**University of Zurich**
**Institute of Mathematics**

Master Thesis

# Counting points on Curves over Finite Fields, a Comparison to the Hasse-Weil Bound

*Author:*
Diana Patrizia Teider

*Supervisor:*
Professor Dr. Joachim Rosenthal
*Co-supervisor:*
Abhinaba Mazumder

August 2024

Diana Teider
dianapatrizia.teider@uzh.ch

## Abstract

This thesis investigates the problem of counting points on algebraic curves over finite fields, specifically comparing these counts to the Hasse-Weil bound.

The study begins by laying the foundation in algebraic function fields and algebraic curves over finite fields. It explores different methods for counting points, including the Hasse-Weil bound and the Serre bound. It also looks at the computational aspect, where random smooth curves are generated and analyzed for their number of rational points. The results show a pattern in the distribution of these points, providing insights into the effectiveness and limitations of the Hasse-Weil bound, especially in the context of singular curves. The thesis concludes by discussing the computational findings.

## Acknowledgements

I would like to express my sincerest gratitude to my supervisors, Professor Dr. Joachim Rosenthal and Abhinaba Mazumder, for their guidance, support, and valuable insights. Their guidance and support were instrumental in enabling me to complete this thesis.

I would also like to thank Jenny Pletscher, Delia Schüpbach, and Sibylle Schalbetter for their support during challenging times.

I would also like to express my gratitude to my family for their understanding and support throughout this process.

Furthermore, I would like to acknowledge Niklas Gassner for allowing me to use his LaTeX header and for his assistance with formatting.

Diana Teider
dianapatrizia.teider@uzh.ch

## Contents

**1 Introduction, Conventions and Notations** . . . . . **4**
1.1 Introduction . . . . . 4
1.2 Conventions and Notations . . . . . 5
**2 Algebraic curves over Finite Fields and Foundations of the Theory of Algebraic Function Fields** . . . . . **6**
2.1 Function Fields and the Riemann-Roch Theorem . . . . . 7
**3 Point Counting over Finite Fields** . . . . . **11**
3.1 The Hasse-Weil Bound . . . . . 11
3.2 Serre bound . . . . . 13
3.3 Examples for known values of $N_q(3)$ . . . . . 15
3.4 Connection with codes . . . . . 16
3.4.1 Linear Codes . . . . . 16
3.4.2 Codes and algebraic curves . . . . . 16
3.5 Elliptic curves and their Number of Points . . . . . 18
**4 Distribution of curves over finite fields with a given number of points** **23**
**5 Computational results** . . . . . **24**
5.1 The Code . . . . . 24
5.2 Methods to randomly generate curves . . . . . 24
5.3 The Affine Plane Curves the Code Generates . . . . . 25
5.4 The Influence on the Number of points by increasing the degree . . . . . 26
5.5 The reason for results of curves of no higher degree than 8 . . . . . 27
5.6 The Influence on the Number of points by increasing the Field Size . . . 28
**6 A comparison of the number of points of singular curves to the Hasse-Weil bound** . . . . . **32**
6.1 Singular Affine Plane Curves the Code generates . . . . . 32
6.2 The Hasse-Weil bound for singular curves . . . . . 32
6.3 Influence of changing the field size on the proportion of curves not satisfying the Hasse-Weil bound - Computational results . . . . . 32
6.3.1 Examples of singular curves having less rational points than expected by the Hasse-Weil lower bound . . . . . 34
6.3.2 The rationale behind the observation that the majority of curves exhibit a greater number of points than anticipated by Hasse-Weil . . . . . 35
6.4 Influence of changing the degree on the proportion of curves not satisfying the Hasse-Weil bound - Computational results . . . . . 37
6.5 Conclusion . . . . . 39
**7 Appendix** . . . . . **40**
7.1 The Sagemath codes . . . . . 40
**References** . . . . . **44**

Diana Teider
dianapatrizia.teider@uzh.ch

# 1. Introduction, Conventions and Notations.

## 1.1. Introduction.

The study of algebraic curves over finite fields and their function fields has long been a source of great fascination for geometers and number theorists, dating back to the seminal work of Hasse and Weil in the 1930s and 1940s. This area of research, where number theory and algebraic geometry meet, has given rise to numerous significant and fruitful ideas, including the new subject of arithmetic algebraic geometry. (p.ix,[1]).

In a series of three papers published between 1977 and 1982, Goppa made some intriguing discoveries about the use of algebraic curves over finite fields, particularly those with a high number of rational points, in the field of coding theory. This led to a renewed interest in the area and attracted new groups of researchers, including coding theorists (p.ix, [1]).

A significant amount of research has been conducted on algebraic curves over finite fields and their function fields, resulting in notable theoretical advancements. These include new techniques for constructing algebraic curves over finite fields with a high density of rational points, which can be viewed as global function fields with a large number of rational places. Additionally, the lower bounds for the quantity in asymptotic theory for the number of rational points on algebraic curves over a finite field of order q have been improved (p. ix, [1]).

This thesis looks at algebraic curves over finite fields and their number of rational points. As mentioned above, there are some bounds for the exact number of points, such as the theoretical Hasse-Weil bound. In this thesis, we compare the number of points on these curves with this theoretical Hasse-Weil bound.

Chapter 1 introduces the basic conventions and notations used throughout the thesis.

Chapter 2 provides a background on algebraic curves and the foundational theory of algebraic function fields.

Chapter 3 explores various methods of point counting over finite fields, with a special emphasis on the Hasse-Weil bound, which is a cornerstone in this area of study. We also look at the Serre bound and discuss the relationship between algebraic curves and coding theory. This shows how the theoretical work can be used in practice.

Chapter 4 looks at how many curves there are over finite fields with a given number of points. This offers a statistical perspective on the theoretical bounds discussed earlier.

In Chapter 5, we describe how to generate and analyze random smooth curves over finite fields. This includes a detailed explanation of the code and algorithms used. The results

Diana Teider
dianapatrizia.teider@uzh.ch

of these computations, particularly the influence of varying degrees and field sizes on the number of rational points, are discussed in detail.

Finally, Chapter 6 compares the computational results with the theoretical Hasse-Weil bound, especially for singular curves, and presents a detailed discussion on the deviations observed.

### 1.2. Conventions and Notations.

For the remainder of this thesis, $K$ is a finite field $F_q$, where $q$ is a power of a prime $p$. 0 is an element of $\mathbb{N}$. Given a set $A$ and a subset $B$, we write $A \subsetneq B$ if $A$ is a proper subset, and $A \subset B$ if $A \subsetneq B$ or $A = B$.

Diana Teider
dianapatrizia.teider@uzh.ch

# 2. Algebraic curves over Finite Fields and Foundations of the Theory of Algebraic Function Fields.

We will start by giving a rough introduction to abstract algebra, as this provides the foundations for all subsequent content.

DEFINITION 2.1. (p.31, [2]) A *field* $F$ is a set of elements with two operations $+$ and $\cdot$ satisfying the following properties.

(1) F is closed under $+$ and $\cdot$
For all $a$, $b$ and $c$ in $F$ the following laws hold.
(2) $a + b = b + a$, $a \cdot b = b \cdot a$.
(3) $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(4) $a \cot(b + c) = a \cot b + a \cdot c$.

Furthermore, identity elements 0 and 1 must exist in $F$ satisfying

(1) $a + 0 = a$ for all $a$ in $F$.
(2) $a \cdot 1 = a$ for all $a$ in $F$.
(3) For any $a$ in $F$, there exists an additive inverse element $(-a)$ in $F$ such that $a + (-a) = 0$.
(4) For any $a \neq 0$ in $F$, there exists a multiplicative inverse element $a^{-1}$ in $F$ such that $a \cdot a^{-1} = 1$.

LEMMA 2.2. *(p.32, [2]) Any field has the following properties.*

*(1)* $a0 = 0$ *for all* $a$ *in* $F$.
*(2)* $ab = 0 \Rightarrow a = 0$ *or* $b = 0$. *(The product of two non-zero elements of a field is also non-zero.)*

*Proof.* (The proof is also from [2])

(1) We have $a0 = a(0 + 0) = a0 + a0$. Adding the additive inverse on both sides gives
$$0 = a0 + (-a0) = a0 + a0 + (-a0) = a0 + 0 = a0.$$
(2) Suppose $ab = 0$. If $a \neq 0$, then $a$ has a multiplicative inverse and so $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$. Hence $ab = 0 \Rightarrow a = 0$ or $b = 0$.

□

DEFINITION 2.3. A *finite field* is a field which has a finite number of elements, this number being called the *order* of the field.

COROLLARY 2.4. *(p. 16, Corollary 1.45, [3]) A finite field has prime characteristic.*

Diana Teider
dianapatrizia.teider@uzh.ch

THEOREM 2.5. *(p. 45, Theorem 2.2, [3]) Let $F$ be a finite field. Then $F$ has $p^n$ elements, where the prime $p$ is the characteristic of $F$ and $n$ is the degree of $F$ over its prime subfield.*

THEOREM 2.6. *(p.33, Theorem 3.2, [2]) There exists a field of order $q$ if and only if $q$ is a prime power ($q = p^h$, where $p$ is prime and $h$ is a positive integer). Furthermore, if $q$ is a prime tower, then there is, up to relabelling, only one field of that order.*

*Proof.* The proof may be found in advanced texts in coding theory or in books on abstract algebra. □

DEFINITION 2.7. A field of order $q$ is often called a *Galois field* of order $q$ and is denoted $GF(q)$.

### 2.1. Function Fields and the Riemann-Roch Theorem.

Since the Hasse-Weil bound is defined using global function fields, we give an introduction to this topic.

DEFINITION 2.8. (p.1, [4]) An *algebraic function field* $F/K$ of one variable over $K$ is an extension field $F \supseteq K$ such that $F$ is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over $K$.

REMARK 2.9. (p. 1, [4]) The elements of $F$ which are *transcendental* over $K$ can be characterized as follows: $z \in F$ is transcendental over $K$ if and only if the extension $F/K(z)$ is of finite degree.

DEFINITION 2.10. (p.1, [1]) A *place* $P$ of $F$ is the maximal ideal of some valuation ring of $F$. We denote by $O_P$ the valuation ring corresponding to $P$. $M_P$ stands for the ideal $P$.

DEFINITION 2.11. (p.1, [1]) A *normalized discrete valuation* of an algebraic function field $F$ over $K$ is a surjective map $\nu : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ which satisfies:

(1) $\nu(x) = \infty$ if and only if $x = 0$;
(2) $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in F$;
(3) $\nu(x + y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in F$;
(4) $\nu(a) = 0$ for any $a \in K^*$.

As a consequence of these axioms we get the following useful strengthening of (3):

(3') $\nu(x + y) = \min(\nu(x), \nu(y))$ for all $x, y \in F$ with $\nu(x) \neq \nu(y)$.

There is a bijective correspondence between the places of $F$ and the normalized discrete valuations of $F$ (p. 2, [1]).

Diana Teider
dianapatrizia.teider@uzh.ch

DEFINITION 2.12. (p.2, [1]) For a place $P$ of $F$, we write $\nu_P$ for the normalized discrete valuation of $F$ corresponding to $P$. We denote by $\mathbb{P}_F$ the set of places of $F$. For a place $P$ of $F/K$, its valuation ring

$$O_P = \{x \in F : \nu_P(x) \geq 0\}$$

is a local ring. Its maximal ideal is

$$M_P = \{x \in O_P : \nu_P(x) > 0\}.$$

DEFINITION 2.13. (p.3, [1]) A *divisor* $D$ of an algebraic function field $F$ is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} m_P P$$

with integer coefficients $m_P$ and $m_P \neq 0$ for at most finitely many $P \in \mathbb{P}_F$. We write $\nu_P(D)$ for the coefficient $m_P$ of $P$. Then

$$D = \sum_{P \in \mathbb{P}_F} \nu_P(D) P.$$

DEFINITION 2.14. (p.3, [1]) The *support* $\mathrm{supp}(D)$ of $D$ is the set

$$\mathrm{supp}(D) = \{P \in \mathbb{P}_F : \nu_P(D) \neq 0\}.$$

DEFINITION 2.15. (p.3, [1]) The *degree* $\deg(D)$ of $D$ is defined by

$$\deg(D) = \sum_{P \in \mathrm{supp}(D)} \nu_P(D) \deg(P).$$

DEFINITION 2.16. (p.3, [1]) A divisor $D$ is called *positive* if $\nu_P(D) \geq 0$ for all $P \in \mathbb{P}_F$. For two divisors $D_1$ and $D_2$ of $F$ we write $D_1 \leq D_2$ if $\nu_P(D_1) \leq \nu_P(D_2)$ for all $P \in \mathbb{P}_F$.

DEFINITION 2.17. (p.3, [1]) Let $P$ be a place of $F$ and $x$ a nonzero element of $F$. The place $P$ is called a *zero* of $x$ if $\nu_P(x) > 0$ and a *pole* of $x$ if $\nu_P(x) < 0$. It is clear that a constant element in $K$ has neither poles nor zeros. However, for $x \in F \backslash K$, $x$ has at least one zero place and one pole place.

Diana Teider
dianapatrizia.teider@uzh.ch

DEFINITION 2.18. (p.3, [1]) Let $x \in F^*$ and denote by $Z(x)$, respectively $N(x)$, the set of zero places, respectively pole places, of $x$. We define the *zero divisor* of $x \in F^*$ by

$$(x)_0 = \sum_{P \in Z(x)} \nu_P(x) P$$

and the *pole divisor* of $x$ by

$$(x)_\infty = \sum_{P \in N(x)} (-\nu_P(x)) P.$$

Then the *principal divisor* of $x$ is given by

$$\operatorname{div}(x) = (x)_0 - (x)_\infty.$$

The degree of $\operatorname{div}(x)$ is equal to 0, i.e.,

$$\deg((x)_0) = \sum_{P \in Z(x)} \nu_P(x) \deg(P) = \sum_{P \in N(x)} (-\nu_P(x)) \deg(P) = \deg((x)_\infty).$$

DEFINITION 2.19. (p.4, [1]) For a divisor $D$ of $F$ we form the *Riemann-Roch space*

$$\mathcal{L}(D) = \{x \in F^* : \operatorname{div}(x) + D \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(D)$ is a finite-dimensional vector space over $K$, and we denote its dimension by $\ell(D)$. We have two facts:

(1) $\ell(0) = 1$;
(2) $\ell(D) = 0$ if $\deg(D) > 0$.

The dimension $\ell(D)$ is the subject of the Riemann-Roch theorem:

THEOREM 2.20. *(p.4, Theorem 1.1.2, [1])(Riemann-Roch Theorem) Let $F$ be an algebraic function field of genus $g$. Then for any divisor $D$ of $F$ we have*

$$\ell(D) \geq \deg(D) + 1 - g,$$

*and equality holds whenever* $\deg(D) \geq 2g - 1$.

*Proof.* The proof of this theorem can be found in [5], Chapter 6, part 3, beginning at p.185. □

Diana Teider
dianapatrizia.teider@uzh.ch

DEFINITION 2.21. (p.4, [1]) Using the Riemann-Roch theorem, we can now define the *genus* of $F$ as the integer

$$g := \max_D(\deg(D) - \ell(D) + 1),$$

where the maximum is extended over all divisors $D$ of $F$.

Diana Teider
dianapatrizia.teider@uzh.ch

# 3. Point Counting over Finite Fields.

The Hasse–Weil bound has a wide range of applications in the field of arithmetic in finite fields [6]. As the Chapters 5 and 6 will demonstrate a comparison of the computational results with this bound, it is necessary to provide an overview at this point. In the following chapter, we will additionally emphasize why point counting is of great importance and see some methods to find the number of points on a curve as well as the Serre bound, a connection with codes and an overview on the number of points of elliptic curves.

## 3.1. The Hasse-Weil Bound.

THEOREM 3.1 (p.28, Theorem 1.6.6,[1]). *Let $F/\mathbb{F}_q$ be a global function field of genus $g$. Then:*

*(i) $Z(F,t)$ is a rational function of the form*

$$Z(F,t) = \frac{L(F,t)}{(1-t)(1-qt)}, \tag{1}$$

*where $L(F,t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$ with integral coefficients and $L(F,0) = 1$. Moreover, $L(F,1)$ is equal to the divisor class number $h(F)$ of $F$.*

*(ii) Factor $L(F,t)$ into the form*

$$L(F,t) = \prod_{i=1}^{2g}(1-\omega_i t) \in \mathbb{C}[t], \tag{2}$$

*then $|\omega_i| = \sqrt{q}$ for all $1 \leq i \leq 2g$.*

*Proof.* Bombieri's elementary proof is presented in [4], Chapter 5. □

THEOREM 3.2 (p.30, Corollary 1.6.9,[1]). *Let $1/\omega_1, ..., 1/\omega_{2g}$ be the roots of the $L$-polynomial $L(t) = \sum_{i=0}^{2g} a_i t^i$ of $F/\mathbb{F}_q$. Then the number $N$ of rational places of $F/\mathbb{F}_q$ is equal to*

$$N = N_1 = q + 1 - \sum_{i=1}^{2g} \omega_i = q + 1 + a_1. \tag{3}$$

*More generally, the number $N_n$ of $\mathbb{F}_{q^n}$-rational places of $F/\mathbb{F}_q$ is equal to*

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n \tag{4}$$

*for all $n \geq 1$, and $g = \frac{(d-1)(d-2)}{2} - s$, where $s$ denotes the number of singularities.*

The proof is also taken from (p.30, [1]).

Diana Teider
dianapatrizia.teider@uzh.ch

*Proof.* By the defintion of $Z_n(t)$ we obtain

$$N_n = \frac{d(log(Z_n(t))}{dt}|_{t=0}. \tag{5}$$

On the other hand, by Theorem 3.1(i) we get

$$\frac{d(log(Z(t))}{dt}|_{t=0} = (\frac{L'(t)}{L(t)} + \frac{1}{1-t} + \frac{q}{1-qt})|_{t=0} = a_1 + 1 + q. \tag{6}$$

Combining (5) with (6) gives

$$N_1 = q + 1 + a_1 = q + 1 - \sum_{i=1}^{2g} \omega_i.$$

In addition, $\omega_1^n$, ..., $\omega_{2g}^n$ are the reciprocal roots of the nth $L$-polynomial in $L_n(t)$. Hence

$$N_n = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n.$$

□

THEOREM 3.3 (p. 198, Theorem 5.2.3,[4]). *The Number of points $N$ on a curve over $\mathbb{F}_q$ with genus $g$ is at most*

$$N \leq q + 1 + 2g\sqrt{q}.$$

*From (p.30, [1]), we even know that*

$$|N - (q+1)| \leq 2g\sqrt{q}, \tag{7}$$

*which also gives us a lower bound.*

*Proof.* From Theorem 3.1(ii) and Theorem 3.2 we obtain

$$|N - (q+1)| = |\sum_{i=1}^{2g} \omega_i| \leq \sum_{i=1}^{2g} |\omega_i| = 2g\sqrt{q}.$$

□

The Hasse Weil bound also makes sense intuitively. $N$ are the number of points on the curve, $q+1$ is the number that is expected and $2g\sqrt{q}$ the deviation.

Diana Teider
dianapatrizia.teider@uzh.ch

### 3.2. Serre bound.

According to [1], the Hasse-Weil bound is sharp for small genera with respect to q, but not a good bound for relatively large genera with respect to q. We will see later, whether the statistics show the same. Either way, there are some improvements of the Hasse-Weil bound, one of them is the Serre bound.

PROPOSITION 3.4. *(p. 31, Proposition 1.6.12, [1])(Serre bound) Let $F/\mathbb{F}_q$ be a global function field of genus $g$. Then the number $N(F)$ of rational points of $F/\mathbb{F}_q$ satisfies*

$$|N(F) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor.$$

The following is a sufficient condition for the existence of at least one place of $F$ of given degree $d \geq 2$ (p. 31, [1]).

LEMMA 3.5. *(p.31, Lemma 1.6.13, [1]) Let $F/\mathbb{F}_q$ be a global function field of genus $g$. Suppose that for some integer $d \geq 2$ we have*

$$d^d - 2gq^{d/2} > \sum_{r|d, r<d} (q^r + 2gq^{r/2}).$$

*Then there exists at least one place of $F$ of degree $d$.*

To prove this lemma, we need to emphasize two relations first (both can be found in [1], p.26). Let $F/\mathbb{F}_q$ a global function field. For each integer $n \geq 1$, consider the constant field extension $F_n = F \cdot \mathbb{F}_{q^n}$. Denote by $N_n$ the number of rational places of $F_n/\mathbb{F}_{q^n}$, which is finite. For each integer $d \geq 1$, denote the number of places of $F$ of degree $d$ by $B_d$. We have the relations:

COROLLARY 3.6. *(p. 26, [1])*
*(1)* $N_n = \sum_{d|n} dB_d$;
*(2)* $B_n = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) N_d$,
*where $\mu$ is the Möbius function.*

Now we can prove Lemma 3.5:

*Proof.* (p. 31, [1]) Let $\omega_1, ..., \omega_{2g}$ be all reciprocal roots of the $L$-polynomial of $F$. For $r \geq 1$ let $B_r$ be the number of places of $F$ of degree $r$ and $s_r = \sum_{i=1}^{2g} \omega_i^r$. Then by Corollary 3.6(2) and Theorem 3.2 we obtain

$$B_d = \frac{1}{d} \sum_{r|d} \mu(\frac{d}{r})(q^r - s_r) \qquad \text{for } d \geq 2.$$

Diana Teider
dianapatrizia.teider@uzh.ch

Hence using Theorem 3.1(ii), we get

$$B_d \geq \frac{1}{d}\left(q^d - 2gq^{d/2} - \sum_{r|d, r<d}(q^r + 2gq^{r/2})\right) > 0.$$

□

Definition 3.7. (p. 32, Definition 1.6.14, [1]) For a fixed prime number $q$ and an integer $g \geq 0$, let $N_q(g)$ denote the *maximum number of rational places* that a global function field $F/\mathbb{F}_q$ of genus $g$ can have (note that $N_q(g)$ is also the maximum number of $\mathbb{F}_q$-rational points that a smooth, projective, absolutely irreducible algebraic curve over $\mathbb{F}_q$ of genus $g$ can have).

Corollary 3.8. *(p. 32, [1]) According to the Serre bound (Proposition 3.4), $N_q(g)$ satisfies*

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

Diana Teider
dianapatrizia.teider@uzh.ch

### 3.3. Examples for known values of $N_q(3)$.

In [7], Jean-Pierre Serre with contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler concentrate on finding sharp explicit upper bounds for the number of points and constructing curves with many points for a given $g$ and $q$.
They initially focus their attention on cases where g is relatively small, and then proceed to investigate cases where g is large. Having a closer look on the explicit case $g = 3$, Serre et al. give a list of the known values for $N_q(3)$ for small q, together with a curve reaching that bound (p. 75, [7]):

| **q** | **N** | **a curve reaching that bound N** |
|---|---|---|
| 2 | 7 | twisted Klein curve $x^3y + x^2y^2 + xz^3 + x^2z^2 + y^3z + yz^3 = 0$ |
| 3 | 10 | $x^4 - x^2z^2 - y^3z + yz^3 = 0$ |
| 4 | 14 | Klein curve (Section 4.1.2, [7]) |
| 5 | 16 | $x^4 + y^4 + 3z^4 = 0$ |
| 7 | 20 | cubic cover $t^3 = y - x^2 + xy$ of the elliptic curve $y^2 - y = x^3 - x^2$ |
| 8 | 24 | Klein curve (Section 4.1.2, [7]) |
| 9 | 28 | Klein curve = Fermat curve = Hermitian curve $x^4 + y^4 + z^4 = 0$ |
| 11 | 28 | $x^4 + y^4 + z^4 + 2(3x^2y^2 + 4x^2z^2 + 4y^2z^2) = 0$ |
| 13 | 32 | Fermat curve $x^4 + y^4 + z^4 = 0$ |
| 17 | 40 | $x^4 + y^4 + z^4 + 4y^2z^2 = 0$ |
| 19 | 44 | $x^4 + y^4 + z^4 + 6(x^2y^2 + x^2z^2 + y^2z^2) = 0$ |
| 23 | 48 | $x^4 + y^4 + z^4 - 5(x^2y^2 + x^2z^2 + y^2z^2) = 0$ |
| 25 | 56 | Klein curve ($S_4$-model) (Section 4.1.2, [7]) |
| 29 | 60 | $x^4 + y^4 + z^4 - 3(x^2y^2 + x^2z^2 + y^2z^2) = 0$ |

TABLE 1. Known values for $N_q(3)$

Diana Teider
dianapatrizia.teider@uzh.ch

## 3.4. Connection with codes.

### 3.4.1. Linear Codes.

The following definitions and remarks about coding theory are from [8].

Definition 3.9. A *linear code* over $\mathbb{F}_q$ is a vector subspace $V$ of $\mathbb{F}_q^n$.

Remark 3.10. A linear code can also be defined as an inclusion of finite dimensional vector spaces $V \subset W$, together with a basis of $W$.
An element $(x_1, ..., x_n) \in \mathbb{F}_q^n$ is called *word*, the elements of $\mathbb{F}_q$ being thought of as letters. If q = 2 (binary code), a word is a sequence of 0s and 1s. Th elements of $V$ are called *codewords*.

Definition 3.11. The *Hamming distance* of two codewords is the number of coordinates where they differ.

Example 3.12. Let $x = (0, 0, 1, 0, 0, 1, 1, 1, 1) \in V$ and $x' = (0, 1, 1, 0, 0, 1, 1, 1, 0)$. Then the Hamming distance between $x$ and $x'$ is 2.

For instance, suppose $x$ is sent and $x'$ is wrongly received due to a noisy channel. Then we have 2 errors at the second and the last positions. The goal is to correct such errors and this is done via an *error-correcting* code.

Remark 3.13. The *parameters* of $V$ of a linear code $V \subset \mathbb{F}_q^n$ are

(1) $n$ which is the length of a word.
(2) $k$ which is the dimension of $V$.
(3) $d$ which is the minimum number of non-zero coordinates in a non-zero element of V.

To have an efficient error-correcting code, $d$ and $k$ need to be large and $n$ needs to be as small as possible [7].

### 3.4.2. Codes and algebraic curves.

Let $V \subset \mathbb{F}_q^n$ be a linear code of dimension $k > 0$. Assume that for every $i \in \{1, ..., \}$, there exists $x = (x_1, ..., x_n) \in V$ with $x_i \neq 0$ (if not, replace $n$ by $n - 1$).
The projection map $\mathbb{F}_q^n \to \mathbb{F}_q$ given by the $i$th component is a linear form, whose restriction to $V$ is non-zero. Therefore it defines an element $P_i$ in the projective space $\mathbb{P}(V^*)$, which is associated with the dual $V^*$ of $V$. Hence we obtain elements $P_1, ..., P_n \in \mathbb{P}(V^*)$, which generate this projective space (they are not contained in the hyperplane). In this context, the parameters of $V$ are as follows:

Diana Teider
dianapatrizia.teider@uzh.ch

(1) $k-1 = \dim\mathbb{P}(V^*)$
(2) $n$ = number of the points $P_i$
(3) $d = n-m$, where m is the maximum number of $P_i$'s, lying on the same hyperplane.

As a consequence, it would be beneficial to have a large set of points in a projective space with not too many in the same hyperplane to ensure an efficient code. [7].
Also Niederreiter and Xing in [1] mention that results on algebraic curves over finite fields and their function fields had a significant impact on coding theory, since they lead to sequences of algebraic-geometry codes of increasing length that beat the asymptotic Gilbert-Varshamov bound (classical benchmark for families of good linear codes) on p.ix. This underlines why one started to focus on the number of points on algebraic curves over finite fields and why this quantity is of great importance.

Diana Teider
dianapatrizia.teider@uzh.ch

### 3.5. Elliptic curves and their Number of Points.

Since some of the computational results are based on smooth curves of degree 3, we give a brief introduction to elliptic curves and their number of points.

Definition 3.14. (p. 9, [9]) An elliptic curve $E$ is the graph of an equation of the form

$$y^2 = x^3 + Ax + B,$$

where $A$ and $B$ are constants. This is referred to the *reduced Weierstrass equation* of an elliptic curve.

In this thesis, $A, B, x$ and $y$ are taken to be elements of a finite field.

Theorem 3.15. *(p. 15, Theorem 2.1, [9]) The points on $E$ form an additive abelian group with $\infty$ as the identity element.*

Definition 3.16. (p. 46, [9]) The *j-invariant* of an elliptic curve $E$ is defined by

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Note that the denominator is the negative of the discriminant of the cubic, hence nonzero by assumption.

Theorem 3.17. *(p. 46, [9], Theorem 2.19) Let $y_1^2 = x_1^3 + A_1x_1 + B_1$ and $y_2^2 = x_2^3 + A_2x_2 + B_2$ be two elliptic curves with j-invariants $j_1$ and $j_2$, respectively. If $j_1 = j_2$, then there exists $\mu \neq 0$ in $\overline{K}$ (= algebraic closure of K) such that*

$$A_2 = \mu^4 A_1, \ B_2 = \mu^6 B_1.$$

*The transformation*

$$x_2 = \mu^2 x_1, \ y_2 = \mu^3 y_1$$

*takes one equation to the other.*

Diana Teider
dianapatrizia.teider@uzh.ch

*Proof.* (p. 46, [9]) First, assume that $A_1 \neq 0$. Since this is equivalent to $j_1 \neq 0$, we also have $A_2 \neq 0$. Choose $\mu$ such that $A_2 = \mu^4 A_1$. Then

$$\frac{4A_2^3}{4A_2^3 + 27B_2^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4\mu^{-12}A_2^3}{4\mu^{-12}A_2^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27\mu^{12}B_1^2},$$

which implies that

$$B_2^2 = (\mu^6 B_1)^2.$$

Therefore, $B_2 = \pm\mu^6 B_1$. If $B_2 = \mu^6 B_1$, we are done. If $B_2 = -\mu^6 B_1$, then change $\mu$ to $i\mu$ (where $i^2 = -1$). This preserves the relation $A_2 = \mu^4 A_1$ and also yields $B_2 = \mu^6 B_1$.

If $A_1 = 0$, then $A_2 = 0$. Since $4A_i^3 + 27B_i^2 \neq 0$, we have $B_1, B_2 \neq 0$. Choose $\mu$ such that $B_2 = \mu^6 B_1$. □

Note that the j-invariant is a means of determining whether two curves are isomorphic over an algebraically closed field.

We now proceed to present the relevant information on counting points. For elliptic curves $E$ of the form $y^2 = x^3 - kx$, there even is an explicit formula for the number of points in $E(\mathbb{F}_p)$.

THEOREM 3.18. *(p. 115, Theorem 4.23, [9]) Let $p$ be an odd prime and let $k \not\equiv 0 \pmod p$. Let $N_p = \#E(\mathbb{F}_p)$, where $E$ is an elliptic curve*

$$y^2 = x^3 - kx.$$

*(1) If $p \equiv 3 \pmod 4$, then $N_p = p + 1$.*
*(2) If $p \equiv 1 \pmod 4$, write $p = a^2 + b^2$, where $a, b$ are integers with $b$ even and $a + b \equiv 1 \pmod 4$. Then*

$$N_p = \begin{cases} p + 1 - 2a \text{ if } k \text{ is a fourth power mod } p \\ p + 1 + 2a \text{ if } k \text{ is a square mod } p \text{ but not a fourth power mod } p \\ p + 1 \pm 2b \text{ if } k \text{ is not a square mod } p. \end{cases}$$

The proof can be found in [9], starting at p. 115.

Since elliptic curves have genus = 1, the Hasse bound can be stated as follows:

Diana Teider
dianapatrizia.teider@uzh.ch

THEOREM 3.19. *(p. 97, Theorem 4,2, [9]) Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

In addition, we present another result pertaining to the explicit number of points on an elliptic curve.

THEOREM 3.20. *(p. 98, Theorem 4.3, [9]) Let $q = p^n$ be a power of a prime $p$ and let $N = q + 1 - a$. There is an elliptic curve $E$ defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and $a$ satisfies one of the following:*

*(1)* $\gcd(a, p) = 1$
*(2) $n$ is even and $a = \pm 2\sqrt{q}$*
*(3) $n$ is even, $p \not\equiv 1 \pmod 3$, and $a = \pm\sqrt{q}$*
*(4) $n$ is odd, $p = 2$ or $3$, and $a = \pm p^{(n+1)/2}$*
*(5) $n$ is even, $p \not\equiv 1 \pmod 4$, and $a = 0$*
*(6) $n$ is odd and $a = 0$.*

The proof can be found in [10], p. 536.

In the following, we show how one can determine the order of $E(\mathbb{F}_{q^n})$ for some $n$, when we have an elliptic curve $E$ defined over a small finite field $\mathbb{F}_q$.

THEOREM 3.21. *(p. 103, Theorem 4.12, [9]) Let $\#E(\mathbb{F}_q) = q + 1 - a$.*
*Write $X^2 - aX + q = (X - \alpha)(X - \beta)$. Then*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

*for all $n \geq 1$.*

The proof for this theorem, as well as the proof for the following lemma can be found on p. 103, [9].

LEMMA 3.22. *(p. 103, Lemma 4.13, [9]) Let $s_n = \alpha^n + \beta^n$. Then $s_0 = 2$, $s_1 = a$, and $s_{n+1} = as_n - qs_{n-1}$ for all $n \geq 1$.*

EXAMPLE 3.23. (p. 104, Example 4.4, [9]) One can check that the elliptic curve $E$ given by $y^2 + xy = x^3 + 1$ over $\mathbb{F}_2$ has 4 points. Therefore, $a = 2 + 1 - 4 = -1$ and we obtain the polynomial

Diana Teider
dianapatrizia.teider@uzh.ch

$$X^2 + X + 2 = \left(X - \frac{-1+\sqrt{-7}}{2}\right)\left(X - \frac{-1-\sqrt{-7}}{2}\right).$$

By Theorem 3.19, we get

$$\#E(\mathbb{F}_4) = 4 + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^2 - \left(\frac{-1-\sqrt{-7}}{2}\right)^2.$$

Now, one can use the recurrence in Lemma 3.20:

$$s_2 = as_1 - 2s_0 = -(-1) - 2(2) = -3.$$

It follows that $\#E(\mathbb{F}_4) = 4 + 1 - (-3) = 8$, which is also what can be checked by listing points.

One can say that Theorem 3.19 allows to determine the group order for certain curves very quickly. Its disadvantage is that it requires the curve to be defined over a small finite field.

An alternative method for defining the order of an elliptic curve is through the use of the Legendre symbol:

Definition 3.24. (p. 104, [9]) The *Legendre symbol* $\left(\frac{x}{p}\right)$ for an odd prime $p$ is defined as follows:

$$\left(\frac{x}{p}\right) = \begin{cases} +1 \text{ if } t^2 \equiv x \pmod{p} \text{ has a solution } t \not\equiv 0 \pmod{p}, \\ -1 \text{ if } t^2 \equiv x \pmod{p} \text{ has no solution } t, \\ 0 \text{ if } x \equiv 0 \pmod{p}. \end{cases}$$

This can be generalized to any finite field $\mathbb{F}_q$ with $q$ odd and for $x \in \mathbb{F}_q$:

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 \text{ if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^\times, \\ -1 \text{ if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q, \\ 0 \text{ if } x = 0. \end{cases}$$

Diana Teider
dianapatrizia.teider@uzh.ch

THEOREM 3.25. *(p. 105, Theorem 4.14, [9]) Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Then*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$$

*Proof.* (p. 105, [9]) For a given $x_0$, there are two points $(x, y)$ with $x$-coordinate $x_0$ if $x_0^3 + Ax_0 + B$ is a nonzero square in $\mathbb{F}_q$, one such point if it is zero, and no points if it is not a square. Therefore, the number of points with $x$-coordinate $x_0$ equals $1 + \left( \frac{x_0^3 + Ax_0 + B}{\mathbb{F}_q} \right)$. Summing over all $x_0 \in \mathbb{F}_q$, and including 1 for the points at $\infty$, we obtain

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left( 1 + \left( \frac{x^3 + Ax + B}{\mathbb{F}_q} \right) \right).$$

Collecting the term 1 from each of the $q$ summands yields the desired formula. □

EXAMPLE 3.26. (p.106, Example 4.5, [9]) Let $E$ be the curve $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. The nonzero squares mod 5 are 1 and 4. Therefore

$$\begin{aligned} \#E(\mathbb{F}_5) &= 5 + 1 + \sum_{x=0}^{4} \left( \frac{x^3 + x + 1}{5} \right) \\ &= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right) \\ &= 6 + 1 - 1 + 1 + 1 + 1 = 9. \end{aligned}$$

Another method for computing the number of points on elliptic curves over finite fields $\mathbb{F}_q$ is Schoof's Algorithm. Those wishing to gain a deeper understanding of the functioning of this algorithm are encouraged to consult [9], p. 123 - 129.

Diana Teider
dianapatrizia.teider@uzh.ch

# 4. Distribution of curves over finite fields with a given number of points.

The following chapter is based on Christophe Ritzenthaler's work together with Jonas Bergström, Everett Howe and Elisa Lorenzo García [11]. Since this work gives another insight on curves over finite fields and their number of points, we give a summary of it.

Having a look at the Hasse-Weil inequality for C a projective, smooth and absolutely irreducible curve of genus $g$ over $\mathbb{F}_q$, where $N$ is the number of points on the curve:

$$|N - (q+1)| \leq 2g\sqrt{q},$$

[11] defines the left part of the inequality as $t$:

$$t := |N - (q+1)|$$

In addition, for a fixed $g$, the parameter $\tau = t/\sqrt{q}$ is set. They see the number of points as some isomorphism class and claim that the number $M_g(q)$ of $\mathbb{F}_q$-isomorphism classes grows like $q^{3g-3}$ when $g \geq 3$, $2q$ when $g = 1$ and $2q^3$ when $g = 2$. We define

$$\mathcal{N}_{q,g}(\tau) = \frac{1}{M_g(q)} \cdot \#\{\mathbb{F}_q - \text{iso classes of curves of genus } g \text{ over } \mathbb{F}_q \text{ with trace } \sqrt{q}\tau\}, \quad (8)$$

which implies that $\mathcal{N}_{q,g}(\tau)$ is the proportion of isomorphism classes for a given trace.

[11] aims to extend the Katz–Sarnak theory (for more interest, one can have a look at [12], Chapter 10), which deals with the distribution of traces of Frobenius for families of curves of genus $g$ over a finite field $\mathbb{F}_q$ as $q$ tends to infinity. They also demonstrate that the Katz–Sarnak limiting distributions do not accurately approximate the number of curves over a given finite field $\mathbb{F}_q$ with a given trace of Frobenius. For elliptic and hyperelliptic curves, the actual number can significantly deviate from the predictions.

In conclusion, understanding the distribution of rational points on algebraic curves can help in constructing curves with specific properties.

Diana Teider
dianapatrizia.teider@uzh.ch

# 5. Computational results.

In this chapter, we will examine some examples of the number of points on randomly generated smooth curves over finite fields. The results are being found by using Sagemath [13]. We begin by setting the field size to 3 and varying the degree of the curves. After that, we fix the degree to 3 and vary the field sizes.

## 5.1. The Code.

Should you be more interested in the code than the description, you will find an example in the appendix and the code can be found on GIT:
(https://git.math.uzh.ch/dteide/my_master_thesis.git). First, it generates random curves of a given degree using the built-in *random element* function. This does not ensure that the curves are smooth (which is needed for the Hasse-Weil bound). Since there was no built-in function to check for smoothness, we had to find another way. A built-in function exists for computing the genus of a curve. Since calculating the genus requires the number of singularities on a curve, this can be used to check the smoothness of the randomly generated curve. Once it has been determined that the curve is smooth, the number of points on the curve can be counted and added to a list. Finally, after performing this operation a specified number of times (e.g. 1000 or 10000), the mean of the number of points in the list is printed. Finally, the Hasse-Weil bound is calculated. The final number of points on the last curve is compared with the bound to verify the accuracy of the code.

## 5.2. Methods to randomly generate curves.

The following brief overview will present three different methods for randomly generating curves. The first of these is the method that was used in the thesis.

The following method will address the one utilized in the code for the computational results presented in this thesis: One may envision a polynomial in which all possible entries are represented, corresponding to the specified degree and with the requisite coefficients absent. In a further step, the code randomly fills the gaps with elements drawn from the specified field, thereby generating a curve. This procedure is relatively straightforward, as it is applicable to a range of degrees and field sizes. However, one potential drawback is that this method may result in an overparametrization of the curve.

An additional approach, as proposed by [11], is to randomly select a j-invariant (discussed in the section on Elliptic curves and their Number of Points) and then perform a calculation of the number of points. This results in the curves being deemed non-equivalent and in the random selection of a curve that can be represented by the j-invariant. As demonstrated in the work of [11], this approach can be extended to higher-degree curves. However, the challenge lies in identifying an invariant for these curves.

Diana Teider
dianapatrizia.teider@uzh.ch

A third method for randomly generating elliptic curves involves taking the same approach as in this thesis, but instead of using a polynomial with all possible entries, one employs a reduced Weierstrass form and randomly selects values for $A$ and $B$. However, this approach has the disadvantage of producing many curves that are equivalent.

### 5.3. The Affine Plane Curves the Code Generates.

We can also have a look at the smooth affine plane curves the code randomly generates. For curves of degree 3 and over $\mathbb{F}_5$, 10 of the affine plane curves look like the following:

- $-x^3 + y^3 + 2xy + y + 2$
- $2x^3 - 2y^3 - 2y^2 - 2x$
- $y^3 + 2x^2 + xy + y^2 - 2y$
- $-2y^3 + x^2 + xy - y^2 - 2y$
- $-2x^3 + y^3 - x^2 - y^2 - 1$
- $-2x^3 - x^2y + 2y^3 - y$
- $x^2y - 2y^3 + xy + x$
- $2xy^2 + y^3 + x^2 - y^2 - y$
- $2x^3 - 2xy^2 - y^3 + x^2 + 2y$
- $2x^2y - 2y^3 + 2x$

where the last curve has 6 points: $\{(0,0),(1,2),(2,1),(3,4),(4,3)\} \cup \{\mathcal{O}\}$. The Hasse interval is $[1.5279, 10.4721]$.

For curves of degree 8 and over $\mathbb{F}_3$, 10 of the affine plane curves look like the following:

- $-x^7y - y^7 - y^6 + xy^2 + 1$
- $-x^7y - y^8 - x$
- $y^8 + x^7 - x^2y^5 - x^4y - y$
- $-x^7y + y^7 + x^5 + y^5 - x$
- $-x^4y^4 + xy^7 + x^7 + x^2 - 1$
- $x^7y + y^7 + x^4y + 1$
- $-x^7y + y^8 + x^3y + 1$
- $x^3y^5 - x^7 - y^7 + 1$
- $xy^7 - x^7 - x^4y^3 + x^2y + 1$
- $-y^8 - x^7 - 1$

where the last curve has the 4 points: $\{(1,1),(1,2),(2,0)\} \cup \{\mathcal{O}\}$. The Hasse-Weil bound for the last affine plane curve with genus $g = 21$ is $[-68.7461, 76.74613]$.

Diana Teider
dianapatrizia.teider@uzh.ch

It is important to note that in this thesis there is a possibility that some of the curves are equivalent. This is due to the fact that the code does not check for curves being in the same equivalence class before adding them to the list of curves.

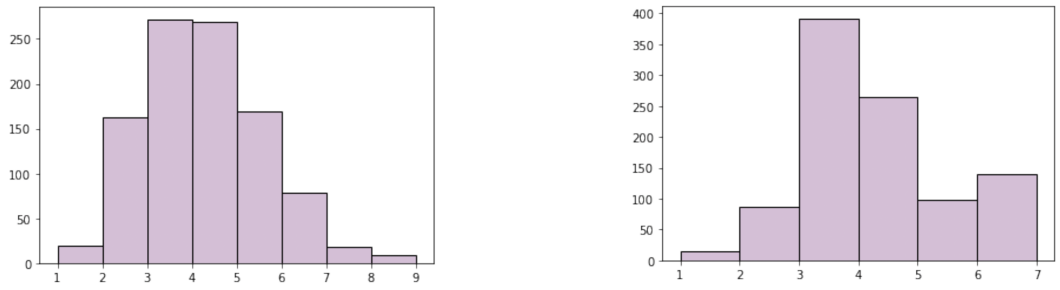
### 5.4. The Influence on the Number of points by increasing the degree.

The following Table shows the statistics of the number of points on 1000 randomly generated smooth curves over $\mathbb{F}_3$.

| **Varying the degree** | | | | |
|---|---|---|---|---|
| Field size | Degree | Average number of points | q + 1 | Deviation to q + 1 |
| 3 | 3 | 4.188 | 4 | 0.188 |
| | 4 | 3.875 | | -0.125 |
| | 5 | 3.769 | | -0.231 |
| | 6 | 3.791 | | -0.209 |
| | 7 | 3.673 | | -0.327 |

TABLE 2. Number of points on curves of various degrees over $\mathbb{F}_3$.

According to the values in Table 2 above, one can see that the average deviation from the expected $q+1$ points is $-0.1408$. Also, for increasing degrees, the average number of points on the curves tend to decrease.




(A) (B)

FIGURE 1. The number of points on curves of degree 5 and of degree 6 over $\mathbb{F}_3$.

In Figures 1a and 1b, we see the possible outcomes for the number of points on the curves on the bottom axis. The left axis shows the number of curves that had the corresponding number of points (which is also the case for the following Figures 1a to 6). These are the outcomes of 1000 randomly generated smooth functions over $\mathbb{F}_3$. (A) visualizes the number of points for curves of degree 5 (with average value = 3.769), (B) for curves of degree 6 (with average value = 3.791).

Diana Teider
dianapatrizia.teider@uzh.ch

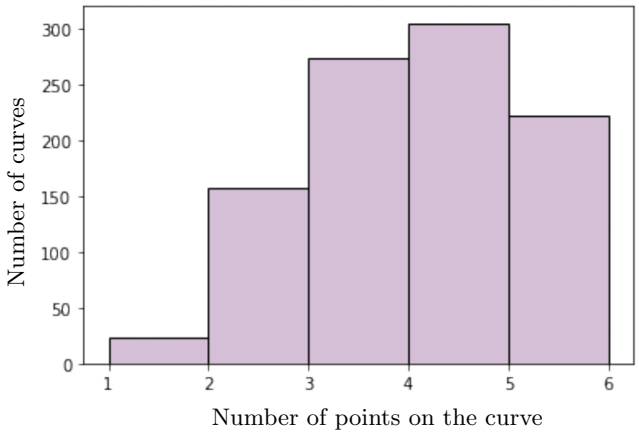



FIGURE 2. The number of points on curves of degree 7 over $\mathbb{F}_3$.

In Figure 2, we see the outcome of 1000 randomly generated smooth functions of degree 7 over $\mathbb{F}_3$. The average number of points on the curves is 2.776.

### 5.5. The reason for results of curves of no higher degree than 8.

The running time of the code increased dramatically as the degree increased. It took the code about 2 weeks to compute results for curves of degree 8. This is due to the large number of ways to generate higher degree curves. It should also be mentioned that the curves are intended to be smooth, which extended the duration of the running time further, since the code performs a smoothness check after the curve has been generated and in case of a singularity, it starts from the top by randomly generating a new curve until it is smooth.
This is why we give the computational results for degree equal to 8 over 500 (instead of 1000 as before) randomly generated curves.

| **Varying the degree** | | | | |
|---|---|---|---|---|
| Field size | Degree | Average number of points | q + 1 | Deviation to q + 1 |
| 3 | 8 | 3.638 | 4 | -0.362 |

TABLE 3. Number of points on curves of degree 8 over $\mathbb{F}_3$.

In Table 3 we see that the average number of points of randomly generated curves of degree 8 and over the field $\mathbb{F}_3$ is 3.638. This is 0.362 less than 4, which is the expected value for the number of points. This also aligns with the observed tendency for the curves to exhibit a lower-than-expected number of rational points.

Diana Teider
dianapatrizia.teider@uzh.ch

### 5.6. The Influence on the Number of points by increasing the Field Size.

The Table 4 shows the computational results of the number of points on 10000 randomly generated smooth curves over a given field size and of degree 3.

| **Varying the field size** | | | | |
|---|---|---|---|---|
| Field size | Degree | Average number of points | q + 1 | Deviation to q + 1 |
| 5 | 3 | 5.9934 | 6 | -0.0066 |
| 7 | | 8.0390 | 8 | 0.0390 |
| 11 | | 12.1191 | 12 | 0.1191 |
| 13 | | 14.0654 | 14 | 0.0654 |
| 19 | | 20.009 | 20 | 0.0090 |
| 37 | | 38.0762 | 38 | 0.0762 |
| 71 | | 72.1957 | 72 | 0.1957 |
| 211 | | 211.7927 | 212 | -0.2073 |
| 383 | | 383.5585 | 384 | -0.4415 |
| 599 | | 599.8039 | 600 | -0.1961 |

TABLE 4. Number of points on curves of degree 3 over various field sizes.

One can see that the average deviation from the expected $q+1$ points is $-0.03471$. We also acknowledge that for average values above the expected $q+1$ the deviation is 0.0841, while the deviation of the average values below $q+1$ is $-0.2129$. The field size with the greatest deviation from the expected number of points is $\mathbb{F}_{383}$ with a deviation of $-0.4415$.

Table 5 shows the data of the number of points on 1000 randomly generated smooth curves over a given field size and degree 3.

| **Varying the field size** | | | | |
|---|---|---|---|---|
| Field size | Degree | Average number of points | q + 1 | Deviation to q + 1 |
| 997 | 3 | 998.251 | 998 | 0.251 |
| 1051 | | 1051.578 | 1052 | -0.422 |
| 1237 | | 1238.708 | 1238 | 0.708 |
| 2221 | | 2222.380 | 2222 | 0.380 |
| 3221 | | 3223.762 | 3222 | 1.762 |
| 4111 | | 4114.51 | 4112 | 2.510 |

TABLE 5. Number of points on curves of degree 3 over various field sizes.

It can be observed that the average deviation from the expected $q+1$ points is 0.865. The data in Table 5 exhibits a greater degree of deviance from the expected number of points than was witnessed in the previous instance.

Diana Teider
dianapatrizia.teider@uzh.ch

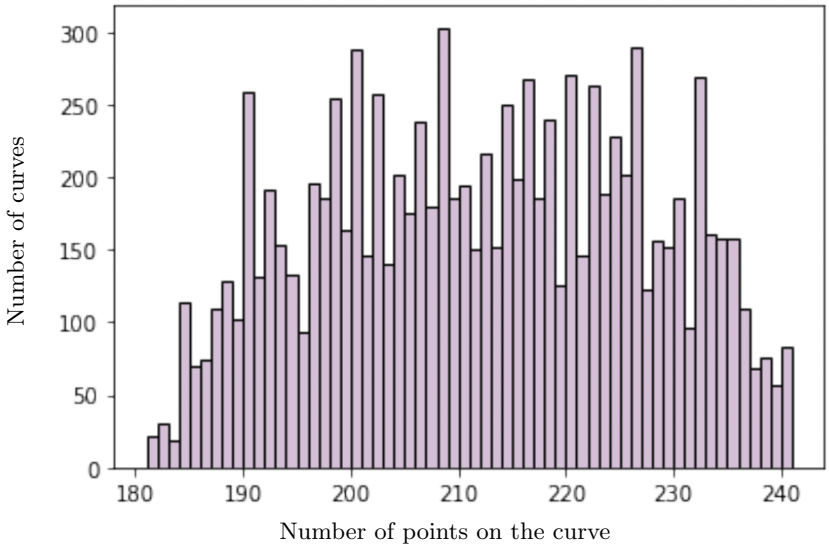



FIGURE 3. The number of points on curves of degree 3 over $\mathbb{F}_{211}$.

In Figure 3, we see the outcome of 10000 randomly generated smooth functions of degree 3 over $\mathbb{F}_{211}$. The average number of points on the curves is 211.7927.

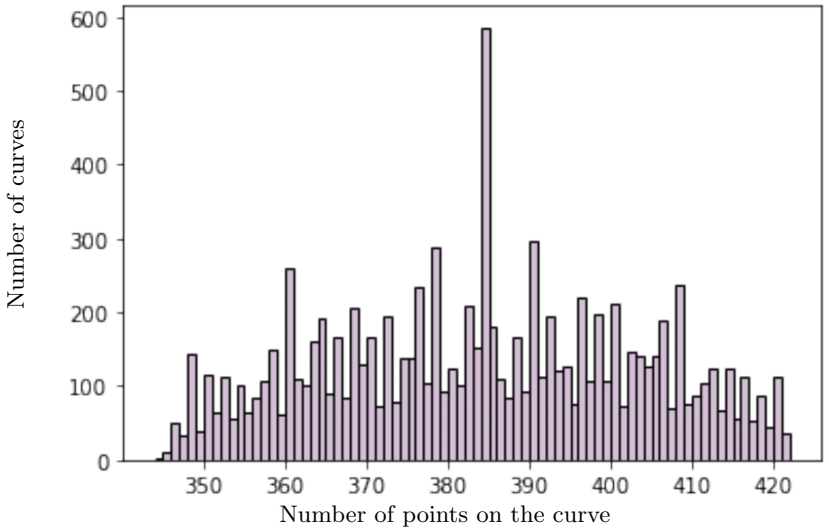



FIGURE 4. The number of points on curves of degree 3 over $\mathbb{F}_{383}$.

In Figure 4, we see the outcome of 10000 randomly generated smooth functions of degree 3 over $\mathbb{F}_{383}$. The average number of points on the curves is 383.5585.

Diana Teider
dianapatrizia.teider@uzh.ch

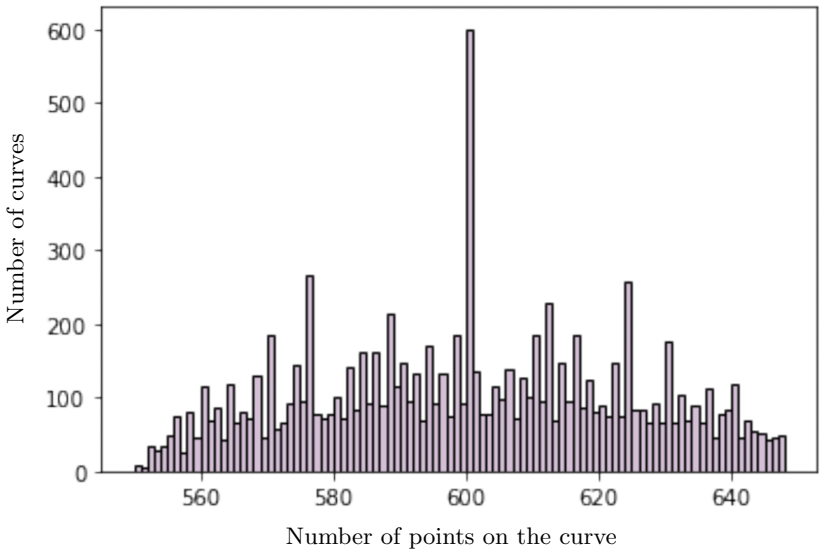



FIGURE 5. The number of points on curves of degree 3 over $\mathbb{F}_{599}$.

In Figure 5, we see the outcome of 10000 randomly generated smooth functions of degree 3 over $\mathbb{F}_{599}$. The average number of points on the curves is 599.8039.

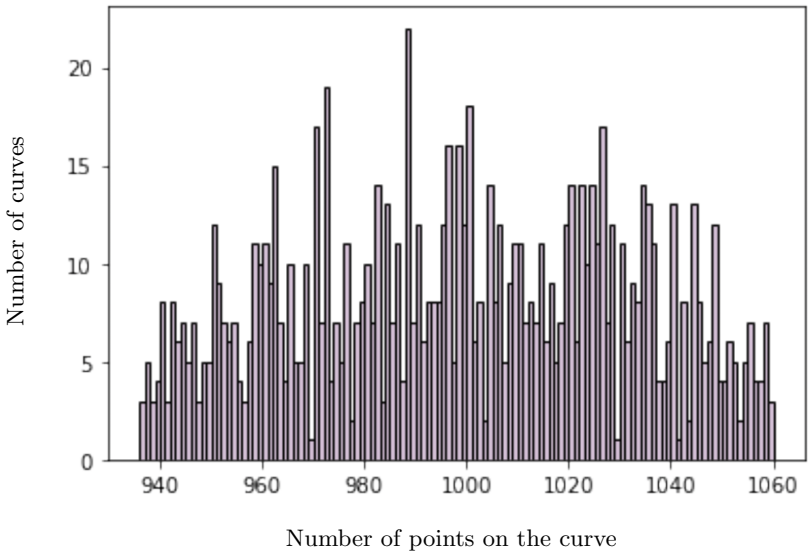



FIGURE 6. The number of points on curves of degree 3 over $\mathbb{F}_{997}$.

In Figure 6, we see the outcome of 1000 randomly generated smooth functions of degree 3 over $\mathbb{F}_{997}$. The average number of points on the curves is 998.251.

Diana Teider
dianapatrizia.teider@uzh.ch

Comparing Figure 3 with Figure 4, it can be observed that there is a markedly more precise peak at approximately 383 in figure 4. On the other hand, the deviation of the expected number of points with only $-0.2073$ for the field size $\mathbb{F}_{211}$ performs better.

In addition, we have give the computational results for 500 randomly generated smooth curves over even bigger field sizes in Table 6.

| **Varying the field size** | | | | |
|---|---|---|---|---|
| Field size | Degree | Average number of points | q + 1 | Deviation to q + 1 |
| 5101 | | 5097.496 | 5102 | -4.504 |
| 7001 | 3 | 7001.108 | 7002 | 0.108 |
| 8011 | | 8007.266 | 8012 | -4.734 |

TABLE 6. Number of points on curves of degree 3 over various field sizes.

In Table 6, one can see that the average deviation from the expected $q + 1$ points is $-3.043$. While the deviation is only 0.108 for $\mathbb{F}_{7001}$, the results for $\mathbb{F}_{5101}$ and $\mathbb{F}_{8011}$ are rather variant.

Diana Teider
dianapatrizia.teider@uzh.ch

# 6. A comparison of the number of points of singular curves to the Hasse-Weil bound.

In the course of this process, it was discovered that the number of points of singular curves does not always satisfy the Hasse-Weil bound. This chapter presents the computational results concerning the number of singular curves that do not satisfy the Hasse-Weil bound. This prompted us to direct our attention to singular curves as well, with a specific interest in examining the extent to which the Hasse-Weil bound is affected by the absence of the requisite smoothness.

The statistics are presented in two stages. Initially, the degree is increased while the field size is fixed at 3. Subsequently, the field size is increased while the degree is fixed at 3.

## 6.1. Singular Affine Plane Curves the Code generates.

The initial step was to adapt the code to generate singular curves at random. This was also achieved by using the built-in function that computes the genus.

An example of a singular affine plane curve of degree 3 and over the finite field $\mathbb{F}_7$ the code generates is $2xy^2 + y^3 + x^2 + xy - 1$. The genus $g$ is equal to -1. The curve has 15 points: $\{(0,1),(0,2),(0,4),(1,0),(1,6),(2,5),(3,3),(4,1),(4,2),(4,3),(5,6),(6,0),(6,4),(6,5)\} \cup \{\mathcal{O}\}$. Since the Hasse-Weil interval for this curve is $[2.7085, 13.2915]$, we know that the number of rational points on this curve lies above the given upper bound.

## 6.2. The Hasse-Weil bound for singular curves.

For the Hasse-Weil bound, smoothness of the curves is provided. This implies that this bound should not be used as a bound for singular curves. In the following section, we will examine how this bound performs for singular curves. Since the genus of singular curves can be negative, we had to switch the upper and lower bounds of the Hasse-Weil bound in these cases. For further details, please refer to the accompanying code in the appendix.

## 6.3. Influence of changing the field size on the proportion of curves not satisfying the Hasse-Weil bound - Computational results.

In this chapter and the next, we present the computational results for the number of singular curves from 1000 that do not satisfy the Hasse-Weil bound. To enhance the clarity of the results, the calculations were conducted in 10 separate runs and the mean of these results was then determined.

Diana Teider
dianapatrizia.teider@uzh.ch

| | Run 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | mean | % |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| field size | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | |
| *total* | 123 | 119 | 106 | 128 | 108 | 111 | 121 | 127 | 113 | 100 | **115.60** | **11.56** |
| *oa* | 123 | 119 | 106 | 128 | 108 | 111 | 121 | 127 | 113 | 100 | **115.60** | **11.56** |
| *ob* | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| *av* | 9.233 | 9.058 | 9.068 | 9.296 | 9.224 | 9.289 | 9.289 | 9.349 | 9.265 | 9.312 | **9.24** | |
| 7 | | | | | | | | | | | | |
| | 546 | 553 | 521 | 516 | 552 | 527 | 539 | 522 | 482 | 546 | **530.40** | **53.04** |
| | 546 | 553 | 521 | 516 | 552 | 527 | 539 | 522 | 482 | 546 | **530.40** | **53.04** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 13.023 | 13.128 | 13.011 | 12.852 | 13.006 | 13.012 | 13.02 | 12.821 | 12.703 | 12.96 | **12.95** | |
| 11 | | | | | | | | | | | | |
| | 863 | 889 | 879 | 890 | 874 | 866 | 861 | 860 | 864 | 888 | **873.40** | **87.34** |
| | 863 | 889 | 879 | 890 | 874 | 866 | 861 | 860 | 864 | 888 | **873.40** | **87.34** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 20.4 | 20.689 | 20.972 | 20.878 | 20.729 | 20.462 | 20.392 | 20.566 | 20.42 | 20.704 | **20.62** | |
| 13 | | | | | | | | | | | | |
| | 894 | 896 | 878 | 892 | 897 | 898 | 903 | 885 | 892 | 880 | **891.50** | **89.15** |
| | 894 | 896 | 878 | 892 | 897 | 898 | 903 | 885 | 892 | 880 | **891.50** | **89.15** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 24.575 | 24.657 | 24.247 | 24.498 | 24.623 | 24.819 | 24.669 | 24.711 | 24.538 | 24.329 | **24.57** | |
| 17 | | | | | | | | | | | | |
| | 921 | 930 | 925 | 922 | 901 | 921 | 935 | 925 | 935 | 918 | **923.30** | **92.33** |
| | 906 | 916 | 906 | 902 | 882 | 907 | 923 | 908 | 916 | 904 | **907.00** | **90.70** |
| | 15 | 14 | 19 | 20 | 19 | 14 | 12 | 17 | 19 | 14 | **16.30** | **1.63** |
| | 32.366 | 32.786 | 32.517 | 32.413 | 32.05 | 32.475 | 32.767 | 32.449 | 32.729 | 32.682 | **32.52** | |
| 23 | | | | | | | | | | | | |
| | 950 | 961 | 941 | 944 | 959 | 946 | 956 | 948 | 953 | 953 | **951.10** | **95.11** |
| | 927 | 944 | 925 | 915 | 938 | 925 | 928 | 926 | 929 | 929 | **928.60** | **92.86** |
| | 23 | 17 | 16 | 29 | 21 | 21 | 28 | 22 | 24 | **24** | **22.50** | **2.25** |
| | 44.318 | 44.748 | 44.503 | 43.83 | 44.657 | 44.415 | 44.263 | 44.219 | 44.348 | 44.245 | **44.35** | |
| 101 | | | | | | | | | | | | |
| | 983 | 989 | 983 | 984 | 983 | 987 | 989 | 983 | 985 | 992 | **985.80** | **98.58** |
| | 978 | 980 | 974 | 976 | 976 | 979 | 981 | 973 | 980 | 985 | **978.20** | **97.82** |
| | 5 | 9 | 9 | 8 | 7 | 8 | 8 | 10 | 5 | **7** | **7.60** | **0.76** |
| | 199.565 | 199.676 | 199.186 | 199.116 | 200.098 | 199.786 | 199.832 | 199.11 | 200.769 | 200.509 | **199.76** | |
| 503 | | | | | | | | | | | | |
| | 999 | 997 | 997 | 997 | 997 | 991 | 999 | 997 | 999 | 997 | **997.00** | **99.70** |
| | 998 | 994 | 992 | 995 | 994 | 988 | 999 | 996 | 999 | 996 | **995.10** | **99.51** |
| | 1 | 3 | 5 | 2 | 3 | 3 | 0 | 1 | 0 | 1 | **1.90** | **0.19** |
| | 1004.561 | 1002.585 | 1001.071 | 1004.119 | 1001.081 | 998.635 | 1008.058 | 1004.109 | 1006.579 | 1004.566 | **1003.54** | |
| 1013 | | | | | | | | | | | | |
| | 1000 | 998 | 999 | 999 | 998 | 999 | 998 | 997 | 997 | 997 | **998.20** | **99.82** |
| | 1000 | 997 | 999 | 999 | 997 | 999 | 998 | 997 | 995 | 996 | **997.70** | **99.77** |
| | 0 | 1 | 0 | 0 | **1** | 0 | 0 | 0 | **2** | 1 | **0.50** | **0.05** |
| | 2025.632 | 2023.537 | 2026.522 | 2025.603 | 2021.52 | 2027.645 | 2024.556 | 2023.583 | 2021.599 | 2021.578 | **2024.18** | |

FIGURE 7. Proportion of singular curves with number of points out of Hasse-Weil bound

total: number of curves out of bound  oa: number of curves above bound
ob: number of curves below bound  av: average number of points

In Figure 7 we see the results for increasing the field sizes and fixing the degree to 3. The two right columns show the average number of singular curves with more or fewer points than expected by Hasse-Weil. The far right column gives the corresponding percentage. Since most singular curves have more points than the upper limit, the few curves that have less than the lower limit are marked in orange. The following section will provide a more detailed examination of the values highlighted in yellow.

Diana Teider
dianapatrizia.teider@uzh.ch

### 6.3.1. Examples of singular curves having less rational points than expected by the Hasse-Weil lower bound.

Marked in yellow in Figure 7, we see that there are 24 singular curves with degree 3 over $\mathbb{F}_{23}$ with fewer points than the lower Hasse-Weil bound. Upon further examination, we observe that all of these curves only have 1 point. In such cases, the point in question is not always identical. 14 of the curves with less than expected points only have the point $(0, 0)$ and no point at infinity. Some examples of these are:

- $-4x^3 + 11x^2y - 5xy^2 - 5y^3$
- $-7x^3 - 11x^2y - 6xy^2 - 10y^3$
- $x^3 + 8x^2y + 9xy^2 - 10y^3$
- $3x^3 + 8x^2y - 5xy^2 - 4y^3$

  .
  .
  .

All these curves have genus equal to $-2$ and hence the Hasse-Weil interval is given by $[5, 43]$. One may notice that all these curves are homogenized and irreducible. The remaining 10 curves only have the point at infinity, some examples of these curves are:

- $-10y^3 + 10y^2 - 1$
- $-5y^3 + 8y^2 - 10y - 4$
- $-5y^3 + 2y^2 + 7y + 1$
- $8y^3 - 9y^2 - 4y - 3$

  .
  .
  .

These curves have genus equal to $-2$ as well and hence also the same Hasse-Weil interval as the curves with the point $(0, 0)$ from before. One can see that these curves are only dependent on $y$.

Having a closer look at the first example of these curves, namely $-10y^3 + 10y^2 - 1$, we can homogenize to get $10y^3 + 10y^2z - z^3$. Computing the derivatives, we see that the point $\mathcal{O} = (1, 0, 0)$ is the point at infinity and the singular point.

In addition, we analyze the second value marked in yellow (read from top to bottom), which is the one over the field $\mathbb{F}_{101}$. There are 7 curves with less points than expected. These curves all have genus $-2$ and the Hasse-Weil interval is given by $[62, 142]$. Three of the curves only have the point $(0, 0)$. The only point on the remaining 4 curves is the point at infinity.

In Figure 7 at the bottom, we observe that there are fewer runs where there are curves with fewer points than expected by the Hasse-Weil interval over the field $\mathbb{F}_{1013}$.
Two of these runs are highlighted in yellow as well. In run 5, the one curve affected is $141x^3+254x^2y+154xy^2+150y^3$. It only has the point $(0,0)$. Note that it is homogenized. In run 9 there occurred two curves having only the point at infinity: $82y^3-184y^2-342y+149$ and $-458y^3-195y^2+220y-379$. Both of these curves have genus equal to $-2$ and the Hasse-Weil interval is given by $[887, 1141]$. It is to be observed that the two curves are dependent on $y$ only.

### 6.3.2. The rationale behind the observation that the majority of curves exhibit a greater number of points than anticipated by Hasse-Weil.

One might inquire as to why the majority of the curves exhibit a greater number of points than anticipated. As illustrated in Figure 7, for the field size 17, over 90% of the curves already exceed the upper bound. This may be attributed to the fact that these curves are reducible. In this case, a polynomial of degree 3 can be reduced into for example three linear factors.

This kind of configuration then represents the union of three lines. It can be demonstrated that the number of points on this curve can be expressed as either

$$3(q+1)-3=3q \quad \text{or} \quad 3(q+1)-1=3q+2,$$

where $q$ represents the field size. This depends on whether the lines intersect three times or only once, respectively. In addition, this leads to the assumption that for singular curves of degree 3 which are reducible, there are approximately $3q$ points. One can extend this line of reasoning to suggest that singular curves of degree $n$ which are reducible, are suspected to have approximately $nq$ points.

Further work would be beneficial to ascertain whether there exists an irreducible singular curve with a greater number of points than predicted by the Hasse-Weil theorem. This is particularly relevant given that the homogenized singular curves of degree 3 with only the point $(0,0)$ (which means that they have less points than the lower Hasse-Weil bound) have been observed to be irreducible.

Diana Teider
dianapatrizia.teider@uzh.ch

In conclusion, the findings derived from our computational analysis so far are as follows:

The observations suggest a hypothesis that a singular curve possessing a single point may be either homogenized or dependent on a single variable.

Furthermore, it can be inferred that singular curves exhibiting only the point (0,0) are likely homogenized, while those with a singular point at infinity are indicative of dependency on a single variable.

It is also evident that as the field size increases, the proportion of curves that fail to satisfy the Hasse-Weil interval rises significantly. Notably, for a field size of 17, this proportion already exceeds 90%. It can be assumed that this occurs because the majority of the curves are reducible, resulting in the union of, for instance, three lines (given that all these results concern curves of degree 3), which then yields a total of approximately $3q$ points.

These findings underscore the impact of increasing the field size on the distribution of points on singular curves, highlighting a drastically growing divergence from the Hasse-Weil interval with higher field sizes.

Diana Teider
dianapatrizia.teider@uzh.ch

### 6.4. Influence of changing the degree on the proportion of curves not satisfying the Hasse-Weil bound - Computational results.

Figure 8 illustrates the behavior of singular curves as the degree increases while maintaining a constant field size of 3. The results are shown for degrees ranging from 4 to 10. Each degree level has ten runs, with metrics of the number of curves with number of points not satisfying the Hasse-Weil interval and the average number of points. The two right columns provide the average number of singular curves with more or fewer points than expected by Hasse-Weil as well as the average number of points. The far right column provides the corresponding percentage.

| | Run 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | mean | % |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| degree | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | |
| *total* | 12 | 6 | 14 | 17 | 19 | 14 | 11 | 9 | 11 | 15 | **12.8** | **1.28** |
| *oa* | 12 | 6 | 14 | 17 | 19 | 14 | 11 | 9 | 11 | 15 | **12.8** | **1.28** |
| *ob* | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| *av* | 5.63 | 5.531 | 5.59 | 5.589 | 5.659 | 5.627 | 5.496 | 5.494 | 5.612 | 5.563 | **5.58** | |
| 4 | | | | | | | | | | | | |
| | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | **0.3** | **0.03** |
| | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | **0.3** | **0.03** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.138 | 5.028 | 5.052 | 5.065 | 5.074 | 5.122 | 5.132 | 5.072 | 5.197 | 5.126 | **5.10** | |
| 5 | | | | | | | | | | | | |
| | 9 | 11 | 9 | 12 | 20 | 16 | 18 | 18 | 11 | 16 | **14** | **1.4** |
| | 9 | 11 | 9 | 12 | 20 | 16 | 18 | 18 | 11 | 16 | **14** | **1.4** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.15 | 5.214 | 5.162 | 5.248 | 5.227 | 5.225 | 5.269 | 5.291 | 5.104 | 5.21 | **5.21** | |
| 6 | | | | | | | | | | | | |
| | 14 | 18 | 21 | 19 | 25 | 18 | 17 | 19 | 27 | 13 | **19.1** | **1.91** |
| | 14 | 18 | 21 | 19 | 25 | 18 | 17 | 19 | 27 | 13 | **19.1** | **1.91** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.287 | 5.36 | 5.306 | 5.45 | 5.312 | 5.428 | 5.284 | 5.372 | 5.437 | 5.33 | **5.36** | |
| 7 | | | | | | | | | | | | |
| | 33 | 23 | 17 | 39 | 19 | 18 | 25 | 26 | 27 | 21 | **24.8** | **2.48** |
| | 33 | 23 | 17 | 39 | 19 | 18 | 25 | 26 | 27 | 21 | **24.8** | **2.48** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.494 | 5.482 | 5.461 | 5.465 | 5.466 | 5.419 | 5.496 | 5.377 | 5.454 | 5.489 | **5.46** | |
| 8 | | | | | | | | | | | | |
| | 17 | 38 | 29 | 21 | 22 | 23 | 20 | 18 | 18 | 31 | **23.70** | **2.37** |
| | 17 | 38 | 29 | 21 | 22 | 23 | 20 | 18 | 18 | 31 | **23.70** | **2.37** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.536 | 5.588 | 5.558 | 5.485 | 5.528 | 5.605 | 5.525 | 5.574 | 5.613 | 5.637 | **5.56** | |
| 9 | | | | | | | | | | | | |
| | 19 | 26 | 18 | 20 | 17 | 25 | 18 | 14 | 30 | 23 | **21.00** | **2.10** |
| | 19 | 26 | 18 | 20 | 17 | 25 | 18 | 14 | 30 | 23 | **21.00** | **2.10** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.59 | 5.713 | 5.749 | 5.632 | 5.684 | 5.765 | 5.642 | 5.651 | 5.702 | 5.687 | **5.68** | |
| 10 | | | | | | | | | | | | |
| | 31 | 24 | 23 | 23 | 32 | 21 | 19 | 16 | 20 | 14 | **22.30** | **2.23** |
| | 31 | 24 | 23 | 23 | 32 | 21 | 19 | 16 | 20 | 14 | **22.30** | **2.23** |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** | **0** |
| | 5.76 | 5.69 | 5.812 | 5.83 | 5.828 | 5.861 | 5.818 | 5.762 | 5.819 | 5.816 | **5.80** | |

FIGURE 8. Proportion of singular curves with number of points out of Hasse-Weil bound

total: number of curves out of bound  oa: number of curves above bound
ob: number of curves below bound  av: average number of points

Diana Teider
dianapatrizia.teider@uzh.ch

It can be observed that as the degree increases, the percentage of curves that fall out of the Hasse-Weil bound also increases. For degree 4, a small percentage (0.03%) of curves are out of the Hasse-Weil bound. This percentage increases gradually with higher degrees, reaching 2.23% for degree 10.
In addition, there is a general increase in the average number of points as the degree increases. However, it remains close to the expected value, deviating slightly, which suggests that while more curves fall out of the Hasse-Weil interval, the variation in the number of points is not extremely large.

For all degrees, the number of curves falling above the expected number of points (oa) is significantly higher than those below (ob). This implies that the deviations are more commonly due to an excess in the number of points rather than a shortfall over the field $\mathbb{F}_3$.

We now conduct a detailed examination of the value highlighted in yellow in Figure 8. Over the field $\mathbb{F}_3$ and for curves of degree 4, there were hardly any curves with their number of points outside of the given Hasse-Weil interval. One of the only curves with more points than expected, marked in yellow, is $-x^2y^2 + xy^3 + y^4 - y^2$. This curve has a genus of $-1$, so the Hasse interval is given by $[1, 7]$. The curve has 8 points: $\{(0,0),(0,1),(0,2),(1,0),(1,1),(2,0),(2,2)\} \cup \{\mathcal{O}\}$, which means that it exceeds upper the Hasse-Weil bound by 1.

These findings underscore the impact of increasing the degree on the distribution of points on singular curves, highlighting a growing divergence from the Hasse-Weil interval with higher degrees.

Diana Teider
dianapatrizia.teider@uzh.ch

### 6.5. Conclusion.

This thesis has provided an examination of point counting on algebraic curves over finite fields and has compared these counts to the Hasse-Weil bound. Through both theoretical exploration and computational analysis, several key insights have emerged.

Firstly, while the Hasse-Weil bound serves as a crucial guideline in the theory of algebraic curves, our results indicate that for higher degree curves and larger field sizes, the actual number of points really lies inside the bound for smooth curves, even for high field sizes and high degrees. For singular curves, the actual number of points significantly deviates from the bound. Mostly, there are more points than expected. In the case of less points, we have often seen that the curve only has one point, the point at infinity or the point $(0, 0)$ as only point.

The observations throughout this study support the hypothesis that a singular curve with a single point is either homogenized or dependent on a single variable.

Additionally, the findings reinforce the inference that singular curves with only the point (0,0) are likely homogenized, whereas those with only a singular point at infinity indicate dependency on a single variable.

Secondly, the computational aspect of this study has highlighted the challenges and intricacies involved in generating and analyzing large datasets of algebraic curves. Finding computational results for randomly generated curves of degree 8 and higher, especially for smooth curves, took a very long time, due to the fact that there are so many possibilities to generate the curves.

Lastly, the connection between algebraic curves and coding theory opens up potential avenues for future research. These theoretical constructs have practical applications in coding and cryptography.

In conclusion, this thesis not only enhances our understanding of point counting on algebraic curves over finite fields in various areas but also underscores the importance of computational methods in verifying and challenging theoretical bounds. The findings presented here lay foundations for further exploration and refinement of these mathematical concepts.

Diana Teider
dianapatrizia.teider@uzh.ch

# 7. Appendix.

## 7.1. The Sagemath codes.

As mentioned above, one can also find the code on GIT:
(https://git.math.uzh.ch/dteide/my_master_thesis.git).

```
from sage.rings.polynomial.polynomial_ring_constructor import PolynomialRing
from sage.rings.finite_rings.integer_mod_ring import IntegerModRing
from sage.rings.finite_rings.finite_field_constructor import FiniteField
from sage.rings.integer_ring import ZZ
import matplotlib.pyplot as plt
import numpy as np
import sage.rings.finite_rings
```

```
finite_field_order = 5
deg = 3
numb_tries = 100
field_sizes =␣
 ↪[5,7,11,13,19,37,71,211,383,599,997,1051,1237,2221,3221,4111,5101,7001,8011]
degrees = [3,4,5,6,7,8]

field_sizes_singular = [5,7,11,13,17,23,101,503,1013]
degrees_singular = [3,4,5,6,7,8,9,10]
```

```
def gen_smooth_and_count(finite_field_order,deg,numb_tries):
    R.<x,y>=PolynomialRing(GF(finite_field_order),2)
    l = 0
    k = []
    plot_list = []

    while l< numb_tries:

        A = R.random_element(degree = deg)

        if A.degree() !=0 and A.degree() != -1 and A.degree() == deg:
            cur = Curve(A)

            G = cur.genus()
```

Diana Teider
dianapatrizia.teider@uzh.ch

```
            D = (A.degree() -1)*(A.degree() -2)/2

            if G == D:
                k.append(A)
                num = len(cur.rational_points()) + 1
                plot_list.append(num)
                l +=1

    return (plot_list,k)
```

```
def gen_sing_and_count_outbreaks(finite_field_order, deg, numb_tries):

    R.<x,y>=PolynomialRing(GF(finite_field_order),2)
    l = 0
    k = []
    plot_list = []

    #for the number of oubreaks, total, above and below
    out = 0
    outabov = 0
    outbelo = 0

    #for lists of curves with outbreaks above or below
    OA = []
    OB = []

    while l<numb_tries:

        A = R.random_element(degree = deg)

        if A.degree() !=0 and A.degree() != -1 and A.degree() == deg:
            cur = Curve(A)

            G = cur.genus()

            D = (A.degree() -1)*(A.degree() -2)/2
```

Diana Teider
dianapatrizia.teider@uzh.ch

```
            S = D - G


            if S != 0 and G != 0:
                k.append(A)
                num = len(cur.rational_points()) + 1
                points = cur.rational_points()
                if num == 2 and '(0, 0)' in str(points):
                    plot_list.append(1)
                else:
                    plot_list.append(num)
                l +=1

                HasseLOW = finite_field_order + 1␣
↪-(2*Integer(G)*((finite_field_order)^(0.5)))
                HasseUP = finite_field_order + 1␣
↪+(2*Integer(G)*((finite_field_order)^(0.5)))
```

```
                if G > 0:
                    if num <= HasseLOW:
                        out +=1
                        outbelo +=1
                        OB.append(A)

                    if num >= HasseUP:
                        out +=1
                        outabov +=1
                        OA.append(A)

                else:
                    if num >= HasseLOW:
                        out +=1
                        outabov +=1
                        OA.append(A)

                    if num <= HasseUP:
                        out +=1
                        outbelo +=1
                        OB.append(A)

    return (plot_list, k, out, outabov, outbelo, OA, OB)
```

Diana Teider
dianapatrizia.teider@uzh.ch

```
output_smooth = {}

for i in field_sizes:
    for j in degrees:
        output_smooth[(i,j)] = gen_smooth_and_count(i,j,numb_tries)

output_singular = {}

for i in field_sizes_singular:
    for j in degrees_singular:
        output_singular[(i,j)] = gen_sing_and_count_outbreaks(i,j,numb_tries)
```

```
#for the smooth curves
field_size = 5
degree = 3

plot_list = output_smooth[(field_size,degree)][0] #one can choose field size␣
 ↪and degree, provided they are in the lists
x = np.linspace(1,numb_tries,numb_tries)


plt.figure(1)
plt.hist(plot_list, bins=np.arange(min(plot_list), max(plot_list),1),␣
 ↪edgecolor='black',color='thistle')
average_value = np.mean(plot_list)
```

```
#for the singular curves
field_size = 5
degree = 3

plot_list = output_singular[(field_size,degree)][0] #one can choose field size␣
 ↪and degree, provided they are in the lists
x = np.linspace(1,numb_tries,numb_tries)


plt.figure(1)
plt.hist(plot_list, bins=np.arange(min(plot_list), max(plot_list),1),␣
 ↪edgecolor='black',color='thistle')
average_value = np.mean(plot_list)
```

# References.

[1] Harald Niederreiter and Chaoping Xing. *Rational points on curves over finite fields : theory and applications*. eng. Reprint. London Mathematical Society lecture note series vol. 285. Cambridge: Cambridge University Press, 2002. ISBN: 9780521665438.

[2] Raymond Hill. *A first course in coding theory*. Oxford University Press, 1986.

[3] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[4] Henning Stichtenoth. *Algebraic function fields and codes*. Vol. 254. Springer Science & Business Media, 2009.

[5] Rick Miranda. *Algebraic curves and Riemann surfaces*. Vol. 5. American Mathematical Soc., 1995.

[6] Xiang dong Hou. "Applications of the Hasse–Weil bound to permutation polynomials". In: *Finite Fields and Their Applications* 54 (2018), pp. 113–132. ISSN: 1071-5797. DOI: https://doi.org/10.1016/j.ffa.2018.08.005. URL: https://www.sciencedirect.com/science/article/pii/S1071579718300972.

[7] Jean-Pierre Serre et al. *Rational points on curves over finite fields*. Société mathématique de France, 2020.

[8] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error-correcting codes*. Vol. 16. Elsevier, 1977.

[9] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.

[10] William C Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'École normale supérieure*. Vol. 2. 4. 1969, pp. 521–560.

[11] Jonas Bergström et al. *Refinements of Katz-Sarnak theory for the number of points on curves over finite fields*. 2023. arXiv: 2303.17825 [math.NT]. URL: https://arxiv.org/abs/2303.17825.

[12] Nicholas M Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*. Vol. 45. American Mathematical Society, 2023.

[13] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.2)*. https://www.sagemath.org. 2024.