Rational Points on Curves over Finite Fields

Søren Have Hansen

September 16, 1996

Preface

These notes treat the problem of counting the number of rational points on a curve defined over a finite field. The notes are an extended version of an earlier set of notes *Aritmetisk Algebraisk Geometri – Kurver* by *Johan P. Hansen* [Han] on the same subject.

In Chapter 1 we summarize the basic notions of algebraic geometry, especially rational points and the Riemann-Roch theorem. For the convenience of the unexperienced algebraic geometer, the chapter uses the language of classical algebraic geometry as e.g. in [Ful69]. In Appendix A the readers familiar with [Har77] may find a scheme/sheaf-theoretic formulation of Chapter 1. Moreover Appendix A contains proofs of many of the results stated in Chapter 1 without proof.

In Chapter 2 we introduce the Zeta function associated to a curve defined over $\mathbb{F}_q$ – a function containing information on the number of rational points on the curve over all finite field extensions of $\mathbb{F}_q$. We prove that the Zeta function is a rational function obeying a certain functional equation. Furthermore we see how the Riemann hypothesis implies the Weil bound (Corollary 2.6) on the number of rational points on the curve.

When first familiar with the notions of rational functions and the Riemann-Roch theorem, Chapter 2 is rather straightforward. In contrast to this, Chapter 3 is more technical and assumes knowledge of field theory, Galois theory and the intimate relation between a smooth projective curve and its function field. Via this connection to field theory the Zeta function as defined in Chapter 2, is in the beginning of Chapter 3 put into a wider context. Afterwards we show the Riemann hypothesis for curves.

In Appendix B the Weil bound (Corollary 2.6) is improved considerably. In Appendix C we give Weil's original proof of the Weil bound.

Søren Have Hansen
Department of Mathematics, University of Aarhus
8000 Aarhus C, Denmark
email: shave@mi.aau.dk

Contents

Chapter 1

Recollections from Algebraic Geometry

Let $k = \mathbb{F}_q$ be the field with $q = p^n$ elements, where $n \geq 1$ is arbitrary. For any $m \geq 1$ we have the Frobenius automorphism $F : \mathbb{F}_q \to \mathbb{F}_q$ raising to p^{th} powers and F is a generator of the Galois group $G = \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

1.1 Affine Varieties

Definition 1.1. *Affine n-space (over k)* is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \{P = (x_1, \ldots, x_n) \mid x_i \in \bar{k}\}.$$

The set of *k-rational points* in $\mathbb{A}^n$ is

$$\mathbb{A}^n(k) = \{P = (x_1, \ldots, x_n) \mid x_i \in k\}.$$

Remark 1.2. $G = \text{Gal}(\bar{k}/k)$ acts on $\mathbb{A}^n$ by

$$\sigma.P = (\sigma(x_1), \ldots, \sigma(x_n))$$

and

$$\mathbb{A}^n(k) = \{P \in \mathbb{A}^n \mid \sigma.P = P \text{ for all } \sigma \in G\}.$$

We see that the number of $\mathbb{F}_q$-rational points on $\mathbb{A}^n$ is q^n.

Definition 1.3. *An affine algebraic set* in $\mathbb{A}^n$ is a set

$$V_I = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for all } f \in I\}$$

where $I \subseteq \bar{k}[X_1, \ldots, X_n]$ is an ideal. *The ideal associated to an affine algebraic set V* is the ideal

$$I(V) = \{f \in \bar{k}[X_1, \ldots, X_n] \mid f(P) = 0 \text{ for all } P \in V\}.$$

An an affine algebraic set is *defined over* k, if its defining ideal is generated by elements in $k[X_1, \ldots, X_n]$. If V is defined over k, the k-rational points on V consists of

$$V(k) = V \cap \mathbb{A}^n(k).$$

We may put a topology on $\mathbb{A}^n$ by taking the V_I to be the closed sets of the topology.

Remark 1.4. Let $f(X) \in k[X_1, \ldots, X_n]$ og $P \in \mathbb{A}^n$. Then

$$f(\sigma.P) = \sigma.(f(P))$$

for all $\sigma \in G = \mathrm{Gal}(\bar{k}/k)$ as σ acts trivially on f's coefficients. So if V is defined over k, the action of G on $\mathbb{A}^n$ induces an action of G on V and

$$V(k) = \{P \in V \mid \sigma.P = P \text{ for all } \sigma \in G\}.$$

Definition 1.5. An affine algebraic set V is called a *variety*, if $I(V)$ is a prime ideal in $\bar{k}[X_1, \ldots, X_n]$. V is said to be defined over k if the underlying algebraic set is. If V is defined over k we call

$$k[V] = k[X_1, \ldots, X_n]/I(V/k)$$

($I(V/k) = I(V) \cap k[X_1, \ldots, X_n]$) the *affine coordinate ring* of V. Notice that $k[V]$ is a domain so we may think of $k[V]$ as polynomial functions on V. The quotient field $k(V)$ of $k[V]$ is called the *function field* of V over k. In a similar manner one defines $\bar{k}[V]$ and $\bar{k}(V)$.

Remark 1.6. If V is defined over k, $G = \mathrm{Gal}(\bar{k}/k)$ induces an action on $\bar{k}[V]$ og $\bar{k}(V)$ by acting on the coefficients. We may then identify $k[V]$ (resp. $k(V)$) as the sub-rings of $\bar{k}[V]$ (resp. $\bar{k}(V)$) invariant under this action.

1.2 Projective Varieties

Definition 1.7. *Projective n-space* $\mathbb{P}^n$ (over k) is by definition the set of all $(n+1)$-tuples

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \setminus \{0\}$$

modulo the equivalence relation $\sim$

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \Leftrightarrow \exists \lambda \in \bar{k}^* : x_i = \lambda y_i \text{ for all i.}$$

We write an element in $\mathbb{P}^n$ in *homogeneous coordinates* as $(x_0 : \ldots : x_n)$. We also define the *k-rational points* in $\mathbb{P}^n$

$$\mathbb{P}^n(k) = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \in k \text{ for all i}\}.$$

We see that, as $\mathbb{A}^n$ bijects with the set $\{(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} : x_i \neq 0\}$, $\mathbb{P}^n$ may in a natural way be identified with $n+1$ copies of $\mathbb{A}^n$. With a suitable topology (defined below) on $\mathbb{P}^n$ these sets becomes open in $\mathbb{P}^n$, hence we have a covering of $\mathbb{P}^n$ with $n+1$ open affine varieties.

Remark 1.8. $G = \mathrm{Gal}(\bar{k}/k)$ acts on $\mathbb{P}^n$ by acting on the the homogeneous coordinates

$$\sigma.(x_0 : \ldots : x_n) = (\sigma(x_0) : \ldots : \sigma(x_n)) \qquad \sigma \in G.$$

Hence

$$\mathbb{P}^n(k) = \{P \in \mathbb{P}^n \mid \sigma.P = P \text{ for all } \sigma \in G\}$$

and the number of k-rational points in $\mathbb{P}^n$ is $\frac{q^n-1}{q-1}$.

Definition 1.9. A *projective algebraic set* is a set

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homogenous } f \in I\}$$

where $I \subseteq \bar{k}[X_0, \ldots, X_n]$ is a homogeneous ideal. *The ideal associated to a projective algebraic set* V is the ideal

$$I(V) = \{f \in \bar{k}[X_0, \ldots, X_n] \mid f(P) = 0 \text{ for all } P \in V\}.$$

A projective algebraic set V is defined over k if its defining ideal I is generated by polynomials in $k[X_0, \ldots, X_n]$. If V is defined over k, the k-rational points on V consists of

$$V(k) = V \cap \mathbb{P}^n(k) = \{P \in V \mid \sigma.P = P \text{ for all } \sigma \in G\}.$$

As in the affine case, the V_I define a topology of closed sets on $\mathbb{P}^n$.

Definition 1.10. A *projective variety* is a projective algebraic set V whose defining ideal is a homogeneous prime ideal. Like in the affine case, V is defined over k as a projective variety if this is the case for V seen as an algebraic set.

Definition 1.11. Let V be a projective variety defined over k. Choose an open affine subset $U \subseteq \mathbb{P}^n$ such that $V \cap U \neq \emptyset$. Then by definition *the function field* $k(V)$ *of* V equals $k(V \cap U)$. Similarly with $\bar{k}(V)$.

Definition 1.12. Let V_1 og V_2 be projective varieties. *A rational map* from $V_1 \subseteq \mathbb{P}^m$ to $V_2 \subseteq \mathbb{P}^n$ is a map given by rational functions

$$\Psi : V_1 \longrightarrow V_2$$
$$P = (x_0 : \ldots : x_m) \mapsto (f_0(P) : \ldots : f_n(P))$$

where $f_i \in \bar{k}(V_1)$ are such that whenever they are all defined, the image $(f_0(P) : \ldots : f_n(P))$ defines a point in V_2. If there exists a rational map $\Phi : V_2 \to V_1$ such that $\Phi \circ \Psi = \mathrm{id}$ (whenever Ψ is defined) and $\Psi \circ \Phi = \mathrm{id}$ (whenever Φ is defined), Ψ (and Φ) are *birational maps* and we say that V_1 and V_2 are *birational*. In case the compositions are defined everywhere, Ψ (and Φ) are *isomorphisms* and we say that V_1 and V_2 are *isomorphic*. If there exists a $\lambda \in \bar{k}^*$ such that $\lambda f_0, \ldots, \lambda f_n \in k(V_1)$ we say that Ψ is *defined over* k.

Remark 1.13. If $\Psi : V_1 \longrightarrow V_2$ is as above, $G = \mathrm{Gal}(\bar{k}/k)$ induces an action on Ψ

$$(\sigma.\Psi)(P) = ((\sigma.f_0)(P) : \ldots : (\sigma.f_n)(P)). \qquad \sigma \in G$$

With this notation Ψ is defined over k if and only if $\sigma.\Psi = \Psi$ for all $\sigma \in G$.

1.3 Curves

Definition 1.14. A *curve* V is a variety of dimension one, that is

$$\dim(V) := \dim \bar{k}[V]_{\mathfrak{m}_P} = 1$$

for all $P \in V$, ($\mathfrak{m}_P \subseteq \bar{k}[V]$ is the maximal ideal of all functions vanishing in P). Although it may not be obvious at first, this definition is coherent with ones geometric intuition.

Example 1.15 (Hermitian Curve). Let $q = r^2$ and consider the curve in $\mathbb{P}^2$ (over k) given by the equation

$$C_1 : \qquad X_0^{r+1} + X_1^{r+1} + X_2^{r+1} = 0. \tag{1.1}$$

Assume $\mathrm{char}(k) = 2$. Let us determine the number of k-rational points on C_1.In the case where $x_2 = 0$ we may assume that $x_1 = 1$ and we must then solve the equation $x_0^{r+1} + 1 = 0$. This equation has $r + 1$ solutions in k hence we have $3(r + 1)$ k-rational points on C_1 with at least one homogeneous coordinate equal to zero.

Now, if all $x_i \neq 0$ we may assume $x_2 = 1$ and we must then solve the equation $x_0^{r+1} + x_1^{r+1} + 1 = 0$. For any $\beta \in k \setminus \{0, 1\}$ the equation $x_1^{r+1} = \beta$ has $r + 1$ solutions for x_1 and the equation $x_0^{r+1} + \beta + 1 = 0$ has $r + 1$ solutions for x_0. So there are $(r - 2)(r - 1)^2$ k-rational points on C_1 with all coordinates different from zero. Summing up, we have the total number of k-rational points on C_1

$$|C_1(k)| = (r - 2)(r - 1)^2 = q\sqrt{q} + 1.$$

Example 1.16 (Klein Quartic). Consider the curve in $\mathbb{P}^2$ (over k) defined by the equation

$$C_2 : \qquad X_0^3 X_1 + X_1^3 X_2 + X_2^3 X_0 = 0. \tag{1.2}$$

The number of k-rational points on C_2 equals $q + 1$ for $q = 2, 4, 16, 32$. For $q = 8$ the number is 24.

Example 1.17. In $\mathbb{P}^2$ (over $\mathbb{F}_{q^2}$) we have the curve

$$C_3 : \qquad X_1^q X_2 + X_1 X_2^q = X_0^{q+1}. \tag{1.3}$$

Now, for any $x_0 \in \mathbb{F}_{q^2}$ the equation $x_1^q + x_1 = x_0^{q+1}$ has q solutions in $\bar{k}$. Let x_1 be one of these. We would like to show that $x_1 \in \mathbb{F}_{q^2}$, so we calculate

$$x_1^{q^2} + x_1^q = \left(x_1^q + x_1\right)^q = \left(x_0^{q+1}\right)^q = x_0^{q^2-1} x_0^{q+1} = x_0^{q+1} = x_1^q + x_1$$

to get $x_1^{q^2} = x_1$, hence $x_1 \in \mathbb{F}_{q^2}$. So the curve has exactly $q \cdot q^2 = q^3$ $\mathbb{F}_{q^2}$-rational points in the affine part $x_2 = 1$ of $\mathbb{P}^2$. Outside, i.e. for $x_2 = 0$, there is a single point $(0 : 1 : 0)$ on C_3. Hence the total number of $\mathbb{F}_{q^2}$-rational points on C_3 is $1 + q^3$.

Definition 1.18. A curve C is said to be *smooth in* $P \in C$ if the local ring $\bar{k}[V]_{\mathfrak{m}_P}$ is a discrete valuation ring. Then $\mathfrak{m}_P$ is a principal ideal and a generator of $\mathfrak{m}_P$ is called a *uniformising parameter*. C is *smooth* if it is smooth in all $P \in C$.

From now on we assume all curves to be smooth and projective unless otherwise stated.

Remark 1.19. Let $f_1, \ldots, f_m \in I$ be generators of the ideal defining the curve $C \subseteq \mathbb{P}^n$. C is smooth in $P \in C$ if and only if

$$\operatorname{rank} \begin{bmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix} = n - 1.$$

(See Remark A.9).

The ideal of the *tangent space to* V *in* $P = (a_1 : \ldots : a_n)$ is generated by

$$\left\{ \sum_{j=1}^{m} \frac{\partial f_i}{\partial x_j}(P)(X_j - a_j) \mid i = 1, \ldots, m \right\}.$$

Example 1.20. The curves in $\mathbb{P}^2$

$$\begin{aligned} C_1 : &\quad X_0^{r+1} + X_1^{r+1} + x_2^{r+1} = 0 \\ C_2 : &\quad X_0^3 X_1 + X_1^3 X_2 + X_2^3 X_0 = 0 \\ C_3 : &\quad X_1^q X_2 + X_1 X_2^q = X_0^{q+1} \end{aligned}$$

are all smooth.

Remark 1.21. Assume the curve $C \subseteq \mathbb{P}^n$ is smooth in $P \in C$. Let $H = V(h)$, $h \in \bar{k}[X_0, \ldots, X_n]$ be a hyperplane in $\mathbb{P}^n$ through P which does not contain the tangent to V in P. Then $h \in \mathfrak{m}_P \subseteq \bar{k}[V]_{\mathfrak{m}_P}$ is a uniformising parameter in P as $h \notin \mathfrak{m}_P^2$.

Remark 1.22. Let $C \subseteq \mathbb{P}^n$ be a curve over k defined by the ideal $I \subseteq \bar{k}[X_0, \ldots, X_n]$. For $f \in \bar{k}[X_0, \ldots, X_n]$ let $f^{(q)}$ be the polynomial obtained by raising the coefficients of f to q^{th} powers. Put

$$I^{(q)} = \text{ ideal generated by } \{f^{(q)} : f \in I\}$$

and let $C^{(q)}$ be the associated curve. There is natural morphism, the *q^{th}-power Frobenius morphism*, given by

$$\begin{aligned} \phi : C &\longrightarrow C \\ (x_0 : \ldots : x_n) &\longmapsto (x_0^q : \ldots : x_n^q). \end{aligned}$$

We must verify that ϕ actually maps C to $C^{(q)}$, so let $P = (x_0 : \ldots : x_n) \in C$, $f^{(q)} \in I^{(q)}$. Then

$$\begin{aligned} f^{(q)}(\phi((x_0 : \ldots : x_n))) &= f^{(q)}((x_0^q : \ldots : x_n^q)) \\ &= f((x_0 : \ldots : x_n))^q = 0 \end{aligned}$$

as $\mathrm{char}(k) = p$ and $P \in C$. As k is perfect $C^{(q)} \simeq C$, so we see that the k-rational points on C are exactly the fixed points under ϕ.

1.4 Divisors and the Riemann-Roch theorem

Definition 1.23. Let C be a curve defined over k. A *divisor* on C is a formal sum

$$D = \sum_{P \in X} n_P \cdot P \qquad\qquad P \in C; \quad n_P \in \mathbb{Z}$$

where finitely many n_P are non-zero. The collection of P's for which n_P is non-zero is called the *support* of D. The *degree* of a divisor D is given by

$$\deg(D) = \sum_{P \in X} n_P \deg(P)$$

where $\deg(P) = \min\{m \mid P \in C(\mathbb{F}_{q^m})\}$. Let $\mathrm{Div}(C)$ (resp. $\mathrm{Div}^0(C)$) be the divisors on C (resp. the divisors on C of degree zero). We have a partial ordering $\leq$ on $\mathrm{Div}(C)$ defined by

$$D \leq D' \;\Leftrightarrow\; n_P \leq n'_P \text{ for all } P \in C$$

for $D' = \sum n'_P \cdot P$.

$G = \mathrm{Gal}(\bar{k}/k)$ acts on $\mathrm{Div}(C)$ and $\mathrm{Div}^0(C)$ by

$$\sigma.D = \sum_{P \in X} n_P \cdot (\sigma.P). \qquad\qquad \sigma \in G$$

A divisor D is *defined over* k, if $\sigma.D = D$ for all $\sigma \in G$. The group of divisors defined over k are denoted $\mathrm{Div}_k(C)$ (resp. $\mathrm{Div}_k^0(C)$).

Definition 1.24. Let C be a curve defined over k and let $f \in \bar{k}(V) \setminus \{0\}$ be a rational function on C. Then the *divisor of* f is given by

$$\mathrm{div}(f) = \sum_{P \in X} \nu_P(f) \cdot P$$

where ν_P is the discrete valuation belonging to the discrete valuation ring $\bar{k}[C]_{\mathfrak{m}_P}$. Two divisors D and D' are *linearly equivalent* if the divisor $D - D'$ is a divisor of a rational

function. We usually write this as $D \sim D'$. If $\nu_P(f) = n > 0$, f is said to have a *zero* in P of order n and if $\nu_P(f) = m < 0$, f is said to have a *pole* in P of order m.

Let $D \in \mathrm{Div}(C)$. Introduce the notation

$$L(D) = \{f \in \bar{k}(V) \setminus \{0\} \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

and

$$\ell(D) = \dim_{\bar{k}} L(D).$$

If $D_0 = \sum_i n_{P_i} \cdot P_i - \sum_j m_{P_j} \cdot P_j$ $(n_{P_i}, m_{P_j} > 0)$ we may thus identify $L(D_0)$ with the vector space of rational functions on C with poles only in the points P_i and there of order no more than n_{P_i} and with zeros in P_j with multiplicity at least m_{P_j}.

Proposition 1.25. *Let C be a curve defined over k and let $D \in \mathrm{Div}_k(C)$. The vector space $L(D)$ has a $\bar{k}$-basis of functions in $k(C)$.*

Proof. Let $f \in L(D)$ be arbitrary. It will suffice to show that f is a $\bar{k}$-linear combination of vectors in $k(C)$. There exists a minimal n such that $f \in \mathbb{F}_{q^n}(C) \cap L(D)$. Pick a basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathbb{F}_{q^n}$ over k. Put

$$w_i = \sum_{k=0}^{n-1} \sigma^k(\alpha_i)\sigma^k(f) \qquad i = 1, \ldots, n$$

where σ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Then $w_i \in k(C)$ for all i as $\sigma(w_i) = w_i$ $(\sigma^n = \mathrm{id})$. We have the identity

$$\begin{bmatrix} \alpha_1 & \ldots & \sigma^{n-1}(\alpha_1) \\ \vdots & \ddots & \vdots \\ \alpha_n & \ldots & \sigma^{n-1}(\alpha_n) \end{bmatrix} \begin{bmatrix} f \\ \vdots \\ \sigma^{n-1}(f) \end{bmatrix} = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$$

and as the matrix represents the automorphism $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ in the base $\{\alpha_1, \ldots, \alpha_n\}$ it is invertible, hence f may be written uniquely as a linear combination of the w_i's. □

Remark 1.26. By introducing the notation

$$L_k(D) = \{f \in k(V) \setminus \{0\} \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

and

$$\ell_k(D) = \dim_k L_k(D),$$

Proposition 1.25 gives us that

$$\ell_k(D) = \dim_k L_k(D) = \dim_{\bar{k}} L(D) = \ell(D).$$

Theorem 1.27 (Riemann-Roch). *Let C be a curve defined over k. There exists a divisor $K \in \mathrm{Div}_k(C)$ and an integer $g \geq 0$ (the genus of C) such that*

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g \tag{1.4}$$
$$\ell_k(D) - \ell_k(K - D) = \deg(D) + 1 - g. \tag{1.5}$$

Proof. Combine Theorem A.17 with Remark 1.26. □

Corollary 1.28. *With assumptions as above, we have*

a) $\ell(K) = g$

b) $\deg(K) = 2g - 2$.

c) If $\deg(D) > 2g - 2$, *we have* $\deg(K - D) < 0$ *and*

$$\ell(D) = \deg(D) + 1 - g.$$

Proof. See Corollary A.18. □

Proposition 1.29. *Let $C \subseteq \mathbb{P}^2$ be a (smooth) curve of degree d. Then the genus g of C is given by the formula*

$$g = \frac{1}{2}(d-1)(d-2).$$

Proof. See Proposition A.19. □

Chapter 2

The Zeta function

So that no confusion arises, we repeat the assumption that all curves are smooth and projective.

2.1 Introduction

Let $C \subseteq \mathbb{P}^n$ be a curve defined over $k(= \mathbb{F}_q)$ and let N_m denote the number of $\mathbb{F}_{q^m}$-rational points on C. When we just consider the number of $\mathbb{F}_q$-rational points, we usually write N.

Definition 2.1. *The Zeta function of C over k* is the formal power series

$$Z(t, C/k) = \exp\Big(\sum_{m=1}^{\infty} N_m \frac{t^m}{m} \Big).$$

We see that $Z(t, C/k)$ stores information on the number of $\mathbb{F}_{q^m}$-rational points on C for all $m \geq 1$.

Remark 2.2. As $C \subseteq \mathbb{P}^n$, N_m is less than or equal to the number of $\mathbb{F}_{q^m}$-rational points $\mathbb{P}^n$, that is

$$N_m \leq \frac{q^{mn} - 1}{q^m - 1} < (n+1)q^{mn}$$

by Remark 1.8. So for $m \geq n+1$ we have $\frac{N_m}{m} < q^{mn}$ and the series

$$\sum_{m=1}^{\infty} N_m \frac{t^m}{m}$$

has radius of convergence q^{-n} which makes $Z(t, C/k)$ an analytic function on the open disc with this radius. We also notice that the logarithmic derivative of $Z(t, C/k)$ is

$$\frac{d}{dt}\big(\ln(Z(t, C/k))\big) = \frac{Z(t, C/k)'}{Z(t, C/k)} = \sum_{m=1}^{\infty} N_m t^{m-1} \tag{2.1}$$

so we may recover the N_m as

$$N_m = \frac{1}{(m-1)!}\Big(\frac{d^m}{dt^m}\ln(Z(t,C/k))\Big)\big|_{t=0}.$$

Remark 2.3. The Zeta function may be defined for arbitrary smooth projective varieties, and was originally defined so by Weil in [Wei49]. In this paper Weil conjectured some remarkably properties of the Zeta function, the Weil conjectures. Quickly after this, Weil himself settled the matters in the case of curves (see Appendix C for his proof), but the general case was unsolved until 1974, where Deligne in [Del74] by means of the 'new' Algebraic Geometry finally resolved the question.

Theorem 2.4 (Weil Conjectures for curves). *Let C be a curve defined over k of genus g and let $Z(t,C/k)$ be its associated Zeta function.*

Rationality: *The Zeta function may be written as*

$$Z(t,C/k) = \frac{P(t)}{(1-t)(1-qt)} \tag{2.2}$$

where $P(t) \in \mathbb{Z}[t]$ is of degree $2g$.

Functional equation: *The Zeta function satisfies the functional equation*

$$Z\big(\tfrac{1}{qt},C/k\big) = q^{1-g}t^{2-2g}Z(t,C/k). \tag{2.3}$$

The Riemann hypothesis: *The polynomial $P(t)$ may be factored as*

$$P(t) = \prod_{i=1}^{2g}(1-\alpha_i t) \qquad \textit{where} \qquad |\alpha_i|^2 = q \textit{ for all } i. \tag{2.4}$$

Before proving the theorem, we derive some corollaries.

Corollary 2.5. *With the notation above, we have*

$$N_m = 1 + q^m - \sum_{i=1}^{2g}\alpha_i^m. \tag{2.5}$$

Proof. By taking the logarithmic derivative of

$$Z(t,C/k) = \frac{\prod_{i=1}^{2g}(1-\alpha_i t)}{(1-t)(1-qt)}$$

(2.1) gives us that

$$\sum_{m=1}^{\infty} N_m t^{m-1} = \frac{1}{1-t} + \frac{q}{1-qt} + \sum_{i=1}^{2g} \frac{-\alpha_i}{1-\alpha_i t}$$
$$= \sum_{i=1}^{2g} \Big(-\sum_{m=0}^{\infty} \alpha_i^{m+1} t^m \Big) + \sum_{m=0}^{\infty} q^{m+1} t^m + \sum_{m=0}^{\infty} t^m.$$

Now compare coefficients. □

Corollary 2.6 (Weil bound). *Let C be a curve of genus g defined over k. Then the number N_m of $\mathbb{F}_{q^m}$-rational points on C is bounded by*

$$|N_m - 1 + q^m| \leq 2g\, q^{\frac{m}{2}}. \tag{2.6}$$

Proof. From Corollary 2.5 we have

$$|N_m - 1 + q^m| = \Big| \sum_{n=1}^{2g} \alpha_i^m \Big| \leq 2g |\alpha_i|^m = 2g\, q^{\frac{m}{2}},$$

the last equality coming from Theorem 2.4. □

Remark 2.7. This bound may in most situations be improved considerably. See Appendix B for an introduction to these techniques.

Example 2.8. Consider the elliptic (genus $g = 1$) curve C in $\mathbb{P}^2$ defined over $\mathbb{F}_2$ by the equation

$$X_0^3 + X_1^3 + X_2^3 = 0.$$

It is easily verified that the curve has $\mathbb{F}_2$-rational points $\{(0:1:1), (1:1:0), (1:0:1)\}$, that is $N_1 = 3$ and granting the theorem, the Zeta function may then be written as

$$3 = N_1 = \frac{d}{dt} \ln(Z(t, C/\mathbb{F}_2))\big|_{t=0} = \Big[\tfrac{a+4t}{1+at+2t^2} + \tfrac{1}{1-t} + \tfrac{2}{1-2t} \Big]_{t=0}.$$

Hence $a = 0$ and

$$P(t) = 1 + 2t^2 = (1 - i\sqrt{2}t)(1 + i\sqrt{2}t).$$

Now Corollary 2.5 implies $N_m = 1 + 2^m - (i\sqrt{2})^m - (-i\sqrt{2})^m$ and thereby

$$N_m = \begin{cases} 1 + 2^m & m \equiv 1 \mod 2 \\ 1 + 2^m + 2(\sqrt{2})^m & m \equiv 2 \mod 4 \\ 1 + 2^m - 2(\sqrt{2})^m & m \equiv 0 \mod 4 \end{cases}$$

Example 2.9. The curve from Example 1.17

$$C: \qquad X_1^q X_2 + X_1 X_2^q = X_0^{q+1}$$

defined over $\mathbb{F}_{q^2}$ has genus $g = \frac{1}{2}(q-1)q$ by Proposition 1.29 and the number of $\mathbb{F}_{q^2}$-rational points was found to be at least

$$1 + q^3 = 1 + q^2 + 2g\,q,$$

hence the maximal allowed by the Weil bound, so C has exactly $1 + q^3$ $\mathbb{F}_{q^2}$-rational points. With the usual notation we then have $N_2 = 1 + q^2 + 2gq$, which substituted into Corollary 2.5 gives

$$2g\,q = -\sum_{i=1}^{2g} \alpha_i^2.$$

This forces $\alpha_i = \sqrt{-q}$, hence

$$N_m = 1 + q^m - i^m(\sqrt{q})^m - (-i)^m(\sqrt{q})^m$$

and thereby

$$N_m = \begin{cases} 1 + q^m & m \equiv 1 \mod 2 \\ 1 + q^m + 2g(\sqrt{q})^m & m \equiv 2 \mod 4 \\ 1 + 2^m - 2g(\sqrt{q})^m & m \equiv 0 \mod 4 \end{cases}$$

In particular, C has the maximal number of $\mathbb{F}_{q^m}$-rational points allowed by the Weil bound whenever $m \equiv 2 \mod 4$. The existence of a curve with this genus and number of $\mathbb{F}_{q^2}$-rational points was only recently shown in [Han92, Prop. 3.2] and shortly after the equation for it given above was found in [HP93].

Example 2.10 (Elliptic curves over $\mathbb{F}_2$). An elliptic curve (genus $g = 1$) defined over $\mathbb{F}_2$ has an equation on Weierstrass form [Har77, IV.4.6]

$$X_1^2 X_2 + a_1 X_0 X_1 X_2 + a_3 X_1 X_2^2 - X_0^3 - a_2 X_0^2 X_2 - a_4 X_0 X_2^2 - a_6 X_2^3 = 0$$

where $a_i \in \mathbb{F}_2$. Obviously there are 32 possible equations, but 16 of these are discarded for now since they give singular curves. The remaining 16 can by elementary changes of coordinates be reduced to the following types

$$\begin{aligned}
&\text{Type 1}: && X_2 X_1^2 + X_2^2 X_1 = X_0^3 + X_0^2 X_2 + X_2^3 \\
&\text{Type 2}: && X_1^2 X_2 + X_0 X_1 X_2 = X_0^3 + X_0^2 X_2 + X_0 X_2^2 \\
&\text{Type 3}: && X_1^2 X_2 + X_1 X_2^2 = X_0^3 \\
&\text{Type 4}: && X_1^2 X_2 + X_0 X_1 X_2 = X_0^3 + X_0 X_2^2 \\
&\text{Type 5}: && X_1^2 X_2 + X_1 X_2^2 = X_0^3 + X_0^2 X_2.
\end{aligned}$$

The number of $\mathbb{F}_2$-rational points for type 1,2,3,4,5 are 1,2,3,4,5 respectively. As in Example 2.9 we determine the associated Zeta functions

$$\begin{array}{lll}
\text{Type 1}: & X_2X_1^2 + X_2^2X_1 = X_0^3X_0^2X_2 + X_2^3 & \dfrac{1-2t+2t^2}{(1-t)(1-2t)} \\
\text{Type 2}: & X_1^2X_2 + X_0X_1X_2 = X_0^3 + X_0^2X_2 + X_0X_2^2 & \dfrac{1+2t^2}{(1-t)(1-2t)} \\
\text{Type 3}: & X_!^2X_2 + X_1X_2^2 = X_0^3 & \dfrac{1+t+2t^2}{(1-t)(1-2t)} \\
\text{Type 4}: & X_1^2X_2X_0X_1X_2 = X_0^3 + X_0X_2^2 & \dfrac{1+2t+2t^2}{(1-t)(1-2t)} \\
\text{Type 5}: & X_1^2X_2 + X_1X_2^2 = X_0^3X_0^2X_2 & \dfrac{1-2t+2t^2}{(1-t)(1-2t)}
\end{array}$$

One may then from the Zeta functions calculate the number of $\mathbb{F}_{2^r}$-rational points on the curves and compare them to the Weil-bound.

As the curves have different numbers of $\mathbb{F}_2$-rational points they are not isomorphic over $\mathbb{F}_2$. In contrast to this, the substitution

$$\begin{aligned}
X_1 &= X_1' + X_0' + \beta X_2' \\
X_0 &= X_0' + X_2' \\
X_2 &= X_2'
\end{aligned}$$

where $\beta \in \mathbb{F}_{2^2}$ is determined by $\beta^2 + \beta + 1 = 0$, defines an isomorphism (over $\mathbb{F}_{2^2}$) between type 5 and type 1 curves. In the same way, the curves of type 4 and type 2 are isomorphic over $\mathbb{F}_{2^2}$ by the substitution

$$\begin{aligned}
X_1 &= X_1' + \beta X_0' \\
X_0 &= X_0' \\
X_2 &= X_2'
\end{aligned}$$

with β as above. One may also show that the type 5 curve is isomorphic to the type 3 curve over $\mathbb{F}_{2^8}$. So the five types of elliptic curves over $\mathbb{F}_2$ divide into two isomorphism classes over $\overline{\mathbb{F}}_2$ – but the 5 curves has different Zeta functions and thereby different arithmetic properties.

Example 2.11 (Klein Quartic). Consider the curves in $\mathbb{P}^2$ defined over $\mathbb{F}_2$ by the equations

$$\begin{array}{ll}
\text{C 1}: & X_0^3X_1 + X_1^3X_2 + X_2^3X_0 = 0 \\
\text{C 2}: & X_0^4 + X_1^4 + X_2^4 + X_0^2X_1^2 + X_0^2X_2^2 + X_1^2X_2^2 + \\
 & \qquad X_0^2X_1X_2 + X_0X_1^2X_2 + X_0X_1X_2^2 = 0
\end{array}$$

Both curves are smooth of degree 4 and therefore by Proposition 1.29 they both have genus $g = 3$. The associated Zeta functions may be calculated

$$C_1 : \qquad Z(t, C_1/\mathbb{F}_2) = \frac{1 + 5t^3 + 8t^6}{(1-t)(1-2t)}$$
$$C_2 : \qquad Z(t, C_2/\mathbb{F}_2) = \frac{1 - 3t + 9t^2 - 13t^3 + 18t^4 - 12t^5 + 8t^6}{(1-t)(1-2t)}$$

We notice that C_1 and C_2 are non-isomorphic over $\mathbb{F}_2$. By calculating N_m recursively for C_1 one finds, that for $m \not\equiv 0 \pmod 3$, $N_m = 1 + 2^m$.

Example 2.12 (Non-isomorphic curves with the same Zeta function). In $\mathbb{P}^2$ we have the elliptic curves defined over $\mathbb{F}_{11}$ by the equations

$$C_1 : \qquad X_1^2 X_2 = X_0^3 - X_0 X_2^2$$
$$C_2 : \qquad X_1^2 X_2 = X_0^3 - X_2^3$$

Both C_1 and C_2 are smooth curves of genus 1 and a straightforward calculation shows that the number of $\mathbb{F}_{11}$-rational points is $1 + 11 = 12$ for both curves. As in Example 2.8 we then find the common Zeta function

$$Z(t, C_1/\mathbb{F}_{11}) = Z(t, C_2/\mathbb{F}_{11}) = \frac{1 + 11t^2}{(1-t)(1-11t)}. \tag{2.7}$$

By [Har77, IV.4.1] the isomorphism class of an elliptic curve is determined by its *j-invariant*

$$j(C) = \frac{1728\ 4a^3}{4a^3 + 27b^2} \tag{2.8}$$

for a curve $C \subseteq \mathbb{P}^2$ with equation

$$X_1^2 X_2 = X_0^3 + aX_0 X_2^2 + bX_2^3. \tag{2.9}$$

We find that $j(C_1) = 1$ and $j(C_2) = 0$ that is, the curves are **not** isomorphic over $\overline{\mathbb{F}}_{11}$ despite having the same Zeta function.

Example 2.13 (Two singular curves). Consider the curves in $\mathbb{P}^2$ defined over $\mathbb{F}_2$ by the equations

$$C_1 : \qquad X_0(X_1 + X_2)^2 + X_1^2 X_2 = 0$$
$$C_2 : \qquad X_0 X_1 X_2 + X_1^3 + X_2^3 = 0$$

The curves are smooth except in the point $P_0 = (1 : 0 : 0)$, where they both have a singularity. The curves are both birational to $\mathbb{P}^1$, hence of genus 0. By calculating the solutions to the

equations directly, we get the following table, where we compare the number of solutions to the number of rational points on $\mathbb{P}^1$.

r	$N_r(C_1)$	$N_r(C_2)$	$N_r(\mathbb{P}^1)$
1	3	2	3
2	5	4	5
3	5	4	5
4	17	16	17
5	33	32	32

It seems that C_2 'lacks' a rational point compared to C_1 and $\mathbb{P}^1$. For an explanation of this, we examine the curves in the affine part $X_0 = 1$, where they have affine equations

$$\begin{aligned} C_1 : &\quad (X_1 + X_2)^2 + X_1^2 X_2 = 0 \\ C_2 : &\quad X_1 X_2 + X_1^3 + X_2^3 = 0 \end{aligned}$$

We see that C_1 has a cusp in P_0, i. e. the tangent cone (with equation $(X_1 + X_2)^2 = 0$) is a doubled line L_1. Conversely, C_2 has a node in P_0, i. e. the tangent cone of C_2 in P_0 (given by the equation $X_1 X_2 = 0$) consists of two distinct lines L_2 og L_3.

Now the projection from P_0 of C_i to $\mathbb{P}^1$ gives birational maps

$$\pi_i : C_i \to \mathbb{P}^1$$

which give rise to bijective maps

$$\begin{aligned} \pi_1 : C_1(\mathbb{F}_{2^r}) \setminus \{P_0\} &\longrightarrow \mathbb{P}^1(\mathbb{F}_{2^r}) \setminus \{P_1\} \\ \pi_2 : C_2(\mathbb{F}_{2^r}) \setminus \{P_0\} &\longrightarrow \mathbb{P}^1(\mathbb{F}_{2^r}) \setminus \{P_2, P_3\} \end{aligned} \tag{2.10}$$

where P_1, P_2 and P_3 are the points in $\mathbb{P}^1$ corresponding to the lines L_i. This explains 'the missing point'.

2.2 Basic properties of the Zeta function

Definition 2.14. A *prime divisor on* C is a divisor $\mathcal{P} \in \mathrm{Div}_k(C)$ which may be written as

$$\mathcal{P} = P + \sigma.P + \ldots + \sigma^{n-1}.P$$

where n is minimal with the property $P \in \mathbb{F}_{q^n}$ and σ is a generator of the cyclic Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/k)$. Let a_d denote the number of prime divisors on C of degree d.

Remark 2.15. If $P \in C$ is rational over $\mathbb{F}_{q^n}$ and if $d|n$ there exists a $\tau \in \mathrm{Gal}(\mathbb{F}_{q^d}/k)$ such that $\tau^d = \mathrm{id}$. Then

$$P + \tau.P + \ldots + \tau^{d-1}.P$$

defines a unique prime divisor of degree d with d $\mathbb{F}_{q^n}$-rational points in its support.

Lemma 2.16. *As usual, let N_m denote the number of $\mathbb{F}_{q^m}$-rational points on C. Then*

$$N_m = \sum_{d|m} d\, a_d. \tag{2.11}$$

Proof. This is a trivial consequence of Remark 2.15. □

Proposition 2.17. *$Z(t, C/k)$ may be written as*

$$Z(t, C/k) = \prod_{\substack{\mathcal{P} \\ \text{prime divisor}}} \Big(\frac{1}{1 - t^{\deg(\mathcal{P})}}\Big). \tag{2.12}$$

Proof. The right hand side equals

$$\prod_{m=1}^{\infty} \Big(\frac{1}{1 - t^m}\Big)^{a_m}$$

which has logarithmic derivative

$$\frac{1}{t} \sum_{m=1}^{\infty} \Big(\frac{m a_m t^m}{1 - t^m}\Big) = \frac{1}{t} \sum_{m=1}^{\infty} \Big(\sum_{d|m} d\, a_d\Big) t^m$$

where the last equality comes from expanding the denominator in a geometric series and finding the coefficient to t^m. Now, since the sum in the parenthesis equals N_m, we just have to compare with Remark 2.2. □

Proposition 2.18. *With notation as above, we have*

$$\prod_{\substack{\mathcal{P} \\ \text{prime divisor}}} \Big(\frac{1}{1 - t^{\deg(\mathcal{P})}}\Big) = \sum_{\substack{D \in \mathrm{Div}_k(C) \\ D \geq 0}} t^{\deg(D)}. \tag{2.13}$$

Proof. As any divisor $D \in \mathrm{Div}_k(C)$, $D \geq 0$ may be written uniquely as

$$D = i_1 \mathcal{P}_1 + \ldots + i_s \mathcal{P}_s$$

where the P_j are prime divisors, the coefficient to t^m on the right hand side is given by the number of tuples of prime divisors $\mathcal{P}_1, \mathcal{P}_2, \ldots$, such that $\sum_i \deg(\mathcal{P}_i) = m$. But as

$$\frac{1}{1 - t^{\deg(\mathcal{P})}} = 1 + t^{\deg(\mathcal{P})} + t^{2\deg(\mathcal{P})} + \ldots$$

the coefficients to t^m are the same on both sides in the equation. □

Definition 2.19. Let A_m denote the number of positive rational divisors on C of degree m

$$A_m = |\{D \in \mathrm{Div}_k(C) : D \geq 0 \text{ and } \deg(D) = m\}|.$$

Proposition 2.20. *With notation as above*

$$Z(t, C/k) = \sum_{n=1}^{\infty} A_m t^m. \tag{2.14}$$

Proof. Combine Proposition 2.17 and Proposition 2.18. □

Notation 2.21.

a) Let the subgroup $\delta\mathbb{Z} \leq \mathbb{Z}$ ($\delta > 0$) denote the image of the degree map

$$\deg : \mathrm{Div}_k(C) \longrightarrow \mathbb{Z}$$

which is a homomorphism of groups.

b) Fix a divisor $D_0 \in \mathrm{Div}_k(C)$ of degree δ.

c) Choose $\nu \in \mathbb{N}$ such that

$$(\nu - 1)\delta < g \leq \nu\delta$$

where g is the genus of C.

d) Let $\{D_1, \ldots, D_h\}$ be a maximal set of positive non-equivalent divisors in $\mathrm{Div}_k(C)$ of degree $\nu\delta$.

e) Choose according to Theorem 1.27 a canonical divisor $K \in \mathrm{Div}_k(C)$. As $\deg(K) = 2g-2$ we may choose $\mu \in \mathbb{N}$ such that $\mu\delta = 2g - 2$.

Lemma 2.22. *Let $D \in \mathrm{Div}_k(C)$ be of degree $\nu\delta$. There exists a unique i ($1 \leq i \leq h$) such that D is linearly equivalent to D_i.*

Proof. According to Theorem 1.27

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

which gives the existence of a non-zero rational function f such that

$$\mathrm{div}(f) + D \geq 0.$$

By Proposition 1.25 we may assume $f \in k(C)$. Then

$$\mathrm{div}(f) + D \in \mathrm{Div}_k(C)$$

and by maximality of the set $\{D_1, \ldots, D_h\}$ we have $D \sim D_i$ for some $1 \leq i \leq h$. The uniqueness follows from the maximality of $\{D_1, \ldots, D_h\}$ and the transitivity of $\sim$. □

Lemma 2.23. *Let $D \in \mathrm{Div}_k(C)$ be of degree $n\delta$. There exists a unique i $(1 \leq i \leq h)$ such that D is linearly equivalent to $(n-\nu)D_0 + D_i$.*

Proof. If $\deg(D) = n\delta$ the divisor $D-(n-\nu)D_0 \in \mathrm{Div}_k(C)$ is of degree $\nu\delta$. Now Lemma 2.22 gives a unique i such that $D-(n-\nu)D_0 \sim D_i$ or equivalently, $D \sim (n-\nu)D_0 + D_i$. □

Proposition 2.24. *With the notation above, the Zeta function may be written as*

$$Z(t, C/k) = \sum_{n=0}^{\infty} \Big(\sum_{i=1}^{h} \frac{q^{\ell(D_i+(n-\nu)D_0)} - 1}{q-1} \Big) t^{n\delta}. \tag{2.15}$$

Proof. By definition of $\ell(D)$, the number of positive divisors linearly equivalent to D is $\frac{q^{\ell(D)}-1}{q-1}$ (cf. Remark A.12). So by Lemma 2.23 the sum in parenthesis equals $A_{n\delta}$, the number of positive rational divisors of degree $n\delta$. By choice of δ, all positive rational divisors has degree in the ideal $\delta\mathbb{Z}$, so by Proposition 2.20 we are done. □

2.3 Functional equation and Rationality

Notation 3.25. Introduce the notation

$$\begin{aligned} Z_1(t) &= \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(D_i+(n-\nu)D_0)} - 1}{q-1} t^{n\delta} \\ Z_2(t) &= Z(t, C/k) - Z_1(t). \end{aligned} \tag{2.16}$$

Lemma 2.26. *With this, we have*

$$\begin{aligned} Z_2(t) &= \sum_{i=1}^{h} \sum_{n+\mu+1}^{\infty} \frac{q^{\ell(D_i+(n-\nu)D_0)} - 1}{q-1} t^{n\delta} - \frac{h}{q-1} \sum_{n=0}^{\infty} t^{n\delta} \\ &= \frac{h}{q-1} \Big(\frac{q^{1-g}(qt)^{(\mu+1)\delta}}{1-(qt)^{\delta}} - \frac{1}{1-t^{\delta}} \Big). \end{aligned} \tag{2.17}$$

Proof.

$$\begin{aligned} Z_2(t) &= Z(t, C/k) - Z_1(t) \\ &= \sum_{n=0}^{\infty} \sum_{i=1}^{h} \frac{q^{\ell(D_i+(n-\nu)D_0)} - 1}{q-1} t^{n\delta} \; - \; \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(D_i+(n-\nu)D_0)}}{q-1} t^{n\delta} \\ &= \sum_{i=1}^{h} \sum_{n+\mu+1}^{\infty} \frac{q^{\ell(D_i+(n-\nu)D_0)}}{q-1} t^{n\delta} \; - \; \frac{h}{q-1} \sum_{n=0}^{\infty} t^{n\delta}. \end{aligned}$$

Now, notice that for $n > \mu$ we have

$$\deg(D_i + (n-\nu)D_0) = n\delta > \mu\delta = 2g-2.$$

Hence for $n > \mu$,

$$\ell(D_i + (n-\nu)D_0) = \deg(D_i + (n-\nu)D_0) + 1 - g = n\delta + 1 - g$$

by Corollary 1.28 c). Then

$$\begin{aligned}
Z_2(t) &= \sum_{i=1}^{h} \sum_{n+\mu+1}^{\infty} \frac{q^{n\delta+1-g}}{q-1}\, t^{n\delta} \;-\; \frac{h}{q-1} \sum_{n=0}^{\infty} t^{n\delta} \\
&= \sum_{i=1}^{h} \sum_{n+\mu+1}^{\infty} \frac{q^{1-g}}{q-1}\, (qt)^{n\delta} \;-\; \frac{h}{q-1} \sum_{n=0}^{\infty} t^{n\delta} \\
&= \frac{hq^{1-g}}{q-1} \sum_{n+\mu+1}^{\infty} (qt)^{n\delta} \;-\; \frac{h}{q-1} \sum_{n=0}^{\infty} t^{n\delta} \\
&= \frac{h}{q-1} \Big(\frac{q^{1-g}(qt)^{(\mu+1)\delta}}{1-(qt)^{\delta}} \;-\; \frac{1}{1-t^{\delta}} \Big)
\end{aligned}$$

the last equality coming from the geometric series. □

Proposition 2.27. *$Z_2(t)$ satisfies the functional equation*

$$Z_2\big(\tfrac{1}{qt}\big) = q^{1-g} t^{2-2g} Z_2(t).$$

Proof. According to Lemma 2.26 we get

$$\begin{aligned}
Z_2\big(\tfrac{1}{qt}\big) &= \frac{h}{q-1} \left(\frac{q^{1-g}\big(q\,\frac{1}{qt}\big)^{(\mu+1)\delta}}{1-\big(q\,\frac{1}{qt}\big)^{\delta}} - \frac{1}{1-\big(\frac{1}{qt}\big)^{\delta}} \right) \\
&= \frac{h}{q-1} \left(\frac{q^{1-g} t^{2-2g} \big(\frac{1}{t}\big)^{\delta}}{1-\frac{1}{t}} - \frac{1}{1-\big(\frac{1}{qt}\big)^{\delta}} \right) \\
&= \frac{h}{q-1} \left(\frac{q^{1-g} t^{2-2g} \big(\frac{1}{t}\big)^{\delta}}{t^{\delta}-1} - \frac{(qt)^{\delta}}{(qt)^{\delta}-1} \right) \\
&= \frac{h}{q-1} \left(\frac{q^{1-g} t^{2-2g}}{t^{\delta}-1} - \frac{(qt)^{-\mu\delta}(qt)^{(\mu+1)\delta}}{(qt)^{\delta}-1} \right) \\
&= \frac{h}{q-1} \left(\frac{q^{1-g} t^{2-2g}}{t^{\delta}-1} - \frac{q^{1-g} q^{1-g} t^{2-2g} (qt)^{(\mu+1)\delta}}{(qt)^{\delta}-1} \right) \\
&= q^{1-g} t^{2-2g} Z_2(t)
\end{aligned}$$

since μ was chosen such that $\mu\delta = 2g-2$. □

Lemma 2.28. *Let K denote the canonical divisor on C. Then*

$$K - (D_i + (n-\nu)D_0) \qquad i = 1, \ldots, h$$

represent the equivalence classes of divisors of degree $(n-\nu)\delta$.

Proof. If D is a divisor of degree $n\delta$, $K - D$ is of degree $(n-\nu)\delta$. Now D is equivalent to D' if and only if $K - D$ is equivalent to $K - D'$ and as

$$D_i + (n-\nu)D_0 \qquad i = 1, \ldots, h$$

represent the equivalence classes of divisors of degree $n\delta$ (Lemma 2.23),

$$K - (D_i + (n-\nu)D_0) \qquad i = 1, \ldots, h$$

represent the equivalence classes of divisors of degree $(n-\nu)\delta$. □

Lemma 2.29.

$$Z_1(t) = \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(K-(D_i+(n-\nu)D_0))}}{q-1}\, t^{(\mu-n)\delta}.$$

Proof. Reverse the summation order in the definition of $Z_1(t)$. □

Proposition 2.30. *$Z_1(t)$ satisfies the functional equation*

$$Z_1\left(\tfrac{1}{qt}\right) = q^{1-g} t^{2-2g} Z_1(t).$$

Proof. By Lemma 2.29

$$Z_1\left(\tfrac{1}{qt}\right) = \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(K-(D_i+(n-\nu)D_0))}}{q-1} \left(\tfrac{1}{qt}\right)^{(\mu-n)\delta}$$

and by Theorem 1.27 we have

$$\begin{aligned} \ell(K - (D_i + (n-\nu)D_0)) + 1 - g &= \ell(D_i - (n-\nu)D_0) - \deg(D_i - (n-\nu)D_0) \\ &= \ell(D_i - (n-\nu)D_0) - n\delta. \end{aligned}$$

Hence

$$\begin{aligned} Z_1\left(\tfrac{1}{qt}\right) &= \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(D_i-(n-\nu)D_0)-n\delta+g-1}}{q-1} \left(\tfrac{1}{qt}\right)^{(\mu-n)\delta} \\ &= \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(D_i-(n-\nu)D_0)}}{q-1} \frac{q^{-n\delta+g-1}}{q^{(\mu-n)\delta}}\, t^{n\delta} t^{-\mu\delta} \\ &= \sum_{i=1}^{h} \sum_{n=0}^{\mu} \frac{q^{\ell(D_i-(n-\nu)D_0)}}{q-1}\, t^{n\delta}\, \frac{q^{g-1}}{q^{2g-2}}\, t^{2-2g} \\ &= q^{1-g} t^{2-2g} Z_1(t). \end{aligned}$$

□

Remark 2.31. This concludes the proof of the functional equation of $Z(t, C/k)$

$$Z\left(\tfrac{1}{qt}, C/k\right) = q^{1-g}t^{2-2g}Z(t, C/k). \tag{2.18}$$

By construction $Z_1(t)$ is a polynomial and by Lemma 2.26 $Z_2(t)$ is a rational function. So the Zeta function is a rational function with poles in the roots of the polynomials $1-(qt)^\delta$ and $1-t^\delta$.

Lemma 2.32. *We have the following identity*

$$Z(t^d, C/\mathbb{F}_{q^d}) = \prod_{\epsilon^d=1} Z(\epsilon t, C/\mathbb{F}_q). \tag{2.19}$$

Proof. By definition, the right-hand side equals

$$\exp\left(\sum_{m=1}^{\infty} N_m \frac{t^m}{m} \sum_{\epsilon^d=1} \epsilon^m\right)$$

which, since

$$\sum_{\epsilon^d=1} \epsilon^m = \begin{cases} 0 & d \nmid m \\ d & d \mid m \end{cases}$$

also may be put as

$$\exp\left(\sum_{m=1}^{\infty} N_{md} \frac{t^{md}}{md}\right).$$

But this equals $Z(t^d, C/\mathbb{F}_{q^d})$. □

Theorem 2.33. *The Zeta function $Z(t, C/k)$ may be written as*

$$Z(t, C/k) = \frac{P(t)}{(1-t)(1-qt)}$$

with $P(t) \in \mathbb{Z}[t]$ of degree $2g$.

Proof. By (2.16) and (2.17)

$$Z(t, C/k) = \frac{P(t)}{(1-t^\delta)(1-(qt)^\delta)}$$

for some $P(t) \in \mathbb{Z}[t]$. By (2.17) $Z_2(t)$ has a pole of order one (simple pole) in those ϵ for which $\epsilon^\delta = 1$. As $Z_1(t)$ is a polynomial $Z(t, C/k)$ then has a simple pole in those ϵ for which

$\epsilon^\delta = 1$. In particular $Z(t^\delta, C/\mathbb{F}_{q^\delta})$ has a simple pole in $t^\delta = 1$. Now we use Lemma 2.32 with $d = \delta$ to get

$$Z(t^\delta, C/\mathbb{F}_{q^\delta}) = \prod_{\epsilon^\delta=1} \frac{P(\epsilon t)}{(1-(\epsilon t)^\delta)(1-(\epsilon tq)^\delta)} = \frac{\prod_{\epsilon^\delta=1} P(\epsilon t)}{(1-t^\delta)^\delta (1-(tq)^\delta)^\delta}.$$

From this it follows that $Z(t^\delta, C/\mathbb{F}_{q^\delta})$ has a pole of order δ in $t^\delta = 1$. But we already knew that $Z(t^\delta, C/\mathbb{F}_{q^\delta})$ had a simple pole in $t^\delta = 1$, hence $\delta = 1$.

Finally, by (2.16) and (2.17)

$$Z(t, C/k) = Z_1(t) + Z_2(t) = Z_1(t) + \frac{h}{q-1}\Big(\frac{q^{1-g}(qt)^{\mu+1}}{1-qt} - \frac{1}{1-t}\Big)$$

where $Z_1(t)$ is a polynomial of degree $\mu = 2g-2$, hence $P(t)$ is of degree $2g$. □

Proposition 2.34. *The polynomial $P(t) \in \mathbb{Z}[t]$ in Theorem 2.33 may be factored as*

$$P(t) = \prod_{i=1}^{2g} (1 - \alpha_i t).$$

Proof. $Z(0, C/k) = \mathrm{e}^0 = 1$ hence $P(0) = 1$, so 0 is not a root in $P(t)$. □

Corollary 2.35. *The α_i may be renumbered such that*

$$\alpha_i \, \alpha_{2g-i} = q \qquad\qquad i = 1, \ldots, g.$$

Proof. From the functional equation (2.18)

$$\frac{\prod_i \big(1 - \alpha_i \frac{1}{qt}\big)}{\big(1-\frac{1}{qt}\big)\big(1-q\frac{1}{qt}\big)} = q^{1-g} t^{2-2g} \frac{\prod_i (1-\alpha_i t)}{(1-t)(1-qt)}$$

hence

$$q^g t^2 \prod_i (1 - \tfrac{\alpha_i}{q}) = \prod_i \alpha_i \big(\tfrac{1}{\alpha_i} - 1\big).$$

By pairing the roots of the two polynomials, we see that after a suitable renumbering, we have $\dfrac{\alpha_i}{q} = \dfrac{1}{\alpha_{2g-i}}$. □

Remark 2.36. Let us recapitulate the analytic properties of the Zeta function. The Zeta function is holomorphic in the complex plane except in $t = 1$ and $t = \frac{1}{q}$ where it has simple poles. The zeroes of the Zeta function $Z(t, C/k)$ are denoted by $\alpha_i^{-1}, \ldots, \alpha_{2g}^{-1}$.

Chapter 3

The Riemann hypothesis

3.1 Some history

Most students have during an introductory course in Calculus been introduced to the *Riemann hypothesis* – usually in the following formulation.

The 'classic' Riemann hypothesis: The Riemann Zeta function $\zeta(s)$ defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \mathrm{Re}[s] > 1$$

extends to a meromorphic function on the entire complex plane with a simple pole in 1 and trivial zeroes in $\{-2, -4, -6, \dots\}$ satisfying the functional equation

$$\Gamma(\tfrac{s}{2})\pi^{-\frac{s}{2}}\zeta(s) = \Gamma(\tfrac{1-s}{2})\pi^{-\frac{1-s}{2}}\zeta(1-s).$$

The Riemann hypothesis then conjectures that the remaining zeroes of $\zeta(s)$ all lie on the line $\mathrm{Re}[s] = \frac{1}{2}$. This has not yet been proved (April 20, 1995). So far, it has been proved that all zeroes (other than $-2, -4, -6, \dots$) lie in the strip $0 < \mathrm{Re}[s] < 1$ and that $\zeta(s)$ has infinitely many zeroes on the line $\mathrm{Re}[s] = \frac{1}{2}$.

One may define the Zeta function for arbitrary commutative fields K with the properties

1. K_ν is a locally compact field for any valuation of K.
2. For all $x \in K \setminus \{0\}$
$$1 = \prod_{\nu} \nu(x)$$
the product being taken over all valuations of K.

($\nu : K^* \to \mathbb{Z}$ is a discrete valuation of K if the valuation ring belonging to ν has quotient field K). It may be shown that only two types of fields have these properties, namely

(A) K is an algebraic number field, i. e. a finite algebraic extension of $\mathbb{Q}$.

(B) K is a function field of dimension 1 over a finite field $\mathbb{F}_q$ (by this we understand, K is of transcendence degree 1 over $\mathbb{F}_q$ and a finite algebraic extension of $\mathbb{F}_q(t)$).

Below we will show the Riemann hypothesis in the function field case (B). First we notice that by making an Euler expansion of $\zeta(s)$, we may rewrite the Riemann zeta function as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\text{prime ideals } \mathfrak{p} \subseteq \mathcal{O}_K} (1 - N(\mathfrak{p}))^{-s})^{-1}$$

$\mathcal{O}_K (= \mathbb{Z})$ being the ring of algebraic integers in the number field $K (= \mathbb{Q})$. This motivates the following definition.

Definition 3.1. Let K be a function field of dimension 1 over $k = \mathbb{F}_q$. By [Har77, I.6.12], K corresponds to a complete smooth projective curve C_K (C_K is called a smooth model of K). Divisors $D = \sum_P n_P \cdot P$ on C_K then correspond to fractional ideals in the number field situation, and we therefore define the *norm* of a divisor

$$N(D) = q^{\deg(D)}$$

where $\deg(D) = \sum n_P \cdot \deg(P)$ with the notation of Chapter 2. Define the *Zeta function associated to* K/k by

$$Z(s, K/k) = \prod_{\mathcal{P}} (1 - N(\mathcal{P})^{-s})^{-1}$$

the product being taken over all prime divisors on C_K. By making the change of variables $t = q^{-s}$, we have

$$Z(t, K/k) = \prod_{\mathcal{P} \text{ prime div.}} \left(1 - t^{\deg(\mathcal{P})}\right)^{-1}. \tag{3.1}$$

Example 3.2. Let $k = \mathbb{F}_q$ as usual and let t be a free variable. We then have the analogy

$\mathbb{Q}$	$k(t)$
$\mathbb{Z}$	$k[t]$
prime numbers $\pm p$	prime divisors $\mathcal{P}$
$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$	$Z(s) = \sum_{D} (q^{\deg(D)})^{-s}$
$\zeta(s) = \prod_{p \text{ prime number}} (1 - p^{-s})^{-1}$	$\prod_{\mathcal{P} \text{ prime divisor}} (1 - (q^{\deg(\mathcal{P})})^{-s})^{-1}$

Remark 3.3. Taking logarithmic derivatives in (3.1) gives

$$\frac{Z'(t,K/k)}{Z(t,K/k)} = \sum_{m=1}^{\infty} \sum_{\mathcal{P} \text{ prime div.}} \deg(\mathcal{P}) t^{m\cdot\deg(\mathcal{P})-1}$$
$$= \sum_{m=1}^{\infty} \Bigg(\sum_{\deg(\mathcal{P})|m} \deg(\mathcal{P}) \Bigg) t^{m-1}.$$

Earlier we saw (Lemma 2.16) that the sum in the parenthesis gives the number of $\mathbb{F}_{q^m}$-rational points on C_K. Then with the notation from Chapter 2

$$Z(t,K/k) = Z(t,C/k) = \exp\Bigg(\sum_{m=1}^{\infty} N_m t^m \Bigg). \tag{3.2}$$

Thus we may identify the function field parallel to the Riemann zeta function defined above with the zeta function defined in Chapter 2. We then have the following results:

Rationality:

$$Z(t,K/k) = \frac{P(t)}{(1-t)(1-qt)} \tag{3.3}$$

where $P(t) \in \mathbb{Z}[t]$, $\deg(P(t)) = 2g$.

Functional equation:

$$Z(\tfrac{1}{qt},K/k) = q^{1-g} t^{2-2g} Z(t,K/k). \tag{3.4}$$

and the *Riemann hypothesis* for K then conjectures that $Z(t,K/k)$ has its zeroes on the line $\mathrm{Re}[s] = \frac{1}{2}$. Now, as $t = q^{-s}$, this is equivalent to $P(t)$ having roots c_i with norm $|c_i| = q^{-\frac{1}{2}}$ as

$$q^{-s} = t = |c_i| = q^{-\frac{1}{2}} \ \Rightarrow \mathrm{Re}[s] = \tfrac{1}{2}$$

($|q^{x+iy}| = q^x$). This explains why we call (2.4) the Riemann hypothesis. So we just need to prove

The Riemann hypothesis: The polynomial introduced above factors as

$$P(t) = \prod_{i=1}^{2g} (1 - \alpha_i t) \tag{3.5}$$

with $|\alpha_i|^2 = q^{\frac{1}{2}}$ for $i = 1, \ldots, 2g$. By Lemma 2.32

$$Z(t^m, C_K/\mathbb{F}_{q^m}) = \prod_{\epsilon^m=1} Z(\epsilon t, C_K/\mathbb{F}_q) \tag{3.6}$$

hence

$$\alpha_i^{-1} \text{ is a root in } Z(t, C_K/\mathbb{F}_q) \;\Leftrightarrow\; (\epsilon\alpha_i^{-1})^m = (\alpha_i^{-1})^m \text{ is a root in } Z(t, C_K/\mathbb{F}_{q^m})$$

for some m^{th} root of unity ϵ. Since also

$$|\alpha_i|^2 = q \;\Leftrightarrow\; |(\epsilon\alpha_i^{-1})^m|^2 = |\alpha_i^m|^2 = q^m$$

we see that it suffices to show the Riemann hypothesis for C_K defined over $\mathbb{F}_{q^m}$ for just one $m \geq 1$.

3.2 Bombieri's Theorem

Proposition 3.4. *With the above notation, the following statements are equivalent*

a) $|\alpha_i| = q^{\frac{1}{2}}$ *for* $i = 1, \ldots, 2g$.

b) $|\alpha_i| \leq q^{\frac{1}{2}}$ *for* $i = 1, \ldots, 2g$.

c) There exists a constant A *such that*

$$|N_m - (1 + q^m)| \leq Aq^{\frac{m}{2}}$$

for all $m \geq 1$.

Proof. a) $\Rightarrow$ b) is trivial, b) $\Rightarrow$ a) follows from the fact that the α_i may be numbered such that $\alpha_i\alpha_{2g-i} = q$ (cf. Corollary 2.35). a) $\Rightarrow$ c) follows from the remarks after Theorem 2.4. c) $\Rightarrow$ b): By taking the logarithmic derivative of the Zeta function we get

$$\sum_{m=1}^{\infty} N_m t^{m-1} = \sum_{i=1}^{2g} \frac{-\alpha_i}{1-\alpha_i t} + \frac{1}{1-t} + \frac{q}{1-qt}.$$

By expanding the last two terms on the right-hand side

$$\sum_{i=1}^{2g} \frac{-\alpha_i}{1-\alpha_i t} = \sum_{m=1}^{\infty} \big(N_m - (1 - q^m)\big) t^{m-1}.$$

We note that the left-hand side is meromorphic with poles in α_i^{-1}, $i = 1, \ldots, 2g$. At the same time

$$|N_m - (1 + q^m)| \leq Aq^{\frac{m}{2}}$$

by our assumption. Hence

$$|N_m - (1 + q^m)|^{\frac{1}{m}} \leq A^{\frac{1}{m}} q^{\frac{1}{2}}.$$

which makes the series

$$\sum_{m=1}^{\infty}\big(N_m - (1-q^m)\big)t^{m-1}$$

convergent for $|t| < q^{\frac{1}{2}}$. The poles must therefore lie outside this open disc, that is $|\alpha_i^{-1}| \geq q^{-\frac{1}{2}}$ or equivalently, $|\alpha_i| \leq q^{\frac{1}{2}}$. □

Remark 3.5. Combined with the considerations in Section 3.1, Proposition 3.4 implies that to show the Riemann hypothesis for C over k $(= \mathbb{F}_q)$, it will suffice to show the existence of a constant A, such that

$$|N - (1+q)| \leq Aq^{\frac{1}{2}}$$

for some $q \gg 0$, where N is the number of $\mathbb{F}_q$-rational points on C.

Now follow three lemmas which constitute the core of the proof of what we below call Bombieri's Theorem (Theorem 3.9).

Lemma 3.6. *Let $P \in C$, C curve defined over k. Then*

a) $\ell(mP) \leq \ell((m+1)P) \leq \ell(mP) + 1$.

b) $\ell(mP) = m + 1 - g$ *if* $m > 2g - 2$.

c) $f(x) \in L(mP) \Rightarrow f(x^q) \in L(qmP)$.

d) $L(mP)$ *has a basis* $f_1, \ldots, f_r$ *(over* $\mathbb{F}_q$*), such that*

$$\nu_P(f_i) < \nu_P(f_{i+1})$$

for $i = 1, \ldots, r-1$.

Proof. a) follows from a) in Lemma A.13, b) follows from c) in Corollary 1.28, c) is obvious with the interpretation of the vector spaces $L(D)$ on page 13 in mind. As we have the filtration

$$(0) \subseteq \mathbb{F}_q = L(0 \cdot P) \subseteq L(P) \subseteq \ldots \subseteq L(mP)$$

it follows from a) that

$$L(mP) \simeq \bigoplus_{i=0}^{m} L(iP)/L((i-1)P)$$

is a decomposition in spaces of dimension one at the most. Then, by taking $f_i \in L(iP) \setminus L((i-1)P)$ whenever $L(iP) \setminus L((i-1)P) \neq 0$, we get the wanted basis. □

Lemma 3.7. *Let $P \in C$, C curve defined over k. Let $n, b \in \mathbb{N}_0$, $np^b < q$, let $s_1, \ldots, s_r \in L(nP)$. Pick a basis $f_1, \ldots, f_r$ for $L(mP)$ such that $\nu_P(f_i) < \nu_P(f_{i+1})$ for $i = 1, \ldots, r-1$. Let $\sigma \in \mathrm{Aut}(C)$ be such that $\sigma(P) = \phi(P)$, where $\phi : C \to C$ is the q^{th} power Frobenius map cf. Remark 1.22. Consider the function*

$$G(x) = s_1^{p^b}(x) f_1^{\sigma}(x^q) + \ldots + s_r^{p^b}(x) f_r^{\sigma}(x^q)$$

where $f_i^{\sigma} = f_i \circ \sigma^{-1}$. We then have

$$G(x) \equiv 0 \;\Leftrightarrow\; s_i(x) \equiv 0 \text{ for } i = 1, \ldots, r.$$

Proof. One way is trivial, so assume $G(x) \equiv 0$ and let h be the minimal index such that $s_h(x) \not\equiv 0$. By assumption

$$s_h^{p^b}(x) f_h^{\sigma}(x^q) = -s_{h+1}^{p^b}(x) f_{h+1}^{\sigma}(x^q) - \ldots - s_r^{p^b}(x) f_r^{\sigma}(x^q).$$

By taking the valuation ν_P on both sides we get

$$\begin{aligned} p^b \nu_P(s_h) + q\nu_P(f_h) &\geq \min_{i>h}\{p^b \nu_P(s_i) + q\nu_P(f_i)\} \\ &\geq -p^b n + q\nu_P(f_{h+1}) \end{aligned}$$

and therefore

$$p^b \nu_P(s_h) \geq -p^b n + q(\nu_P(f_{h+1}) - \nu_P(f_h)) \geq -p^b n + q > 0.$$

Hence the function $s_h \in L(nP)$ has both a pole and a zero in P so $s_h \equiv 0$, which is a contradiction. □

Lemma 3.8. *Let $m, n \in \mathbb{N}$ be such that $m, n > 2g-2$ and $(n+1-g)(m+1-g) > p^b+m+1-g$, with b as above. Pick a basis $f_1, \ldots, f_r$ for $L(mP)$. There exist $s_1, \ldots, s_r \in L(nP) \setminus \{0\}$ such that the function*

$$s_1^{p^b}(x) f_1(x) + \ldots + s_r^{p^b}(x) f_r(x)$$

is identically zero.

Proof. Let $s_1, \ldots, s_r \in L(nP) \setminus \{0\}$. The function $s_1^{p^b}(x) f_1(x) + \ldots + s_r^{p^b}(x) f_r(x)$ has no other poles than P and

$$\nu_P\big(s_1^{p^b}(x) f_1(x) + \ldots + s_r^{p^b}(x) f_r(x)\big) \geq -(p^b n + m). \tag{3.7}$$

By Lemma 3.6

$$\ell((p^b + n)P) = p^b + m + 1 - g.$$

Now consider the map (well-defined by (3.7))

$$\begin{aligned} \varphi : \overbrace{L(nP) \oplus \ldots \oplus L(nP)}^{r \text{ factors}} &\longrightarrow L((p^b n + m)P) \\ (s_1, \ldots, s_r) &\mapsto s_1^{p^b}(x) f_1(x) + \ldots + s_r^{p^b}(x) f_r(x) \end{aligned}$$

where $r = m + 1 - g$ by Lemma 3.6. Because

$$\begin{aligned} \dim(\text{LHS}) = r(n+1-g) &= (m+1-g)(n+1-g) \\ &> p^b n + m + 1 - g = \dim(\text{RHS}) \end{aligned}$$

by Lemma 3.6, $\ker(\varphi)$ is non-trivial and the assertion follows. □

Theorem 3.9 (Bombieri [Bom76]). *Let C be a curve of genus g defined over $k(= \mathbb{F}_q)$. Assume $q > (1+g)^4$ and $q = p^a$ where a is even and let $\sigma \in \mathrm{Aut}(C)$. Then*

$$N^\sigma(C) \leq 1 + q + (2g+1)q^{\frac{1}{2}}$$

where $N^\sigma(C)$ is the number of points $P \in C$ such that $\sigma(P) = \phi(P)$; see the Dictionary p. 36).

Proof. If $N^\sigma(C) = 0$ there is nothing to show, so we may assume that C has a point P such that $\phi(P) = \sigma(P)$.

Put $b = \frac{a}{2}, n = q^{\frac{1}{2}} - 1, m = q^{\frac{1}{2}} + 2g$. By assumption, $b, n, m \in \mathbb{N}$. Choose a basis $f_1, \ldots, f_r$ for $L(mP)$ as in Lemma 3.6. Now one checks that $m, n > 2g-2$ and $(n+1-g)(m+1-g) > p^b n + m + 1 - g$ for $q > (1+g)^4$, in order to apply Lemma 3.8 to give us $s_1, \ldots, s_r \in L(nP) \setminus \{0\}$ such that

$$s_1^{p^b}(x) f_1(x) + \ldots + s_r^{p^b}(x) f_r(x) \equiv 0. \tag{3.8}$$

Then consider the function

$$G(x) = s_1^{p^b}(x) f_1^\sigma(x^q) + \ldots + s_r^{p^b}(x) f_r^\sigma(x^q)$$

which, since $p^b n < q$, is not identically zero by Lemma 3.7.

Suppose $Q \neq P$ is another point such that $\phi(Q) = \sigma(Q)$. If Q has coordinates y, we then have $f_i^\sigma(y^q) = f_i(y)$. But then y is a zero for $G(x)$ by (3.8). So $G(x)$ has at least $N^\sigma(C) - 1$ zeroes. As $G(x)$ is a p^b power, every zero has multiplicity at least p^b so $G(x)$ has at least $p^b(N^\sigma(C) - 1)$ zeroes counted with multiplicity. On the other hand $G(x) \in L((p^b n + mq)P)$ by Lemma 3.6 hence

$$p^b(N^\sigma(C) - 1) \leq p^b n + mq \tag{3.9}$$

as the degree of a rational function is zero (Lemma A.13). By substituting the values of b, m, n we get from (3.9) that

$$N^\sigma(C) - 1 \leq q^{\frac{1}{2}} - 1 + (q^{\frac{1}{2}} + 2g)q^{\frac{1}{2}}.$$

Hence $N^\sigma(C) \leq 1 + q + (2g+1)q^{\frac{1}{2}}$ as claimed. □

Corollary 3.10. *Let C be a curve of genus g defined over $k(= \mathbb{F}_q)$. Suppose $q > (1+g)^4$ and $q = q^a$ where a is even. Then*

$$N(C) \leq 1 + q + (2g+1)q^{\frac{1}{2}}.$$

Proof. Let $\sigma = \mathrm{id}_C$ in Theorem 3.9. □

3.3 Galois coverings

The rest of this chapter will rely on the $1-1$ correspondence between curves and function fields cf. [Har77, I.6.12]. Thereby we may freely choose in what setup we will prove a given result. The function field theory we use is treated in the first three chapters of [FJ86]. That exposition is rather compressed though, so references are for the reader's convenience given to the more elementary [Lan93].

Let us fix the notation: given a discrete valuation $\nu : K^* \to \mathbb{Z}$ we put

$$\begin{aligned} R_\nu &= \{x \in K^* : \nu(x) \geq 0\} && \text{; the valuation ring associated to } \nu \\ \mathfrak{m}_\nu &= \{x \in K^* : \nu(x) > 0\} && \text{; the maximal ideal in the local ring } R_\nu \\ k_\nu &= R_\nu/\mathfrak{m}_\nu. \end{aligned}$$

Dictionary 3.11. We list some properties of the $1-1$ correspondence between smooth projective curves and function fields of dimension 1 over K.

Function field terminology	*Geometric terminology*
$k(t)$	$\mathbb{P}^1_k$
Function fields of dimension 1 over k	Curves C_K with function field K
Discrete valuations ν of K/k, R_ν (also called prime divisors of K/k)	Closed points $P \in C_K$, $k[C_K]_{\mathfrak{m}_P}$ (a closed point defines an irr. divisor on C_K)
Valuations ν such that $\deg(\nu) := [k_\nu : k] = m$	Prime divisors $\mathcal{P}$ such that $\deg(\mathcal{P}) = m$
The q^{th} power Frobenius morphism $\phi : \nu(x) \mapsto \nu(x^q)$	The q^{th} power Frobenius morphism $\phi : P = (x) \mapsto (x^q)$
Valuations ν such that $\phi(\nu) = \nu$ the number of these we write $N(K)$, also equal to $\lvert\{\nu : \deg(\nu) = 1\}\rvert$	k-rational points $P \in C_K$ the number of these we write $N(C_K)$, also equal to $\lvert\{\mathcal{P} \in \mathrm{Div}_k C_K : \deg(\mathcal{P}) = 1\}\rvert$
Galois extensions $K \subseteq K'$ such that k is algebraically closed in K	Galois coverings $C_{K'} \to C_K$ (cf. Lemma 3.14)
Valuations ν such that given $\sigma \in \mathrm{Gal}(K'/K)$: $\phi(\nu) = \nu \circ \sigma$	Points $P \in C_K$ such that given $\sigma \in \mathrm{Gal}(K'/K)$: $\phi(P) = \sigma.P$
$N^\sigma(K) = \sum_{\phi(\nu)=\nu\circ\sigma} \deg(\nu)$	$N^\sigma(C_K) = \sum_{F(P)=\sigma.P} \deg(P)$

Remark 3.12. Let $L \subseteq K$ be a finite Galois extension of function fields of dimension 1 over an arbitrary (not necessarily finite) field k' of characteristic $p > 0$. Let C_L and C_K be the associated curves cf. [Har77, I.6.12].

We will now examine the action of $G = \mathrm{Gal}(K/L)$ on C_K and C_L and the behavior of the k'-rational points under this action.

As C_K (resp. C_L) is the set of discrete valuations of K/k' (resp. L/k'), the inclusion $\pi^\# : L \hookrightarrow K$ induces a morphism

$$\pi : C_K \to C_L,$$

where a valuation $\nu : K^* \to \mathbb{Z}$ such that $\nu|_{k'^*} = 0$ is mapped to $\nu|_L$. As any valuation τ of L/k' extends to a valuation of K/k' [Lan93, Corollary 4.4 p. 483], π is surjective. We note that

$$\pi^{-1}(\tau) = \big\{\text{valuations } \nu : K^* \to \mathbb{Z} : \nu|_L = \tau\big\} \tag{3.10}$$

so $|\pi^{-1}(\tau)| < \infty$ by [Lan93, Corollary 4.9 p. 485]. G acts on C_L and C_K in the natural way: for any $\nu \in C_L$, $\sigma(\nu) = \nu \circ \sigma$ for $\sigma \in G$. We note that, as $\sigma|_L = \mathrm{id}_L$ for all $\sigma \in G$, C_L is fixed under the action of G. If $\nu \in C_K$ is such that $\nu|_L \in C_L$, we see that

$$\sigma(\nu)|_L = \nu \circ \sigma|_L = \nu|_L.$$

Hence, as G consists of all automorphisms of K fixing L, the valuations

$$\{\nu \in C_K : \nu|_L = \tau \in C_L\}$$

are all conjugated under G's action. Therefore

$$|\pi^{-1}(\tau)| = |\{\nu \in C_K : \nu|_L = \tau\}| \leq |G| = [K : L]. \tag{3.11}$$

What about the k'-rational points – what do they look like in this interpretation. By Appendix A

$$X(k') = \big\{x \in X : x \text{ } k'\text{-rational}\big\} \leftrightarrow \big\{x \in X : k[X]_{\mathfrak{m}_x}/\mathfrak{m}_x \hookrightarrow k'\big\}.$$

If C is a curve over k' we have (cf. Dictionary above)

$$\big\{\nu \in C : \nu \text{ } k'\text{-rational}\big\} \leftrightarrow \big\{\nu : K^* \to \mathbb{Z} : \deg(\nu) = [k_\nu : k'] = 1\big\}.$$

So if k' is algebraically closed in K all points are k'-rational (see Lemma 3.14 below), and G acts on $C_K(k')$ over $C_L(k')$ (i.e. G acts on $C_K(k')$ fixing the points of $C_L(k')$). This is not the case if k' fails to be algebraically closed in K.

Definition 3.13. Let $\pi : Y \to X$ be a morphism of curves defined over k. π is said to be a *Galois covering over* k if the induced map of function fields

$$\pi^\# : K(X) \to K(Y)$$

is a finite Galois extension and the associated Galois group acts on $Y(k)$ over $X(k)$.

Lemma 3.14. *Let $L \subseteq K$ be a finite Galois extension of function fields of dimension 1 over k. Let k' be the algebraic closure of k in K. Then*

a) $[k' : k] < \infty$, i.e. k' is a finite field $\mathbb{F}_{q^m}$.

b) $L \cdot k' \subseteq K \cdot k'$ is a finite Galois extension of function fields of dimension 1 over k' and

$$\pi : C_{K \cdot k'} \to C_{L \cdot k'}$$

is a Galois covering of curves defined over k'.

Proof. a) We have inclusions

$$\underbrace{k \subseteq L}_{\text{finitely generated}} \subseteq K \qquad \Rightarrow \qquad k \subseteq K \text{ finitely generated as } [K : L] < \infty$$

hence

$$\underbrace{k \subseteq k' \subseteq K}_{\text{finitely generated}} \qquad \Rightarrow \qquad k \subseteq k' \text{ finitely generated .}$$

By construction $k \subseteq k'$ is an algebraic extension and we conclude $[k' : k] < \infty$.

b) The extension $L \cdot k' \subseteq K \cdot k'$ is a finite Galois extension as the extensions $k \subseteq k'$ and $L \subseteq K$ are. We are left to showing that, for any valuation ν of K/k' such that $[k_\nu : k'] = 1$ we have

$$[k_{\sigma(\nu)} : k'] = 1 \qquad \text{for all } \sigma \in G = \mathrm{Gal}(K/L).$$

Let τ be the restriction of $\sigma(\nu)$ to $k'(t)$. Either t or t^{-1} is in R_τ so assume WLOG $t \in R_\tau$. As $\mathfrak{m}_\tau \subseteq R_\tau \subseteq k'(t)$, $\mathfrak{m}_\tau \cap k'[t] = \mathfrak{p}$, a prime ideal different from (0). Then $R_\tau/\mathfrak{m}_\tau \simeq k'[t]/\mathfrak{p}$. As $k'[t]$ is a PID, $\mathfrak{p}$ is generated by a polynomial $p \in k'[t]$ and therefore k_τ is a finite algebraic extension of degree $\leq \deg(f)$. We also have $[k_{\sigma(\nu)} : k_\tau] \leq [K : k'(t)]$ by [Lan93, Proposition 4.6 p. 483]. So as $[K : k'(t)] < \infty$, $k_{\sigma(\nu)}$ is a finite, hence algebraic extension of k_τ in K. But as k' was algebraically closed in K we must then have $[k_{\sigma(\nu)} : k'] = 1$. □

Construction 3.14. Let C be a (smooth) curve defined over k with function field K. As k is perfect and as $1 = \dim(C) = \mathrm{tr\,deg}_k K$, there exists $t \in K$ such that t is transcendent over k and K is a finite separable extension of $k(t)$. Now let K' be the minimal normal extension of $k(t)$ containing K. Denoting the different embeddings of K into an algebraic closure of K over $k(t)$ by $\sigma_1, \ldots, \sigma_n$, we necessarily have

$$K' = \sigma_1(K) \cdot \ldots \cdot \sigma_n(K).$$

(cf. [Lan93, p. 242 bottom]). As successive separable extensions give a separable extension ([Lan93, Theorem 4.5 p. 241]), $k(t) \subseteq K'$ is a separable extension. From [Lan93, Thm. 3.4

p. 238] follows that the extension $K \subseteq K'$ is normal as the extension $k(t) \subseteq K'$ is. Altogether this gives Galois extensions $k(t) \subseteq K'$ and $K \subseteq K'$ with Galois groups $G = \mathrm{Gal}(K'/k(t))$ and $H = \mathrm{Gal}(K'/K)$.

Letting C' denote the curve associated to K', we have coverings

$$C' \to C \to \mathbb{P}^1_k$$

over k. At this point it may not be the case that G acts on $C'(k)$ over k, but by Lemma 3.14 we may extend k finitely

$$k = \mathbb{F}_p \subseteq \mathbb{F}_{q^2} \subseteq \ldots \subseteq \mathbb{F}_{q^m}$$

until G acts on $C'(\mathbb{F}_{q^m})$. Then

$$C'(\mathbb{F}_{q^m}) \to C(\mathbb{F}_{q^m}) \to \mathbb{P}^1_{\mathbb{F}_{q^m}}$$

are Galois coverings over $\mathbb{F}_{q^m}$. That is, given a curve defined over k we have (possibly after replacing k by a finite extension) constructed Galois coverings

$$C' \to \mathbb{P}^1_k \qquad \text{og} \qquad C' \to C$$

with Galois groups G and H.

Lemma 3.16. *Let L be a function field of dimension 1 over k. Let K be a finite Galois extension of L with Galois group G. Assume k is algebraically closed in L and K. Then*

$$N(L) = \frac{1}{|G|} \sum_{\gamma \in G} N^\gamma(K).$$

Proof. We have the injection $\pi^\# : L \hookrightarrow K$. Let ν' be a valuation of K/k and let $\nu = \nu'|_L$. Suppose $\phi(\nu) = \nu$, then

$$\phi(\nu')|_L = \phi(\nu'|_L) = \phi(\nu) = \nu$$

as the Frobenius morphism commutes with restriction. As G acts transitively on the valuations over ν we have

$$\phi(\nu) = \nu \;\Leftrightarrow\; \exists \gamma \in G : \nu' \circ \gamma = \phi(\nu'). \tag{3.12}$$

Introduce the notation

$$\begin{aligned} e(\nu'|\nu) &= |\{\gamma \in G : \nu' \circ \gamma = \phi(\nu')\}| \\ f(\nu'|\nu) &= [k_{\nu'} : k_\nu] \\ g(\nu) &= |\pi^{-1}(\nu)|. \end{aligned}$$

for $\nu' \in \pi^{-1}(\nu)$. Then

$$\begin{aligned}\sum_{\gamma\in G} N^\gamma(K) &= \sum_{\gamma\in G} \sum_{\phi(\nu)=\nu\circ\gamma} \deg(\nu') \\ &= \sum_{\phi(\nu)=\nu} \sum_{\nu'\in\pi^{-1}(\nu)} e(\nu'|\nu)\deg(\nu')\end{aligned}$$

by (3.12). Given ν_i' and $\nu_j' \in \pi^{-1}(\nu)$ there exists $\sigma \in G$ such that $\nu_i' = \nu_j' \circ \sigma$ as G acts transitively on $\pi^{-1}(\nu)$. Therefore

$$\begin{aligned}e(\nu_i'|\nu) &= |\{\gamma \in G : \nu_i' \circ \gamma = \phi(\nu_i')\}| = |\{\gamma \in G : \nu_j' \circ \sigma\gamma = \phi(\nu_j' \circ \sigma)\}| \\ &= |\{\gamma \in G : \nu_j' \circ \sigma\gamma\sigma^{-1} = \phi(\nu_j')\}| = e(\nu_j'|\nu).\end{aligned}$$

In the same way we get $f(\nu_i'|\nu) = f(\nu_j'|\nu)$ for all $\nu_i', \nu_j' \in \pi^{-1}(\nu)$. Write $e(\nu)$ (resp. $f(\nu)$) for the common values. Then

$$\begin{aligned}\sum_{\gamma\in G} N^\gamma(K) &= \sum_{\phi(\nu)=\nu} \sum_{\nu'\in\pi^{-1}(\nu)} e(\nu'|\nu)[k_{\nu'} : k] \\ &= \sum_{\phi(\nu)=\nu} \sum_{\nu'\in\pi^{-1}(\nu)} e(\nu'|\nu)[k_{\nu'} : k_\nu][k_\nu : k] \\ &= \sum_{\phi(\nu)=\nu} \sum_{\nu'\in\pi^{-1}(\nu)} e(\nu'|\nu)f(\nu'|\nu)\deg(\nu) \\ &= \sum_{\phi(\nu)=\nu} e(\nu)f(\nu)g(\nu)\deg(\nu).\end{aligned}$$

Now as $f(\nu) = [k_{\nu'} : k_\nu] = |\{\sigma \in G : \sigma(R_\nu) = R_\nu\}|$, counting will give $e(\nu)f(\nu)g(\nu) = |G|$ ([Lan93, Corollary 6.3 p. 490]). Hence

$$\sum_{\gamma\in G} N^\gamma(K) = \sum_{\phi(\nu)=\nu} |G| \cdot \deg(\nu) = |G| \cdot N(L)$$

and the lemma follows. □

Corollary 3.17. *Let $\pi : C_K \to C_L$ be a Galois covering of curves defined over k. Then*

$$N(C_L) = \frac{1}{|G|} \sum_{\gamma\in G} N^\gamma(C_K). \tag{3.13}$$

In particular, if $X = \mathbb{P}^1_k$

$$1 + q = \frac{1}{|G|} \sum_{\gamma\in G} N^\gamma(C_K). \tag{3.14}$$

(G is the Galois group for the extension $L \subseteq K$).

Proof. As $\pi : C_K \to C_L$ is a Galois covering, k is necessarily algebraically closed in K and also in L as $k \subseteq L \subseteq K$. Now combine Lemma 3.16 with the Dictionary on page 36. □

Proposition 3.18. *Let C be a curve of genus g defined $\mathbb{F}_q$ ($q \gg 0$). There exists a constant A such that*

$$N(C) \geq 1 + q - Aq^{\frac{1}{2}}.$$

Proof. By the above, we may construct Galois coverings

$$C' \to \mathbb{P}^1_{\mathbb{F}_q} \qquad \text{and} \qquad C' \to C$$

with Galois groups G and H respectively (eventually after making a finite extension of $\mathbb{F}_q$). By Theorem 3.9 there exists a constant A' such that

$$N^\gamma(C') \leq 1 + q + A'q^{\frac{1}{2}}$$

for all $\gamma \in G$. Then

$$\begin{aligned}\sum_{\gamma\in G} N^\gamma(C') &= \sum_{\xi\in H} N^\xi(C') \;+\; \sum_{\gamma\in G\setminus H} N^\gamma(C') \\ &\leq \sum_{\xi\in H} N^\xi(C') \;+\; \sum_{\gamma\in G\setminus H} 1 + q + A'q^{\frac{1}{2}} \\ &= \sum_{\xi\in H} N^\xi(C') \;+\; \big(|G| - |H|\big)\big(1 + q + A'q^{\frac{1}{2}}\big).\end{aligned}$$

Corollary 3.17 applied to the covering $C' \to \mathbb{P}^1_{\mathbb{F}_q}$ gives

$$\begin{aligned}\sum_{\xi\in H} N^\xi(C') &\geq |G|(q+1) - \big(|G| - |H|\big)\big(1 + q + A'q^{\frac{1}{2}}\big) \\ &= |H|(q+1) - (|G| - |H|)A'q^{\frac{1}{2}}\end{aligned}$$

and Corollary 3.17 applied to the covering $C' \to C$ gives

$$N(C) = \frac{1}{|H|}\sum_{\xi\in H} N^\xi(C') \;\geq\; q + 1 - \tfrac{|G|-|H|}{|H|}A'q^{\frac{1}{2}}.$$

Now put $A = \frac{|G|-|H|}{|H|}A'$. □

Remark 3.19. As the constant A, found above in Proposition 3.18, is larger than or equal to the constant obtained in Corollary 3.10 we have

$$|N(C) - (1+q)| \;\leq\; Aq^{\frac{1}{2}}$$

for some $q \gg 0$. By Remark 3.5 we then have shown the Riemann hypothesis for C (or the function field associated to C if one prefers this point of view).

Appendix A

Scheme- and sheaf theoretic formulation

In this appendix we reformulate most of the definitions and results from Chapter 1 in terms of sheaves and schemes. We use the notation and terminology from [Har77] and the reader is assumed to be familiar with this book's first three chapters. The term points will allways denote closed points unless otherwise stated.

A.1 Affine schemes

Definition A.1. Put $R = \bar{k}[X_1, \ldots, X_n]$. Then

$$\mathbb{A}^n = \mathrm{Spec}(R)$$

is the *affine $\bar{k}$-scheme of dimension n.* More generally, if $X \to \mathrm{Spec}(K)$ is a scheme over K (K a field), then the *k-rational points* are the elements in $\mathrm{Mor}_X(\mathrm{Spec}(k), X)$. That is

$$\{k\text{-rational points in } X\} \leftrightarrow \{\text{points } x \in X \text{ with } k(x) \hookrightarrow k\}.$$

So in our case, the k-rational points in $\mathbb{A}^n$ are given by a prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ together with an injection $k(\mathfrak{p}) \hookrightarrow k$. As R is Noetherian we may write

$$\mathfrak{p} = (f_1, \ldots, f_k) \qquad\qquad f_i \in R \text{ irreducible.}$$

Then $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}} = (R/\mathfrak{p})_0$ so if $k(\mathfrak{p})$ shall be embedded in k, all the f_i must have roots in k, as we adjoin the roots of the f_i by dividing out with $\mathfrak{p}$. In case $\mathfrak{p}$ is a closed point, i. e. a maximal ideal $\mathfrak{m} \in \mathfrak{m}\,\mathrm{Spec}(R)$, we have

$$\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$$

with $a_i \in k$, whereby the closed k-rational points of $\mathbb{A}^n$ bijects with the set

$$\{(a_1, \ldots, a_n) : a_i \in k\}.$$

Remark A.2. $G = \mathrm{Gal}(\bar{k}/k)$ acts on $\mathbb{A}^n$

$$\sigma.\mathfrak{p} = (\sigma.f_1, \ldots, \sigma.f_k) \text{ for } \mathfrak{p} = (f_1, \ldots, f_k)$$

by acting on the coefficients of the f_i. Put

$$\mathbb{A}^n(k) = \{\mathfrak{p} \in \mathbb{A}^n : \sigma.\mathfrak{p} \text{ for all } \sigma \in G\}.$$

Then the closed points of $\mathbb{A}^n(k)$ are given by

$$\mathbb{A}^n(k)_{cl} = \{\mathfrak{m} \in \mathfrak{m}\,\mathrm{Spec}(R) : \sigma.\mathfrak{m} \text{ for all } \sigma \in G\}.$$

But as the maximal ideals are on the form $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$, we have $\sigma.\mathfrak{m} = (X_1 - \sigma(a_1), \ldots, X_n - \sigma(a_n))$ and therefore

$$\sigma.\mathfrak{m} = \mathfrak{m} \;\Leftrightarrow\; \sigma(a_i) = a_i \qquad\qquad i = 1, \ldots, n.$$

So we may make the identification

$$\mathbb{A}^n(k)_{cl} = \{(a_1, \ldots, a_n) : \sigma(a_i) = a_i \;\; ; i = 1, \ldots, n, \text{ for all } \sigma \in G\}.$$

Definition A.3. The *closed subscheme defined by the ideal* $I \subseteq R$ is

$$V_I = \{\mathfrak{p} \in \mathbb{A}^n : \mathfrak{p} \supseteq I\} \simeq \mathrm{Spec}\, R/I.$$

Then

$$\begin{aligned} V_{I,cl} &= \{\mathfrak{m} \in \mathbb{A}^n : \mathfrak{m} \supseteq I\} \\ &= \{(X_1 - a_1, \ldots, X_n - a_n) : f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\} \end{aligned}$$

as $\mathfrak{m} \supseteq I \Leftrightarrow f(\mathfrak{m}) = 0$ for all $f \in I$ where

$$\begin{aligned} f(\mathfrak{m}) &= \text{the image of } f \text{ in } k(\mathfrak{m}) = R/\mathfrak{m} \subseteq \bar{k} \\ &= f(a_1, \ldots, a_n) \text{ for } \mathfrak{m} \text{ on the form } \mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n). \end{aligned}$$

The k-rational points on the affine scheme $V = \mathrm{Spec}\, R/I$ are $\mathrm{Mor}(\mathrm{Spec}(k), V)$. V is *defined over* k if there exists a morphism of schemes $V \to \mathrm{Spec}(k)$.

Remark A.4. In Remark A.2 we saw how $G = \mathrm{Gal}(\bar{k}/k)$ acts on $\mathbb{A}^n = \mathrm{Spec}\, R$. In the same way, G acts on any closed subscheme $V = \mathrm{Spec}\, R/I$ of $\mathbb{A}^n$.

Definition A.5. An affine scheme $V = \mathrm{Spec}\, R/I$ is called a *variety* if I is a prime ideal in R. $\Gamma(V, \mathcal{O}_V) = R/I$ is the global sections of the sheaf of regular functions $\mathcal{O}_V$ on V. Suppose V is defined over k, that is

$$V = \mathrm{Spec}\big(k[X_1, \ldots, X_n]/I(V/k)\big)$$

where $I(V/k) = I(V) \cap k[X_1, \ldots, X_n]$. The quotient field $k(V)$ of the domain $k[X_1, \ldots, X_n]/I(V/k)$ is called the *function field* of V over k. In a similar way one defines $\bar{k}(V)$.

A.2 Projective schemes

Definition A.6. Put $S = \bar{k}[X_0, \ldots, X_n]$. Then

$$\mathbb{P}^n = \operatorname{Proj} S$$

is the *projective $\bar{k}$-scheme of dimension n*. One then shows the same identifications as in the affine case above. The *function field* of a projective *variety* $V = \operatorname{Proj} S/I$ ($I \subseteq S$ homogeneous prime ideal) is given by $\bar{k}(U)$ where $U \subseteq V$ is an open affine subset of $\mathbb{P}^n$ such that $V \cap U \neq \emptyset$.

A.3 Curves

Definition A.7. A *curve* over k is a Noetherian, separated, irreducible, reduced scheme of finite type and of dimension 1, $X \to \operatorname{Spec}(k)$ where k is algebraically closed.

Definition A.8. A scheme X is *smooth in* $P \in X$ if $\mathcal{O}_{X,P}$ is a regular local ring. So if $\dim X = 1$ we have

$$X \text{ is smooth in } P \in X \;\Leftrightarrow \mathcal{O}_{X,P} \text{ is a DVR}$$

by [AM69, Proposition 9.3]. A scheme is *smooth* if all of its points are.

Remark A.9. If $V \subseteq \mathbb{P}^n$ is a curve defined by the prime ideal $I = (f_1, \ldots, f_m)$, $f_i \in S$, then $\operatorname{codim}(\mathfrak{p}) = n - 1$ for all $\mathfrak{p} \in \operatorname{Proj}(S)$. So the Jacobian criterion [Eis95, Theorem 16.19] gives that

$$\operatorname{rank}(J(\mathfrak{p})) = n - 1 \Leftrightarrow (S/I)_{\bar{\mathfrak{p}}} \;\; (= \mathcal{O}_{V,\mathfrak{p}}) \text{ is regular} \Leftrightarrow V \text{ is smooth at } \mathfrak{p}$$

where $J(\mathfrak{p})$ is the Jacobian of the f_i calculated in the point $\mathfrak{p} \in \operatorname{Proj}(S)$.

A.4 Divisors and the Riemann-Roch theorem

Let $(X, \mathcal{O}_X)$ be a scheme with sheaf of total quotient rings $\mathcal{K}$.

Remark A.10. Let D be a Cartier divisor on X represented by $\{U_i, f_i\}$ where $X = \bigcup_i U_i$ and $f_i \in \Gamma(U_i, \mathcal{K}^*)$ is such that $f_i/f_j \in \Gamma(U_i \cap U_j, \mathcal{O}_X^*)$. We have the associated linebundle (rank one invertible sheaf) $\mathcal{L}(D)$ given by

$$\mathcal{L}(D)|_{U_i} = \frac{1}{f_i} \cdot \mathcal{O}_X|_{U_i}. \tag{A.1}$$

This is well-defined as f_i/f_j is invertible, hence defines an isomorphism, on $U_i \cap U_j$. Hereafter, assume that X is irreducible, reduced, separated, Noetherian and locally factorial, where locally factorial means that the local rings $\mathcal{O}_{X,x}$ are all UFD's. This is for example the case when X is smooth (a regular local ring is a UFD). With these assumptions, $\mathcal{K}$ is a constant

sheaf equal to the function field K of X and by [Har77, II.6.11], Weil and Cartier divisors are then two and the same objects under the correspondence

$$\{\text{Cartier divisors}\} \leftrightarrow \{\text{Weil divisors}\} \tag{A.2}$$

$$\{U_i, f_i\} \rightarrow \sum_{i,Y} \nu_Y(f_i) \cdot Y \tag{A.3}$$

$$\{U_i, f_{x_i}\} \leftarrow D \tag{A.4}$$

where f_{x_i} is chosen such that $(f_{x_i}) = D_{x_i}$, the divisor on $\mathrm{Spec}(\mathcal{O}_{X,x_i})$ induced by D. So we see, that for $f \in \Gamma(X, K^*)$

$$(f) + D \geq 0 \Leftrightarrow \nu_Y(f) + \nu_Y(f_i) \geq 0$$

for all irreducible $Y \subseteq X$ of codimension 1 with $Y \cap U_i \neq \emptyset$. In other words, $\nu_Y(f \cdot f_i) \geq 0$ for all Y, i (Y as above) with $Y \cap U_i \neq \emptyset$. Then $\{U_i, f \cdot f_i\}$ defines a global section in $\mathcal{O}_X$, hence by (A.1), $f \in \Gamma(X, \mathcal{L}(D))$. Actually, this argument goes both ways, that is

$$f \in \Gamma(X, \mathcal{L}(D)) \Leftrightarrow (f) + D \geq 0.$$

Now let $\mathcal{L}$ be an arbitrary linebundle on X given by local isomorphisms

$$\varphi_i : \mathcal{L}|_{U_i} \xrightarrow{\simeq} \mathcal{O}_X|_{U_i} \qquad X = \textstyle\bigcup_i U_i$$

Above we saw, that if $s \in \Gamma(X, \mathcal{L})$ then $\{U_i, \varphi_i(s)\}$ is an effective Cartier divisor on X. Write $(s)_0$ for this Cartier divisor.

Proposition A.11 ([Har77, II.7.7]). *Let X be a smooth projective variety over the algebraically closed field k. Let D_0 be a Cartier divisor on X and let $\mathcal{L} = \mathcal{L}(D)$ be the associated linebundle.*

a) For all $s \in \Gamma(X, \mathcal{L}) \setminus \{0\}$, $(s)_0$ is an effective divisor linearly equivalent to D_0; $(s)_0 \sim D_0$.

b) If $D \sim D_0$ there exists $s \in \Gamma(X, \mathcal{L}) \setminus \{0\}$ such that $(s)_0 \sim D$.

c) For $s, s' \in \Gamma(X, \mathcal{L})$ we have

$$(s)_0 = (s')_0 \Leftrightarrow \exists\ \lambda \in k^* : \lambda s = s'.$$

Proof. a) As $\Gamma(X, \mathcal{L})$ is naturally embedded in $\Gamma(X, \mathcal{K}) = K$, we may think of s as a rational function $f \in K$. Now as $D_0 = \{U_i, f_i\}$ where $f_i \in \Gamma(U_i, \mathcal{K}^*) = K^*$ and as $\mathcal{L}(D_0)|_{U_i} = \frac{1}{f_i} \cdot \mathcal{O}_X|_{U_i}$ we have local isomorphisms

$$\varphi_i : \mathcal{L}(D_0)|_{U_i} \rightarrow \mathcal{O}_X|_{U_i}$$

by multiplying with f_i. Then

$$(s)_0 = \{U_i, \varphi_i(s)\} = \{U_i, f_i f\}$$

and therefore $(s)_0 = (f) + D_0$, that is $D_0 \sim (s)_0$.

b) If $D > 0$ and $D \sim D_0$ that is, there exists $f \in K$ such that $D = D_0 + (f)$, then $(f) - D_0 > 0$. But as we noted above, this implies that $f \in \Gamma(X, \mathcal{L}(D_0)) = \Gamma(X, \mathcal{L})$ and then $(f)_0 \sim D_0 \sim D$ by a).

c) As in a), $s, s' \in \Gamma(X, \mathcal{L})$ may be viewed as rational functions $f, f' \in K$ such that

$$(f/f') = (f) - (f') = (s)_0 - (s')_0 = 0.$$

But then $f/f' \in \Gamma(X, \mathcal{O}_X^*)$ and as X is projective $\Gamma(X, \mathcal{O}_X^*) = k^*$.

□

Remark A.12. Letting $|D_0|$ denote the set of effective divisors linearly equivalent to D_0, we may make the identification

$$|D_0| = \{D \in \mathrm{Div}(X) : D \geq 0 \ \wedge \ D \sim D_0\} = (\Gamma(X, \mathcal{L}(D_0)) \setminus \{0\})/\bar{k}^*. \tag{A.5}$$

As $\Gamma(X, \mathcal{L}(D_0)) = \mathrm{H}^0(X, \mathcal{L}(D_0)) := L(D_0)$ is of finite dimension over $\bar{k}$ ([Har77, III.5.2]) we put

$$\ell(D_0) = \dim_{\bar{k}} \Gamma(X, \mathcal{L}(D_0)) = \dim_{\bar{k}} L(D_0). \tag{A.6}$$

By (A.5), $|D_0|$ may be identified with projective $\bar{k}$-space of dimension $\ell(D_0) - 1$.

Now let X be a smooth curve in $\mathbb{P}^2 (= \mathbb{P}^2_{\bar{\mathbb{F}}_q})$ with function field K and let D_0 be a divisor on X. Write D_0 as

$$D_0 = \sum_{P \in X} n_P \cdot P \qquad \text{finitely many } n_P \neq 0$$

cf. (A.2). Then

$$\begin{aligned} L(D_0) &= \{f \in K^* : (f) \geq -D_0\} \\ &= \{f \in K^* : \nu_P(f) \geq -n_P \text{ for all } P \in X\}. \end{aligned}$$

If $D_0 = \sum_i n_{P_i} \cdot P_i \ - \ \sum_j m_{P_j} \cdot P_j$ $(n_{P_i}, m_{P_j} > 0)$ we may thus identify $L(D_0)$ with the vector space of rational functions on X with poles only in the points P_i and there of order no more than n_{P_i} and with zeros in P_j with multiplicity at least m_{P_j}.

We gather some simple observations in

Lemma A.13. *Let $X \subseteq \mathbb{P}^2$ be a smooth projective defined over k. Then*

a) $D \leq D' \Rightarrow L(D) \subseteq L(D')$ *and* $\dim_k L(D)/L(D') \leq \deg(D - D')$.

b) $D \sim D' \Rightarrow \ell(D) = \ell(D')$.

c) $L(0) = k$.

d) $\deg((f)) = 0$ *for* $f \in K^*$.

e) $\deg(D) < 0 \Rightarrow L(D) = \{0\}$.

Proof. a) Let $D = \sum_P n_P \cdot P$. Note that $L(D) \subseteq L(D+P)$ as $f \in L(D) \Rightarrow \nu_P(f) \geq -n_P \geq -(n_P+1)$ so $f \in L(D+P)$. Now as

$$D' = D + P_1 + \ldots + P_s$$

for some $P_i \in X$ it suffices to show that $\dim_k L(D+P)/L(D) \leq 1$ for all $P \in X$. Define $\varphi : L(D+P) \to k$ by

$$\varphi(f) = (t^{n_P+1} \cdot f)\text{'s image in } \mathcal{O}_{X,P}/\mathfrak{m}_P \simeq k$$

where $t \in \mathcal{O}_{X,P}$ is a generator of $\mathfrak{m}_P \subset \mathcal{O}_{X,P}$. φ is linear and

$$\ker(\varphi) = \{f \in L(D+P) : \nu_P(f) \geq -n_P \text{ for all } P \in X\} = L(D).$$

So φ induces an injection $L(D+P)/L(D) \hookrightarrow k$ and the claim follows.

b) This is clear from (A.5) as $\sim$ is an equivalence relation.

c) $L(0) = \{f \in K^* : \nu_P(f) \geq 0 \text{ for all } P \in X\} = k$.

d) Any $f \in K^*$ may be written as $f = g/h$, where g, h are homogeneous forms of the same degree m. But then

$$\deg((f)) = \deg((g/h)) = \deg((g)) - \deg((h)) = 0.$$

e) $L(D) = \{f \in K^* : (f) + D \geq 0\} = \{f \in K^* : (f) \geq -D\}$. But if $\deg(D) < 0$ we have

$$\{f \in K^* : (f) \geq -D\} \subseteq \{f \in K^* : \deg((f)) \geq -\deg(D) > 0\} = \{0\}$$

where we get the last equality from d).

□

Remark A.14. Let $X \subseteq \mathbb{P}^2$ be a smooth projective curve defined over k and let

$$\omega_X = \wedge^{\dim(X)}\Omega_{X/\bar{k}} = \wedge^1\Omega_{X/\bar{k}} = \Omega_{X/\bar{k}}$$

be the canonical linebundle on X. The *geometric genus of* X is then

$$p_g(X) = \dim_{\bar{k}} \Gamma(X, \omega_X).$$

Let us calculate ω_X. Assume X is defined by the irreducible homogeneous polynomial $f \in S = \bar{k}[X_0, X_1, X_2]$ of degree d. Then we have the short exact sequence of graded S-modules

$$0 \longrightarrow S(-d) \xrightarrow{\cdot f} S \longrightarrow S/(d) \longrightarrow 0$$

which gives rise to a short exact sequence of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2}(-d) \longrightarrow \mathcal{O}_{\mathbb{P}^2} \longrightarrow \mathcal{O}_X \longrightarrow 0$$

where $\mathcal{O}_{\mathbb{P}^2}(-d) \simeq \mathcal{I}_X$. Thinking of X as a divisor on $\mathbb{P}^2$, the adjunction formula ([Har77, II.8.18]) gives us

$$\omega_X \simeq \omega_{\mathbb{P}^2} \otimes_{\mathcal{O}_{\mathbb{P}^2}} \mathcal{L}(X) \otimes_{\mathcal{O}_{\mathbb{P}^2}} \mathcal{O}_X.$$

From [Har77, II.8.20.1] we have $\omega_{\mathbb{P}^2} \simeq \mathcal{O}_{\mathbb{P}^2}(-3)$ and by [Har77, II.6.13, II.6.18], $\mathcal{L}(X) \simeq \mathcal{L}(-X)^{-1} \simeq \mathcal{I}_X^{-1}$. This adds up to

$$\omega_X \simeq \mathcal{O}_{\mathbb{P}^2}(-3) \otimes_{\mathcal{O}_{\mathbb{P}^2}} \mathcal{O}_{\mathbb{P}^2}(-d)^{-1} \otimes_{\mathcal{O}_{\mathbb{P}^2}} \mathcal{O}_X = \mathcal{O}_X(d-3)$$

(where we consider $\mathcal{O}_X$ as an $\mathcal{O}_{\mathbb{P}^2}$-module). Then, if X is a curve of degree 3, $\omega_X \simeq \mathcal{O}_X$ and

$$p_g(X) = \dim_{\bar{k}} \Gamma(X, \omega_X) = \dim_{\bar{k}} \Gamma(X, \mathcal{O}_X) = 1.$$

Proposition A.15 ([Har77, Exercise III.5.3]). *Let X be a projective scheme of dimension r over the field k. Define the arithmetic genus p_a of X by*

$$p_a(X) = (-1)^r(\chi(\mathcal{O}_X) - 1)$$

where χ is the Euler characteristic

$$\chi(\mathcal{F}) = \sum_i (-1)^i \dim_k \mathrm{H}^i(X, \mathcal{F})$$

of a coherent sheaf $\mathcal{F}$ on X. We notice that the definition of $p_a(X)$ is independent of the embedding of X into projective space.

a) If X is irreducible and reduced and k is algebraically closed then $\mathrm{H}^0(X, \mathcal{O}_X) \simeq k$ and

$$p_a(X) = \sum_{i=0}^{r-1} (-1)^i \dim_k \mathrm{H}^{r-i}(X, \mathcal{O}_X).$$

In particular, if X is a curve, we have $p_a(X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$.

b) If furthermore X is a closed subvariety of $\mathbb{P}^r_k$ we have

$$p_a(X) = (-1)^r(P_X(0) - 1)$$

where P_X is the Hilbert polynomial associated to X.

Proof. a) As X is projective we have a closed immersion $i : X \to \mathbb{P}^n_k$. Then $\Gamma(X, \mathcal{O}_X) = \Gamma(\mathbb{P}^n_k, i_*\mathcal{O}_X) = \Gamma(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}) = k$ by [Har77, III.2.10, I.3.4]. So

$$p_a(X) = (-1)^r \Big(\sum_i (-1)^i \dim_k \mathrm{H}^i(X, \mathcal{O}_X) - 1 \Big) = \sum_{i=0}^{r-1} (-1)^i \dim_k \mathrm{H}^{r-i}(X, \mathcal{O}_X).$$

If X is a curve, $r = 1$ and we get $p_a(X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$.

b) By [Har77, Exercise III.5.2] the Hilbert polynomial P_X associated to X satisfies $P_X(n) = \chi(\mathcal{O}_X(n))$. But then $p_a(X) = (-1)^r(\chi(\mathcal{O}_X) - 1) = (-1)^r(P_X(0) - 1)$.

□

Proposition A.16 ([Har77, IV.1.1]). *Let X be a smooth projective curve over the algebraically closed field k. Then*

$$p_a(X) = p_g(X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X).$$

The common value g we call the genus of the curve X.

Proof. We have in Proposition A.15 seen that $p_a(X) = \dim_k \mathrm{H}^1(X, \mathcal{O}_X)$. From Serre-duality [Har77, III.7.6] we get

$$\mathrm{H}^1(X, \mathcal{O}_X)^\vee \simeq \mathrm{Ext}^0(\mathcal{O}_X, \omega_X) = \mathrm{Hom}(\mathcal{O}_X, \omega_X) = \mathrm{H}^0(\mathcal{O}_X, \omega_X).$$

But then $\dim_k \mathrm{H}^1(X, \mathcal{O}_X) = \dim_k \mathrm{H}^0(\mathcal{O}_X, \omega_X) = p_g(X)$. □

Theorem A.17 (Riemann-Roch). *Let X be a smooth projective curve of genus g over the algebraically closed field k and let D be a divisor on X. Then*

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g$$

where $K \in \mathrm{Div}(X)$ represents the divisor class associated to $\omega_X \in \mathrm{Pic}(X)$ cf. the isomorphism $\mathrm{Div}(X) \simeq \mathrm{Pic}(X)$ ([Har77, II.6.15]).

Proof. See [Har77, IV.1.3]. □

Corollary A.18. *With the above assumptions we have*

a) $\ell(K) = g$

b) $\deg(K) = 2g - 2$.

c) If $\deg(D) > 2g - 2$ *then* $\deg(K - D) < 0$ *and* $\ell(D) = \deg(D) + 1 - g$.

Proof. a) $\ell(K) = \dim_k \Gamma(X, \mathcal{L}(K)) = \dim_k \Gamma(X, \omega_X) = p_g(X) = g$.

b) Riemann-Roch applied to $D = K$ gives

$$\ell(K) - \ell(0) = \deg(K) + 1 - g.$$

So as $\ell(0) = \dim_k \Gamma(X, \mathcal{O}_X) = 1$, we have $\deg(K) = 2g - 2$ by a).

c) $\deg(K - D) = \deg(K) - \deg(D) = 2g - 2 - \deg(D) < 0$, hence Riemann-Roch gives

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g$$

and as $\deg(K - D) < 0$, Lemma A.13 implies $\ell(K - D) = 0$.

□

Proposition A.19 ([Har77, Exercise III.4.7]). *Let X be a curve in $\mathbb{P}^2 = \operatorname{Proj} S$, defined by the homogeneous polynomial $f \in S$ of degree d. Then*

a) $\dim_k \mathrm{H}^0(X, \mathcal{O}_X) = 1$.

b) $\dim_k \mathrm{H}^1(X, \mathcal{O}_X) = \frac{1}{2}(d-1)(d-2)$.

Proof. As X is a closed subscheme of $\mathbb{P}^2$ defined by the homogeneous polynomial f of degree d we have the short exact sequence of graded S-modules

$$0 \longrightarrow S(-d) \xrightarrow{\cdot f} S \longrightarrow S/(d) \longrightarrow 0$$

which gives rise to a short exact sequence of $\mathcal{O}_X$-modules

$$0 \longrightarrow \mathcal{O}_{\mathbb{P}^2}(-d) \longrightarrow \mathcal{O}_{\mathbb{P}^2} \longrightarrow \mathcal{O}_X \longrightarrow 0$$

where $\mathcal{O}_{\mathbb{P}^2}(-d) \simeq \mathcal{I}_X$. By [Har77, III.1.1A] we now get a long exact sequence of cohomology groups

$$\begin{aligned} 0 \to \mathrm{H}^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d)) \to \mathrm{H}^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) \to \mathrm{H}^0(X, \mathcal{O}_X) \to \mathrm{H}^1(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d)) \to \\ \mathrm{H}^1(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) \to \mathrm{H}^1(X, \mathcal{O}_X) \to \mathrm{H}^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d)) \to \mathrm{H}^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) \to \ldots \end{aligned} \quad (A.7)$$

By [Har77, III.5.1] this reduces to

$$\begin{aligned} 0 \to 0 \to \mathrm{H}^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) \xrightarrow{\simeq} \mathrm{H}^0(X, \mathcal{O}_X) \to 0 \to \\ 0 \to \mathrm{H}^1(X, \mathcal{O}_X) \xrightarrow{\simeq} \mathrm{H}^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d)) \to 0 \to 0. \end{aligned} \quad (A.8)$$

Hence

$$\begin{aligned} \dim_k \mathrm{H}^0(X, \mathcal{O}_X) &= \dim_k \mathrm{H}^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}) = \dim_k k = 1 \\ \dim_k \mathrm{H}^1(X, \mathcal{O}_X) &= \dim_k \mathrm{H}^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d)) \end{aligned}$$

and as $\mathrm{H}^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d))$ may identified with the k-vector space spanned by

$$\{X_0^{n_0} X_1^{n_1} X_2^{n_2} : n_i < 0 \ \wedge \ n_0 + n_1 + n_2 = -d\}$$

cf. [Har77, p. 226], we see that

$$\begin{aligned} \dim_k \mathrm{H}^2(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(-d)) &= |\{X_0^{n_0} X_1^{n_1} X_2^{n_2} : n_i \geq 0 \wedge \ n_0 + n_1 + n_2 = d - 3\}| \\ &= \frac{1}{2}(d-1)(d-2). \end{aligned}$$

□

Corollary A.20. *Let C be a projective curve in $\mathbb{P}^2$ defined by the homogeneous polynomial f of degree d. Then C has genus*

$$g = \frac{1}{2}(d-1)(d-2). \tag{A.9}$$

Proof. Combine Proposition A.19 and Proposition A.16. □

Appendix B

Weil's explicit formulas

B.1 The formulas

The Weil bound (Corollary 2.6) on the number of rational points on a given curve of genus g, may in most cases be improved. We use the notation from Chapter 2. All curves are still assumed smooth and projective.

Remark B.1. Let C curve of g. From Corollary 2.5 we have for all $m \geq 1$

$$N_m = 1 + q^m - \sum_{n=1}^{2g} \alpha_i^m. \tag{B.1}$$

Determine $\theta_j \in \mathbb{R}$ such that $\alpha_j = \sqrt{q}\mathrm{e}^{i\theta_j}$. By Corollary 2.35 we may assume that $\overline{\alpha}_j = \alpha_{2g-j}$, hence

$$\begin{aligned} N_m &= 1 + q^m - \sum_{j=1}^{g} \alpha_j^m + \overline{\alpha}_j^m = 1 + q^m - q^{\frac{m}{2}} \sum_{j=1}^{g} \mathrm{e}^{(im\theta_j)} + \mathrm{e}^{(-im\theta_j)} \\ &= 1 + q^m - 2q^{\frac{m}{2}} \sum_{j=1}^{g} \cos(m\theta_j) \end{aligned} \tag{B.2}$$

Now let $\{c_n\}_{n\geq 1}$ be real numbers, almost all equal to zero. Multiply by c_m in (B.2) and divide with $q^{\frac{1}{2}}$, thereby

$$N_1 c_m q^{-\frac{m}{2}} = c_m q^{\frac{m}{2}} + c_m q^{-\frac{m}{2}} - 2\sum_{j=1}^{g} c_m \cos(m\theta_j) - (N_m - N_1)c_m q^{-\frac{m}{2}}. \tag{B.3}$$

Introduce the notation

$$f(\theta) = 1 + 2\sum_{n=1}^{\infty} c_n \cos(n\theta) = 1 + \sum_{n=1}^{\infty} c_n \big(\mathrm{e}^{in\theta} + \mathrm{e}^{-in\theta}\big) \qquad \theta \in \mathbb{R}$$

$$\Psi_d(t) = \sum_{n=1}^{\infty} c_{nd} t^{nd} \qquad d \in \mathbb{N},\ t \in \mathbb{R}$$

By summing (B.3) over m we get

$$\begin{aligned} N_1 \Psi_1\big(q^{-\frac{1}{2}}\big) &= N_1 \sum_{m=1}^{\infty} c_m q^{-\frac{m}{2}} \\ &= \Psi_1\big(q^{\frac{1}{2}}\big) + \Psi_1\big(q^{-\frac{1}{2}}\big) - \sum_{j=1}^{g} (f(\theta_j) - 1) - \sum_{m=1}^{\infty} (N_m - N_1) c_m q^{-\frac{m}{2}}. \end{aligned}$$

Notice that

$$\sum_{m=1}^{\infty} N_m c_m q^{-\frac{m}{2}} = \sum_{m=1}^{\infty} \sum_{d|m} d a_d c_m q^{-\frac{m}{2}} \sum_{d=1}^{\infty} d a_d \sum_{m=1}^{\infty} c_{md} q^{-\frac{md}{2}} = \sum_{d=1}^{\infty} d a_d \Psi_d\big(q^{-\frac{1}{2}}\big) \tag{B.4}$$

so we may write (B.3) as

$$N_1 \cdot \Psi_1\big(q^{-\frac{1}{2}}\big) = \Psi_1\big(q^{\frac{1}{2}}\big) + \Psi_1\big(q^{-\frac{1}{2}}\big) + g - \sum_{j=1}^{g} f(\theta_j) - \sum_{d=2}^{\infty} d a_d \Psi_d\big(q^{-\frac{1}{2}}\big). \tag{B.5}$$

This equation is usually called *Weil's explicit formula.*

Proposition B.2. *With the above notation, assume the $\{c_n\}$ have the following properties*

a) $c_n \geq 0$, not all $c_n = 0$.

b) $f(\theta) \geq 0$ for all $\theta \in \mathbb{R}$.

Then

$$N \ \leq\ \frac{g}{\Psi_1\big(q^{-\frac{1}{2}}\big)} + \frac{\Psi_1\big(q^{\frac{1}{2}}\big)}{\Psi_1\big(q^{-\frac{1}{2}}\big)} + 1 \tag{B.6}$$

with equality if and only if

$$\sum_{j=1}^{g} f(\theta_j) = 0 \qquad \text{and} \qquad \sum_{d=2}^{\infty} d a_d \Psi_d\big(q^{-\frac{1}{2}}\big) = 0.$$

Proof. As $N_m \geq N = N_1$ for all $m \geq 1$ and as all $c_n \geq 0$ by assumptions, we get

$$0 \leq \sum_{m=1}^{\infty} (N_m - N_1) c_m q^{-\frac{m}{2}} = \sum_{d=2}^{\infty} d a_d \Psi_d\left(q^{-\frac{1}{2}}\right). \tag{B.7}$$

Also by assumption, $0 \leq \sum_{j=1}^{g} f(\theta_j)$, so (B.5) implies

$$N \leq \frac{g}{\Psi_1\left(q^{-\frac{1}{2}}\right)} + \frac{\Psi_1\left(q^{\frac{1}{2}}\right)}{\Psi_1\left(q^{-\frac{1}{2}}\right)} + 1$$

as $\Psi_1\left(q^{-\frac{1}{2}}\right) > 0$. The last assertion is obvious from (B.5). □

Remark B.3. 1. With the above notation, $c_1 = \frac{1}{2}$, $c_i = 0$ for $i \geq 2$, give the Weil bound (Corollary 2.6), $N \leq 1 + q + 2g\sqrt{q}$.

2. In the Theory of Error-correcting Codes on Curves, one is interested in curves where, given the genus g of the curve the number N of k-rational points on the curve is as large as possible. By finding $\{c_n\}$ which have the properties required above, we get a bound on the ratio

$$\frac{N}{g} \leq \frac{1}{\Psi_1\left(q^{-\frac{1}{2}}\right)} + \frac{1}{g}\left(\frac{\Psi_1\left(q^{\frac{1}{2}}\right)}{\Psi_1\left(q^{-\frac{1}{2}}\right)} + 1\right)$$

with equality in some cases. When equality is obtained, we say that the curve is *maximal* (with respect to the explicit formulas). With this in mind, we now see that the curves in Example 2.9 and Example 2.11 are maximal (with respect to the Weil bound). Other maximal curves are found and described in [HS90, Han92, Pet92]. In [Lac87] a whole family of maximal curves is described. See also [GvdG95].

Example B.4. Assume $q = 2^{2r+1}$ for some $r \geq 1$. Put $q_0 = 2^r$. Consider the curve $C \subseteq \mathbb{P}^2$ defined over $k = \mathbb{F}_q$ and given by the equation

$$C: \qquad x^{q_0}(z^q + zx^{q-1}) = y^{q_0}(y^q + yx^{q-1}). \tag{B.8}$$

In [HS90] it is shown that the curve has genus $g = q_0(q-1)$. The Weil bound then gives

$$N \leq 1 + q + 2q_0(q-1)\sqrt{q} = 1 + \sqrt{2}q^2 + (1 - \sqrt{2})q.$$

N is found to be $N = 1 + q^2$ as $C(k)$ consists of $\mathbb{P}^2(k) \setminus V((x)) = \mathbb{A}^2(k)$ plus the point at infinity. By taking $c_1 = \frac{\sqrt{2}}{2}$, $c_2 = \frac{1}{4}$, $c_i = 0$ for $i \geq 3$, (B.6) gives

$$N \leq \frac{q_0(q-1)}{\frac{1}{2q_0} + \frac{1}{4q}} + 1 + \frac{q_0 + \frac{q}{4}}{\frac{1}{2q_0} + \frac{1}{4q}} = 1 + q^2. \tag{B.9}$$

Hence, C is maximal with respect to the explicit formulas.

B.2 Optimization

We will now, given N, q ($q \geq 3$), find the best choice of the $\{c_n\}$, i.e. the best possible lower bound on g. Oesterlé found an explicit recipe for finding the $\{c_n\}$ giving a bound on g. For $q \geq 3$ (and in some cases also for $q = 2$) he constructed a measure μ on S^1 such that

$$\int_{S^1} \tfrac{1}{2} d\mu = (N-1) \sum_{n=1}^{\infty} c_n q^{-\frac{n}{2}} - \sum_{n=1}^{\infty} c_n q^{\frac{n}{2}}$$

and showed that this happens exactly when the $\{c_n\}$ optimize the bound on g. Following [Ser85] we will briefly explain Oesterlé's constructions. Let N and q be given (and fixed). Above we saw (B.6) that for $\{c_n\}$ chosen as in Proposition B.2 we have

$$g \geq (N-1) \sum_{n=1}^{\infty} c_n q^{-\frac{n}{2}} - \sum_{n=1}^{\infty} c_n q^{\frac{n}{2}} \tag{B.10}$$

and we want to maximize the right hand side. Let $\theta_1, \ldots, \theta_n$ be as above. Let δ denote the Dirac measure and introduce the measure μ on $S^1 = \{z \in \mathbb{C} : |z| = 1\}$:

$$\mu = \sum_{j=1}^{g} \delta_{\mathrm{e}^{i\theta_j}} + \delta_{\mathrm{e}^{-i\theta_j}}.$$

We then have $\mu \geq 0$ and $\mu(S^1) = 2g$. We may rewrite (B.2) as

$$\frac{(1+q^n) - N_n}{q^{\frac{1}{2}}} = \sum_{j=1}^{g} 2\cos(n\theta_j) = \sum_{j=1}^{g} \mathrm{e}^{in\theta_j} + \mathrm{e}^{-in\theta_j} = \int_{S^1} t^n d\mu = \int_{S^1} \tfrac{1}{2}(t^n + t^{-n}) d\mu$$

and we will see that, looking for c_n maximizing the RHS of (B.10), is the same as looking for measures μ on S^1 such that

$$\int_{S^1} t^n d\mu \leq q^{\frac{n}{2}} - (N-1) q^{-\frac{n}{2}} := \gamma_n \tag{B.11}$$

for all $n \geq 1$.

Definition B.5. When varying μ and the $\{c_n\}$, let $g'(N,q)$ be the lower bound of $\frac{1}{2}\int_{S^1} d\mu$ and let $g(N,q)$ denote the maximum of the RHS in (B.10)

Lemma B.6. *If μ satisfy* (B.11) *and the $\{c_n\}$ satisfies* (B.10) *we have*

$$-\sum_{n=1}^{\infty} c_n \gamma_n \leq \int_{S^1} \tfrac{1}{2} d\mu. \tag{B.12}$$

In particular, $g(N,q) \leq g'(N,q)$.

Proof. As f is positive and given by $f = 1 + \sum_n c_n(t^n + t^{-n})$ on S^1 and as

$$\mu(t^n) = \int_{S^1} t^n d\mu \leq \gamma_n$$

we have

$$0 \leq \mu(f) = \mu(1) + 2\sum_{n=1}^{\infty} c_n \mu(t^n).$$

Hence

$$\int_{S^1} \tfrac{1}{2} d\mu = \mu(\tfrac{1}{2}) \geq -\sum_{n=1}^{\infty} c_n \mu(t^n) \geq -\sum_{n=1}^{\infty} c_n \gamma_n.$$

□

Lemma B.7. *We have equality in* (B.12) *if and only if*

a) μ's support on S^1 is contained in the zeroes of the function $f = 1 + \sum_n c_n(t^n + t^{-n})$ on S^1.

b) There is equality in (B.11) *for all n for which $c_n \neq 0$.*

Proof. With the proof of Lemma B.6 in mind, we want $\mu(f) = 0$, so a) is straightforward. Since we also want $\mu(t^n) = \gamma_n$ unless $c_n = 0$, b) is also obvious. □

Theorem B.8. *Let μ be as described in Lemma* B.7. *Then*

$$g(N, q) = \int_{S^1} \tfrac{1}{2} d\mu = -\sum_{n=1}^{\infty} c_n \gamma_n.$$

Proof. From Lemma B.6 we have $g(N, q) \leq g'(N, q)$ and by (B.12), $g'(N, q) \geq -\sum_n c_n \gamma_n$. By assumption

$$g'(N, q) \leq \int_{S^1} \tfrac{1}{2} d\mu = -\sum_{n=1}^{\infty} c_n \gamma_n$$

hence

$$g(N, q) \leq g'(N, q) \leq g(N, q)$$

and we have equality. □

Proposition B.9. *For $q + 1 \leq N \leq q^{\frac{3}{2}} + 1$ the Weil bound is optimal.*

Proof. Earlier we saw that the Weil bound corresponds to the choice $c_1 = \frac{1}{2}$, $c_n = 0$ $(n \geq 2)$. We must show that this choice is optimal. By the above, it will suffice to construct a measure μ on S^1 such that equality is obtained in (B.12). In that situation we have

$$g(N, q) = -\tfrac{1}{2}\gamma_1 = -\tfrac{1}{2}\big(q^{\frac{1}{2}} - (N-1)q^{-\frac{1}{2}}\big) = \tfrac{1}{2}\big((N-1)q^{-\frac{1}{2}} - q^{\frac{1}{2}}\big) \geq 0.$$

So let μ be the Dirac measure in $t = -1$ (angle $\theta = \pi$) with weight $2(-\frac{1}{2}\gamma_1)$. We must check

- $1+\cos(\theta) \geq 0$ and $c_n \geq 0$: OK.
- $\mathrm{Supp}(\mu) \subseteq \ker(1+\cos(\theta))$: OK.
- $\mu(t) = \gamma_1$: $\mu(t) = 2(-\frac{1}{2}\gamma_1)(-1) = \gamma_1$ by construction.
- $\mu(t^n) \leq \gamma_n$ for $n \geq 2$:

$$\begin{aligned} \mu(t^2) = 2(-\tfrac{1}{2}\gamma_1)(-1)^2 = -\gamma_1 \leq \gamma_2 & \quad \Leftrightarrow \\ -q^{-\frac{1}{2}} + (N-1)q^{-\frac{1}{2}} \leq q - (N-1)q^{-1} & \quad \Leftrightarrow \\ (N-1)\big(q^{-\frac{1}{2}} + q^{-1}\big) \leq q + q^{\frac{1}{2}} & \quad \Leftrightarrow \\ (N-1)\big(1 - q^{\frac{1}{2}}\big) \leq q^{\frac{3}{2}}\big(1 - q^{\frac{1}{2}}\big) & \quad \Leftrightarrow \\ N - 1 \leq q^{\frac{3}{2}} & \end{aligned}$$

  and the last inequality is true by the condition on N. $\mu(t^3) = -2(-\frac{1}{2}\gamma_1) = \gamma_1$ and as $-2(-\frac{1}{2}\gamma_1) \leq 0$ and $\gamma_3 \geq 0$ we have $\mu(t^3) \leq \gamma_3$. $\mu(t^4) = 2(-\frac{1}{2}\gamma_1) = -\gamma_1 \leq \gamma_2 \leq 4$ as γ_n grows for large n. This generalizes for larger n.

By Lemma B.7 we now have equality in (B.12). □

Definition B.10. Define the following notation $\lambda = N-1$, $\alpha = q^{\frac{1}{2}}$ and define $m \in \mathbb{N}$ by $\alpha^m < \lambda \leq \alpha^{m+1}$, i.e. $m = \left[\frac{\log\lambda}{\log\alpha}\right]$. We may assume $m \geq 2$ as $m = 1$ gives $q^{\frac{1}{2}} < N - 1 \leq q$ which may be obtained by taking g=0. Put

$$u = \frac{\alpha^{m+1} - \lambda}{\lambda\alpha - \alpha^m}.$$

By construction $0 \leq u < 1$. Define furthermore $\varphi_0 \in \left[\frac{\pi}{m+1}, \frac{\pi}{m}\right[$ by taking φ_0 to be a solution of

$$\cos\Big(\frac{m+1}{2}\varphi\Big) + u\,\cos\Big(\frac{m-1}{2}\varphi\Big) = 0. \tag{B.13}$$

Later we will see that the condition $\varphi_0 \in \left[\frac{\pi}{m+1}, \frac{\pi}{m}\right[$ determines φ_0 uniquely.

Remark B.11. With the notation introduced, we may rewrite (B.11) as

$$\int_{S^1} t^n d\mu \leq \alpha^n - \lambda\alpha^{-n} \qquad n \geq 1$$

Now we will construct a measure μ on S^1 satisfying this equation and such that

a) μ is concentrated in a symmetric set $T \subseteq S^1$ with $|T| = m - 1$.

b) We have

$$\int_{S^1} t^n d\mu = \alpha^n - \lambda\alpha^{-n} \qquad n = 1, \dots, m-1.$$

c) μ may be written as

$$\mu = \sum_{t\in T} \nu_t \delta_t \qquad \nu_t > 0$$

where $\nu_t = \nu_{\bar{t}}$.

On the other hand, we want $\{c_n\}$ such that

$$f(t) = 1 + \sum_{n=1}^{m-1} c_n(t^n + t^{-n}) \qquad c_n \geq 0$$

is zero on T and non-negative on S^1. If this is possible Theorem B.8 implies

$$g(N,q) = \int_{S^1} \tfrac{1}{2} d\mu = -\sum_{n=1}^{m-1} c_n(\alpha^n - \lambda\alpha^{-n})$$

with the notation introduced.

Lemma B.12. *Suppose we have found $T \subseteq S^1$ as above. Then T is contained in the set of solutions to*

$$s^{m+1} + 1 + u(s^m + s) = 0. \tag{B.14}$$

Proof. Let T be given. T has $m-1$ elements in S^1. By assumption

$$\int_{S^1} t^n d\mu = \sum_{t\in T} \nu_t t^n = \alpha^n - \lambda\alpha^{-n} \qquad n = 1, \dots, m-1$$

We see that this equation is equivalent to: for any polynomial Φ, $\deg(\Phi) \leq m-1$ with constant term equal to zero we have

$$\sum_{t\in T} \nu_t \Phi(t) = \Phi(\alpha) - \lambda\Phi(\alpha^{-1}). \tag{B.15}$$

Let $P(X) = \prod_{t\in T}(X - t)$. As T is symmetric, $P(X^{-1}) = P(X) \cdot X^{1-m}$, so

$$-\frac{1}{X^2} P'(X^{-1}) = P'(X)X^{1-m} + (1-m)P(X)X^{-m}.$$

So for $t \in T$ we have $-\bar{t}^2 P'(\bar{t}) = P'(t)t^{1-m}$ as $\bar{t} = \frac{1}{t}$. Now choose $t \in T$ and define

$$Q_t(X) = X \prod_{t' \in T \setminus \{t\}} (X - t') = \frac{X\,P(X)}{X - t}.$$

Thereby $\deg(Q_t) \leq m - 1$ and

$$Q_t(t') = \begin{cases} 0 & t' \neq t \\ t\,P'(t) & t' = t \end{cases}$$

and by applying (B.15) to $\Phi = Q_t$ we get

$$\nu_t Q_t(t) = Q_t(\alpha) - \lambda Q_t(\alpha^{-1})$$

so that

$$\nu_t = \frac{Q_t(\alpha) - \lambda Q_t(\alpha^{-1})}{t\,P'(t)}.$$

We may reformulate this as

$$\begin{aligned} t\,P'(t)\nu_t &= \frac{\alpha P(\alpha)}{\alpha - t} - \lambda \frac{\alpha^{-1} P(\alpha^{-1})}{\alpha^{-1} - t} \\ &= P(\alpha)\left(\frac{\alpha}{\alpha - t} - \lambda \frac{\alpha^{-m}}{\alpha^{-1} - t}\right) \\ &= \frac{1 - \alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2} \end{aligned}$$

the last equality coming from $P(\alpha^{-1}) = P(\alpha)\alpha^{1-m}$. Now as $\nu_t = \nu_{\bar{t}}$ we have

$$\frac{1}{tP'(t)}\left(\frac{1 - \alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2}\right) = \frac{1}{\bar{t}P'(\bar{t})}\left(\frac{1 - \alpha\bar{t} - \lambda\alpha^{1-m} + \bar{t}\lambda\alpha^{-m}}{1 - \alpha\bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2}\right).$$

Since $-P'(\bar{t}) = P'(t) \cdot t^{3-m}$ we get

$$-t^{1-m}\left(\frac{1 - \alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m}}{1 - \alpha t - \alpha^{-1}t + t^2}\right) = \frac{1 - \alpha\bar{t} - \lambda\alpha^{1-m} + \bar{t}\lambda\alpha^{-m}}{1 - \alpha\bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2}$$

and as $t^2(1 - \alpha\bar{t} - \alpha^{-1}\bar{t} + \bar{t}^2) = t^2 - \alpha t - \alpha^{-1}t + 1$ we have

$$\begin{gathered} -t^{m+1}(1 - \alpha\bar{t} - \alpha^{-m}\bar{t}) = 1 - \alpha t - \lambda\alpha^{1-m} + t\lambda\alpha^{-m} \\ t^{m+1}(1 - \lambda\alpha^{1-m}) + t^m(\lambda\alpha^{-m} - \alpha) - t(\alpha - \lambda\alpha^{-m}) + (1 - \lambda\alpha^{1-m}) = 0. \end{gathered}$$

Hence

$$t^{m+1} + 1 + \frac{\lambda\alpha^{-m} - \alpha}{1 - \lambda\alpha^{1-m}}(t^m + t) = 0$$

and as $u = \frac{\alpha^{m+1} - \lambda}{\lambda\alpha - \alpha^m} = \frac{\lambda\alpha^{-m} - \alpha}{1 - \lambda\alpha^{1-m}}$ the assertion follows. □

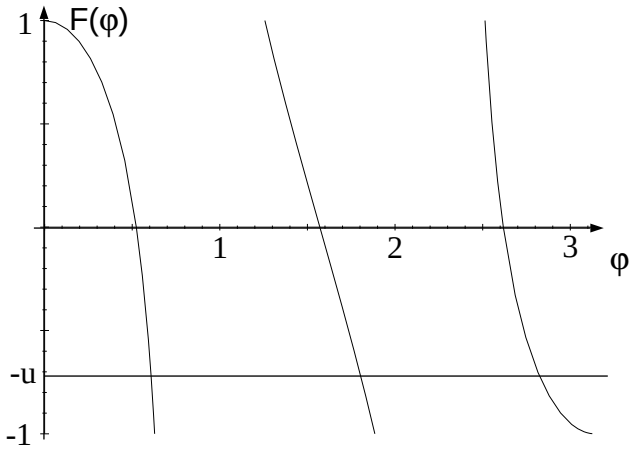


Figure B.1: The graph of F for $m = 5$.

Lemma B.13. *The equation* (B.14) *has* $m+1$ *solutions in* S^1 *and exactly one of the form* $t = \mathrm{e}^{\pm i\varphi_0}$ *with* $\varphi_0 \in \left[\frac{\pi}{m+1}, \frac{\pi}{m}\right[$.

Proof. First notice, that if m is even -1 is a solution and if m is odd this is not the case. Now put

$$F(\varphi) = \frac{\cos\left(\frac{m+1}{2}\varphi\right)}{\cos\left(\frac{m-1}{2}\varphi\right)}.$$

We see that $F(\varphi_0) = -u$ by definition of φ_0. If $s = \mathrm{e}^{i\varphi}$ with $F(\varphi) = -u$ we have

$$\begin{aligned} -u = F(\varphi) &= \frac{\cos\left(\frac{m+1}{2}\varphi\right)}{\cos\left(\frac{m-1}{2}\varphi\right)} && \Rightarrow \\ -u = F(\varphi) &= \frac{s^{\frac{m+1}{2}\varphi} + s^{-\frac{m+1}{2}\varphi}}{s^{\frac{m-1}{2}\varphi} + s^{-\frac{m-1}{2}\varphi}} && \Rightarrow \\ -u &= \frac{s^{m+1}+1}{s^m + s} \end{aligned}$$

that is, s solves (B.14). This is also the case if $s = \mathrm{e}^{-i\varphi}$. Now a given m corresponds to a $u \in [0, 1[$ and we must show that $F(\varphi) = -u$ has $\frac{m}{2}$ solutions if m is even and $\frac{m+1}{2}$ solutions if m is odd. Consider the example $m = 5$ where we have the graph of $F(\varphi)$ above. We see that $F(\varphi) = -u$ has 3 solutions with the first in the interval $\left[\frac{\pi}{6}, \frac{\pi}{5}\right[$, as wanted. The same behaviour is seen in the general case. □

Definition B.14. a) Let T be the complement of $\mathrm{e}^{\pm i\varphi_0}$ in the set of solutions on S^1 to (B.15).

b) Define $\nu_t \in \mathbb{C}$ by solving the $m-1$ equations in $m-1$ unknowns.

$$\sum_{t\in T} \nu_t t^n = \alpha^n - \lambda\alpha^{-n} \qquad n = 1, \dots, m-1.$$

Lemma B.15. *We have*

a) $\nu_t > 0$ *for all* $t \in T$.

b) $\nu_t = \nu_{\bar{t}}$ *for all* $t \in T$.

c) For $n \geq m$ *we have*

$$\sum_{t\in T} \nu_t t^n \leq \alpha^n - \lambda\alpha^{-n}$$

whenever $\alpha \geq \sqrt{3}$.

Proof. Long technical calculations – omitted. □

Definition B.16. a) Define the polynomial $P(X) = \prod_{t\in T}(X - t)$ and write

$$P(X)P(X^{-1}) = \sum_{n=-(m-1)}^{m-1} a_n X^n$$

As the ν_t are real, $P(z)P(z^{-1}) = P(z)P(\bar{z}) = P(z)\overline{P(z)} \geq 0$ and as $0 \notin T$ we have $a_0 > 0$. Therefore me may define

$$\begin{aligned} f(t) &= \frac{1}{a_0} P(t)P(t^{-1}) \qquad t \in S^1 \\ &= 1 + \sum_{n=1}^{m-1} c_n(t^n + t^{-n}) \end{aligned}$$

where $c_n = \frac{a_n}{a_0}$ for $n = 1, \dots, m-1$.

b) Define the measure on S^1

$$\mu = \sum_{t\in T} \nu_t \delta_t.$$

Theorem B.17. μ *and* f *defined above satisfies the conditions of Remark* B.11 *and*

$$g(N, q) = \int_{S^1} \tfrac{1}{2} d\mu = -\sum_{n=1}^{m-1} c_n(\alpha^n - \lambda\alpha^{-n})$$

for $q \geq 3$.

Proof. By construction $f(t) = 0$ except on T and is non-negative on S^1. Also by construction the conditions on μ are satisfied. Now by Lemma B.15 we may apply Theorem B.8. □

Corollary B.18.

$$g \geq g(N,q) = \sum_{n=1}^{m-1} c_n(\lambda\alpha^{-n} - \alpha^n) = \frac{(\lambda-1)\alpha\cos(\varphi_0) + \alpha^2 - \lambda}{\alpha^2 - 2\alpha\cos(\varphi_0) + 1}$$

for $q \geq 3$.

Proof. For $n = 0, \ldots, m-1$ one finds that

$$a_n = (m-n)\cos(n\varphi_0)\sin(\varphi_0) + \sin((m-n)\varphi_0) \tag{B.16}$$

and by substitution in Theorem B.17 we get the wanted expression. □

Remark B.19. For $\alpha = \sqrt{2}$, i.e. $q = 2$ this method does not necessarily give the optimal bound because, for some λ the inequality

$$\sum_{t\in T} \nu_t t^n \leq \alpha^n - \lambda\alpha^{-n}$$

is not satisfied for all $n \geq m$. For $\lambda \leq 130$ this is the case for the following values of N:

$$51, 52, 53, 70, 71, \ldots, 77, 98, 99, \ldots, 110.$$

Remark B.20. In [LT95] the content of this appendix is written in more detail and the explicit formulas are generalized to higher-dimensional varieties by means of the Betti numbers. But, as also pointed out in [LT95], it is only in the case of curves where it is possible to determine the optimal bound.

The explicit formulas were seen for the first time in Weil's paper [Wei52] and have since been used occasionally, especially by Serre [Ser83, Ser85]. See also [LW54, Sch91, Tsf94, vdGvdV93].

B.3 Examples

Example B.21. Let $q = 3$ and $N = 20$. We here give the input/output from the mathematics program Maple (read $\phi = \varphi_0$).

```
> q:= 3;
```

$$q := 3$$

```
> N:=20;
```

$$N := 20$$

```
> lambda:=N-1;
```

$$\lambda := 19$$

```
> alpha:=sqrt(q);
```

$$\alpha := \sqrt{3}$$

```
> M:=max(trunc(simplify(log(lambda)/log(alpha))),2);
```

$$M := 5$$

```
> u:= (alpha^(M+1) - lambda)/(lambda*alpha - alpha^M);
```

$$u := \frac{4}{15}\sqrt{3}$$

```
> phi:=fsolve(cos((M+1)*X/2) + u * cos((M-1)*X/2)=0,X,Pi/(M+1)..Pi/M);
```

$$\phi := .5842209818$$

```
> a:= array(0..(M-1));
```

$$a := \mathrm{array}0..4, [\,]\,)$$

```
> for i to M do a[i-1]:= (M-(i-1))*cos((i-1)*PHI)*sin(PHI)
> + sin((M-(i-1))*PHI) od;
```

$$a_0 := 2.837296694$$

$$a_1 := 2.414213562$$

$$a_2 := 1.735673683$$

$$a_3 := 1.000000000$$

$$a_4 := .3826834323$$

```
> c:= array(0..(M-1));
```

$$c := \text{array}0..4, [\ ])$$

```
> for i to M do c[i-1]:= a[i-1]/a[0] od;
```

$$c_0 := 1.000000000$$

$$c_1 := .8508851285$$

$$c_2 := .6117349964$$

$$c_3 := .3524481603$$

$$c_4 := .1348760717$$

```
> g(N,q):= ((lambda-1)*alpha*cos(phi)+alpha^2-lambda)/ (alpha^2 - 2*alpha*
> cos(phi) +1);
```

$$\text{g}(20, 3\ ) := \frac{15.01455611\sqrt{3} - 16}{4 - 1.668284012\sqrt{3}}$$

```
> gBOUND(N,q) := ceil(evalf(g(N,q)));
```

$$\text{gBOUND}(20, 3\ ) := 10$$

```
> clear;
```

$$clear$$

```
> q:= 2;
```

$$q := 2$$

```
> alpha:=sqrt(q);
```

$$\alpha := \sqrt{2}$$

```
> gBOUNDS:=array(3..100);
```

$$gBOUNDS := \text{array}(3..100, [\ ])$$

```
> for  N from 3 to 100 do lambda:=N-1: M:=max(trunc(simplify(log(lambda)/log
> (alpha))),2) : u:= (alpha^(M+1) - lambda)/(lambda*alpha - alpha^M) :
> phi:=fsolve(cos((M+1)*X/2) + u * cos((M-1)*X/2)=0,X,Pi/(M+1)..Pi/M):
> g(N,q):= ((lambda-1)*alpha*cos(phi)+alpha^2-lambda)/
> (alpha^2 - 2*alpha*cos(phi) +1):
> gBOUND(N,q) := ceil(g(N,q)): gBOUNDS[N]:=evalf(gBOUND(N,q))  od:
> NMAXS:= array(3..100);
```

$$NMAXS := \text{array}(3..100, [\,])$$

```
> print(gBOUNDS);
```

N	3	4	5	6	7	8	9	10	11
$g \geq$	0	1	1	2	3	4	5	6	7
N	12	13	14	15	16	17	18	19	20
$g \geq$	9	10	11	12	14	15	16	18	19
N	21	22	23	24	25	26	27	28	29
$g \geq$	20	22	23	25	26	28	29	31	32
N	30	31	32	33	34	35	36	37	38
$g \geq$	34	35	37	38	40	41	43	44	46
N	39	40	41	42	43	44	45	46	47
$g \geq$	48	49	51	52	54	56	57	59	60
N	48	49	50	51	52	53	54	55	56
$g \geq$	62	64	65	67	69	70	72	74	75
N	57	58	59	60	61	62	63	64	65
$g \geq$	77	79	80	82	84	85	87	89	90
N	66	67	68	69	70	71	72	73	74
$g \geq$	92	94	95	97	99	101	102	104	106
N	75	76	77	78	79	80	81	82	83
$g \geq$	107	109	111	113	114	116	118	119	121
N	84	85	86	87	88	89	90	91	92
$g \geq$	123	125	126	128	130	132	133	135	137
N	93	94	95	96	97	98	99	100	
$g \geq$	139	140	142	144	146	148	149	151	

```
> NBOUNDS:= array(3..100);
```

$$NBOUNDS := \text{array}(3..100, [\,])$$

```
> for i from 3 to 100 do : for j from 3 to 100 do : if gBOUNDS[j] <=i then
> NBOUNDS[i]:=j fi  : od: od ;
> for i from 3 to 100 do : WeilBOUNDS[i]:=floor(1+2+2*i*sqrt(2)) : od :
> print(NBOUNDS,(WeilBOUNDS));
```

g	3	4	5	6	7	8	9
$N \leq$	7 (11)	8 (14)	9 (17)	10 (19)	11 (22)	11 (25)	12 (28)
g	10	11	12	13	14	15	16
$N \leq$	13 (31)	14 (34)	15 (36)	15 (39)	16 (42)	17 (45)	18 (48)
g	17	18	19	20	21	22	23
$N \leq$	18 (51)	19 (53)	20 (56)	21 (59)	21 (62)	22 (65)	23 (68)
g	24	25	26	27	28	29	30
$N \leq$	23 (70)	24 (73)	25 (76)	25 (79)	26 (82)	27 (85)	27 (87)
g	31	32	33	34	35	36	37
$N \leq$	28 (90)	29 (93)	29 (96)	30 (99)	31 (101)	31 (104)	32 (107)
g	38	39	40	41	42	43	44
$N \leq$	33 (110)	33 (113)	34 (116)	35 (118)	35 (121)	36 (124)	37 (127)
g	45	46	47	48	49	50	51
$N \leq$	37 (130)	38 (133)	38 (135)	39 (138)	40 (141)	40 (144)	41 (147)
g	52	53	54	55	56	57	58
$N \leq$	42 (150)	42 (152)	43 (155)	43 (158)	44 (161)	45 (164)	45 (167)
g	59	60	61	62	63	64	65
$N \leq$	46 (169)	47 (172)	47 (175)	48 (178)	48 (181)	49 (184)	50 (186)
g	66	67	68	69	70	71	72
$N \leq$	50 (189)	51 (192)	51 (195)	52 (198)	53 (200)	53 (203)	54 (206)
g	73	74	75	76	77	78	79
$N \leq$	54 (209)	55 (212)	56 (215)	56 (217)	57 (220)	57 (223)	58 (226)
g	80	81	82	83	84	85	86
$N \leq$	59 (229)	59 (232)	60 (234)	60 (237)	61 (240)	62 (243)	62 (246)
g	87	88	89	90	91	92	93
$N \leq$	63 (249)	63 (251)	64 (254)	65 (257)	65 (260)	66 (263)	66 (266)
g	94	95	96	97	98	99	100
$N \leq$	67 (268)	68 (271)	68 (274)	69 (277)	69 (280)	70 (283)	70 (285)

The first part of the calculations explains itself: for $q = 3$ and $N = 20$ we find that $g \geq 10$.

Afterwards we consider the case $q = 2$ where we calculate bounds on g for N from 3 to 100. Finally we find the lower bound on N given g. For comparison the Weil bound is also given in parenthesis. We see that the bounds are considerably improved. The calculations reproduce the table in [Ser85] page SeTh38c.

Remark B.22. One should still have in mind that the bounds are not always attained. For example, it is shown in [Ser85] that there exists no curve of genus 7 with more than 10 rational points. See also [GvdG95].

Appendix C

Weil's original proof of the Weil bound

When Weil originally proved the Weil bound (Corollary 2.6) on the number of $\mathbb{F}_q$-rational points on a curve C, he used intersection theory on the surface $C \times_k C$, $k = \mathbb{F}_q$. At that time, intersection theory was only developed for smooth curves and surfaces. Later on intersection theory has been developed in full generality, see [Ful83]. We use the notation introduced there. Below we give Weil's elegant proof.

C.1 Notation

Let C be a (smooth projective) curve of genus g defined over k. By abuse of notation we denote the k-linear Frobenius homomorphism [Har77, IV.2.4.1] by $F : C' \to C$. F raises coordinates of closed points to q^{th} powers, hence the points fixed under F are exactly the $\mathbb{F}_q$-rational points. On functions, F corresponds to the map $f \mapsto f^q$, $f \in \Gamma(C', \mathcal{O}_{C'})$. Since F maps the generic point of C onto itself, F is flat by [Har77, III.9.7]. One may also argue for this by observing that F locally makes $\mathcal{O}_{C'}$ a free $\mathcal{O}_C$-module. Finally note that as k is perfect, $C' \simeq C$ [Har77, IV.2.4.1] so we may write $F : C \to C$. Fix the notation

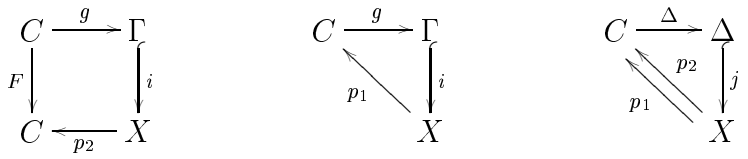
$$\begin{array}{ll} X = C \times_k C & N = |C(\mathbb{F}_q)| \\ \Gamma \subseteq X \text{ graph of } F & \Delta \subseteq X \text{ diagonal} \\ l = C \times \{P_2\} & m = \{P_1\} \times C \end{array}$$

where P_1 and P_2 are closed points on C. Suppose $D \in \mathrm{Div}(X) = Z_1(X)$ is such that

$$\deg(D \cdot l) = a \qquad \text{and} \qquad \deg(D \cdot m) = b.$$

We will then say that D is of *type* (a, b). If $\deg(D \cdot E) = 0$ for all $E \in \mathrm{Div}(X)$ we say that D is *numerically equivalent* to 0, $D \equiv 0$, cf. [Ful83, p. 374].

We have commutative diagrams



where $g = (\mathrm{id}, F)$. A priori C is assumed smooth and projective (hence complete), so p_i are proper morphisms [Har77, III.10.2, III.9.2]. As F is finite of degree q [Har77, IV.2.4.3], F is proper [Ful83, B.2.4]. Furthermore we note that i, j are proper morphisms and that Δ is an isomorphism.

C.2 The proof

We start by stating the following two theorems from [Har77]. Notice that [Har77] use the former notation $C.D$ for $\deg(C \cdot D)$, C, D divisors. Proofs are omitted.

Theorem C.1 (Hodge Index Theorem). *Let H be an ample divisor on X and $D \in \mathrm{Div}(X)$. Assume $D \not\equiv 0$ and $\deg(D \cdot H) = 0$. Then $\deg(D^2) < 0$.*

Proof. See [Har77, V.1.9] □

Theorem C.2 (Nakai-Moishezon Criterion). *A divisor D on X is ample if and only if $\deg(D^2) > 0$ and $\deg(D \cdot F) > 0$ for all irreducible curves F in X.*

Proof. See [Har77, V.1.10] □

Lemma C.3. *With notation as above*

a) $\deg(\Delta^2) = 2 - 2g$.

b) $\deg(\Gamma^2) = q(2g - 2)$.

c) $\deg(\Gamma \cdot \Delta) = N$.

d) Γ *is of type* $(q, 1)$.

e) Δ *is of type* $(1, 1)$.

f) $\deg(l^2) = \deg(m^2) = 0$.

g) $\deg(l \cdot m) = 1$.

Proof. First observe that

$$\Gamma = i_* g_* C \qquad l = p_2^*\{P_2\}. \qquad m = p_1^*\{P_1\} \qquad \Delta = j_*\Delta_* C$$

a): As $\dim(C) = 1$, we have

$$\omega_C = \Omega_{C/k} = \Delta^*(\mathcal{I}/\mathcal{I}^2)$$

where $\mathcal{I} \subseteq \mathcal{O}_X$ is the ideal sheaf defining $\Delta = \Delta(C)$ (closed as C is separated). Now as

$$\Delta \cdot \Delta = [\mathcal{I}^{-1}|_\Delta] = [\mathcal{I}^{-1} \otimes_{\mathcal{O}_X} \mathcal{O}_\Delta] = [\mathcal{I}^{-1} \otimes_{\mathcal{O}_X} \mathcal{O}_X/\mathcal{I}] = [(\mathcal{I}/\mathcal{I}^2)]^{-1}$$

$\deg(\Delta \cdot \Delta) = \deg([\mathcal{I}/\mathcal{I}^2]^{-1}) = -\deg([\Delta_*\omega_C]) = \deg(K_C) = 2-2g$ where we write K_C for the canonical divisor on C.

b):

$$\begin{aligned}\Gamma \cdot \Gamma &= (p_2^* F_* C) \cdot (p_2^* F_* C) = p_2^*(F_* C \cdot F_* C) \\ &= p_2^* F_*(C \cdot F^* F_* C)\end{aligned}$$

hence $\deg(\Gamma^2) = \deg(F)\deg(C \cdot C) = q(2-2g)$ cf. [Ful83, Definition 1.4, p. 13].

c):

$$\begin{aligned}\Gamma \cdot \Delta &= (i_* g_* C) \cdot (j_*\Delta_* C) = i_*(g_* C \cdot (\Delta \cap \Gamma)) \\ &= i_*([\Delta \cap \Gamma]) = i_*\left(\sum_{F(P_i)=P_i} \{P_i\} \times \{P_i\}\right)\end{aligned}$$

and therefore $\deg(\Gamma \cdot \Delta) = \#\ P_i\text{'s} = N$.

d):

$$\begin{aligned}\Gamma \cdot m = \Gamma \cdot (\{P_1\} \times C) &= (i_* g_* C) \cdot (p_1^*\{P_1\}) = i_* g_*(C \cdot (g i p_1)^* C) \\ &= i_* g_*(C \cdot id^*\{P_1\}) = i_*(\{P_1\} \times \{F(P_1)\})\end{aligned}$$

hence $\deg(\Gamma \cdot m) = \deg(\{P_1\} \times \{F(P_1)\}) = 1$. Furthermore

$$\begin{aligned}\Gamma \cdot l = \Gamma \cdot (C \times \{P_2\}) &= (i_* g_* C) \cdot (p_2^*\{P_2\}) = i_* g_*(C \cdot (g i p_2)^* C) \\ &= i_* g_*(C \cdot F^*\{P_2\}) = i_*(F_* F^*\{P_2\} \times \{P_2\})\end{aligned}$$

so $\deg(\Gamma \cdot m) = \deg(F_* F^*\{P_2\} \times \{P_2\}) = \deg(F) = q$ as F is bijective.

e): By symmetry it suffices to examine $C \cdot l$. We have

$$\begin{aligned}\Delta \cdot l = \Delta \cdot (C \times \{P_2\}) &= (j_*\Delta_* C) \cdot (p_2^*\{P_2\}) \\ &= j_*\Delta_*((i\Delta p_2)^*\{P_2\} \times C) = j_*\Delta_*(\{P_2\}) = j_*(\{P_2\} \times \{P_2\})\end{aligned}$$

hence $\deg(\Delta \cdot l) = 1$.

f): $\deg(l \cdot l) = \deg(\mathcal{O}_X(l)|_l) = \deg(\mathcal{O}_C) = 0$; similarly for m.

g): $\deg(l \cdot m) = \deg(\mathcal{O}_X(l)|_m) = \deg(\{P_1\} \times \{P_2\}) = 1$.

In b), c), d) and e) we used the projection formula [Ful83, Proposition 2.3]. □

Proposition C.4 ([Har77, Exercise V.1.9 b)]). *Let $D \in \mathrm{Div}(X)$ be of type (a, b). Then*

$$\deg(D^2) \leq 2ab \tag{C.1}$$

with equality if and only if $D - (bl + am) \equiv 0$.

Proof. Put $H = l + m$ og $E = l - m$. Then $\deg(D \cdot H) = \deg(D \cdot l) + \deg(D \cdot m) = a + b$ and $\deg(D \cdot E) = (a - b)$. From Lemma C.3 we furthermore get

$$\deg(E^2) = -2 \qquad \deg(H^2) = 2 \qquad \deg(E \cdot H) = 0. \tag{C.2}$$

Now by Theorem C.2 H is ample (the only irreducible curves in X being rationally equivalent to l or m and $\deg(H^2) = 2 > 0$). Put $D' = -4D + 2(a+b)H - 2(a-b)E$. Then $\deg(D' \cdot H) = 0$. We calculate $\deg(D' \cdot D')$:

$$\begin{aligned} \deg(D' \cdot D') &= 16 \deg(D^2) - 16(a+b)^2 + 16(a-b)^2 - 8(a-b)^2 + 8(a+b)^2 \\ &= 16(\deg(D^2) - 2ab). \end{aligned}$$

For $D' \not\equiv 0$ Theorem C.1 implies that $\deg(D' \cdot D') < 0$, hence $\deg(D^2) < 2ab$. For $D' \equiv 0$

$$0 \equiv -4D + 2(a+b)H - (a-b)E = -4(D - (bl + am)).$$

and in this case $\deg(D^2) = \deg((bl + am)^2) = 2ab$ by Lemma C.3 □

Remark C.5. The above proposition generalizes to the case where X is the product of two different curves. The proof needs only few modifications.

Theorem C.6 (Weil). *With notation as above,*

$$|N - (q+1)| \leq 2g\sqrt{q}. \tag{C.3}$$

Proof. For $r, s \in \mathbb{Z}$ let $D = r\Gamma + s\Delta$. Then by Lemma C.3

$$\begin{aligned} \deg(D^2) &= r^2 \deg(\Gamma^2) + 2rs \deg(\Gamma \cdot \Delta) + s^2 \deg(\Delta^2) \\ &= r^2 q(2 - 2g) + s^2(2 - 2g) + 2rsN \end{aligned}$$

and D is of type $(r + s, rq + s)$. So for all r, s

$$r^2 q(2 - 2g) + s^2(2 - 2g) + 2rs \leq (r + s)(rq + s) \tag{C.4}$$

by Proposition C.4. This may be written as

$$\begin{aligned} N &\leq \tfrac{1}{rs}((r+s)(rq+s) - (1-g)(r^2q + s^2)) = 1 + q + \tfrac{r}{s}gq + \tfrac{s}{r}g \qquad \text{for } rs > 0 \\ N &\geq \tfrac{1}{rs}((r+s)(rq+s) - (1-g)(r^2q + s^2)) = 1 + q + \tfrac{r}{s}gq + \tfrac{s}{r}g \qquad \text{for } rs < 0 \end{aligned}$$

Now put $x = \frac{r}{s}$ and $h(x) = xgq + \frac{1}{x}g$. Thinking of h as a real function, we find that $h(x)$ has extrema in $x = \pm\frac{1}{\sqrt{q}}$ where it assumes the values $\pm 2g\sqrt{q}$ respectively. As h is positive for $x > 0$ and negative for $x < 0$ we have

$$N - (1+q) \leq \inf_{x>0} h(x) = 2g\sqrt{q}$$
$$N - (q+1) \geq \sup_{x<0} h(x) = -2g\sqrt{q}$$

hence $|N-(q+1)| \leq 2g\sqrt{q}$. The proof also demonstrates that the bound only may be attained if q is a square. □

Appendix D

Further Reading

We here give a short commented list of textbooks treating many of the subjects mentioned in the notes. For more specialized literature we refer to the full bibliography.

D.1 Algebraic Geometry

[Har77] Provides an excellent introduction to the more advanced Algebraic Geometry, such as sheaves, schemes and cohomology.

[Mum88] Is somewhat more geometric oriented than [Har77] but not as comprehensive. A good supplement for [Har77] though.

D.2 Algebra

[Eis95] Is specifically written to provide the necessary commutative algebra needed in [Har77]. Very comprehensive.

[Lan93] Introductory textbook on Algebra. Preparation for [Eis95].

D.3 Curves

[Sil85] An extensive treatise of the theory of elliptic curves. Weil conjectures for elliptic curves are shown by methods different from those of these notes. In these notes we have adapted much of the terminology used in [Sil85] so reading the book should not be difficult, at least not in the beginning.

[Mor91] The first one-third of this book is essentially Chapters 1-3 of these notes formulated in terms of function fields. Contains a good introduction to Algebraic-Geometric codes on curves.

D.4 Error-Correcting Codes

[**vL82**] An introduction to the general theory of Error-Correcting Codes.

[**vLvdG88**] A short but good introduction to Coding Theory and Algebraic-Geometric codes on curves.

[**TVat91**] Today's standard textbook on the subject of Algebraic-Geometric codes on curves.

[**Sti93**] A self-contained purely algebraic exposition of the theory of algebraic functions and its applications to Coding Theory. Weil conjectures for function fields are introduced and proved.

Bibliography

[AM69] M.F. Atiah and I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[Bom76] Enrico Bombieri, *Hilberts 8th problem: an analogue*, Math. developments arising from Hilberts problems, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., 1976, pp. 269–274.

[Del74] Pierre Deligne, *La conjecture de Weil*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

[Eis95] David Eisenbud, *Commutative algebra with a view towards algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, 1995.

[FJ86] M. D. Fried and M. Jarden, *Field arithmetic*, Ergeb. Math. Grenzgb., 3. folge, vol. 11, Springer-Verlag, 1986.

[Ful69] William Fulton, *Algebraic curves*, W. A. Benjamin, New York, 1969.

[Ful83] William Fulton, *Intersection theory*, Ergeb. Math. Grenzgb., 3. folge, vol. 2, Springer-Verlag, 1983.

[GvdG95] Marcel van der Vlugt Gerard van der Geer, *How to construct curves over finite fields with many points*, preprint 9511005 in the alg-geom archive, 1995.

[Han] Johan P. Hansen, *Aritmetisk algebraisk geometri - Kurver*, Notes, University of Aarhus.

[Han92] Johan P. Hansen, *Deligne-Lusztig varieties and group codes*, Coding Theory and Algebraic Geometry (Luminy 1991) (H. Stichtenoth and M. A. Tsfasman, eds.), Lecture Notes in Math., vol. 1518, Springer-Verlag, 1992, pp. 63–81.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer Verlag, 1977.

[HP93] Johan P. Hansen and Jens Peter Pedersen, *Automorphism groups of Ree type, Deligne-Lusztig curves and function fields*, J. Reine Angew. Math. **440** (1993), 99–109.

[HS90] Johan P. Hansen and Henning Stichtenoth, *Group codes on certain algebraic curves with many rational points*, AAECC (Applicable Algebra in Engineering, Communication and Computing) **1** (1990), 67–77.

[Lac87] Gilles Lachaud, *Sommes d'eisenstein et nombre de points de certaines courbes algebriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), 729–732.

[Lan93] Serge Lang, *Algebra*, 3 ed., Addison-Wesley, 1993.

[LT95] G. Lachaud and M. A. Tsfasman, *Formules explicites pour le nombre de points des variété sur un corps fini*, preprint no. 95-25, 1995, L.M.D., C.N.R.S., Luminy.

[LW54] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[Mor91] Carlos Moreno, *Algebraic curves over finite fields*, Cambridge Tracts in Mathematics, vol. 97, Cambridge University Press, 1991.

[Mum88] David Mumford, *The red book of varieties and schemes*, Lecture Notes in Math., vol. 1358, Springer-Verlag, 1988.

[Pet92] Jens Peder Petersen, *A function field related to the Ree group*, Coding Theory and Algebraic Geometry (Luminy 1991) (H. Stichtenoth and M. A. Tsfasman, eds.), Lecture Notes in Math., vol. 1518, Springer-Verlag, 1992, pp. 122–131.

[Sch91] René Schoof, *Algebraic curves over* $\mathbf{F}_2$ *with many rational points*, J. Number Theory **38** (1991), no. 2, 6–14.

[Ser83] Jean-Pierre Serre, *Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), 397–402.

[Ser85] Jean-Pierre Serre, *Rational points on curves over finite fields*, Notes taken by Fernando Q. Gouvéa, Harvard University, 1985.

[Sil85] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1985.

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, 1993.

[Tsf94] Michael A. Tsfasman, *Nombre de points des surfaces sur un corps fini*, preprint no. 94-27, 1994, L.M.D., C.N.R.S., Luminy.

[TVat91] M. A. Tsfasman and S. G. Vl˘ aduţ, *Algebraic geometric codes*, Mathematics and its applications (Soviet Series), vol. 58, Kluwer Academic Publishers Group, 1991.

[vdGvdV93] Gerard van der Geer and Marcel van der Vlugt, *Curves over finite fields of characteristic 2 with many rational points*, C. R. Acad. Sci. Paris Sér. I Math. **317** (1993), 593–597.

[vL82] Jacobus H. van Lint, *Introduction to coding theory*, Graduate Texts in Mathematics, vol. 86, Springer-Verlag, 1982.

[vLvdG88] Jacobus H. van Lint and Gerard van der Geer, *Introduction to coding theory and algebraic geometry*, DMV Seminar, vol. 12, Birkhäuser, 1988.

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), no. 5, 497–508.

[Wei52] André Weil, *Sur les "formules explicites" de la théorie des nombres premiers : [1952b]*, Coll. Papers, vol. II, Springer-Verlag, 1952, pp. 48–61.

Index