ABC Conjecture in Function Fields

Ming Yean Lim

February 21, 2024

1 Introduction

In number theory, we often work over the ring $\mathbb{Z}$, its field of fractions, or a number field, i.e. a finite field extension $K/\mathbb{Q}$. The ring $\mathbb{Z}$ shares many properties in common with the ring of polynomials over a finite field $\mathbb{F}_q[T]$. For instance:

- they are both Euclidean domains, hence are PIDs, UFDs, and Dedekind domains;
- they have countably many primes;
- they have finite groups of units;
- any quotient by a non-zero ideal is finite.

One of the most basic questions one can ask in number theory is the solutions to Diophantine equations, among the most famous is

$$x^N + y^N = z^N$$

where $N \geq 3$ and $x, y, z \in \mathbb{Z}$. Fermat's last theorem asserts that this has no non-trivial solutions. One can ask the same question over $\mathbb{F}_q[T]$, and indeed we will see that the analogue of Fermat's last theorem is true in this setting.

The analogue of a number field over $\mathbb{F}_q[T]$ is a *global function field*, it is simply a finite extension of $\mathbb{F}_q(T)$. More generally, a *function field over* F is a finite extension K of $F(T)$. We will assume F is algebraically closed in K, in this case we call F the *constant field.*

Recall that for a number field K, non-archimedean valuations of K correspond to primes of its ring of integers $\mathcal{O}_K$. In other words:

Proposition 1.1. *We have a correspondence*

$$\begin{array}{ccc} \{\textit{primes in } \mathcal{O}_K\} & \longleftrightarrow & \{\textit{DVRs } R \subseteq K \textit{ with } \operatorname{Frac}(R) = K\} \\ \mathfrak{p} & \longmapsto & (\mathcal{O}_K)_{\mathfrak{p}} \end{array}$$

Proof. Let R be a DVR in K with maximal ideal P. R contains $\mathbb{Z}$ and is integrally closed in K, hence $\mathcal{O}_K \subseteq R$. $\mathfrak{p} = P \cap \mathcal{O}_K$ is a prime[1] of $\mathcal{O}_K$. If $x \in \mathcal{O}_K \setminus \mathfrak{p}$, then $x \notin P$, so $x^{-1} \in R$. This shows that $(\mathcal{O}_K)_\mathfrak{p} \subseteq R$. Finally, $(\mathcal{O}_K)_\mathfrak{p}$ is a DVR, and DVRs are maximal subrings inside their fields of fractions, so $R = (\mathcal{O}_K)_\mathfrak{p}$. ■

This motivates the following definition:

Definition 1.2. Let K/F be a function field. A *prime* in K is a DVR R with maximal ideal P such that $F \subseteq R \subseteq K$ and $\mathrm{Frac}(R) = K$. We will often refer to prime by its maximal ideal P. We let $v_P : K^\times \to \mathbb{Z}$ denote the corresponding valuation. The *degree* of a prime P is $\deg P = [R/P : F]$.

Lemma 1.3. $\deg P$ *is finite.*

Proof. Pick $y \in P \setminus F$. We will show $[R/P : F] \leq [K : F(y)]$. Suppose $u_1, \ldots, u_m \in R$ are such that their reductions modulo P, $\overline{u}_1, \ldots, \overline{u}_n$ are linearly independent over F. We will show $u_1, \ldots, u_m$ are linearly independent over $F(y)$. Suppose not, then we have polynomials $f_i \in F[y]$ such that $f_1 u_1 + \ldots + f_m u_m = 0$. We may assume that y does not divide all f_i, so reducing this modulo P gives a linear relation between the $\overline{u}_i$, contradiction. ■

Example 1.4. Let's find the primes of $K = F(T)$. Suppose R is a prime in K, v the corresponding valuation.

Case 1: Suppose $v(f) \geq 0$ for all $f \in F[T]$. Pick an irreducible f such that $v(f) > 0$. If $g \in F[T]$ is not divisible by f, then $af + bg = 1$ for some $a, b \in F[T]$. Then $v(bg) = v(1 - af) = 0$, so $v(g) = 0$. We get that v is the *f-adic valuation*, denoted v_f, and $R = F[T]_{(f)}$.

Case 2: There is an irreducible $f \in F[T]$ with $v(f) < 0$. Write $f(T) = a_n T^n + \ldots + a_1 T + a_0$ where $a_i \in F$. From this we see that $v(T) < 0$. We may assume $v(T) = -1$, thus for $g \in F[T]$, $v(g) = -\deg g$, and $R = F[T^{-1}]_{(T^{-1})}$. We write $v_\infty = v$.

In case 1 above, the degree of the prime is the dimension of $F[T]_{(f)}/(f)F[T]_{(f)} \cong F[T]/(f)$ over F, which is the degree of the polynomial f. These primes also correspond to the points on an affine piece of $\mathbb{P}^1_F$. The prime in case 2 corresponds to the point at infinity. Note that K is the function field of $\mathbb{P}^1_F$.

In general, one may associate to a function field K/F a nonsingular complete[2] curve C over F such that K is the function field of C. See [Har77, §1.6] for details.

Example 1.5. Let $E : y^2 = f(x)$ be an elliptic curve over F. Then its function field is

$$K = \mathrm{Frac}\,\frac{F[x,y]}{(y^2 - f(x))}$$

[1] $\mathfrak{p}$ is nonzero: We have $\mathbb{Q} \not\subseteq R$ as the integral closure of $\mathbb{Q}$ in K is K. Thus there is an integer prime p such that $1/p \notin R$, so $p \in \mathbb{Z} \cap P \subseteq \mathfrak{p}$.

[2] proper over F

2 Divisors

In this section we will introduce divisors, which play a similar role to fractional ideals in number fields. We give the definitions necessary to state the Riemann-Roch theorem for function fields.

Let K/F be a function field.

Definition 2.1. A *divisor* of K is a formal linear combination $D = \sum_P n_P P$ of primes P in K. The group of divisors of K is the abelian group of such divisors, denoted $\mathrm{Div}(K)$. We say D is *effective* if all $n_P \geq 0$, and denote this by $D \geq 0$.

To each $a \in K^\times$, we may associate a divisor

$$(a) = \sum_P v_P(a)P$$

It turns out that there are only finitely many P such that $v_P(a) \neq 0$, so this is a well-defined divisor (see [Ros02, Proposition 5.1]). We thus have a homomorphism $(\cdot) : K^\times \to \mathrm{Div}(K)$, an element of its image is called a *principal divisor*.

We also define

$$(a)_0 = \sum_{v_P(a)>0} v_P(a)P \qquad \text{and} \qquad (a)_\infty = \sum_{v_P(a)<0} -v_P(a)P$$

called the *zero divisor* and *polar divisor* of a respectively. Thus divisors allow us to keep track of zeros and poles of functions. We define the *degree* of a divisor by extending deg linearly:

$$\deg\left(\sum_P n_P P\right) = \sum_P n_P \deg P$$

giving a homomorphism $\deg : \mathrm{Div}(K) \to \mathbb{Z}$.

Proposition 2.2. *For $a \in K^\times$, we have*

1. $\deg(a)_0 = \deg(a)_\infty = [K : F(a)]$,
2. $\deg(a) = 0$,
3. $(a) = 0$ *iff* $a \in F^\times$

Proof. See [Ros02, Proposition 5.1]. Note that $a \in F^\times$ implies $(a) = 0$ is trivial since we ask that $F \subseteq P$ for primes P. ■

Definition 2.3. To each $D \in \mathrm{Div}(K)$ we associate an F-vector space

$$L(D) = \{x \in K^\times \mid (x) + D \geq 0\} \cup \{0\}$$

called the *Riemann-Roch space*. Its dimension over F is finite, denoted by $\ell(D)$.

We can interpret $L(D)$ as the space of functions with poles no worse than those given by D.

Lemma 2.4. *If* $\deg D < 0$*, then* $\ell(D) = 0$*.*

Theorem 2.5 (Riemann-Roch)**.** *There is an integer* $g = g_K \geq 0$ *and a divisor* C *such that for any* $A \in \mathrm{Div}(K)$*, we have*

$$\ell(A) = \deg A - g + 1 + \ell(C - A)$$

The integer g is unique, called the *genus* of K. The divisor C is unique up to linear equivalence – any other C will differ by a principal divisor, such a C is called a *canonical divisor*.

Example 2.6. Let us compute the genus of $K = F(T)$. Let P_∞ denote the prime at infinity, as in Example 1.4. $L(nP_\infty)$ is the set of polynomials in $F[T]$ of degree at most n. Indeed the conditions $v_g(f) \geq 0$ for all irreducible polynomials $g \in F[T]$ is equivalent to f being a polynomial, and $v_\infty(f) + n \geq 0$ is equivalent to $\deg f \leq n$. Thus,

$$n + 1 = \ell(nP_\infty) = n - g + 1$$

if n is sufficiently large. We conclude $g = 0$.

3 Extensions of Function Fields

Let K/F be a function field. Let L be a finite extension of K and E be the algebraic closure of F in L. L is then a function field with constant field E. If $E = F$, we say that L/K is a *geometric extension*.

In the rest of this section, we assume L/K be a finite separable geometric extension of function fields with perfect constant field F.

As in algebraic number theory, we can study ramification of primes in function fields.

Definition 3.1. Let $\mathcal{O}_P$ be a prime in K with maximal ideal P and $\mathcal{O}_\mathfrak{P}$ be a prime in L with maximal ideal $\mathfrak{P}$. We say that $\mathfrak{P}$ *lies above* P if $\mathcal{O}_P = K \cap \mathcal{O}_\mathfrak{P}$ and $P = K \cap \mathfrak{P}$. In this case we write $\mathfrak{P} \mid P$. We define the *ramification index* to be the integer $e = e(\mathfrak{P}/P)$ such that $P\mathcal{O}_\mathfrak{P} = \mathfrak{P}^e$ and the *residue class degree* $f = f(\mathfrak{P}/P) = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : \mathcal{O}_P/P]$.

Now we shall identify the prime $\mathfrak{P}$ lying above a given prime P. Let R be the integral closure of $\mathcal{O}_P$ in L. If $\mathfrak{P}$ lies above P, then $\mathcal{O}_P \subseteq \mathcal{O}_\mathfrak{P}$, so $R \subseteq \mathcal{O}_\mathfrak{P}$. Let $\mathfrak{p} = \mathfrak{P} \cap R$, which is a prime of R. If $x \in R \setminus \mathfrak{p}$, then $x^{-1} \in \mathcal{O}_\mathfrak{P}$. Thus $R_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{P}$ and so $R_\mathfrak{p} = \mathcal{O}_\mathfrak{P}$.

We have shown that primes in K lying above P correspond to primes of R lying above P. Thus if $PR = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$, then the primes lying above P are $\mathfrak{P}_i = \mathfrak{p}_i R_{\mathfrak{p}_i}$. The e_i are the ramification indices of $\mathcal{P}_i$ over P. Let $f_i = f(\mathcal{P}_i/P)$.

Proposition 3.2. $\sum_{i=1}^{g} e_i f_i = [L : K]$.

Proof. See [Ser79, Ch. 1 §5] ∎

We can extend a divisor of K to a divisor of L: Define the homomorphism $i_{L/K} : \mathrm{Div}(K) \to \mathrm{Div}(L)$ by $i_{L/K}(P) = \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)\mathfrak{P}$ and extending linearly.

Proposition 3.3. *Let $D \in \mathrm{Div}(K)$. Then $\deg_L(i_{L/K}(D)) = [L : K] \deg_K D$.*

Proof. It suffices to consider $D = P$ prime. If $\mathfrak{P} \mid P$, then

$$\deg_L \mathfrak{P} = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : F] = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : \mathcal{O}_P/P][\mathcal{O}_P/P : F] = f(\mathcal{P}/P) \deg_K P$$

Note we used that L/K is a geometric extension here. Thus

$$\deg_L(i_{L/K}(P)) = \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P) \deg_L \mathfrak{P} = \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P) f(\mathfrak{P}/P) \deg_K P = [L : K] \deg_K P$$

as required. ∎

Proposition 3.4. *Let $a \in K^\times$. Then $i_{L/K}(a) = (a)$.*

Proof. We compute

$$\begin{aligned} i_{L/K}(a) = i_{L/K}\left(\sum_P v_P(a)P\right) &= \sum_P v_P(a) \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)\mathfrak{P} \\ &= \sum_{\mathfrak{P}} v_P(a) e(\mathfrak{P}/P)\mathfrak{P} = \sum_{\mathfrak{P}} v_\mathfrak{P}(a)\mathfrak{P} = (a) \end{aligned}$$ ∎

Theorem 3.5 (Riemann-Hurwitz)**.** *We have*

$$2g_L - 2 \geq [L : K](2g_K - 2) + \sum_{\mathfrak{P}} (e(\mathfrak{P}/P) - 1) \deg_L \mathfrak{P}$$

where the sum is over all primes $\mathfrak{P}$ of L.

The actual statement is more precise than this (see [Ros02, Theorem 7.16]), but this will suffice for our purposes. The proof of this goes by studying differentials on K and its pullback to L.

Corollary 3.6. $g_L \geq g_K$.

4 The ABC Conjecture

The ABC conjecture was born out of a discussion between Oesterlé and Masser [Oes88] in 1985 in the context of Szpiro's conjecture. The ABC conjecture states the following:

Conjecture 4.1. *For all $\varepsilon > 0$, there exists $C(\varepsilon) > 0$ such that*

$$\max(|a|, |b|, |c|) \leq C(\varepsilon)(\operatorname{rad} abc)^{1+\varepsilon} \tag{1}$$

for all triples (a, b, c) of nonzero integers satisfying $a + b + c = 0$.

In the statement above, $\operatorname{rad} n = \prod_{p|n} p$ is the product of all primes divisors of n. This conjecture implies Szpiro's conjecture, which in turn implies Fermat's last theorem for exponent N sufficiently large (see [Sil09, §VIII.11]).

Let us reformulate the ABC conjecture as follows: Set $u = a/c$ and $v = b/c$. Recall the height of a rational number r/s with $(r, s) = 1$ is $\operatorname{ht}(r/s) = \log \max(|r|, |s|)$. Taking logarithms on both sides of (1), we get

$$\max(\operatorname{ht}(u), \operatorname{ht}(v)) \leq c(\varepsilon) + (1 + \varepsilon) \sum_{p|abc} \log p$$

where $c(\varepsilon) = \log C(\varepsilon)$.

Let K be a function field over F. We have an analogue of height, namely for $u \in K \setminus F$, we can consider its *degree* $\deg u = [K : F(u)]$. Actually we will instead consider the *separable degree* $\deg_s u = [K : F(u)]_s$. The analogue of $\log p$ is the degree $\deg P$. We now state the analogue of the ABC conjecture over function fields:

Theorem 4.2. *Let K be a function field with perfect constant field F. Suppose $u, v \in K \setminus F$ and $u + v = 1$. Then*

$$\deg_s u = \deg_s v \leq 2g_K - 2 + \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P$$

where $A = (u)_0$, $B = (v)_0$, and $C = (u)_\infty = (v)_\infty$.

In the above, $\operatorname{Supp} D$ is the *support* of a divisor D. If $D = \sum_P n_P P$, then $\operatorname{Supp} D = \{P \mid n_P \neq 0\}$. We remark that the equality $\deg_s(u) = \deg_s(v)$ follows from the fact $F(u) = F(v)$. The equality $(u)_\infty = (v)_\infty$ follows from the fact that if $v_P(u) < 0$, then $v_P(1 - u) = v_P(u)$. Note further that $\operatorname{Supp} A$, $\operatorname{Supp} B$, and $\operatorname{Supp} C$ are disjoint.

Theorem 4.2 (in the case where F is algebraically closed of characteristic 0) was already known to be true prior to Conjecture 4.1 (see [Mas83]).

Proof of Theorem 4.2 (Sketch). Set $k = F(u)$ and assume that K/k is separable of degree n. Let $\mathfrak{p}_0$, $\mathfrak{p}_1$, $\mathfrak{p}_\infty$ be the (degree 1) primes in $F(u)$ that are the zero divisors of u, $1 - u$, and $1/u$ respectively. We have $A = i_{K/k}(\mathfrak{p}_0)$, $B = i_{K/k}(\mathfrak{p}_1)$, and $C = i_{K/k}(\mathfrak{p}_\infty)$ (see Proposition 3.4).

Recalling that $g_k = 0$ (see Example 2.6), Riemann-Hurwitz implies

$$2g_K - 2 \geq -2n + \sum_P (e(P/\mathfrak{p}) - 1) \deg_K P \tag{2}$$

where the sum is over all primes P in K, and $\mathfrak{p}$ is the prime in k below P. Instead of summing over all P we shall sum only over $P \in \operatorname{Supp}(A+B+C)$. Noting that $P \in \operatorname{Supp} A$ iff $P \mid \mathfrak{p}_0$, we have

$$\begin{aligned}
\sum_{P\in\operatorname{Supp} A} (e(P/\mathfrak{p}) - 1) \deg_K P &= \sum_{P\in\operatorname{Supp} A} e(P/\mathfrak{p}_0) \deg_K P - \sum_{P\in\operatorname{Supp} A} \deg_K P = i_{K/k} \\
&= \deg_K(i_{K/k}\mathfrak{p}_0) - \sum_{P\in\operatorname{Supp} A} \deg_K P \\
&\overset{(3.3)}{=} n - \sum_{P\in\operatorname{Supp} A} \deg_K P
\end{aligned} \tag{3}$$

Similarly,

$$\sum_{P\in\operatorname{Supp} B} (e(P/\mathfrak{p}) - 1) \deg_K P = n - \sum_{P\in\operatorname{Supp} B} \deg_K P$$

and

$$\sum_{P\in\operatorname{Supp} C} (e(P/\mathfrak{p}) - 1) \deg_K P = n - \sum_{P\in\operatorname{Supp} C} \deg_K P$$

Adding these three inequalities gives

$$\sum_{P\in\operatorname{Supp}(A+B+C)} (e(P/\mathfrak{p}) - 1) \deg_K P = 3n - \sum_{P\in\operatorname{Supp}(A+B+C)} \deg_K P$$

Combining this with (2), we get

$$2g_K - 2 \geq n - \sum_{P\in\operatorname{Supp}(A+B+C)} \deg_K P$$

which gives the conclusion.

In case K/k is inseparable, let M be the maximal separable subextension of K/k. K/M is purely inseparable and one can show the following:

1. $g_M = g_K$,
2. For each prime P' of M, there is a unique prime P of K lying above it,
3. $\deg_K P = \deg_M P'$.

and use this to conclude. See [Ros02, Theorem 7.16] for details. ■

As a corollary, let us now prove an analogue of Fermat's last theorem for function fields:

Proposition 4.3. *Let K be a function field with perfect constant field F. Let $N > 0$, not divisible by $p = \operatorname{char} F$. If*

1. *$g_K = 0$ and $N \geq 3$; or*
2. *$g_K \geq 1$ and $N > 6g_K - 3$,*

then there are no non-constant solutions to $X^N + Y^N = 1$ in K.

Proof. Suppose we have a non-constant solution $(u, v) \in (K \setminus F)^2$. Then we apply Theorem 4.2 to (u^N, v^N) to get

$$\deg_s u^N \leq 2g_K - 2 + \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P$$

Let M be the maximal separable subextension of $K/F(u)$. The extension $F(u)/F(u^N)$ is separable of degree N, since $p \nmid N$. Thus M is the maximal separable subextension of $K/F(u^N)$, so $\deg_s u^N = [M : F(u)][F(u) : F(u^N)] = N \deg_s u$.

Equation 3 shows that

$$\sum_{P \in \operatorname{Supp} A} \deg_K P \leq \deg_s u$$

Thus,

$$N \sum_{P \in \operatorname{Supp} A} \deg_K P \leq 2g_K - 2 + \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P$$

We have similar inequalities for B and C in place of A. Summing these up,

$$N \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P \leq 6g_K - 6 + 3 \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P$$

so

$$(N-3) \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P \leq 6g_K - 6$$

If $g_K = 0$, then we must have $N < 3$. If $g_K \geq 1$, then we must have $N - 3 \leq 6g_K - 6$, so $N \leq 6g_K - 3$. ■

We remark that this is not the best possible bound N. If $(u, v) \in (K \setminus F)^2$ is a non-constant solution, then it turns out that if $p \nmid N$, then $F(u, v)$ has genus $(N-1)(N-2)/2$. By Riemann-Hurwitz, we have $(N-1)(N-2)/2 \leq g_K$. Thus there are no non-constant solutions if $(N-1)(N-2)/2 > g_K$.

A Riemann Hypothesis for Function Fields

We now have the terminology to state the Riemann Hypothesis for function fields. Recall that if K is a number field, its Dedekind zeta function is

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}$$

where the sum is over all nonzero ideals $\mathfrak{a}$ of $\mathcal{O}_K$ and $N\mathfrak{a} = \left|\mathcal{O}_K/\mathfrak{a}\right|$ is the absolute norm of an ideal (see [Neu99, Ch. VII]). We define the zeta function for a global function field K over $\mathbb{F}_q$ analogously:

$$\zeta_K(s) = \sum_{A \geq 0} \frac{1}{(NA)^s}$$

over effective divisors A, where $NA = q^{\deg A}$. This has an Euler product

$$\zeta_K(s) = \prod_{P \text{ prime}} (1 - (NP)^{-s})^{-1}$$

It admits a meromorphic continuation to $\mathbb{C}$ with simple poles at $s = 0$ and $s = 1$, and satisfies a functional equation.

Example A.1. If $K = \mathbb{F}_q(T)$, then $\zeta_K(s) = (1 - q^{-s})^{-1}(1 - q^{1-s})^{-1}$.

The zeta function is often given in a different form. From the Euler product,

$$\zeta_K(s) = \prod_{d=1}^{\infty} (1 - q^{-ds})^{-a_d}$$

where a_d is the number of primes of K of degree d. Set $u = q^{-s}$. The zeta function becomes

$$Z_K(u) = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}$$

Taking logarithms,

$$\log Z_K(u) = \sum_{d=1}^{\infty} -a_d \log(1 - u^d) = \sum_{d=1}^{\infty} a_d \sum_{m=1}^{\infty} \frac{u^{dm}}{m} = \sum_{n=1}^{\infty} \left(\sum_{d|n} d a_d \right) \frac{u^n}{n}$$

Let $N_n = \sum_{d|n} d a_d$, so that

$$Z_K(u) = \exp\left(\sum_{n=1}^{\infty} N_n \frac{u^n}{n} \right)$$

Theorem A.2. *There is a polynomial $L_K(u) \in \mathbb{Z}[u]$ of degree $2g$ such that $L_K(0) = 1$, $L_K'(0) = a_1 - q - 1$, and*

$$Z_K(u) = \frac{L_K(u)}{(1-u)(1-qu)}$$

Factor $L_K(u) = \prod_{i=1}^{2g}(1 - \pi_i u)$.

Theorem A.3 (Riemann Hypothesis)**.** *All the zeros of $\zeta_K(s)$ lie on the line $\operatorname{Re} s = 1/2$. Equivalently, $|\pi_i| = \sqrt{q}$ for all i.*

Corollary A.4. $|a_1 - q - 1| \leq 2g\sqrt{q}$.

Proof. $a_1 - q - 1 = L_K'(0) = -\pi_1 - \ldots - \pi_{2g}$, then take absolute values. ∎

This has implications for counting points on curves over finite fields. Let C be a nonsingular curve over $\mathbb{F}_q$ with function field K. We claim that $N_n = \#C(\mathbb{F}_{q^n})$. We have a bijection

$$C(\mathbb{F}_{q^n}) \longleftrightarrow \{(P \in C, \mathbb{F}_q\text{-homomorphism } \mathcal{O}_P/P \to \mathbb{F}_{q^n})\}$$

(see e.g. [SP, Tag 01J5]). Since $\mathcal{O}_P/P \cong \mathbb{F}_{q^{\deg P}}$, there is a homomorphism $\mathcal{O}_P/P \to \mathbb{F}_{q^n}$ iff $\deg P \mid n$. In this case there are exactly $\deg P$ such $\mathbb{F}_q$-homomorphisms. This establishes the claim. We conclude that

$$Z_K(u) = \exp\left(\sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n})\frac{u^n}{n}\right)$$

If C is an elliptic curve, then $g = 1$ and $a_1 = \#C(\mathbb{F}_q)$. Corollary A.4 then gives Hasse's theorem.

References

[Har77] Robin Hartshorne. *Algebraic Geometry.* Graduate Texts in Mathematics 52. Springer, 1977.

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry.* Graduate Studies in Mathematics. American Mathematical Society, 1996.

[Mas83] R. C. Mason. "The hyperelliptic equation over function fields". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 93.2 (1983), pp. 219–230.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften 322. Springer, 1999.

[Oes88] Joseph Oesterlé. "Nouvelles approches du "théoreme" de Fermat". In: *Astérisque* 161.162 (1988), pp. 165–186.

[Ros02] Michael Rosen. *Number Theory in Function Fields.* Graduate Texts in Mathematics 210. Springer, 2002.

[Ser79] Jean-Pierre Serre. *Local Fields.* Graduate Texts in Mathematics 67. Springer, 1979.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* 2nd ed. Graduate Texts in Mathematics 106. Springer, 2009.

[SP] The Stacks project authors. *The Stacks project.* `https://stacks.math.columbia.edu`. 2024.