Poncelet pairs

In this section, we answer our main research question about the probability of obtaining a 3-Poncelet pair among the valid pairs for each pencil in Table 2.3.2.

With the aid of Table 5.1.1, we can now count the number of valid pairs in \mathcal{P}_j that correspond to a 3-Poncelet pair by counting the number of pairs (r, s) such that $H_{2,j}(r, s) = 0$. Since we only consider distinct conic pairs, we have Lemma 5.2.1 based on [23], which will help us adjust our counts for the case where $r = s$.

Lemma 5.2.1. *Let $H_{2,j}$ be the form of H_2 under \mathcal{P}_j and $C_j(\eta)$ be the matrix representation of the element corresponding to $\eta \in \mathbf{P}^1(\mathbb{F}_q)$ in pencil \mathcal{P}_j . Then:*

1. $H_{2,j}(\eta, \eta) = 0$ if and only if $\text{char } \mathbb{F}_q = 3$ or $C_j(\eta)$ is singular,
2. all valid pairs (r, s) that satisfy $H_{2,j}(r, s) = 0$ are smooth pairs.

Proof. Let $A = B = C_j(\eta)$, then $\Delta(t) = \sqrt{\det(tA + A)} = \sqrt{(t+1)^3 \det(A)} = \sqrt{\lambda t^3 + \beta t^2 + \gamma t + \epsilon}$ where $\lambda = \det(A)$, $\beta = 3 \det(A)$, $\gamma = 3 \det(A)$, $\epsilon = \det(A)$.

By Lemma 5.1.1, $H_{2,j}(s, s) = \frac{12 \det(A)^2 - 9 \det(A)^2}{8 \det(A) \sqrt{\det(A)}} = \frac{3}{8} \sqrt{\det(A)}$, which is zero if and only if $\frac{3}{8}$ is 0 in \mathbb{F}_q which is the case when $\text{char } \mathbb{F}_q = 3$, or $\det(A) = 0$ which happens when $A = C_j(\eta)$ is singular.

For the second statement, this is trivially true for $j = 18$ since all conics in this pencil are smooth. For $j \neq 18$, suppose there is a valid pair (r, s) that satisfies $H_{2,j}(r, s) = 0$, which is not a smooth pair. In this case, we can use Table 5.1.1 to substitute every value of r associated with a singular element as summarized in Table 2.3.2 and show that if $H_{2,j}(r, s) = 0$, then we either get $r = s$ or an irregular pair (r, s) . In either case, we conclude that (r, s) is not a valid pair and get a contradiction.

Starting with $j = 3$, the singular elements are $\eta \in \{0, 1, \infty\}$ and we obtain

$$H_{2,3}(0, s) = s^4, H_{2,3}(1, s) = (s-1)^4, H_{2,3}(\infty, s) \neq 0, \forall s \in \mathbb{F}_q$$

where we see that $H_{2,3}(r, s) = 0$ if and only if $r = s$.

For $j \in \{4, 6, 15\}$, the singular elements are $\eta \in \{0, \infty\}$ and we obtain

$$H_{2,j}(0, s) = s, H_{2,j}(\infty, s) \neq 0, \forall s \in \mathbb{F}_q$$

where we see that $H_{2,j}(r, s) = 0$ if and only if $r = s$.

For $j \in \{5, 8\}$, the only singular element is $\eta = \infty$, but $(\infty, s), \forall s \in \mathbb{F}_q$ correspond to an irregular pair.

For $j \in \{14, 19\}$, the only singular element is $\eta = \infty$ and

$$H_{2,j}(\infty, s) \neq 0, \forall s \in \mathbb{F}_q$$

where we see that $H_{2,j}(r, s) = 0$ if and only if $r = s$.

For $j = 16$, the singular elements are $\eta \in \{\eta_+, \eta_-, \infty\}$ and we obtain

$$H_{2,16}(\eta_+, s) = (s - \eta_+)^4, H_{2,16}(\eta_-, s) = (s - \eta_-)^4, H_{2,16}(\infty, s) \neq 0, \forall s \in \mathbb{F}_q$$

where we see that $H_{2,3}(r, s) = 0$ if and only if $r = s$.

Lastly, for $j = 17$, the singular elements are $\eta \in \{0, \infty\}$, but $(0, s)$ and $(\infty, s), \forall s \in \mathbb{F}_q$ correspond to an irregular pair.

□

We will use Lemma 5.2.1 to remove pairs (r, s) that satisfy $H_{2,j}(r, s) = 0$ but should not be counted. Moreover, it proves that for the triangle case, all valid pairs that correspond to 3-Poncelet pairs are smooth pairs. That is, there are no 3-Poncelet pairs $(\mathcal{A}, \mathcal{B})$ where \mathcal{A} is singular and \mathcal{B} is smooth.

We can now start counting for each pencil \mathcal{P}_j the number of valid pairs (r, s) satisfying $H_{2,j}(r, s) = 0$. We will mainly use the $D(f)$, the discriminant of a polynomial f , to facilitate the counting. In using discriminants, it will be important to know whether something is a non-zero square or zero in \mathbb{F}_q . With this, we define

$$Z_\varphi^* = \{s \in \mathbb{F}_q \mid \varphi(s) = y^2, y \in \mathbb{F}_q \setminus \{0\}\} = \text{set of values which makes } \varphi(s) \text{ a non-zero square,}$$

$$Z_\varphi = \{s \in \mathbb{F}_q \mid \varphi(s) = 0\} = \text{set of roots of } \varphi(s).$$

We first deal with the case where $H_{2,j}(r, s)$ is quadratic in r ; that is, $j \in \{3, 14, 16, 18, 19\}$. Here we treat $H_{2,j}(r, s)$ as a polynomial in $(\mathbb{F}_q[s])[r]$, the collection of polynomials in r having polynomials in s as coefficient. This makes the discriminant of $H_{2,j}(r, s)$ a function of s , and we denote this discriminant by $D_j(s)$. For a fixed s , $D_j(s)$ will tell us how many pairs (r, s) satisfy $H_{2,j}(r, s) = 0$, and summing up all these counts for all valid values of s , we obtain the exact count that we want. In particular, each $s \in Z_{D_j}$ will contribute one pair and $s \in Z_{D_j}^*$ will contribute two pairs. Upon computing the discriminants, we observe that all of them take the form

$$D_j(s) = 16(\kappa_j(s))^2 \varphi_j(s), \quad j \in \{3, 14, 16, 18, 19\} \quad (5.2.1)$$

for some $\kappa_j(s), \varphi_j(s) \in \mathbb{F}_q[s]$.

We summarize in Tables 5.2.1 and 5.2.2 useful information about $\kappa_j(s)$ and $\varphi_j(s)$, respectively.

Table 5.2.1: Summary of roots in \mathbb{F}_q for $\kappa_j(s)$

\mathcal{P}_j	$\kappa_j(s)^\dagger$	Roots in \mathbb{F}_q
\mathcal{P}_3	$\kappa_3(s) = s(s - 1)$	0, 1
\mathcal{P}_{14}	$\kappa_{14}(s) = es^2 - s + 1$	None
\mathcal{P}_{16}	$\kappa_{16}(s) = s^2 - s + (-4de + d + e)$	η_+^{**}, η_-^{**}
\mathcal{P}_{18}	$\kappa_{18}(s) = s^3 + bs^2 + cs + 1$	None
\mathcal{P}_{19}	$\kappa_{19}(s) = vs^2 + \rho s + \sigma^2$	None

[†] $\kappa_j(s)$ as in Equation 5.2.1

** η_+, η_- as in Table 2.3.2

Table 5.2.2: Summary of discriminants for $\varphi_j(s)$

\mathcal{P}_j	$\varphi_j(s)^\dagger$	Discriminant $D(\varphi_j)$
\mathcal{P}_3	$\varphi_3(s) = s^2 - s + 1$	-3
\mathcal{P}_{14}	$\varphi_{14}(s) = e^2s^2 - es + (-3e + 1)$	$-3e^2(1 - 4e)$
\mathcal{P}_{16}	$\varphi_{16}(s) = s^2 - s + (12de - 3d - 3e + 1)$	$-3(1 - 4d)(1 - 4e)$
\mathcal{P}_{18}	$\varphi_{18}(s) = (b^2 - 3c)s^2 + (bc - 9)s + (-3b + c^2)$	$-3(b^2c^2 - 4c^3 - 4b^3 - 27 + 18bc)$
\mathcal{P}_{19}	$\varphi_{19}(s) = v^2s^2 + v\rho s + (-3v\sigma^2 + \rho^2)$	$-3v^2(\rho^2 - 4v\sigma^2)$

[†] $\varphi_j(s)$ as in Equation 5.2.1

We state important observations about κ_j and $\varphi_j(s)$ in Lemma 5.2.2 and Lemma 5.2.3

Lemma 5.2.2. *For any $\kappa_j(s)$ in Table 5.2.1 and $s \in \mathbb{F}_q$, then $\kappa_j(s) = 0$ if and only if $C_j(s)$, the matrix representation of the element corresponding to s in pencil \mathcal{P}_j , is singular.*

Proof. Comparing the singular elements of the pencil in Table 2.3.2 and the roots of $\kappa_j(s)$ in Table 5.2.1, we can see that for $s \in \mathbb{F}_q$, $\kappa_j(s)$ is zero if and only if $C_j(s)$ is singular. We just need to show how we obtained the roots of $\kappa_j(s)$.

Roots of κ_3 are straightforward, and the quadratic formula is used to obtain those of κ_{16} . Referring to the assumptions on Table 2.3.1, $T^2 + T + e$ is irreducible, which implies that $1 - 4e$ is non-square in \mathbb{F}_q . But this is also the discriminant of κ_{14} , so it is also irreducible and does not have any root in \mathbb{F}_q . κ_{18} follows from the assumption that $T^3 + bT^2 + cT + 1$ is irreducible. Finally, κ_{19} have discriminant $\rho^2 - 4v\sigma^2$ which is assumed to be non-square. \square

Lemma 5.2.3. *Let $D(\varphi_j)$ be any discriminant in Table 5.2.2, then $D(\varphi_j) = 0$ if and only if $\text{char } \mathbb{F}_q = 3$. That is, $\varphi_j(s)$ is a square of a linear polynomial in $\mathbb{F}_q[s]$ if and only if $\text{char } \mathbb{F}_q = 3$.*

Proof. From the assumptions on Table 2.3.1, $T^2 + T + d$ and $T^2 + T + e$ are irreducible and we must have $1 - 4d$, $1 - 4e$, and e to be non-zero which are factors that appear on $D(\varphi_{14})$ and $D(\varphi_{16})$. By irreducibility of $T^3 + bT^2 + cT + 1$, a result from [4] states that its discriminant, $b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bc$, must be non-zero and this factor appear on $D(\varphi_{18})$. Finally, since v and $\rho^2 - 4v\sigma^2$ are all non-square, then they are also non-zero, and these factors appear on $D(\varphi_{19})$.

With this, we can see that all $D(\varphi_j)$ in Table 5.2.2 have the form -3 multiplied by a non-zero factor. Hence, the whole quantity is 0 if and only if -3 is 0 in \mathbb{F}_q , which happens if and only if $\text{char } \mathbb{F}_q = 3$. \square

A useful lemma adapted from the main argument in [3] is given below as Lemma 5.2.4.

Lemma 5.2.4. *Suppose $\varphi(s) = u_2s^2 + u_1s + u_0 \in \mathbb{F}_q[s]$ is a quadratic polynomial that is not a square of a linear polynomial in $\mathbb{F}_q[s]$ and u_2 is a non-zero square in \mathbb{F}_q .*

Let $Z_\varphi^* = \{s \in \mathbb{F}_q \mid \varphi(s) = y^2, y \in \mathbb{F}_q \setminus \{0\}\}$, and $Z_\varphi = \{s \in \mathbb{F}_q \mid \varphi(s) = 0\}$. Then,

$$\left| Z_\varphi^* \right| = \frac{q - 1 - \left| Z_\varphi \right|}{2}$$

Proof. Recall that the non-zero square elements in \mathbb{F}_q form a group under multiplication, and the product of a square and a non-square element of \mathbb{F}_q will yield a non-square element. Since u_2 is a non-zero square, then $\varphi(s)$ is a non-zero square if and only if $\frac{\varphi(s)}{u_2}$ is a non-zero square. Hence, $\left| Z_\varphi^* \right| = \left| Z_{\frac{\varphi}{u_2}}^* \right|$. Moreover, the zeros of $\varphi(s)$ do not change when we divide it by a non-zero element of \mathbb{F}_q . So, we also have $\left| Z_\varphi \right| = \left| Z_{\frac{\varphi}{u_2}} \right|$. Thus, without loss of generality, we can assume that $u_2 = 1$; otherwise, we just consider $\frac{\varphi(s)}{u_2}$.

By completing the square, we obtain $\varphi(s) = (s - \beta)^2 + \gamma$ where $\beta, \gamma \in \mathbb{F}_q$ but $\gamma \neq 0$ by the assumption that $\varphi(s)$ is not a square of a linear polynomial. Now, we are interested in s such that

$$\varphi(s) = (s - \beta)^2 + \gamma = y^2 \tag{5.2.2}$$

where $y \in \mathbb{F}_q$. Isolating γ on one side of the equation gives us

$$y^2 - (s - \beta)^2 = \underbrace{(y - s + \beta)}_{\omega} \underbrace{(y + s - \beta)}_{\frac{\gamma}{\omega}} = \gamma$$

Since γ is non-zero, the first factor $\omega = (y - s + \beta)$ is a non-zero element of \mathbb{F}_q and the second factor $(y + s - \beta)$ can be expressed as $\frac{\gamma}{\omega}$. Thus, we get $y = \omega + s - \beta$ and substituting this back

to Equation 5.2.2, we obtain $(s - \beta)^2 + \gamma = (\omega + s - \beta)^2$ where we can solve for s in terms of ω as

$$s = \beta + \frac{\gamma}{2\omega} - \frac{\omega}{2} \quad (5.2.3)$$

Here, each $\omega \in \mathbb{F}_q \setminus \{0\}$ corresponds to a value of s that will make $\varphi(s)$ a square in \mathbb{F}_q . In this case, for a fixed s where $\varphi(s)$ is square, Equation 5.2.3 can be treated as quadratic polynomial in ω with the form

$$\omega^2 + (2s - 2\beta)\omega - \gamma = 0$$

and discriminant $4\varphi(s)$.

Hence, each s making $\varphi(s)$ a non-zero square will have two corresponding ω but only one ω corresponding to each s for which $\varphi(s) = 0$. With this, we have $q - 1$ possible values for ω corresponding to the elements of $\mathbb{F}_q \setminus \{0\}$ and we remove one ω for each s corresponding to a root of $\varphi(s)$ which leaves us the remaining $q - 1 - |Z_\varphi|$ values of ω corresponding to s which makes $\varphi(s)$ a non-zero square. Since we only get one s per two values of ω in this case, we obtain the final count to be

$$|Z_\varphi^*| = \frac{q - 1 - |Z_\varphi|}{2}$$

□

Now we are ready to count valid pairs (r, s) that correspond to 3-Poncelet pairs. For this purpose, we denote the set of valid pairs that correspond to 3-Poncelet pairs as

$\Gamma_j(H_2) = \{(r, s) \in \Phi_j \mid H_{2,j}(r, s) = 0\}$, which we can decompose into three disjoint sets

$\Gamma_j(H_2(\cdot, \cdot)) = \{(r, s) \in \Gamma_j(H_2) \mid r, s \in \mathbb{F}_q\}$,

$\Gamma_j(H_2(\cdot, \infty)) = \{(r, s) \in \Gamma_j(H_2) \mid r \in \mathbb{F}_q, s = \infty\}$, and

$\Gamma_j(H_2(\infty, \cdot)) = \{(r, s) \in \Gamma_j(H_2) \mid r = \infty, s \in \mathbb{F}_q\}$.

5.2.1 Pencils $\mathcal{P}_3, \mathcal{P}_{14}, \mathcal{P}_{16}, \mathcal{P}_{19}$

Proposition 5.2.5. For $\text{char } \mathbb{F}_q \neq 3$ and $j \in \{3, 14, 16, 19\}$, $|\Gamma_j(H_2)| = q - 1 - 2|Z_{\kappa_j}|$ with κ_j as shown in Table 5.2.1. In particular,

$$|\Gamma_j(H_2)| = q - 5, \quad j \in \{3, 16\}, \quad \text{and}$$

$$|\Gamma_j(H_2)| = q - 1, \quad j \in \{14, 19\}.$$

Proof. By Lemma 5.2.2, $\kappa_j(s) \neq 0$ for all valid pairs (r, s) . Moreover, we can see that all $s \in \mathbb{F}_q$ corresponding to a singular conic is an element of $Z_{\varphi_j}^*$ since

$$\varphi_3(0) = \varphi_3(1) = 1, \quad \varphi_{16}(\eta_+) = \varphi_{16}(\eta_-) = (1 - 4d)(1 - 4e)$$

which by the irreducibility condition in Table 2.3.1, implies that both $(1 - 4e)$ and $(1 - 4d)$ are non-squares and so their product is a non-zero square. Thus, we remove the elements of Z_{κ_j} from $Z_{\varphi_j}^*$ since they do not correspond to a valid pair.

Since the form of our discriminant $D_j(s)$ is a product of $\varphi_j(s)$ and $16(\kappa_j(s))^2$, where we have shown that the latter factor is always a non-zero square, we have that each element of Z_{φ_j} will contribute one pair (r, s) since it will make $D_j(s) = 0$. Meanwhile, elements of $Z_{\varphi_j}^*$ that are not in Z_{κ_j} will contribute two pairs of (r, s) since this will make $D_j(s)$ a non-zero square. Since $H_2(\infty, s) \neq 0$ for all $s \neq \infty$ and ∞ corresponds to a singular conic for the pencils in our current case, then ∞ does not contribute to any pairs. Thus,

$$\begin{aligned} |\Gamma_j(H_2)| &= |\Gamma_j(H_2(\cdot, \cdot))| + \underbrace{|\Gamma_j(H_2(\cdot, \infty))|}_{=0} + \underbrace{|\Gamma_j(H_2(\infty, \cdot))|}_{=0} \\ &= 2\left(|Z_{\varphi_j}^*| - |Z_{\kappa_j}|\right) + |Z_{\varphi_j}|. \end{aligned}$$

By Lemma 5.2.3, all $\varphi_j(s)$ are not a square of a linear polynomial, and since each $\varphi_j(s)$ will have a coefficient of s^2 that is a non-zero square in \mathbb{F}_q , we can use Lemma 5.2.4. All pairs (r, s)

in $\Gamma_j(H_2)$ satisfy $r \neq s$ since $\text{char } \mathbb{F}_q \neq 3$ and by Lemma 5.2.1, $H_2(s, s)$ only happens when s corresponds to a non-singular conic which we already removed by removing elements in Z_{κ_j} . Therefore, we obtain the final count as

$$|\Gamma_j(H_2)| = 2 \left(\underbrace{\frac{q-1-|Z_{\varphi_j}|}{2}}_{\text{Lemma 5.2.4}} - |Z_{\kappa_j}| \right) + |Z_{\varphi_j}| = q-1-2|Z_{\kappa_j}|.$$

□

Proposition 5.2.6. For $\text{char } \mathbb{F}_q = 3$ and $j \in \{3, 14, 16, 19\}$, $|\Gamma_j(H_2)| = q - |Z_{D_j}|$ with D_j as defined in Equation 5.2.1. In particular,

$$|\Gamma_j(H_2)| = q - 3, \quad j \in \{3, 16\}, \quad \text{and}$$

$$|\Gamma_j(H_2)| = q - 1, \quad j \in \{14, 19\}.$$

Proof. By Lemma 5.2.3, all $D_j(s)$ will always be a square. In effect, $s \in \mathbb{F}_q$ will contribute two pairs if it is not a root of $D_j(s)$, and each root contributes one pair. $D_3(s)$ have three roots in \mathbb{F}_q which are $0, 1, -1$. $D_{16}(s)$ also have three roots in \mathbb{F}_q given by $\eta_+, \eta_-, -1$ with η_+, η_- defined as in Table 2.3.2. $D_{14}(s)$ and $D_{19}(s)$ both only have one root in \mathbb{F}_q given by $-e^{-1}$ and $v^{-1}\rho$, respectively.

Since $\text{char } \mathbb{F}_q = 3$, Lemma 5.2.1, states that all $s \in \mathbb{F}_q$ satisfies $H_{2,j}(s, s) = 0$ and hence, we should remove q pairs in counting since these are not valid pairs. Lastly, ∞ does not contribute to any pairs by the same arguments in the proof of Proposition 5.2.5. Thus,

$$\begin{aligned} |\Gamma_j(H_2)| &= |\Gamma_j(H_2(\cdot, \cdot))| + \underbrace{|\Gamma_j(H_2(\cdot, \infty))|}_{=0} + \underbrace{|\Gamma_j(H_2(\infty, \cdot))|}_{=0} \\ &= 2(q - |Z_{D_j}|) + |Z_{D_j}| - \underbrace{q}_{\text{Lemma 5.2.1}} = q - |Z_{D_j}|. \end{aligned}$$

□

5.2.2 Pencil \mathcal{P}_{18}

Before dealing with \mathcal{P}_{18} , we prove this lemma to simplify our proof.

Lemma 5.2.7. *Suppose $\text{char } \mathbb{F}_q \neq 2$. Then we can always find $b \in \mathbb{F}_q \setminus \{0\}$ such that $T^3 + bT^2 + 1$ is an irreducible polynomial in $\mathbb{F}_q[T]$.*

Proof. Note that $T = 0$ is not a root of $T^3 + bT^2 + 1$, so the only possible roots are the non-zero elements of \mathbb{F}_q , which is generated by the primitive element α and each of them takes the form α^k for $k \in \{1, \dots, q-1\}$. Now, a cubic polynomial in $\mathbb{F}_q[T]$ is irreducible if and only if it does not have any root in \mathbb{F}_q . But for $T = \alpha^k$ for some $k \in \{1, \dots, q-1\}$

$$\alpha^{3k} + b\alpha^{2k} + 1 = 0 \iff b = -\alpha^k - \alpha^{-2k}.$$

Hence, if we choose $b \in \mathbb{F}_q \setminus \{-\alpha^k - \alpha^{-2k} \mid k \in \{1, \dots, q-1\}\}$, then this b satisfies the condition that $T^3 + bT^2 + 1$ does not have a root in \mathbb{F}_q , making it irreducible in $\mathbb{F}_q[T]$. This choice is possible since $\{-\alpha^k - \alpha^{-2k} \mid k \in \{1, \dots, q-1\}\}$ has at most $q-1$ elements while \mathbb{F}_q has q elements. Lastly, b cannot be zero since $T^3 + 1$ is not irreducible. \square

Proposition 5.2.8. *For $\text{char } \mathbb{F}_q \neq 3$, $|\Gamma_{18}(H_2)| = q + 1$.*

Proof. By Lemma 5.2.7, we can choose $c = 0$ and $b \neq 0$ such that $T^3 + bT^2 + 1$ is irreducible. Referring to Table 5.1.1, observe that $H_{2,18}(r, s) = H_{2,18}(\infty, s)r^2 + f_1(s)r + f_0(s)$, where $f_1(s), f_0(s) \in \mathbb{F}_q[s]$.

First, let $s \in \mathbb{F}_q$ such that $H_{2,18}(\infty, s) \neq 0$. In this case, $H_{2,18}(r, s)$ is a quadratic polynomial in r so we can interpret the discriminant $D_{18}(s)$ as in Equation 5.2.1. By Lemma 5.2.2, $\kappa_{18}(s)$ is always non-zero and thus, $D_{18}(s)$ is a non-zero square or zero if and only if $\varphi_{18}(s)$ is also a non-zero square or zero. Moreover, our choice of b and c allow us to use Lemma 5.2.4 since the coefficient of s^2 in $\varphi_{18}(s)$ will just be b^2 .

For $s \in \mathbb{F}_q$ such that $H_{2,18}(\infty, s) = 0$, [23] pointed out that we have $D_{18}(s) = f_1(s)^2$ is always a square and this implies that for such s , $\varphi_{18}(s)$ is a square. We will show that s is not a root of

quadratic in r .

Now, we will show that for $s \in \mathbb{F}_q$ such that $H_{2,18}(\infty, s) = 0$, $H_2(r, s)$ will be a linear function of r . To do this, we use the resultant again and see that

$$\text{resultant}(H_{2,18}(\infty, s), f_1(s), s) = 16b^2(4b^3 + 27)^3,$$

which is also non-zero by the same argument as the previous resultant. This implies that $H_2(\infty, s)$ and $f_1(s)$ cannot be simultaneously zero.

Hence, for each element $(\infty, s) \in \Gamma_{18}(H_2(\infty, \cdot))$, we obtain an additional pair of solution $(r, s) \in \Gamma_{18}(\cdot, \cdot)$ corresponding to the solution of the linear equation which yields $r = \frac{f_0(s)}{f_1(s)}$.

Finally, we have $H_{2,18}(r, \infty)$ which is a quadratic polynomial with discriminant that reduces to $(4b)^2$, a non-zero square by our choice of b and c , giving us an additional 2 pairs. The pairs (r, s) we obtain here will have $r \neq s$ by Lemma 5.2.1 since we have no singular conics for this pencil and $\text{char } \mathbb{F}_q \neq 3$. Taking all of this into consideration, we obtain the count

$$\begin{aligned} |\Gamma_{18}(H_2)| &= |\Gamma_{18}(H_2(\cdot, \cdot))| + \underbrace{|\Gamma_{18}(H_2(\cdot, \infty))|}_{=2} + |\Gamma_{18}(H_2(\infty, \cdot))| \\ &= 2 \left(\underbrace{|Z_{\varphi_{18}}^*| - |\Gamma_{18}(H_2(\infty, \cdot))|}_{H_{2,18}(r,s) \text{ quadratic in } r} \right) + |Z_{\varphi_{18}}| + \underbrace{|\Gamma_{18}(H_2(\infty, \cdot))| + 2}_{H_{2,18}(r,s) \text{ linear in } r} + |\Gamma_{18}(H_2(\infty, \cdot))| \\ &= 2 \left(\underbrace{\frac{q-1-|Z_{\varphi_{18}}|}{2}}_{\text{Lemma 5.2.4}} - |\Gamma_{18}(H_2(\infty, \cdot))| \right) + |Z_{\varphi_{18}}| + 2|\Gamma_{18}(H_2(\infty, \cdot))| + 2 = q + 1. \end{aligned}$$

□

Proposition 5.2.9. For $\text{char } \mathbb{F}_q = 3$, $|\Gamma_{18}(H_2)| = q$.

Proof. By Lemma 5.2.7, we can choose $c = 0$ and $b \neq 0$ such that $T^3 + bT^2 + 1$ is irreducible. Observe that $H_{2,18}(\infty, 0) = 4b \neq 0$. Thus, $0 \notin \Gamma_{18}(H_2(\infty, \cdot))$. For $s \in \mathbb{F}_q \setminus \Gamma_{18}(H_2(\infty, \cdot))$, $H_{2,18}(r, s)$ is quadratic in r and $D_{18}(s) = (4(s^3 + bs^2 + 1)(bs))^2$ will always be a square and

is zero exactly when $s = 0$, which we have shown to be not in $\Gamma_{18}(H_2(\infty, \cdot))$. Hence, each non-zero s not in $\Gamma_{18}(H_2(\infty, \cdot))$ will contribute two pairs (r, s) and we get one pair for $s = 0$.

Computing the resultant as discussed in the proof of Proposition 5.2.8,

$$\text{resultant}(H_{2,18}(\infty, s), f_1(s), s) = 64b^{11}$$

in char $\mathbb{F}_q = 3$, which is non-zero. Thus, we get one pair (r, s) where $r = \frac{f_0(s)}{f_1(s)}$ is the solution to the linear equation $H_{2,j}(r, s) = 0$, for each $s \in \Gamma_{18}(H_2(\infty, \cdot))$.

Considering the quadratic polynomial $H_2(r, \infty)$, the discriminant is still $(4b)^2$, which is a non-zero square. This gives us an additional two pairs.

Finally, by Lemma 5.2.1, we need to remove the pairs (s, s) where $s \in \mathbf{P}^1(\mathbb{F}_q)$ which removes a total of $q + 1$ pairs. Taking all these into account, we obtain

$$\begin{aligned} |\Gamma_j(H_2)| &= |\Gamma_j(H_2(\cdot, \cdot))| + \underbrace{|\Gamma_j(H_2(\cdot, \infty))|}_{=2} + |\Gamma_j(H_2(\infty, \cdot))| \\ &= 2 \underbrace{\left(q - 1 - |\Gamma_j(H_2(\infty, \cdot))| \right)}_{H_{2,18}(r,s) \text{ quadratic in } r} + 1 + \underbrace{|\Gamma_j(H_2(\infty, \cdot))|}_{H_{2,18}(r,s) \text{ linear in } r} \\ &+ 2 + \underbrace{|\Gamma_j(H_2(\infty, \cdot))|}_{\text{Lemma 5.2.1}} - (q + 1) = q. \end{aligned}$$

□

5.2.3 Pencils $\mathcal{P}_4, \mathcal{P}_6, \mathcal{P}_{15}, \mathcal{P}_{17}$

Proposition 5.2.10. For $\text{char } \mathbb{F}_q \neq 3$ and $j \in \{4, 6, 15, 17\}$, $|\Gamma_j(H_2)| = q - 1$.

Proof. All of these share the same form of $H_{2,j}(r, s)$, which is degree 1 in both r and s with the roles of r and s reversed for $j = 17$. Choosing $s \in \mathbb{F}_q \setminus \{0\}$, $H_{2,j}(r, s) = 0$ if and only if $r = \frac{s}{4}$ for $j \neq 17$ and $r = 4s$ for $j = 17$. Thus, there is only one value of r for each s , giving us a total of $q - 1$ pairs. We do not count the pairs of the form (∞, s) for $j \neq 17$ and $(0, s)$ for $j = 17$ since they correspond to the irregular pairs. \square

Proposition 5.2.11. For $\text{char } \mathbb{F}_q = 3$ and $j \in \{4, 6, 15, 17\}$, $|\Gamma_j(H_2)| = 0$.

Proof. If $\text{char } \mathbb{F}_q = 3$, we get the condition that $H_{3,j} = 0$ if and only if $r = s$, which cannot happen since valid pairs need to be distinct. We can also use Proposition 5.2.10, which gives us $q - 1$ pairs, but since $\text{char } \mathbb{F}_q = 3$, Lemma 5.2.1 states that $q - 1$ pairs should be removed. \square

5.2.4 Pencils $\mathcal{P}_5, \mathcal{P}_8$

Proposition 5.2.12. For $\text{char } \mathbb{F}_q \neq 3$ and $j \in \{5, 8\}$, $|\Gamma_j(H_2)| = 0$.

Proof. All valid pairs (r, s) will have $H_{2,j}(r, s) = 3 \neq 0$. Pairs of the form (∞, s) correspond to irregular pairs and will not be counted. \square

Proposition 5.2.13. For $\text{char } \mathbb{F}_q = 3$ and $j \in \{5, 8\}$, $|\Gamma_j(H_2)| = q(q - 1)$.

Proof. All valid pairs (r, s) will satisfy $H_{2,j}(r, s) = 0$. Pairs of the form (∞, s) correspond to irregular pairs, which we do not count. Since the only singular conic in this case corresponds to ∞ , then the only condition we need to satisfy is that $r, s \in \mathbb{F}_q$ with $r \neq s$, giving us a total of $q(q - 1)$ pairs. \square

5.2.5 Main theorem for 3-Poncelet pairs

We summarize all the counts derived for this case in Theorem 5.2.14.

Theorem 5.2.14. *Any valid pair corresponding to a 3-Poncelet pair must be a smooth pair. The number of pairs corresponding to 3-Poncelet pairs among the valid pairs, for each pencil, is summarized in Table 5.2.3.*

Table 5.2.3: Count of 3-Poncelet pairs for each pencil in $\mathbf{P}^2(\mathbb{F}_q)$

\mathcal{P}_j	$\text{char } \mathbb{F}_q \neq 3$	$\text{char } \mathbb{F}_q = 3$
$\mathcal{P}_3, \mathcal{P}_{16}$	$q - 5$	$q - 3$
$\mathcal{P}_4, \mathcal{P}_6, \mathcal{P}_{15}, \mathcal{P}_{17}$	$q - 1$	0
$\mathcal{P}_5, \mathcal{P}_8$	0	$q(q - 1)$
$\mathcal{P}_{14}, \mathcal{P}_{19}$	$q - 1$	$q - 1$
\mathcal{P}_{18}	$q + 1$	q

Proof. The fact that all valid pairs corresponding to 3-Poncelet pairs are smooth pairs follows from Lemma 5.2.1. The counts are obtained from Propositions 5.2.5, 5.2.6, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.12, and 5.2.13. \square

Using Theorem 5.2.14, we can now compute the probabilities of obtaining a 3-Poncelet pair in pencil \mathcal{P}_j under the probability space stated at the beginning of Chapter 5. In particular, considering the sample space of valid pairs Φ_j and the uniform measure, the probability of obtaining a 3-Poncelet pair in pencil \mathcal{P}_j is given by

$$\mathbb{P}(\Gamma_j(H_2)|\Phi_j) = \frac{|\Gamma_j(H_2)|}{|\Phi_j|}.$$

Upon restricting the sample space to smooth pairs Ψ_j , the probability of obtaining a 3-Poncelet pair in pencil \mathcal{P}_j is given by

$$\mathbb{P}(\Gamma_j(H_2)|\Psi_j) = \frac{|\Gamma_j(H_2) \cap \Psi_j|}{|\Psi_j|}.$$

Since $|\Gamma_j(H_2) \cap \Psi_j| = |\Gamma_j(H_2)|$ by Theorem 5.2.14, the counts used as numerators in the probability are the same for both the valid pairs and smooth pairs. However, the denominators differ, and we need to adjust the counting for the irregular pairs. We summarize the count of valid and smooth pairs for each pencil in Table 5.2.4.

Table 5.2.4: Count of valid pairs and smooth pairs for each pencil in $\mathbf{P}^2(\mathbb{F}_q)$

\mathcal{P}_j	Smooth Pairs	Valid Pairs
$\mathcal{P}_3, \mathcal{P}_{16}$	$(q-2)(q-3)$	$q(q-2)$
$\mathcal{P}_4, \mathcal{P}_{15}$	$(q-1)(q-2)$	$(q-1)^2$
$\mathcal{P}_5, \mathcal{P}_8$	$q(q-1)$	$q(q-1)$
$\mathcal{P}_6, \mathcal{P}_{17}$	$(q-1)(q-2)$	$(q-1)(q-2)$
$\mathcal{P}_{14}, \mathcal{P}_{19}$	$q(q-1)$	q^2
\mathcal{P}_{18}	$(q+1)q$	$(q+1)q$

Finally, we provide the probabilities in Corollary 5.2.15.

Corollary 5.2.15. *The probabilities of obtaining a valid pair or a smooth pair corresponding to a 3-Poncelet pair for each pencil \mathcal{P}_j under our assumed probability space are summarized in Table 5.2.5.*

Table 5.2.5: Probabilities of obtaining a 3-Poncelet pair for each pencil in $\mathbf{P}^2(\mathbb{F}_q)$

\mathcal{P}_j	Smooth Pairs		Valid Pairs	
	$\text{char } \mathbb{F}_q \neq 3$	$\text{char } \mathbb{F}_q = 3$	$\text{char } \mathbb{F}_q \neq 3$	$\text{char } \mathbb{F}_q = 3$
$\mathcal{P}_3, \mathcal{P}_{16}$	$\frac{q-5}{(q-2)(q-3)}$	$\frac{1}{q-2}$ for $q > 3^\dagger$	$\frac{q-5}{q(q-2)}$	$\frac{q-3}{q(q-2)}$
$\mathcal{P}_4, \mathcal{P}_{15}$	$\frac{1}{q-2}$	0	$\frac{1}{q-1}$	0
$\mathcal{P}_5, \mathcal{P}_8$	0	1	0	1
$\mathcal{P}_6, \mathcal{P}_{17}$	$\frac{1}{q-2}$	0	$\frac{1}{q-2}$	0
$\mathcal{P}_{14}, \mathcal{P}_{19}$	$\frac{1}{q}$	$\frac{1}{q}$	$\frac{q-1}{q^2}$	$\frac{q-1}{q^2}$
\mathcal{P}_{18}	$\frac{1}{q}$	$\frac{1}{q+1}$	$\frac{1}{q}$	$\frac{1}{q+1}$

† : The sample space is empty for $q = 3$

Remark 5.2.16. *Following the approach of [3] of combining probabilities from multiple pencils, we recover their main result that the asymptotic probability of obtaining a 3-Poncelet pair among smooth, transversally intersecting conics in $\mathbf{P}^2(\mathbb{F}_q)$ is $\frac{1}{q}$ when $\text{char } \mathbb{F}_q \neq 3$. Under the same approach, our computation suggests that this asymptotic probability remains to be $\frac{1}{q}$ even if $\text{char } \mathbb{F}_q = 3$.*

5.3 Probabilities for 4-Poncelet pairs

In this section, we answer our main research question about the probability of obtaining a 4-Poncelet pair among the valid pairs for each pencil in Table 2.3.2.

Similar to the triangle case, we also have a version of Lemma 5.2.1 to detect pairs (r, s) that satisfy $H_{3,j}(r, s) = 0$ but $r = s$.

Lemma 5.3.1. *Let $H_{3,j}$ be the form of H_3 under \mathcal{P}_j and $C_j(\eta)$ be the matrix representation of the element corresponding to $\eta \in \mathbf{P}^1(\mathbb{F}_q)$ in pencil \mathcal{P}_j . Then, $H_{3,j}(\eta, \eta) = 0$ if and only if $C_j(\eta)$ is singular.*

Proof. Let $A = B = C_j(\eta)$, then $\Delta(t) = \sqrt{\det(tA + A)} = \sqrt{(t+1)^3 \det(A)} = \sqrt{\lambda t^3 + \beta t^2 + \gamma t + \epsilon}$ where $\lambda = \det(A)$, $\beta = 3 \det(A)$, $\gamma = 3 \det(A)$, $\epsilon = \det(A)$.

By Lemma 5.1.1, $H_{3,j}(s, s) = \frac{8 \det(A)^3 - 36 \det(A)^3 + 27 \det(A)^3}{16 \det(A)^2 \sqrt{\det(A)}} = \frac{-1}{16} \sqrt{\det(A)}$, which is zero if and only if $\det(A) = 0$ which happens when $A = C_j(\eta)$ is singular. \square

Adapting a similar notation from the triangle case, we denote the set of valid pairs that correspond to 4-Poncelet pairs as

$\Gamma_j(H_3) = \{(r, s) \in \Phi_j \mid H_{3,j}(r, s) = 0\}$, which we decompose into three disjoint sets

$\Gamma_j(H_3(\cdot, \cdot)) = \{(r, s) \in \Gamma_j(H_3) \mid r, s \in \mathbb{F}_q\}$,

$\Gamma_j(H_3(\cdot, \infty)) = \{(r, s) \in \Gamma_j(H_3) \mid r \in \mathbb{F}_q, s = \infty\}$, and

$\Gamma_j(H_3(\infty, \cdot)) = \{(r, s) \in \Gamma_j(H_3) \mid r = \infty, s \in \mathbb{F}_q\}$.

Our approach to count 4-Poncelet pairs is to treat $H_{3,j}(r, s)$ as a polynomial in $(\mathbb{F}_q[s])[r]$ where we can see from Table 5.1.2 that it is at most cubic in r for all j .

5.3.1 Pencils $\mathcal{P}_3, \mathcal{P}_{16}$

Proposition 5.3.2. For $j \in \{3, 16\}$, $|\Gamma_j(H_3)| = 3q - 6$ and $|\Gamma_j(H_3) \cap \Psi_j| = 3q - 9$.

Proof. We can show that $H_{3,j}(r, s) = f_1(r, s)f_2(r, s)f_3(r, s)$ where each factor $f_i(r, s)$ is linear. Since the product is zero if at least one of the factors is zero, define

$$A_i = \{(r, s) \in \Phi_j \mid f_i(r, s) = 0\}, i = 1, 2, 3.$$

The union $\bigcup_{i=1}^3 A_i$ contains all pairs (r, s) such that $H_3(r, s) = 0$ and its cardinality can be obtained by the Inclusion-Exclusion principle. That is,

$$\left| \bigcup_{i=1}^3 A_i \right| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

For \mathcal{P}_3 , we immediately see from Table 5.1.2 that we can let

$$f_1(r, s) = r - s^2, f_2(r, s) = (2s - 1)r - s^2, f_3(r, s) = r + (s^2 - 2s).$$

Now, $f_1(r, s) = 0 \iff r = s^2$ which gives us q pairs since we can choose any $s \in \mathbb{F}_q$. For the second factor, we consider two cases. If $2s - 1 = 0$ then $s = \frac{1}{2}$ which will make $f_2(r, s) = \frac{-1}{4} \neq 0$ which does not contribute any pair. If $2s - 1 \neq 0$, then $f_2(r, s) = 0 \iff r = \frac{s^2}{2s-1}$ which gives us $q - 1$ pairs since we cannot choose $s = \frac{1}{2}$. Finally, $f_3(r, s) = 0 \iff r = 2s - s^2$ which gives us again q pairs. Going to the pairwise relations, $f_1(r, s) = f_2(r, s) = 0 \iff r = s^2 = \frac{s^2}{2s-1}$. Note that from the argument above, $s \neq \frac{1}{2}$ since $f_2(r, s) = 0$. Thus, we can solve the quadratic equation $s^2 = \frac{s^2}{2s-1}$ which is equivalent to $2s^2(s - 1) = 0$. Hence, we only have 2 choices for this pair, which are $s = 0$ or $s = 1$. This will be the same idea for $f_1(r, s) = f_3(r, s) = 0$ and $f_2(r, s) = f_3(r, s) = 0$ which will both yield the same solution of $s = 0$ and $s = 1$. This also

immediately gives us that $f_1(r, s) = f_2(r, s) = f_3(r, s) = 0 \iff s \in \{0, 1\}$. Finally, we use Lemma 5.3.1 to remove unwanted pairs $(0, 0)$ and $(1, 1)$.

Notice that $H_{3,3}(\infty, s) = 2s - 1$ and is zero if and only if $s = \frac{1}{2}$. Thus, the pair $(\infty, \frac{1}{2})$ is the only valid pair in $\Gamma_3(H_3(\infty, \cdot))$. The set $\Gamma_3(H_3(\cdot, \infty))$ is empty since we don't consider the case where $C_j(s)$ is singular.

Thus, for $j = 3$, we obtain the count

$$\begin{aligned} |\Gamma_j(H_3)| &= |\Gamma_j(H_3(\cdot, \cdot))| + \underbrace{|\Gamma_j(H_3(\cdot, \infty))|}_{=0} + \underbrace{|\Gamma_j(H_3(\infty, \cdot))|}_{=1} \\ &= \underbrace{q + (q - 1) + q - 2 - 2 - 2 + 2}_{\text{Inclusion-Exclusion}} - \underbrace{2}_{\text{Lemma 5.3.1}} + 1 = 3q - 6. \end{aligned}$$

Restricting to the smooth conics, we need to find the valid pairs in $\Gamma_j(H_3)$ that are not smooth. We already have the pair $(\infty, \frac{1}{2})$ from $r = \infty$. Looking at the other singular elements, if $r = 0$, then we obtain $H_{3,3}(0, s) = s^5(s - 2)$ which gives us one valid pair $(0, 2)$. Finally, for $r = 1$, $H_{3,3}(1, s) = (s - 1)^5(s + 1)$ giving us another valid pair $(1, -1)$. In total, we have 3 valid pairs corresponding to 4-Poncelet pairs that are not smooth pairs. Hence, for $j = 3$,

$$|\Gamma_j(H_3) \cap \Psi_j| = |\Gamma_j(H_3)| - 3 = 3q - 9.$$

A similar structure occurs for $j = 16$ by observing that we can let the first linear factor of $H_{3,16}(r, s)$ as

$$f_1(r, s) = (2s - 1)r - \left(s^2 + \frac{u^2 - 1}{4}\right),$$

and the quadratic factor can be expressed as a product of two linear polynomials in $(\mathbb{F}_q[s])[r]$, which we denote by

$$f_2(r, s) = ur - \left(us + s^2 - s - \frac{u^2 - 1}{4}\right), f_3(r, s) = ur - \left(us - s^2 + s + \frac{u^2 - 1}{4}\right),$$

where $u = \sqrt{(1-4d)(1-4e)} \in \mathbb{F}_q \setminus \{0\}$ since, by assumptions in Table 2.3.1, $1-4d$ and $1-4e$ are both non-squares, which means their product must be a non-zero square.

In this case, $f_1(r, s)$ will give one pair for each $s \neq \frac{1}{2}$, giving us a total of $q-1$ pairs while the other factors will contribute q pairs. For the pairwise contributions, we have $f_i(r, s) = f_j(r, s) = 0$ for $i \neq j$ if and only if $s \in \{\eta_+, \eta_-\}$ where $\eta_+ = \frac{1+u}{2}$ and $\eta_- = \frac{1-u}{2}$ are the elements in \mathbb{F}_q that corresponds to singular conics in pencil \mathcal{P}_{16} as shown in Table 2.3.2. We also get one contribution for the pair $(\infty, \frac{1}{2})$ and no contribution for $s = \infty$. Altogether, we get the same number of valid pairs that are 4-Poncelet pairs as in the case of $j = 3$.

Lastly, we have $H_{3,16}(\eta_+, s) = 0$ if and only if $s \in \{\eta_+, \frac{1-3u}{2}\}$, and $H_{3,16}(\eta_-, s) = 0$ if and only if $s \in \{\eta_-, \frac{1+3u}{2}\}$ which gives us the 3 valid pairs, $(\eta_+, \frac{1-3u}{2}), (\eta_-, \frac{1+3u}{2}), (\infty, \frac{1}{2}) \in \Gamma_j(H_3)$, that are not smooth pairs which again implies that we have the same number of smooth pairs that are 4-Poncelet pairs as in the case of $j = 3$.

□

5.3.2 Pencils $\mathcal{P}_{14}, \mathcal{P}_{19}$

Proposition 5.3.3. For $j \in \{14, 19\}$, $|\Gamma_j(H_3)| = q$ and $|\Gamma_j(H_3) \cap \Psi_j| = q-1$.

Proof. For this case, we have $H_3(r, s) = f_1(r, s)f_2(r, s)$ where $f_1(r, s)$ is linear while $f_2(r, s)$ is quadratic polynomial that does not have any roots for all $s \in \mathbb{F}_q$ and hence, $H_{3,j}(r, s) = 0$ if and only if the linear factor is $f_1(r, s) = 0$.

First, let us show that the linear factors are zero for $q-1$ pairs. For $j = 14$, the linear factor is 0 if and only if $r = \frac{es^2-1}{2es-1}$ which gives us one pair (r, s) for each $s \in \mathbb{F}_q \setminus \{\frac{1}{2e}\}$. Similarly, for $j = 19$, the linear factor is 0 if and only if $r = \frac{vs^2-\sigma^2}{2vs+\rho}$ which gives us one pair (r, s) for each $s \in \mathbb{F}_q \setminus \{\frac{-\rho}{2v}\}$.

Going to the quadratic factor, for $j = 14$, $D(f_2(r, s)) = 4(es^2-s+1)^2(1-4e)$. By the assumption in Table 2.3.1 that T^2+T+e is irreducible, we have that its discriminant $1-4e$ is non-square. Since the polynomial es^2-s+1 shares the same discriminant, it is also irreducible and will not

have any roots in \mathbb{F}_q . Hence, the factor $4(es^2 - s + 1)^2$ is always a non-zero square and $D(f_2(r, s))$ is always a non-square for any $s \in \mathbb{F}_q$. For $j = 19$, $D(f_2(r, s)) = 4(vs^2 + \rho s + \sigma^2)^2(\rho^2 - 4v\sigma^2)$ and using the assumptions in Table 2.3.1, $vs^2 + \rho s + \sigma^2$ is non-zero for any $s \in \mathbb{F}_q$ since its discriminant, $\rho^2 - 4v\sigma^2$, is non-square. Thus, $D(f_2(r, s))$ is always a non-square for any $s \in \mathbb{F}_q$.

Finally, the coefficient of r in the linear factor turns out to be $H_{3,j}(\infty, s)$ which gives us the valid pairs $(\infty, \frac{1}{2e})$ for $j = 14$ and $(\infty, \frac{-\rho}{2v})$ for $j = 19$. Adding all these contributions, we obtain

$$\begin{aligned} |\Gamma_j(H_2)| &= |\Gamma_j(H_2(\cdot, \cdot))| + \underbrace{|\Gamma_j(H_2(\cdot, \infty))|}_{=0} + \underbrace{|\Gamma_j(H_2(\infty, \cdot))|}_{=1} \\ &= (q - 1) + 1 = q. \end{aligned}$$

Since the valid pairs in $\Gamma_j(H_3)$ that are not smooth pairs are just those in $\Gamma_j(H_2(\infty, \cdot))$

$$|\Gamma_j(H_3) \cap \Psi_j| = |\Gamma_j(H_3)| - 1 = q - 1.$$

□

5.3.3 Pencil \mathcal{P}_{18}

For the case of pencil \mathcal{P}_{18} , $H_{3,18}$ from Cayley's condition becomes cumbersome, so we instead use a geometric argument based on our discussion of degenerate Poncelet polygons in Section 3.3 to show that we cannot construct a Poncelet tetragon for any pair in this pencil.

Proposition 5.3.4. $|\Gamma_{18}(H_3)| = 0$.

Proof. Suppose $(\mathcal{A}, \mathcal{B})$ is a 4-Poncelet pair in pencil \mathcal{P}_{18} . If we start our construction at $P_1 = [0 : 0 : 1] \in \mathcal{A} \cap \mathcal{B}$, we obtain a degenerate Poncelet 4-gon, and since 4 is even, we should have two vertices that are base points by Proposition 3.3.6. By Proposition 3.3.7, $P_2 = P_4$, and P_3 should also be a base point. But from Table 2.3.2, we only have one base point $[0 : 0 : 1]$ for pencil \mathcal{P}_{18} which is in $\mathbf{P}^2(\mathbb{F}_q)$ and the irreducibility of $T^3 + bT^2 + cT + 1$ implies that the homogeneous coordinates of the remaining base points cannot be obtained from

a solution of a quadratic equation in $\mathbb{F}_q[T]$.

With this, the remaining base points cannot be obtained as an intersection of any line and conic in $\mathbf{P}^2(\mathbb{F}_q)$, and we cannot have a construction starting from $P_1 = [0 : 0 : 1]$ that will give us a vertex leading to a base point other than $[0 : 0 : 1]$. This forces us to have $P_1 = P_3 = [0 : 0 : 1]$ which also makes P_2 a base point by Lemma 3.3.3. This contradicts Lemma 3.3.4 since we have $P_1 = P_2 = P_3 = [0 : 0 : 1]$ which is a base point of intersection multiplicity 1. \square

5.3.4 Pencils $\mathcal{P}_4, \mathcal{P}_6, \mathcal{P}_{15}, \mathcal{P}_{17}$

Proposition 5.3.5. For $j \in \{4, 6, 15, 17\}$, $|\Gamma_j(H_3)| = |\Gamma_j(H_3) \cap \Psi_j| = q - 1$.

Proof. All of these share the same form of $H_{3,j}(r, s)$, which is degree 1 in both r and s with the roles of r and s reversed for $j = 17$. Choosing $s \in \mathbb{F}_q \setminus \{0\}$, $H_{3,j}(r, s) = 0$ if and only if $r = \frac{s}{2}$ for $j \neq 17$ and $r = 2s$ for $j = 17$. Thus, there is only one value of r for each s , giving us a total of $q - 1$ pairs. We will not count the pairs of the form (∞, s) for $j \neq 17$ and $(0, s)$ for $j = 17$ since they correspond to the irregular pairs. \square

5.3.5 Pencils $\mathcal{P}_5, \mathcal{P}_8$

Proposition 5.3.6. For $j \in \{5, 8\}$, $|\Gamma_j(H_3)| = 0$.

Proof. All valid pairs (r, s) will have $H_{2,j}(r, s) \neq 0$. Pairs of the form (∞, s) correspond to irregular pairs, which we do not count. \square

5.3.6 Main theorem for 4-Poncelet pairs

We summarize all the counts for this case in Theorem 5.3.7.

Theorem 5.3.7. The number of pairs corresponding to 4-Poncelet pairs among the valid pairs and smooth pairs, for each pencil, is summarized in Table 5.3.1.

Proof. See Propositions 5.3.2, 5.3.3, 5.3.4, 5.3.5, and 5.3.6. \square

Table 5.3.1: Count of 4-Poncelet pairs for each pencil in $\mathbf{P}^2(\mathbb{F}_q)$

\mathcal{P}_j	Smooth Pairs	Valid Pairs
$\mathcal{P}_3, \mathcal{P}_{16}$	$3(q - 3)$	$3(q - 2)$
$\mathcal{P}_4, \mathcal{P}_6, \mathcal{P}_{15}, \mathcal{P}_{17}$	$q - 1$	$q - 1$
$\mathcal{P}_5, \mathcal{P}_8$	0	0
$\mathcal{P}_{14}, \mathcal{P}_{19}$	$q - 1$	q
\mathcal{P}_{18}	0	0

Using Theorem 5.3.7 and Table 5.2.4, we provide the probabilities in Corollary 5.3.8.

Corollary 5.3.8. *The probabilities of obtaining a valid pair or a smooth pair corresponding to a 4-Poncelet pair for each pencil \mathcal{P}_j under our assumed probability space are summarized in Table 5.3.2.*

Table 5.3.2: Probabilities of obtaining a 4-Poncelet pair for each pencil in $\mathbf{P}^2(\mathbb{F}_q)$

\mathcal{P}_j	Smooth Pairs	Valid Pairs
$\mathcal{P}_3, \mathcal{P}_{16}$	$\frac{3}{q-2}$ for $q > 3^\dagger$	$\frac{3}{q}$
$\mathcal{P}_4, \mathcal{P}_{15}$	$\frac{1}{q-2}$	$\frac{1}{q-1}$
$\mathcal{P}_5, \mathcal{P}_8$	0	0
$\mathcal{P}_6, \mathcal{P}_{17}$	$\frac{1}{q-2}$	$\frac{1}{q-2}$
$\mathcal{P}_{14}, \mathcal{P}_{19}$	$\frac{1}{q}$	$\frac{1}{q}$
\mathcal{P}_{18}	0	0

† : The sample space is empty for $q = 3$

Remark 5.3.9. *The computed probabilities of obtaining a 4-Poncelet pair for pencils with transversally intersecting elements are consistent with the asymptotic results in [23].*

6. Conclusion

This thesis provides a systematic discussion about Poncelet polygons and probabilities regarding n -Poncelet pairs in $\mathbf{P}^2(\mathbb{F}_q)$ for $n = 3$ and $n = 4$.

A natural direction for further research is to compute the probabilities of obtaining an n -Poncelet pair in a fixed pencil in $\mathbf{P}^2(\mathbb{F}_q)$ for $n > 4$. This direction can be thought of as fixing the number of sides n and studying how the probability varies with the order q .

It will also be interesting to ask a symmetric question on how the number of sides n is distributed for a fixed order q . We performed a computational experiment where, for every valid pair in $\mathbf{P}^2(\mathbb{F}_q)$ with $q \leq 19$, we computed n , the number of sides of the Poncelet polygon that can be constructed from that pair. From this, we state as a conjecture one pattern that we noticed involving non-smooth valid pairs that intersect non-transversally.

Conjecture 6.0.1. *For pencils \mathcal{P}_4 and \mathcal{P}_{15} in $\mathbf{P}^2(\mathbb{F}_q)$ and $k = 2 \operatorname{char} \mathbb{F}_q$, the pair $(0, s)$, where $s \in \mathbb{F}_q \setminus \{0\}$, correspond to a k -Poncelet pair.*

In fact, we already provided an instance of this conjecture in Section 4.4 where we considered in $\mathbf{P}^2(\mathbb{F}_3)$ the pair $(0, 1)$ in pencil \mathcal{P}_4 and hence, we expect a 6-Poncelet pair. This might have a connection with the result in [17], which considers Poncelet n -gons where $n = \operatorname{char} \mathbb{F}_q$.

A. Representation of finite field elements

In this appendix, we discuss Conway polynomials and how they are used to represent finite fields.

Conway polynomials are irreducible polynomials in $\mathbb{F}_p[x]$ that are particularly useful in computer algebra systems, which provide canonical choices for constructing a representation for finite fields. We denote by $C_{p,k}(x)$ the Conway polynomial of degree k in $\mathbb{F}_p[x]$.

One of the useful properties of Conway polynomials is that each root of the Conway polynomial is a primitive element. Another special property is the compatibility condition, which means that for a Conway polynomial $C_{q,n}$ with root α , and for any divisor m of n , then $\alpha^{\frac{q^n-1}{q^m-1}}$ is a root of $C_{q,m}$.

We provide in Table A.0.1 some Conway polynomials used in calculations for small order finite fields.

$q = p^k$	$9 = 3^2$	$25 = 5^2$	$27 = 3^3$	$121 = 11^2$
$C_{p,k}(x)$	$x^2 + 2x + 2$	$x^2 + 4x + 2$	$x^3 + 2x + 1$	$x^2 + 7x + 2$

Table A.0.1: Conway polynomials used for representation of \mathbb{F}_q

We illustrate with $q = 9 = 3^2$ how we can use this in representing elements of our finite field. Let α be the primitive element which is a root of $C_{3,2}(x) = x^2 + 2x + 2$. Table A.0.2 summarizes all these representations.

Power	0	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7
Polynomial	0	1	α	$\alpha + 1$	$2\alpha + 1$	2	2α	$2\alpha + 2$	$\alpha + 2$

Table A.0.2: Representation of Elements of \mathbb{F}_9

As a sample calculation, let us show that $\alpha^3 = 2\alpha + 1$.

$$\alpha^3 = \alpha(\alpha^2) = \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1.$$

Here, we used the fact that α is a root of the Conway polynomial and thus, $\alpha^2 = -2\alpha - 2$. Finally, using modulo 3 arithmetic, $-2\alpha - 2 = \alpha + 1$.

This representation can also be used to calculate square roots of any element in \mathbb{F}_3 . Note that 2 is not a square in \mathbb{F}_3 but looking at Table A.0.2, we can see that it has a square root in \mathbb{F}_9 with $\sqrt{2} = \alpha^{4/2} = \alpha + 1$.

B. Enumeration of Poncelet triangles

In this appendix, we list all 3-Poncelet pairs in $P^2(\mathbb{F}_q)$ for each pencil in Table 2.3.2. We do this for all possible $q \leq 19$, and provide the number of degenerate Poncelet triangles, Poncelet triangles in the extended plane, and non-degenerate Poncelet triangles in the plane that can be constructed for each of these pairs.

Computations on this part are done with the aid of the Galois package [15] in Python.

Poncelet triangles in pencil \mathcal{P}_3

$q = 3$: No Poncelet triangles for this order.

$q = 5$: No Poncelet triangles for this order.

$q = 7$: All Poncelet triangles are degenerate for all pairs in Table B.0.1. There are 4 degenerate triangles.

Table B.0.1: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_3, q = 7$

r	3	5
s	5	3

$q = 9$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.2, there are 4 degenerate triangles and 2 triangles in the extended plane.

Table B.0.2: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_3, q = 9$

r	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
s	$2\alpha + 1$	$2\alpha + 2$	2α	$\alpha + 2$	α	$\alpha + 1$

$q = 11$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.3, there are 4 degenerate triangles and 4 triangles in the extended plane.

$q = 13$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.4, there are 4 degenerate triangles and 6 triangles in the extended plane.

Table B.0.3: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_3, q = 11$

r	2	2	6	6	10	10
s	6	10	2	10	2	6

Table B.0.4: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_3, q = 13$

r	3	4	5	6	8	9	10	11
s	12	10	2	7	7	12	4	2

$q = 17$: Table B.0.5 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there are 4 degenerate triangles. The remaining $10 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.5: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_3, q = 17$

r	3	3	6	6	8	8	10	10	12	12	15	15
s	5	14	7	11	4	13	5	14	7	11	4	13
non-degenerate triangles	0	2	0	2	0	2	2	0	2	0	2	0

$q = 19$: Table B.0.6 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there are 4 degenerate triangles. The remaining $12 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.6: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_3, q = 19$

r	3	4	5	6	7	8	9
s	13	9	17	7	17	12	11
non-degenerate triangles	2	2	2	2	2	0	2

r	11	12	13	14	15	16	17
s	9	8	3	13	3	11	7
non-degenerate triangles	2	0	2	2	2	2	2

$q = 25$: Table B.0.7 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there are 4 degenerate triangles. The remaining $18 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Poncelet triangles in pencil \mathcal{P}_4

$q = 3$: There are no Poncelet triangles if $\text{char } \mathbb{F}_q = 3$.

Table B.0.7: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_3, q = 25$

r	$\alpha + 1$	$\alpha + 2$	$\alpha + 3$	$\alpha + 4$	2α	$2\alpha + 2$	$2\alpha + 2$
s	$2\alpha + 1$	3α	$3\alpha + 3$	$2\alpha + 3$	α	2	3
non-degenerate triangles	2	2	2	2	2	4	4
r	$2\alpha + 2$	$2\alpha + 2$	$2\alpha + 4$	$3\alpha + 1$	$3\alpha + 2$	$3\alpha + 4$	$3\alpha + 4$
s	4	$3\alpha + 4$	α	$4\alpha + 1$	$4\alpha + 1$	2	3
non-degenerate triangles	4	4	2	2	2	4	4
r	$3\alpha + 4$	$3\alpha + 4$	4α	$4\alpha + 2$	$4\alpha + 3$	$4\alpha + 4$	
s	4	$2\alpha + 2$	3α	$3\alpha + 3$	$2\alpha + 3$	$2\alpha + 1$	
non-degenerate triangles	4	4	2	2	2	2	

$q = 5$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.8, there are 3 degenerate triangles and 1 triangle in the extended plane.

Table B.0.8: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 5$

r	1	2	3	4
s	4	3	2	1

$q = 7$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.9, there are 3 degenerate triangles and 3 triangles in the extended plane.

Table B.0.9: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 7$

r	1	2	3	4	5	6
s	4	1	5	2	6	3

$q = 9$: No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

$q = 11$: For all pairs in Table B.0.10, there is 1 non-degenerate triangle in the plane, 3 degenerate triangles, and 4 triangles in the extended plane.

Table B.0.10: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 11$

r	1	2	3	4	5	6	7	8	9	10
s	4	8	1	5	9	2	6	10	3	7

$q = 13$: For all pairs in Table B.0.11, there is 1 non-degenerate triangle in the plane, 3 degenerate triangles, and 6 triangles in the extended plane.

$q = 17$: For all pairs in Table B.0.12, there are 2 non-degenerate triangles in the plane, 3 degenerate triangles, and 7 triangles in the extended plane.

Table B.0.11: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 13$

r	1	2	3	4	5	6	7	8	9	10	11	12
s	4	8	12	3	7	11	2	6	10	1	5	9

Table B.0.12: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 17$

r	1	2	3	4	5	6	7	8
s	4	8	12	16	3	7	11	15
r	9	10	11	12	13	14	15	16
s	2	6	10	14	1	5	9	13

q = 19 : For all pairs in Table B.0.13, there are 2 non-degenerate triangles in the plane, 3 degenerate triangles, and 9 triangles in the extended plane.

Table B.0.13: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 19$

r	1	2	3	4	5	6	7	8	9
s	4	8	12	16	1	5	9	13	17
r	10	11	12	13	14	15	16	17	18
s	2	6	10	14	18	3	7	11	15

q = 25 : For all pairs in Table B.0.14, there are 3 non-degenerate triangles in the plane, 3 degenerate triangles, and 12 triangles in the extended plane.

Table B.0.14: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_4, q = 25$

r	1	2	3	4	α	$\alpha + 1$	$\alpha + 2$	$\alpha + 3$
s	4	3	2	1	4α	$4\alpha + 4$	$4\alpha + 3$	$4\alpha + 2$
r	$\alpha + 4$	2α	$2\alpha + 1$	$2\alpha + 2$	$2\alpha + 3$	$2\alpha + 4$	3α	$3\alpha + 1$
s	$\alpha + 1$	3α	$3\alpha + 4$	$3\alpha + 3$	$3\alpha + 2$	$3\alpha + 1$	2α	$2\alpha + 4$
r	$3\alpha + 2$	$3\alpha + 3$	$3\alpha + 4$	4α	$4\alpha + 1$	$4\alpha + 2$	$4\alpha + 3$	$4\alpha + 4$
s	$2\alpha + 3$	$2\alpha + 2$	$2\alpha + 1$	α	$\alpha + 4$	$\alpha + 3$	$\alpha + 2$	$\alpha + 1$

Poncelet triangles in pencil \mathcal{P}_5

Due to the form of H_2 for this pencil, only q with $\text{char } \mathbb{F}_q = 3$ will have a Poncelet triangle.

q = 3 : All Poncelet triangles in this case are either degenerate or in the extended plane. For all the pairs of (r, s) , there are 2 degenerate triangles and 1 triangle in the extended plane.

q = 9 : For all the pairs of (r, s) , there is 1 non-degenerate triangle in the plane, 2 degenerate triangles, and 4 triangles in the extended plane.

q = 27 : For all the pairs of (r, s) , there are 4 non-degenerate triangles in the plane, 2 degenerate triangles, and 13 triangles in the extended plane.

Poncelet triangles in pencil \mathcal{P}_6

Since this pencil has the same form of $H_2(r, s)$ as that of \mathcal{P}_4 , we refer to the table of values in that subsection.

q = 3 : No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

q = 5 : All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.8, there are 2 degenerate triangles and 4 triangles in the extended plane.

q = 7 : All Poncelet triangles in this case are in the plane. For all pairs in Table B.0.9, there are 2 non-degenerate triangles in the plane and 2 degenerate triangles.

q = 9 : No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

q = 11 : All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.10, there are 2 degenerate triangles and 10 triangles in the extended plane.

q = 13 : All Poncelet triangles in this case are in the plane. For all pairs in Table B.0.11, there are 4 non-degenerate triangles in the plane and 2 degenerate triangles.

q = 17 : All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.12, there are 2 degenerate triangles and 16 triangles in the extended plane.

q = 19 : All Poncelet triangles in this case are in the plane. For all pairs in Table B.0.13, there are 6 non-degenerate triangles in the plane and 2 degenerate triangles.

q = 25 : All Poncelet triangles in this case are in the plane. For all pairs in Table B.0.14, there are 8 non-degenerate triangles in the plane and 2 degenerate triangles.

Poncelet triangles in pencil \mathcal{P}_8

Due to the form of H_2 for this pencil, only q with $\text{char } \mathbb{F}_q = 3$ will have a Poncelet triangle.

$q = 3$: Table B.0.15 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $3 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

r	0	0	1	1	2	2
s	1	2	0	2	0	1
non-degenerate triangles	1	0	0	1	1	0

Table B.0.15: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_8, q = 3$

$q = 9$: There are 72 pairs to consider in this case, so we will not list the specific values.

Among the 72 pairs, 36 of them contain 3 non-degenerate triangles in the plane and 1 degenerate triangle. The remaining 36 pairs contain 1 degenerate triangle and 9 triangles in the extended plane.

$q = 27$: There are 702 pairs to consider in this case, so we will not list the specific values.

Among the 702 pairs, 351 of them contain 9 non-degenerate triangles in the plane and 1 degenerate triangle. The remaining 351 pairs contain 1 degenerate triangle and 27 triangles in the extended plane.

Poncelet triangles in pencil \mathcal{P}_{14}

$q = 3$: All Poncelet triangles are degenerate for all pairs in Table B.0.16. There are 4 degenerate triangles.

Table B.0.16: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_{14}, q = 3$

r	0	2
s	2	0

$q = 5$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.17, there are 2 degenerate triangles and 2 triangles in the extended plane.

Table B.0.17: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_{14}, q = 5$

r	2	2	4	4
s	3	4	2	3

q = 7 : Table B.0.18 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $4 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.18: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 7$

r	0	1	2	3	4	5
s	2	6	3	2	6	3
non-degenerate triangles	0	1	0	0	1	0

q = 9 : Table B.0.19 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $6 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.19: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 9$

r	0	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 2$
s	$2\alpha + 2$	α	1	$\alpha + 1$	2	2α	0	$\alpha + 2$
non-degenerate triangles	0	1	1	1	1	0	0	0

q = 11 : Table B.0.20 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $8 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.20: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 11$

r	2	2	4	4	6	6	8	8	10	10
s	0	10	3	9	0	1	3	9	1	2
non-degenerate triangles	1	1	0	2	1	1	2	0	1	1

q = 13 : Table B.0.21 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $10 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

q = 17 : Table B.0.22 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $14 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.21: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 13$

r	0	1	3	4	6	7	9	10	10	10	10	11
s	4	6	12	8	1	3	6	3	4	8	12	1
non-degenerate triangles	2	1	2	2	1	2	1	2	2	2	2	1

Table B.0.22: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 17$

r	2	2	5	5	6	6	7	7
s	15	16	0	13	15	9	0	5
non-degenerate triangles	2	2	1	3	2	2	3	1

r	11	11	12	12	13	13	16	16
s	1	13	3	9	1	5	2	3
non-degenerate triangles	3	1	2	2	1	3	2	2

$q = 19$: Table B.0.23 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $16 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.23: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 19$

r	1	3	4	6	7	9	11	12	12
s	5	18	9	1	11	5	2	3	7
non-degenerate triangles	1	2	3	3	2	1	2	2	2

r	12	12	13	16	17	17	17	17	18
s	8	11	9	1	2	3	7	18	8
non-degenerate triangles	2	2	3	3	2	2	2	2	2

$q = 25$: Table B.0.24 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there are 2 degenerate triangles. The remaining $22 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Poncelet triangles in pencil \mathcal{P}_{15}

Since this pencil has the same form of $H_2(r, s)$ as that of \mathcal{P}_4 , we refer to the table of values in that subsection.

$q = 3$: No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

$q = 5$: For all pairs in Table B.0.8, there is 1 non-degenerate triangle in the plane, 1 degenerate

Table B.0.24: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{14}, q = 25$

r	0	1	2	$\alpha + 1$	$\alpha + 2$	$\alpha + 3$	2α	$2\alpha + 1$
s	$\alpha + 4$	$\alpha + 4$	2α	$4\alpha + 3$	4	4	$\alpha + 1$	3
non-degenerate triangles	3	3	4	4	3	3	4	3
r	$2\alpha + 2$	$2\alpha + 3$	$2\alpha + 4$	3α	$3\alpha + 1$	$3\alpha + 2$	$3\alpha + 3$	$3\alpha + 4$
s	4α	2α	$3\alpha + 3$	2	α	3	$\alpha + 1$	$2\alpha + 3$
non-degenerate triangles	2	4	2	4	3	3	4	2
r	$3\alpha + 4$	$3\alpha + 4$	$3\alpha + 4$	4α	$4\alpha + 1$	$4\alpha + 2$	$4\alpha + 3$	$4\alpha + 4$
s	3α	$3\alpha + 3$	4α	$4\alpha + 3$	$2\alpha + 3$	α	2	3α
non-degenerate triangles	2	2	2	4	2	3	4	2

triangle, and 2 triangles in the extended plane.

q = 7 : For all pairs in Table B.0.9, there is 1 non-degenerate triangle in the plane, 1 degenerate triangle, and 4 triangles in the extended plane.

q = 9 : No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

q = 11 : For all pairs in Table B.0.10, there are 2 non-degenerate triangles in the plane, 1 degenerate triangle, and 5 triangles in the extended plane.

q = 13 : For all pairs in Table B.0.11, there are 2 non-degenerate triangles in the plane, 1 degenerate triangle, and 7 triangles in the extended plane.

q = 17 : For all pairs in Table B.0.12, there are 3 non-degenerate triangles in the plane, 1 degenerate triangle, and 8 triangles in the extended plane.

q = 19 : For all pairs in Table B.0.13, there are 3 non-degenerate triangles in the plane, 1 degenerate triangle, and 10 triangles in the extended plane.

q = 25 : For all pairs in Table B.0.14, there are 4 non-degenerate triangles in the plane, 1 degenerate triangle, and 13 triangles in the extended plane.

Poncelet triangles in pencil \mathcal{P}_{16}

q = 3 : No Poncelet triangles for this order.

$q = 5$: No Poncelet triangles for this order.

$q = 7$: For all pairs in Table B.0.25, there are 2 non-degenerate triangles in the plane and 1 triangle in the extended plane.

Table B.0.25: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in \mathcal{P}_{16} , $q = 7$

r	0	1
s	1	0

$q = 9$: For all pairs in Table B.0.26, there are 2 non-degenerate triangles in the plane and 4 triangles in the extended plane.

Table B.0.26: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in \mathcal{P}_{16} , $q = 9$

r	0	1	α	$\alpha + 2$	$2\alpha + 1$	$2\alpha + 2$
s	α	$2\alpha + 1$	0	$2\alpha + 2$	1	$\alpha + 2$

$q = 11$: For all pairs in Table B.0.27, there are 2 non-degenerate triangles in the plane and 6 triangles in the extended plane.

Table B.0.27: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in \mathcal{P}_{16} , $q = 11$

r	5	5	6	6	7	7
s	6	7	5	7	5	6

$q = 13$: For all pairs in Table B.0.28, there are 2 non-degenerate triangles in the plane and 8 triangles in the extended plane.

Table B.0.28: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in \mathcal{P}_{16} , $q = 13$

r	0	1	2	5	6	8	9	12
s	7	7	12	3	11	3	11	2

$q = 17$: Table B.0.29 shows n = number of triangles in the plane that are non-degenerate. The remaining $18 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.29: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in \mathcal{P}_{16} , $q = 17$

r	0	0	1	1	6	6	8	8	10	10	12	12
s	3	15	3	15	4	11	7	14	4	11	7	14
non-degenerate triangles	2	4	4	2	4	2	4	2	2	4	2	4

$q = 19$: Table B.0.30 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $20 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.30: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{16}, q = 19$

r	0	1	2	3	5	6	7
s	12	8	8	17	15	3	18
non-degenerate triangles	4	4	4	4	2	4	4
r	8	12	13	14	15	17	18
s	2	18	2	17	5	3	12
non-degenerate triangles	4	4	4	4	2	4	4

$q = 25$: Table B.0.31 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $26 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

r	2	2	2	2	4	4	4
s	3	4	α	$4\alpha + 1$	2	3	α
non-degenerate triangles	6	6	6	6	6	6	6
r	4	$\alpha + 2$	$\alpha + 3$	2α	$2\alpha + 1$	$2\alpha + 3$	$2\alpha + 4$
s	$4\alpha + 1$	4α	$4\alpha + 2$	$\alpha + 4$	0	1	$\alpha + 1$
non-degenerate triangles	6	4	4	4	4	4	4
r	3α	$3\alpha + 1$	$3\alpha + 2$	$3\alpha + 3$	$4\alpha + 3$	$4\alpha + 4$	
s	1	$4\alpha + 2$	4α	0	$\alpha + 4$	$\alpha + 1$	
non-degenerate triangles	4	4	4	4	4	4	

Table B.0.31: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{16}, q = 25$

Poncelet triangles in pencil \mathcal{P}_{17}

This pencil has a similar form of $H_2(r, s)$ as that of pencil \mathcal{P}_4 where r and s are interchanged. We will still refer to the table of values in that subsection, bearing in mind that we interchange the rows for r and s .

$q = 3$: No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

$q = 5$: For all pairs in Table B.0.8, there are 2 non-degenerate triangles in the plane.

$q = 7$: For all pairs in Table B.0.9, there are 8 triangles in the extended plane.

$q = 9$: No Poncelet triangles for this order since $\text{char } \mathbb{F}_q = 3$.

$q = 11$: For all pairs in Table B.0.10, there are 4 non-degenerate triangles in the plane.

$q = 13$: For all pairs in Table B.0.11, there are 14 triangles in the extended plane.

$q = 17$: For all pairs in Table B.0.12, there are 6 non-degenerate triangles in the plane.

$q = 19$: For all pairs in Table B.0.13, there are 20 triangles in the extended plane.

$q = 25$: For all pairs in Table B.0.14, there are 26 triangles in the extended plane.

Poncelet triangles in pencil \mathcal{P}_{18}

$q = 3$: All Poncelet triangles in this case are either degenerate or in the extended plane. For all pairs in Table B.0.32, there is 1 degenerate triangle and 2 triangles in the extended plane.

Table B.0.32: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_{18}, q = 3$

r	1	2	∞
s	∞	1	2

$q = 5$: Table B.0.33 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $4 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.33: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 5$

r	0	0	2	2	4	4
s	1	3	1	∞	3	∞
non-degenerate triangles	0	1	1	0	0	1

$q = 7$: Table B.0.34 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $6 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.34: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 7$

r	1	3	4	5	6	6	6	6
s	0	6	2	∞	0	2	3	∞
non-degenerate triangles	1	0	1	1	1	1	1	1

$q = 9$: Table B.0.35 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $8 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.35: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 9$

r	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$	∞
s	∞	1	$\alpha + 1$	$\alpha + 2$	$2\alpha + 1$	α	$2\alpha + 2$	2α	2
non-degenerate triangles	2	2	1	1	1	1	1	1	2

$q = 11$: Table B.0.36 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $10 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.36: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 11$

r	0	0	3	3	5	5	7	7	8	8	∞	∞
s	7	9	6	8	2	∞	6	∞	2	7	8	9
non-degenerate triangles	2	1	1	2	1	2	2	1	2	1	1	2

$q = 13$: Table B.0.37 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $12 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.37: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 13$

r	0	2	3	4	5	6	8	9	10	12	12	12	12	∞
s	6	3	10	12	0	3	0	∞	∞	4	6	8	10	8
non-degenerate triangles	1	2	1	3	2	2	2	2	2	1	1	1	1	1

$q = 17$: Table B.0.38 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $16 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

$q = 19$: Table B.0.39 shows n = number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $18 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.38: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 17$

r	0	0	1	1	2	2	5	5	7
s	5	16	13	∞	0	1	2	13	2
non-degenerate triangles	2	3	2	3	2	3	2	3	3
r	7	13	13	14	14	15	15	16	16
s	8	10	16	5	∞	0	10	1	8
non-degenerate triangles	2	3	2	3	2	3	2	2	3

Table B.0.39: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 19$

r	0	2	3	5	6	7	8	9	10	11
s	10	0	18	6	15	13	15	6	18	17
non-degenerate triangles	3	4	3	2	2	4	2	2	3	3
r	12	13	14	15	17	17	17	17	18	∞
s	9	∞	3	9	0	3	11	13	∞	10
non-degenerate triangles	2	3	4	2	4	4	4	4	3	3

$q = 25$: Table B.0.40 shows $n =$ number of triangles in the plane that are non-degenerate. For all these pairs, there is 1 degenerate triangle. The remaining $24 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.40: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{18}, q = 25$

r	0	0	0	0	2	2	2
s	1	3	$\alpha + 1$	$4\alpha + 2$	1	$2\alpha + 1$	$3\alpha + 3$
non-degenerate triangles	4	4	4	4	4	4	4
r	2	4	4	4	4	$\alpha + 1$	$\alpha + 2$
s	∞	3	$\alpha + 2$	$4\alpha + 3$	∞	$\alpha + 2$	$2\alpha + 1$
non-degenerate triangles	4	4	4	4	4	4	4
r	$\alpha + 3$	$\alpha + 4$	$2\alpha + 1$	$2\alpha + 2$	$2\alpha + 4$	$3\alpha + 1$	$3\alpha + 3$
s	2	4α	$\alpha + 1$	4	0	0	$4\alpha + 2$
non-degenerate triangles	5	3	4	5	5	5	4
r	$3\alpha + 4$	4α	$4\alpha + 2$	$4\alpha + 3$	$4\alpha + 4$		
s	4	$\alpha + 4$	$4\alpha + 3$	$3\alpha + 3$	2		
non-degenerate triangles	5	3	4	4	5		

Poncelet triangles in pencil \mathcal{P}_{19}

$q = 3$: For all pairs in Table B.0.41, there is 1 non-degenerate triangle in the plane and 1 triangle in the extended plane.

Table B.0.41: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_{19}, q = 3$

r	0	1
s	1	0

q = 5 : For all pairs in Table B.0.42, there is 1 non-degenerate triangle in the plane and 3 triangles in the extended plane.

Table B.0.42: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ in $\mathcal{P}_{19}, q = 5$

r	2	2	3	3
s	0	3	0	2

q = 7 : Table B.0.43 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $8 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.43: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 7$

r	0	2	3	4	5	6
s	5	4	1	5	4	1
non-degenerate triangles	1	1	2	1	1	2

q = 9 : Table B.0.44 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $10 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.44: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 9$

r	1	2	α	$\alpha + 1$	$\alpha + 2$	2α	$2\alpha + 1$	$2\alpha + 2$
s	α	2α	2	$\alpha + 2$	$2\alpha + 2$	1	$\alpha + 1$	$2\alpha + 1$
non-degenerate triangles	1	1	1	2	2	1	2	2

q = 11 : Table B.0.45 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $12 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.45: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 11$

r	2	2	3	3	7	7	8	8	9	9
s	6	10	6	10	1	9	1	4	4	7
non-degenerate triangles	3	1	1	3	2	2	2	2	2	2

q = 13 : Table B.0.46 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $14 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.46: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 13$

r	0	0	0	0	1	2	3	4	9	10	11	12
s	2	5	8	11	11	5	10	3	10	3	8	2
non-degenerate triangles	3	3	3	3	3	3	2	2	2	2	3	3

$q = 17$: Table B.0.47 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $18 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.47: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 17$

r	1	1	2	2	3	3	7	7
s	4	16	0	13	11	14	6	14
non-degenerate triangles	3	3	3	3	2	4	4	2
r	10	10	14	14	15	15	16	16
s	3	11	3	6	0	4	1	13
non-degenerate triangles	2	4	4	2	3	3	3	3

$q = 19$: Table B.0.48 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $20 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.48: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 19$

r	1	2	2	2	2	3	6	7	7
s	11	1	12	16	17	18	10	8	11
non-degenerate triangles	3	3	3	3	3	4	4	3	3
r	7	7	8	10	12	13	15	16	18
s	12	16	17	14	8	18	10	1	14
non-degenerate triangles	3	3	3	2	3	4	4	3	2

$q = 25$: Table B.0.49 shows $n =$ number of triangles in the plane that are non-degenerate. The remaining $26 - 3n$ points in \mathcal{A} are vertices of a triangle in the extended plane.

Table B.0.49: Valid pairs (r, s) satisfying $H_2(r, s) = 0$ and number of non-degenerate triangles in the plane in $\mathcal{P}_{19}, q = 25$

r	0	0	0	0	1	2	3	4
s	1	4	$\alpha + 3$	$4\alpha + 2$	3α	$2\alpha + 4$	$3\alpha + 1$	2α
non-degenerate triangles	3	3	3	3	5	4	4	5
r	α	$\alpha + 1$	$\alpha + 2$	$\alpha + 3$	$\alpha + 4$	2α	$2\alpha + 1$	$2\alpha + 2$
s	2α	$3\alpha + 1$	$4\alpha + 2$	α	4	4α	$3\alpha + 2$	$3\alpha + 2$
non-degenerate triangles	5	4	3	5	3	5	4	4
r	3α	$3\alpha + 3$	$3\alpha + 4$	4α	$4\alpha + 1$	$4\alpha + 2$	$4\alpha + 3$	$4\alpha + 4$
s	α	$2\alpha + 3$	$2\alpha + 3$	3α	1	4α	$\alpha + 3$	$2\alpha + 4$
non-degenerate triangles	5	4	4	5	3	5	3	4

Bibliography

- [1] Marcel Berger. *Geometry. II*. Universitext. Translated from the French by M. Cole and S. Levy. Springer-Verlag, Berlin, 1987, pp. x+406. ISBN: 3-540-17015-4. DOI: 10.1007/978-3-540-93816-3. URL: <https://doi.org/10.1007/978-3-540-93816-3>.
- [2] Arthur Cayley. “On the Porism of the In-And-Circumscribed Polygon”. In: *Philosophical Transactions of the Royal Society of London* 151 (1861), pp. 225–239. ISSN: 02610523. URL: <http://www.jstor.org/stable/108734> (visited on 04/27/2026).
- [3] Jaydeep Chipalkatti. “On the Poncelet triangle condition over finite fields”. In: *Finite Fields Appl.* 45 (2017), pp. 59–72. ISSN: 1071-5797,1090-2465. DOI: 10.1016/j.ffa.2016.11.014. URL: <https://doi.org/10.1016/j.ffa.2016.11.014>.
- [4] Leonard Eugene Dickson. “Criteria for the irreducibility of functions in a finite field”. In: *Bull. Amer. Math. Soc.* 13.1 (1906), pp. 1–8. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1906-01403-3. URL: <https://doi.org/10.1090/S0002-9904-1906-01403-3>.
- [5] Leonard Eugene Dickson. “On quadratic forms in a general field”. In: *Bull. Amer. Math. Soc.* 14.3 (1907), pp. 108–115. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1907-01568-9. URL: <https://doi.org/10.1090/S0002-9904-1907-01568-9>.
- [6] Vladimir Dragović and Milena Radnović. “Isoperiodic families of Poncelet polygons inscribed in a circle and circumscribed about conics from a confocal pencil”. In: *Geom. Dedicata* 218.3 (2024), Paper No. 81, 23. ISSN: 0046-5755,1572-9168. DOI: 10.1007/s10711-024-00929-9. URL: <https://doi.org/10.1007/s10711-024-00929-9>.
- [7] Vladimir Dragović and Milena Radnović. “Poncelet porism in singular cases”. In: *Regul. Chaotic Dyn.* 30.4 (2025), pp. 598–611. ISSN: 1560-3547,1468-4845. DOI: 10.1134/S1560354725040094. URL: <https://doi.org/10.1134/S1560354725040094>.

- [8] Vladimir Dragović and Milena Radnović. *Poncelet porisms and beyond*. Frontiers in Mathematics. Integrable billiards, hyperelliptic Jacobians and pencils of quadrics. Birkhäuser/Springer Basel AG, Basel, 2011, pp. viii+293. ISBN: 978-3-0348-0014-3. DOI: 10.1007/978-3-0348-0015-0. URL: <https://doi.org/10.1007/978-3-0348-0015-0>.
- [9] David Dummit and Richard Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.
- [10] Leopold Flatto. *Poncelet's theorem*. Chapter 15 by S. Tabachnikov. American Mathematical Society, Providence, RI, 2009, pp. xvi+240. ISBN: 978-0-8218-4375-8. DOI: 10.1090/mbk/056. URL: <https://doi.org/10.1090/mbk/056>.
- [11] William Fulton. *Algebraic curves. An introduction to algebraic geometry*. Mathematics Lecture Note Series. Notes written with the collaboration of Richard Weiss. W. A. Benjamin, Inc., New York-Amsterdam, 1969, pp. xiii+226.
- [12] Phillip Griffiths and Joe Harris. “A Poncelet theorem in space”. In: *Comment. Math. Helv.* 52.2 (1977), pp. 145–160. ISSN: 0010-2571,1420-8946. DOI: 10.1007/BF02567361. URL: <https://doi.org/10.1007/BF02567361>.
- [13] Phillip Griffiths and Joseph Harris. “On Cayley’s explicit solution to Poncelet’s porism”. In: *Enseign. Math. (2)* 24.1-2 (1978), pp. 31–40. ISSN: 0013-8584.
- [14] James William Peter Hirschfeld. *Projective geometries over finite fields*. Second. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998, pp. xiv+555. ISBN: 0-19-850295-8.
- [15] Matt Hostetter. *Galois: A performant NumPy extension for Galois fields*. Nov. 2020. URL: <https://github.com/mhostetter/galois>.
- [16] Carl Jacobi. “Ueber die anwendung der elliptischen transcendenten auf ein bekanntes problem der elementargeometrie”. In: *Journal für die reine und angewandte Mathematik* (1828).

- [17] Shin-Yao Jow and Chia-Tz Liang. “Poncelet’s theorem for conics in any position and any characteristic”. In: *Comm. Algebra* 51.8 (2023), pp. 3510–3520. ISSN: 0092-7872,1532-4125. DOI: 10.1080/00927872.2023.2186123. URL: <https://doi.org/10.1080/00927872.2023.2186123>.
- [18] Keith Kendig. *A guide to plane algebraic curves*. Vol. 46. The Dolciani Mathematical Expositions. MAA Guides, 7. Mathematical Association of America, Washington, DC, 2011, pp. xvi+193. ISBN: 978-0-88385-353-5. DOI: 10.5948/UP09781614442035.009. URL: <https://doi.org/10.5948/UP09781614442035.009>.
- [19] Katharina Kusejko. “Poncelet’s theorem in finite projective planes and beyond”. PhD thesis. ETH Zurich, 2016. URL: <https://doi.org/10.3929/ethz-a-010682687>.
- [20] Jean Victor Poncelet. “Traité des propriétés projectives des figures”. In: *Metz, Paris* (1822).
- [21] Jürgen Richter-Gebert. *Perspectives on projective geometry*. A guided tour through real and complex geometry. Springer, Heidelberg, 2011, pp. xxii+571. ISBN: 978-3-642-17285-4. DOI: 10.1007/978-3-642-17286-1. URL: <https://doi.org/10.1007/978-3-642-17286-1>.
- [22] Joseph Silverman and John Tate. *Rational points on elliptic curves*. Second. Undergraduate Texts in Mathematics. Springer, Cham, 2015, pp. xxii+332. ISBN: 978-3-319-18587-3. DOI: 10.1007/978-3-319-18588-0. URL: <https://doi.org/10.1007/978-3-319-18588-0>.
- [23] Tianhao Wang. *Counting pairs of conics over finite fields that satisfy the Poncelet n -gon condition*. 2025. arXiv: 2309.16978 [math.RA]. URL: <https://arxiv.org/abs/2309.16978>.