Koblitz's Conjecture for the Drinfeld Module

by

Lalit Kumar Jain

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2008

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Let E be an elliptic curve over the rationals without complex multiplication such that any elliptic curve $\mathbb{Q}$-isogenous to E has trivial $\mathbb{Q}$-torsion. Koblitz conjectured that the number of primes less than x for which $|E(\mathbb{F}_p)|$ is prime is asymptotic to

$$C_E \frac{x}{(\log x)^2}$$

for C_E a real positive constant dependent on E. Miri and Murty showed that for infinitely many p, $|E(\mathbb{F}_p)|$ has at most 16 prime factors using the lower bound sieve and assuming the Generalized Riemann Hypothesis. This thesis generalizes Koblitz's conjectures to a function field setting through Drinfeld modules. Let ϕ be a Drinfeld module of rank 2, and $\mathbb{F}_q$ a finite field with every $\mathbb{F}_q[t]$-isogeny having no $\mathbb{F}_q[t]$-torsion points and with $\mathrm{End}_{\overline{k}}(\phi) = \mathbb{F}_q[t]$. Furthermore assume that for each monic irreducible $l \in \mathbb{F}_q[t]$, the extension generated by adjoining the l-torsion points of ϕ to $\mathbb{F}_q(t)$ is geometric. Then there exists a positive constant C_ϕ depending on ϕ such that there are more than

$$C_\phi \frac{q^x}{x^2}$$

monic irreducible polynomials P with degree less then x such that $\chi_\phi(P)$ has at most 13 prime factors. To prove this result we develop the theory of Drinfeld modules and a translation of the lower bound sieve to function fields.

Acknowledgements

The Pure Mathematics department at the University of Waterloo has been my home for the last several years. I would like to thank all the students, faculty, and staff that I have come to know over this time for their friendship, mentorship and advice. Most importantly I am grateful for the infinite patience and wisdom that Professor Wentang Kuo and Professor Yu-Ru Liu have shown me as my supervisors. My partner on this research project, Lloyd Eliott, has been an outstanding collaborator and an amazing person to work with. Finally but certainly not least I would like to thank Patrice Camire and Sourav Sen Gupta for many discussions and thoughts that helped this thesis come to fruition.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

The twin prime conjecture asks whether infinitely many pairs of the form $p, p+2$ where both p and $p+2$ are prime exist. This question has generated countless amounts of research and has motivated many techniques. In the following we study a problem, though seemingly unrelated to the twin prime conjecture, which shares the same structure and can be studied by similar means. We begin this study with an overview of classical approaches to the twin prime conjecture.

1.1.1 Heuristics

Consider the following question: "How many primes p between 5 and n have the property that $p+2$ is prime?" Recall that the prime number theorem gives an asymptotic expression for the number of primes less then n as $n/\log n$. Heuristically the 'probability' that an integer $1 \leq m \leq n$ is prime (denoted $P(m)$) is just $1/\log n$. This tempts us to say

$$P(p \text{ and } p+2 \text{ are prime}) = \frac{1}{(\log n)^2}$$

However this is under the assumption that the events, 'p is prime' and '$p+2$ is prime' are independent, which is certainly not the case.

To account for dependence we use conditional probabilities. Note that for an arbitrary integer $m \leq n$

$$P(p \text{ and } p{+}2 \text{ are prime}) = \frac{P(p+2 \text{ is prime}|p \text{ is prime})}{P(m \text{ is prime})} P(p \text{ is prime}) P(m \text{ is prime}). \tag{1.1}$$

Now if we know that p is prime, then $p \not\equiv 0 \mod l$ for any prime $l \neq p$. Thus $p+2$ can lie in $l-1$ congruence classes modulo l of which $l-2$ are nonzero, hence $P(l \nmid p) = \frac{l-2}{l-1}$. If we assume that the probability that $l \nmid p$ is independent for different primes l, then

$$P(p+2 \text{ is prime}|p \text{ is prime}) = \prod_{\substack{l \geq 3 \\ l \text{ prime}}} \frac{l-2}{l-1}.$$

This probability is approximately .66. Using similar reasoning as above we can also see that

$$P(m \text{ is prime}) = \prod_{\substack{l \geq 3 \\ l \text{ prime}}} \frac{l-1}{l}.$$

Also we see that by the above $P(p \text{ is prime}) = P(m \text{ is prime}) = 1/\log n$. Combining these results and using (1.1) gives,

$$P(p \text{ and } p+2 \text{ are prime}) = \prod_{\substack{l \geq 3 \\ l \text{ prime}}} \left(1 - \frac{1}{(l-1)^2}\right) \frac{1}{(\log n)^2}.$$

In particular Hardy and Littlewood extended this heuristic to the following conjecture

Conjecture 1.1.1 ([6])**.** *The number of twin prime pairs less then n, is asymptotic to*

$$2 \prod_{\substack{l \geq 3 \\ l \text{ prime}}} \left(1 - \frac{1}{(l-1)^2}\right) \frac{n}{(\log n)^2}.$$

Note that in our analysis we are assuming that p is any integer, however we know for a fact that $p+2$ must be odd so since there is a 1/2 probability of a random integer being odd, leading too the correction factor of two so we do not just count half the number of twin prime pairs.

1.1.2 A Sieve

To establish the heuristics in the previous section, we need to be able to compute an asymptotic formula for

$$\sum_{\substack{p\le x\\ p+2 \text{ is prime}}} 1.$$

Presently such a direct attack is infeasible. As often happens in number theory we are forced to study a weighted version of this sum using sieve methods.

In [1] Bombieri applied the lower bound sieve to establish the following result

Theorem 1.1.1. *There are infinitely many primes p such that $p+2$ has at most 4 distinct prime factors.*

Our exposition of this result is due to Murty and Cojocaru [2].

Bombieri studied the sum

$$\sum_{p\le x}\left(\sum_{\substack{d\le x^{1/8}(\log x)^{-B}\\ d \text{ squarefree}\\ d|p+2}} 1\right)^2\left(2-\sum_{\substack{q\le x^{1/4}(\log x)^{B}\\ q|p+2}} 1\right)$$

where B is a positive constant and the λ_d are positive weights bounded in absolute value by one. Using the lower bound sieve, he managed to show that for large x the expression is positive. Thus for infinitely many x there must exist primes p for which

$$2-\sum_{\substack{q\le x^{1/4}(\log x)^{B}\\ q|p+2}} 1 \tag{1.2}$$

is positive. So for infinitely many p, $p+2$ has at most one odd prime factor less than $x^{1/4}(\log x)^B$, yet $p+2$ can have at most 3 prime factors greater then $x^{1/4}(\log x)^B$. Thus there are infinitely many primes for which $p+2$ has at most 4 prime factors. We will study the lower bound sieve in more depth in Chapter 4.

1.2 Koblitz's Conjecture

1.2.1 An analogous problem

In a seminal paper in 1988 Neal Koblitz outlined the fundamentals of elliptic curve cryptography (see [8]). His method was based on the difficulty of the discrete logarithm problem for certain elliptic curves defined over finite fields. In particular a secure choice can be made by choosing an elliptic curve E and a finite field $\mathbb{F}_p$ so that the group of points, $E(\mathbb{F}_p)$ has prime order.

For a fixed elliptic curve E let N_p be the size of the set of points on the elliptic curve over the finite field $\mathbb{F}_p$ for p prime. To prevent singularities we insist that $p \nmid \Delta$ where Δ is the discriminant of E. In addition E must not be $\mathbb{Q}$-isogenous to a curve with nontrivial $\mathbb{Q}$-torsion or have complex multiplication. In this case Koblitz formulated the following conjecture

$$|\{\text{primes } p \leq n, p \nmid \Delta, N_p \text{ is prime }\}| \asymp C\frac{n}{(\log n)^2}.$$

where C is a positive constant of the form $\prod_{l \text{ prime}} a(l)$ which depends on E. To understand this, we can use the heuristic method used for the twin prime conjecture. Firstly we need to compute the probability that a given prime l does not divide N_p. Let $E[l]$ denote the l-torsion points of E. Recall the following

Lemma 1.2.1. *For an elliptic curve E defined over $\mathbb{C}$, we have the following isomorphism of groups:*

$$E[l] \cong \frac{\mathbb{Z}}{l\mathbb{Z}} \times \frac{\mathbb{Z}}{l\mathbb{Z}}.$$

In particular the extension $\mathbb{Q}(E[l])/\mathbb{Q}$ obtained by adjoining the coordinates of the points in $E[l]$ to $\mathbb{Q}$ is Galois.

Proof. Recall that the Weierstrass $\wp$ function induces a complex analytic isomorphism between the elliptic curve E and the torus $\frac{\mathbb{R}^2}{\mathbb{Z}+\tau\mathbb{Z}}$ for an algebraic number τ given by the Uniformization theorem (see for example [17], Corollary 5.1.1). Thus the points of order l correspond to the points

$$\left(\frac{m}{l}, \frac{n\tau}{l}\right) \text{ where } 0 \leq m, n \leq l-1.$$

If (x, y) denotes a generic point of E then the equations giving $[m](x, y) = 0$ where $[m]$ denotes the $\mathbb{Z}$ module operation of multiplying by m on a point of E, are rational functions in x and y and the coefficients of E. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}})$, then $(\sigma(x), \sigma(y))$ will satisfy $[m](\sigma(x), \sigma(y)) = 0$ and so given $P \in E[l]$ we see $\sigma(P) \in E[l]$.

□

This isomorphism gives rise to an action of the Galois group G_l of the Galois extension $\mathbb{Q}(E[l])/\mathbb{Q}$ onto the two dimensional $\mathbb{Z}/l\mathbb{Z}$ vector space $E[l]$. In particular

$p \neq l$ is unramified in this extension if and only if $p \nmid N_E$ (the conductor of E) i.e. if E has good reduction over p. Furthermore N_p is divisible by l if and only if the Frobenius element σ_P of every P lying over p corresponds to an element in G_l fixing a subspace of dimension one of $E[l]$. For p unramified, the σ_P form a conjugacy class of G_l that we denote by the Artin symbol σ_p (see [18] for details).

Note that if E had non-trivial l-torsion then this would imply a point of order l in $E(\mathbb{F}_p)$ for all but finitely many primes p. Then N_p would not be prime since it is divisible by l.

Serre ([16]) proved that for elliptic curves without complex multiplication, $G_l = \mathrm{GL}(2, \mathbb{Z}/l\mathbb{Z})$ for all but finitely many primes l. Let L' denote the set of exceptions. For the Artin symbol σ_p to fix a subspace of dimension one of $E[l]$ we see that for each $P|p$, σ_P must have eigenvalue one and hence σ_p must be contained in the conjugacy class of matrices in $GL(2, \mathbb{Z}/l\mathbb{Z})$ with eigenvalue one. The probability of this occurring is

$$\frac{|\{g \in G_l | g \text{ has eigenvalue } 1\}|}{|G_l|}.$$

We can explicitly compute this ratio in the case $l \notin L'$ to see that

$$P(l|N_p) = \frac{l^2 - 2}{(l^2 - 1)(l - 1)}.$$

To put this probability in perspective note that

$$\frac{l^2 - 2}{(l^2 - 1)(l - 1)} = \frac{1}{l} + \frac{1}{l^2} + O\left(\frac{1}{l^3}\right) \geq \frac{1}{l}.$$

So the probability that l does divide N_p is slightly bigger then if N_p was random.

Now we can compute the probability that N_p is prime given that $p \leq n$. Restricting to the case where L' is empty, (so called 'Serre Curves'), and recalling the formulation of Section 1.1.1

$$P(p \text{ and } N_p \text{ are prime}) = \frac{P(N_p \text{ is prime}|p \text{ is prime})}{P(m \text{ is prime})} P(p \text{ is prime}) P(m \text{ is prime}).$$

for any $m \leq n$. Also

$$P(N_p \text{ is prime}|p \text{ is prime}) = \prod_{l \geq 3} P(l \nmid N_p) = \prod_{l \geq 3} \left(\frac{1 - \frac{l^2-2}{(l^2-1)(l-1)}}{1 - \frac{1}{l}} \right)$$

Table 1.1: Predicted and computed estimates for $f(n)$ (see [8])

n	Predicted $f(n)$	$f(n)$
2000	26	30
4000	42	42
6000	55	51
10000	80	77
14000	103	103
18000	125	123
22000	145	141
26000	165	165
30000	184	183

so

$$P(p \text{ and } N_p \text{ are prime}) = \prod_{l \geq 3} \left(1 - \frac{l^2 - l - 1}{(l^2-1)(l-1)^2}\right) \frac{1}{\log n^2}.$$

This density is approximately .5052. In the case where L' is not empty we simply change the respective probabilities, $P(l \nmid N_p)$, for the primes in L'.

As a concrete example Koblitz considers the Serre curve $y^2 + y = x^3 - 3$. Let $f(n)$ denote $|\{p \leq n : p \nmid \Delta, N_p \text{ is prime }\}|$. Table 1.2.1 lists some values of $f(n)$ and the corresponding prediction by Koblitz's conjecture. A sketch of this elliptic curve is also given in Figure 1.1.

The Tchebotarev density theorem gives an effective estimate on the number of unramified primes whose Frobenius elements lie in the conjugacy class of G_l which have eigenvalue one.

Theorem 1.2.2 (The Effective Tchebotarev Density Theorem, [9])**.** *Let L/K be a finite extension of number fields and given a prime $p \in K$ let σ_p denote the Artin symbol of p. Let G be the Galois group of this extension and C a union of conjugacy classes in G. Then assuming the Generalized Riemann Hypothesis (abv. GRH), if $\pi_C(x)$ denotes the number of primes p in K with σ_p in C and $N_{K/\mathbb{Q}}p$ (the norm of p) less than some $x \in \mathbb{Z}$,*

$$\pi_C(x) = \frac{|C|}{|G|}\pi_K(x) + O\left(\frac{|C|}{|G|}x^{1/2}(\log d_L + [L:\mathbb{Q}]\log x)\right)$$

where $\pi_K(x)$ denotes the number of primes in K with norm less than x and d_L is the discriminant of L.

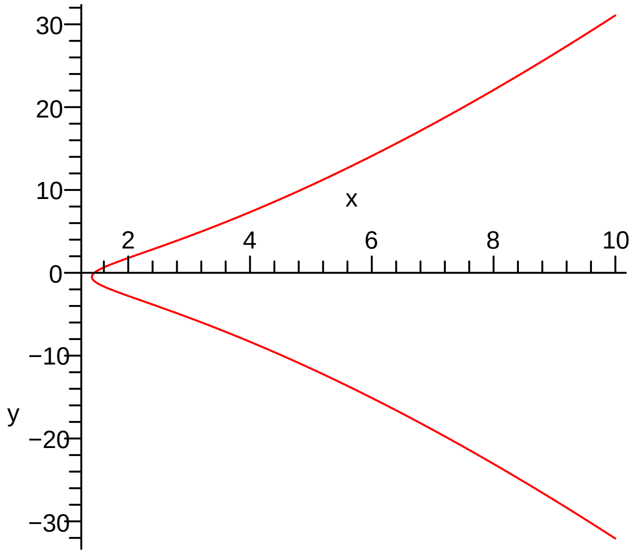

Figure 1.1: The Serre curve $y^2 + y = x^3 - 3$

In the case of Koblitz's conjecture, K is $\mathbb{Q}$, L is $\mathbb{Q}(E[l])$ and C is the set of all elements of G_l with eigenvalue one (denoted by C_1). When $l \notin L'$, $|C_1| = l^2 - 2$ and $|G_l| = (l-1)(l^2-1)$ giving,

$$\{p \le x : l|N_p, p \text{ is unramified}\} = \{p \le x : \sigma_P \text{ has eigenvalue one for all } P|p, p \text{ is unramified}\} \tag{1.3}$$

$$= \frac{l^2-2}{(l-1)(l^2-1)} \mathrm{li} x + O(l^{3/2} x^{1/2} \log(l N_E x)) \tag{1.4}$$

In general define a multiplicative function

$$\delta(l) = \frac{(l-1)(l^2-1)}{l^2-2} \tag{1.5}$$

for $l \notin L'$.

For $l \in L'$, define $\delta(l)$ to be the reciprocal of the size of the conjugacy class of elements in G_l with eigenvalue one, C_1, to $|G_l|$. For this to be well defined $|C_1|$ must be nonzero. In this case N_p would be divisible by l for a positive density of primes p namely, density $|C_1|/|G_l|$. But this cannot happen since E has no $\mathbb{Q}$-torsion and by the following theorem due to Katz.

Theorem 1.2.3 ([7], Theorem 2)**.** *Let E be an elliptic curve over a number field K, and $m \geq 2$ an integer. If we have*

$$N_p \equiv 0 \mod m$$

for a set of primes p of density one in K, then there exists a K-isogenous elliptic curve E' over K for which

$$|\textit{Torsion of } E'(K)| \equiv 0 \mod m.$$

By the Ogg-Neron-Shafarevich criterion for elliptic curves δ is multiplicative and we have that

$$|\{p \leq x : d|N_p, p \text{ is unramified}\}| = \frac{1}{\delta(d)}\mathrm{li}x + O(d^{3/2}x^{1/2}\log(dN_E x)). \tag{1.6}$$

for any d squarefree.

1.2.2 A First Sieve Approach

Miri and Murty applied the lower bound sieve to Koblitz's conjecture in an analogous fashion to the twin prime conjecture to prove the following result.

Theorem 1.2.4 ([11])**.** *Assume the GRH. Let E be an elliptic curve without complex multiplication. Then there exists a real positive constant C_E such that there are at least*

$$C_E\frac{x}{(\log x)^2}$$

primes $p \leq x$ such that N_p has at most 16 prime factors counting multiplicity.

We now sketch an outline of their proof beginning with a formulation of the sieve methods used.

1.2.3 The General Sieve Problem

Let $\mathcal{A}$ be a finite set of integers and for p prime let $\mathcal{A}_p = \{a : a \in \mathcal{A}, p|f(a)\}$ for some function $f : \mathcal{A} \to \mathbb{Z}$. For d-squarefree let $\mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p$. Choose X to be a close approximation to the size of $\mathcal{A}$ and δ a multiplicative function so that $(1/\delta(d))X$

is a close approximation to the size of $\mathcal{A}_d$. Define the remainder terms r_d to be

$$r_d := |\mathcal{A}_d| - \frac{1}{\delta(d)}X.$$

Let $\mathcal{P}$ be a set of primes and $P(z) = \prod_{\substack{p \le z \\ p \in \mathcal{P}}} p$. The general sieve problem requires us to determine the number of elements in $\mathcal{A}$ which are not divisible by any primes in $\mathcal{P}$. Hence we have to 'sift' $\mathcal{A}$ by the set of primes $\mathcal{P}$ or compute the sieving function

$$S(\mathcal{A},\mathcal{P},z) = |\{a \in \mathcal{A} : (f(a),P(z)) = 1\}| = |\mathcal{A} \backslash \bigcup_{p|P(z)} \mathcal{A}_p|.$$

The most elementary techniques in sieving involve inclusion exclusion arguments however we will study a weighted version of the sieve problem given by the lower bound sieve.

Recall that given two arithmetic functions, ν and κ, the Dirichlet convolution is

$$\nu * \kappa(n) = \sum_{d|n} \nu(d)\kappa\left(\frac{n}{d}\right)$$

Theorem 1.2.5. *Keep the notation as above. Let $\delta(d)$ be a multiplicative function for d squarefree. Let δ_1 be the Dirichlet convolution $\delta * \mu$. Then for any $y, z > 0$ and for any sequence of real numbers α_t, λ_d which are supported at squarefree positive integers composed of primes of $\mathcal{P}$, we have*

$$\sum_{a \in \mathcal{A}} \left(\sum_{\substack{t \le y \\ a \in \mathcal{A}_t}} \alpha_t \right) \left(\sum_{\substack{d \le z \\ a \in \mathcal{A}_d}} \lambda_d \right)^2 = \Delta X + E \tag{1.7}$$

where

$$E := O\left(\sum_{\substack{m \le yz^2 \\ m|P(yz)}} \left(\sum_{\substack{t \le y \\ t|m}} |\alpha_t| \right) \left(\sum_{\substack{d \le z \\ d|m}} |\lambda_d| \right)^2 |r_m| \right)$$

and

$$\Delta = \sum_{\substack{t \le y, d \le z \\ t|P(y), d|P(z) \\ (t,d)=1}} \frac{\alpha_t}{\delta(t)\delta_1(d)} \left(\sum_{\substack{r \le z/d \\ r|P(z) \\ r|t}} \mu(r) z_{dr} \right)^2 \tag{1.8}$$

with

$$z_r = \mu(r)\delta_1(r) \sum_{\substack{s \le z/r \\ s | P(z)}} \frac{\lambda_{sr}}{\delta(sr)} \tag{1.9}$$

for any positive squarefree integer r composed of primes of $\mathcal{P}$.

Note that with our definition of z_r

$$\lambda_d = \mu(d)\delta(d) \sum_{\substack{r \le z/d \\ r | P(z)}} \frac{\mu^2(rd)}{\delta_1(rd)} z_{rd} \tag{1.10}$$

thus a choice of z_r gives a choice of λ_d. We will omit a proof of the lower bound sieve in the classical case. However in a later section we will give a proof of an adapted version.

1.2.4 Applying the Sieve

For the specific case of Koblitz's conjecture we use the following setup. Let $\mathcal{A} = \{p : p \le x\}$ and $f(p) = N_p$. We need an estimate on $|\mathcal{A}_d|$ and X. We can easily see that $X = \pi(x)$ where as usual $\pi(x)$ denotes the number of primes less than or equal to x. To compute $|\mathcal{A}_d|$ we recall the discussion given in Section 1.2.2 and apply the effective form of the Tchebotarev density theorem given in (1.6).

$$\begin{aligned} |\mathcal{A}_d| &= |\{p \le x : d | N_p, d \nmid \Delta\}| && (1.11) \\ &= \frac{1}{\delta(d)} \mathrm{li} x + O(d^{3/2} x^{1/2} \log(dNx)) && (1.12) \end{aligned}$$

where $\delta(d)$ is given by (1.5). This implies:

$$r_d \ll d^3 x^{1/2} \log(dNx).$$

For now let $y, z > 1$ be free parameters and choose bounded sequences α_t and λ_d supported at squarefree integers such that $\alpha_t = 0$ for $t > y$, $\lambda_d = 0$ if $d > z$ and with

$|\lambda_d| < 1$. We first consider the error term E from Theorem 1.2.5

$$\begin{aligned} E &\ll \sum_{\substack{m \le yz^2 \\ m|P(yz)}} \left(\sum_{\substack{t \le y \\ t|m}} |\alpha_t| \right) \left(\sum_{\substack{d \le z \\ d|m}} |\lambda_d| \right)^2 |r_m| \\ &\ll \sum_{m \le yz^2} d(m)^3 m^3 x^{1/2} (\log(mNx)) \\ &\ll (yz^2)^4 x^{1/2+\epsilon} \log(xN). \end{aligned}$$

where $d(m)$ is the number of positive divisors of m. If we require $yz^2 \ll x^{1/8-\epsilon}$ then we can see that this error is $\ll x^{1-\epsilon}$.

We will now choose the α_t and z_r (since this gives a choice for λ_d) in two different ways. Our first choice is

$$\alpha_t = \begin{cases} 1, & \text{if } t = 1, \\ 0, & \text{otherwise} \end{cases} \tag{1.13}$$

and

$$z_r = \begin{cases} z_1, & \text{if } r < z \text{ and } r \text{ is squarefree,} \\ 0, & \text{otherwise} \end{cases} \tag{1.14}$$

for z_1 a positive constant.

With this choice, equation (1.7) is

$$\sum_{p \le x} \left(\sum_{\substack{d|N_p \\ d<z}} \lambda_d \right)^2 = z_1^2 \left(\sum_{m<z} \frac{\mu^2(d)}{\delta_1(d)} \mathrm{li} x \right) + O(x^{1-\epsilon}) \tag{1.15}$$

where our error term comes from the computation above.

Let our second choice of α_t be

$$\alpha_t = \begin{cases} 1, & \text{if } t \text{ is prime } < y, \\ 0, & \text{otherwise} \end{cases} \tag{1.16}$$

This allows α_t to count divisors of N_p. With the same choice of z_r as above, equation (1.8) becomes

$$\Delta = \sum_{\substack{t\le y, d\le z\\ t|P(y), d|P(z)\\ (t,d)=1}} \frac{\alpha_t}{\delta(t)\delta_1(d)} \left(\sum_{\substack{r\le z/d\\ r|P(z)\\ r|t}} \mu(r) z_{dr} \right)^2 \tag{1.17}$$

$$= \sum_{d<z} \frac{\mu^2(d)}{\delta_1(d)} \left(\sum_{\substack{\frac{z}{d}<l<y\\ l\nmid d}} \frac{1}{\delta(l)} \right) z_1^2 \tag{1.18}$$

At this point we apply some involved estimates and the GRH on the previous result and equation 1.2.5 to conclude

$$\sum_{a\in A} \left(\sum_{\substack{t\le y\\ a\in A_t}} \alpha_t \right) \left(\sum_{\substack{d\le z\\ a\in A_d}} \lambda_d \right)^2 \sim (\mathrm{li} x)\left(\left(1 + \log\left(\frac{\log y}{\log z}\right)\right) \sum_{m<z} \frac{\mu^2(m)}{\delta_1(m)} z_1^2 \right). \tag{1.19}$$

with α_t and z_r from our second choice. Though the details of this calculation will be omitted we will prove something similar in Chapter 4.

Choose

$$y = x^{1/16+\epsilon}$$

and

$$z = x^{1/32-\epsilon}$$

thus preserving the condition that $yz^2 < x^{1/8-\epsilon}$. Then subtracting equation (1.19) from twice equation (1.15) gives the asymptotic

$$\sum_{a\in \mathcal{A}} \left(2 - \sum_{\substack{t\\ a\in \mathcal{A}_t}} \alpha_t \right) \left(\sum_{\substack{d\\ a\in \mathcal{A}_d}} \lambda_d \right)^2 \sim \mathrm{li} x \left(\left(1 - \log\left(\frac{\log y}{\log z}\right)\right) \sum_{m<z} \frac{\mu^2(m)}{\delta_1(m)} z_1^2 \right). \tag{1.20}$$

Now

$$\begin{aligned} 1 - \log\left(\frac{\log y}{\log z}\right) &= 1 - \log\left(\frac{\log(x^{1/16+\epsilon})}{\log(x^{1/32-\epsilon})}\right) \\ &= 1 - \log\left(\frac{\frac{1}{16}+\epsilon}{\frac{1}{32}-\epsilon}\right) > 0 \end{aligned}$$

Since this quantity is positive as x tends to infinity, for infinitely many primes p

$$\left(2 - \sum_{\substack{t \\ a \in \mathcal{A}_t}} \alpha_t\right) > 0. \tag{1.21}$$

Our choice of α_t now implies that $\sum_{\substack{t \\ a \in \mathcal{A}_t}} \alpha_t$ counts the prime divisors of N_p less then y. So for infinitely many primes N_p has at most one prime factor less then y. Now since $p \le x$ and by Hasse's bound, $N_p \ll p$ (see [17]), we see that N_p can have at most 15 prime factors greater then y. Thus N_p can have at most 16 prime factors. Note the similarity between equation (1.20) and the expression (1.2) used by Bombieri for the twin prime conjecture.

Now recall from (1.10) that

$$\lambda_d = \mu(d)\delta(d) \sum_{\substack{r \le z/d \\ r | P(z)}} \frac{\mu^2(rd)}{\delta_1(rd)} z_{rd} \tag{1.22}$$

thus with our choice of z_d we see

$$\begin{aligned} \sum_{\substack{d | N_p \\ d < z}} \lambda_d &\ll \sum_{d < z} \delta(d) \sum_{r \le \frac{z}{d}} \frac{1}{\delta_1(rd)} |z_1| \\ &\ll \log z \\ &\ll \log x. \end{aligned}$$

Combining the previous estimate, (1.15) and the estimate li$x \asymp \dfrac{x}{\log x}$, the number of primes satisfying (1.21) is at least

$$C_E \frac{x}{(\log x)^2},$$

where C_E is a real positive constant depending on E.

1.2.5 An Improved Result

By applying stronger sieving techniques we can hope to improve on Miri and Murty's result. Steuding and Weng have effectively applied the linear sieve with logarithmic weights to prove the following.

Theorem 1.2.6 ([18]). *Assume the GRH. Let E be an elliptic curve without complex multiplication such that any elliptic curve $\mathbb{Q}$-isogenous to E has trivial $\mathbb{Q}$ torsion. Then there exists a real positive constant C_E such that there are at least*

$$C_E \frac{x}{(\log x)^2}$$

primes $p \le x$ such that N_p is a product of at most 8 primes counting multiplicity.

Chapter 2

Function Fields and the Drinfeld Module

2.1 Function Fields

2.1.1 Number Theory in Function Fields

Fix a finite field $\mathbb{F}_q$ of prime characteristic p with size $q = p^c$ with $c \in \mathbb{N}$. Let $A = \mathbb{F}_q[t]$ be the polynomial ring over $\mathbb{F}_q$ with $k = \mathbb{F}_q(t)$, as the rational function field. In general a function field will be a finite algebraic extension of k. Function fields possess a rich arithmetic structure analogous to that of the integers. Many arithmetic quantities such as the Euler-Phi function and the prime counting function translate well and have the same properties as their counterparts in the integers. Furthermore Drinfeld modules give effective generalizations of cyclotomic fields and elliptic curves.

This chapter will explain these connections and describe the number theoretic properties of A. The ultimate goal is to translate Koblitz's conjecture for elliptic curves to Drinfeld modules. The majority of this section is based on the exposition in [15].

Given $f \in A$, we can express $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0$ for $a_i \in \mathbb{F}_q$. The degree of f, denoted by $\deg f$ is the highest power of f with a nonzero coefficient. By convention we define the degree of 0 to be $-\infty$.

The following theorem says that A is a Euclidean domain and hence a unique factorization domain.

Theorem 2.1.1. *Let $f, g \in A$ with $g \neq 0$. Then there exist elements $q, r \in A$ such that $f = qg + r$ and $r = 0$ or $\deg r < \deg g$. Moreover q and r are uniquely determined by these conditions.*

Proof. See Theorem 1.1 in [15]. □

Define

$$|g| = \begin{cases} q^{\deg g} & \text{if } g \neq 0, \\ 0 & \text{if } g = 0. \end{cases}$$

Theorem 2.1.2. *Let $g \in A$ and $g \neq 0$, then A/gA is a finite ring with $|g|$ elements.*

Proof. Using the division algorithm, we can quickly see that

$$\{r \in A | \deg r < m\}$$

is a set of coset representatives for gA. There are $|g|$ such representatives. □

For $m \in \mathbb{Z}$, $|m| = |\mathbb{Z}/m\mathbb{Z}|$, motivating the notation $|g|$ above. We have the following theorem about units.

Lemma 2.1.3. *Let P be an irreducible polynomial in A and let e be a positive integer. Then the size of the unit group of A/P^eA (denoted $(A/P^eA)^*$) is $|P|^{e-1}(|P|-1)$.*

Proof. First we consider the case when $e = 1$. Since P is prime and A is a Euclidean domain, PA is maximal hence A/PA is a field. Thus $|(A/PA)^*| = |P| - 1$. In the case where $e > 1$, PA/P^eA is the unique maximal ideal of A/PA. Since $(A/PA)^* = A/P^eA - PA/P^eA$ we see that $|A/PA| = |P|^e - |PA/P^eA| = |P|^e - |P|^{e-1}$, concluding the proof. □

Given $f \in A$ and $g \in A$, with $\deg g < \deg f$, g will be a unit in A/fA if and only if g is relatively prime to f. Let $\varphi(f)$, the Euler-Phi function, denote the size of the unit group of A/fA.

Theorem 2.1.4. *If $f \in A$ has the prime decomposition $f = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$ then*

$$\varphi(f) = |f| \prod_{P|f} \left(1 - \frac{1}{|P|}\right).$$

Proof. From the Chinese Remainder Theorem

$$\frac{A}{fA} = \frac{A}{P_1^{e_1}A} \times \frac{A}{P_2^{e_2}A} \cdots \times \frac{A}{P_n^{e_n}A}$$

thus

$$\begin{aligned}
\varphi(f) = \left|\frac{A}{fA}\right| &= \prod_{P_i|f} \left|\frac{A}{P_i^{e_i}A}\right| \\
&= \prod_{P_i|f} |P_i|^{e_i-1}(|P_i|-1) \\
&= |f| \prod_{P_i|f} \left(1 - \frac{1}{|P_i|}\right)
\end{aligned}$$

□

2.1.2 Prime Number Theorem

The rich structure of function fields gives a natural analogue of the classical zeta function.

Define the zeta function of A to be the series,

$$\zeta_A(s) = \sum_{\substack{f \in A \\ f \text{ monic}}} \frac{1}{|f|^s}.$$

Since there are q^d monic polynomials in A of degree d, we have

$$\zeta_A(s) = \sum_{d \geq 0} \frac{q^d}{q^{ds}} = \frac{1}{1-q^{1-s}},$$

an analytic function for all complex numbers s with real part greater then 1.

Analogous to the case for the classical Riemann zeta function, $\zeta_A(s)$ affords an Euler product representation given by

$$\zeta_A(s) = \prod_{P \text{ monic irreducible}} \left(1 - \frac{1}{|P|^s}\right)^{-1}.$$

Let m_d be the number of monic irreducibles of degree d, then

$$\zeta_A(s) = \prod_{d \geq 1} \left(1 - \frac{1}{q^{ds}}\right)^{-m_d}.$$

This equation is the basis for the prime number theorem in function fields.

Theorem 2.1.5. *The number m_d of monic irreducible polynomials of degree d in A is given by*

$$m_d = \frac{q^d}{d} + \mathrm{O}\left(\frac{q^{\frac{d}{2}}}{d}\right).$$

Remark 2.1.6. If we let $x = q^d$ and $\pi_q(d) = m_d$ then we can rewrite the previous expression as

$$\pi_q(d) = \frac{x}{\log_q x} + \mathrm{O}\left(\frac{\sqrt{x}}{\log_q x}\right).$$

This is similar to the conjectured classical version of the prime number theorem dependent on the Riemann Hypothesis. In function fields the Riemann Hypothesis trivially holds due to the 'nice' form of the zeta function.

Proof. Firstly

$$\prod_{d \geq 1} \left(1 - \frac{1}{q^{ds}}\right)^{-m_d} = \frac{1}{1 - q^{1-s}}.$$

Let $u = q^{-s}$ and take logarithms of both sides of the previous expression.

$$\sum_{d=1}^{\infty} -m_d \log(1 - u^d) = -\log(1 - qu).$$

After differentiating and multiplying both sides by u we arrive at

$$\sum_{d=1}^{\infty} \frac{qm_d}{1 - u^d} u^d = \frac{qu}{1 - qu}$$

so by comparing coefficients of u^n on both sides we see

$$\sum_{d|n} dm_d = q^n.$$

Using Möbius inversion on the above gives

$$m_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Now note that the highest power of q occurring in the sum above is q^n. The next highest power is $q^{\frac{n}{2}}$ followed by at most n terms with power no higher then $q^{\frac{n}{3}}$. Thus

$$\left| m_n - \frac{q^n}{n} \right| \leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}}$$

giving our result. □

2.1.3 The Tchebotarev Density Theorem

The Tchebotarev density theorem is necessary to compute the size of the sets being sieved in the classical version of Koblitz's conjecture. We will need an analogous effective version of the theorem in the function field case. Let L/K denote a finite Galois extension of function fields, with integral rings O_L and O_K respectively. Let $G = \mathrm{Gal}(L/K)$ and let C denote a union of conjugacy classes of G.

Given a prime P in K and a prime $\mathfrak{P}$ lying over it, we know that $\mathrm{Gal}(\frac{O_L}{\mathfrak{P}O_L}/\frac{O_K}{PO_K})$ is a cyclic group (since it is an extension of finite fields) generated by an element $\sigma_{\mathfrak{P}}$ where for any $f \in O_L/\mathfrak{P}O_L$, $\sigma_{\mathfrak{P}}(f) = f^{|O_K/PO_K|}$.

$$\begin{tikzcd}
\mathfrak{P} \arrow[r] \arrow[d] & O_K \arrow[r] \arrow[d] & K \arrow[d] \\
P \arrow[r] & O_L \arrow[r] & L
\end{tikzcd}$$

Let the decomposition group of $\mathfrak{P}$ be $D(\mathfrak{P}/P) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$. Note that since the decomposition group fixes $\mathfrak{P}$, there is a group homomorphism $D(\mathfrak{P}/P) \to \mathrm{Gal}(\frac{O_L}{\mathfrak{P}O_L}/\frac{O_K}{PO_K})$ with the kernel defined to be the inertia group, $I_{\mathfrak{P}}$. In fact we can show that this homomorphism is surjective so

$$\frac{D(\mathfrak{P}/P)}{I_{\mathfrak{P}}} \cong \mathrm{Gal}\left(\frac{O_L}{\mathfrak{P}O_L}/\frac{O_K}{PO_K}\right).$$

When P is unramified in L, the inertia group of each $\mathfrak{P}$ over P is trivial, so $\sigma_{\mathfrak{P}}$ corresponds to an element of G. We can show that as $\mathfrak{P}$ ranges over the primes dividing P the resulting $\sigma_{\mathfrak{P}}$ determine a conjugacy class of G completely determined by P which we designate by σ_P (see [15]).

For x a positive integer we can define

$$\pi_C(x, L/K) = |\{P| \deg P = x, P \text{ is unramified in the extension } L/K, \text{ and } \sigma_P \subseteq C\}.$$

Before we can state the effective version of the Tchebotarev density theorem, we need to define several quantities related to the extension L/K. Let $\mathbb{F}_K, \mathbb{F}_L$ denote the constant fields of K and L respectively and let $r_L = [L \cap \overline{\mathbb{F}}_K : \mathbb{F}_K]$. When $r_L = 1$ we say the extension L/K is *geometric.* Define $d_K = [\mathbb{F}_K : \mathbb{F}_q]$ and g_L, g_K to be the genera of L and K respectively.

The effective version of the Tchebotarev density theorem gives the following.

Theorem 2.1.7 ([3]). *Let L/K be a finite Galois extension with Galois group G. Let $C \subseteq G$ be a conjugacy class whose restriction to $\mathbb{F}_L$ is the a-th power of the Frobenius automorphism of $\mathbb{F}_K$. Then for $x \in \mathbb{N}$, if $x \not\equiv a \mod r_L$*

$$\pi_C(x, L/K) = 0.$$

If $x \equiv a \mod r_L$, we have

$$\begin{aligned} &\left|\pi_C(x, L/K) - r_L \frac{|C|}{|G|}\frac{(q^{d_K})^x}{x}\right| \\ &\le \frac{2}{x}\frac{|C|}{|G|}\big((|G| + g_L r_L)(q^{d_K})^{x/2} + |G|(2g_K + 1)(q^{d_K})^{x/4} + g_L r_L + |G|d/d_K\big) \end{aligned} \tag{2.1}$$

Note that if we take $k = K = L$ then applying the theorem gives

$$\pi(x) = \frac{q^x}{x} + \mathrm{O}\left(\frac{q^{\frac{x}{2}}}{x}\right)$$

which is just the prime number theorem in function fields.

2.2 Drinfeld Modules

Given a commutative k-algebra B, it is implicitly an A-module through the algebra multiplication. Let τ denote the Frobenius element of $k = \mathbb{F}_q(t)$ where $\tau(X) = X^q$ for $X \in k$. Then τ is an endomorphism on B and in particular any polynomial in τ over k is also an endomorphism of B. Given $h \in k$ and $u \in B$, the action of τ on $h \cdot u$ is

$$\tau(h \cdot u) = (h \cdot u)^q = h^q u^q = h^q \tau(u).$$

Instead of being a k-algebra homomorphism, τ performs the 'twisted action' $\tau h = h^q \tau$ for $h \in k$. Also if $a \in \mathbb{F}_q$ then $\tau(a \cdot u) = a\tau(u)$ so τ is $\mathbb{F}_q$ linear. Denote the ring of polynomials in τ over k with this 'twisted' multiplication as $k < \tau >$. This is known as a twisted polynomial ring, and in particular we see that each element of this ring induces an endomorphism of B.

We can view $k < \tau >$ in a more natural way as the set of additive polynomials that are $\mathbb{F}_q$ linear over k.

Definition 2.2.1. A polynomial $F \in k[X]$ is additive if inside the ring of polynomials in two variables, $k[X, Y]$, $F(X + Y) = F(X) + F(Y)$. We denote the set of $\mathbb{F}_q$ linear additive polynomials by $\mathsf{A}(k)$.

If F, G are two additive polynomials, note that

$$\begin{aligned} F(G(X+Y)) &= F(G(X)+G(Y)) \\ &= F(G(X))+F(G(Y)) \end{aligned}$$

so composition makes $\mathsf{A}(k)$ into a ring.

Since k has characteristic p the polynomial

$$G(X) = a_n X^{q^n} + a_{n-1} X^{q^{n-1}} + \cdots + a_0 X$$

with coefficients in k is an additive polynomial. In particular we can find an element $g \in k < \tau >$ such that $g(\tau)(f) = G(f)$ for any $f \in k$, namely

$$g(\tau) = a_n \tau^n + a_{n-1}\tau^{n-1} + \cdots + a_0.$$

Thus there exists a natural correspondence between additive polynomials of the form of G and polynomials in $k < \tau >$.

Theorem 2.2.2. *Every $\mathbb{F}_q$ linear additive polynomial $G(X)$ is of the form*

$$G(X) = a_n X^{q^n} + a_{n-1} X^{q^{n-1}} + \cdots + a_1 X^q + a_0 X.$$

with $a_i \in \mathbb{F}_q$. Furthermore given the map determined by

$$G \to g(\tau)$$

where $g(\tau) = a_n\tau^n + a_{n-1}\tau^{n-1} + \cdots + a_1\tau + a_0$ demonstrated above from $\mathsf{A}(k)$ to $k < \tau >$ is an isomorphism.

Proof. It is clear that every polynomial of the form given is in $\mathsf{A}(k)$. We prove the other direction by induction on the degree of $G(X)$. The result is clear for constant and linear polynomials. Since G is additive $G(X+Y) = G(X)+G(Y)$ and $\frac{\partial}{\partial X}G(X+Y) = \frac{\partial}{\partial X}G(X)$. Setting $X = 0$ we see that the formal derivative of $G(X)$ must be a constant. Let $G(X) = \sum a_i X^i$, $G'(X)$ is a constant if and only if for each $i > 1$ not divisible by p, $a_i = 0$. Thus we can write

$$G(X) = a_1 X + \sum_{i \geq 1} a_{pi} X^{p^i} = a_1 X + H(X)^p$$

for some polynomial $H(X)$ with coefficients in the field l obtained from k by adjoining the p^{th} roots of the coefficients a_{pi}. Note that for $a \in \mathbb{F}_q$

$$G(aX) = a_1 aX + \sum_{i \geq 1} a_{pi} a^{p^i} X^{p^i},$$

so $G(aX) = aG(X)$ if and only if $a_{pi} = 0$ for $p^i \neq q^j$ for some j. Thus

$$G(X) = a_1 X + H(X)^q.$$

$H(X)$ is an additive polynomial in $l[X]$ so by induction $H(X) = \sum b_j X^{q^j}$ and

$$G(x) = a_1 X + \sum_j b_j^q X^{q^{j+1}}$$

and since $b_j^q \in k$ the result follows. The second claim now easily follows. □

From the previous theorem we now see that $\mathsf{A}(k)$ and $k < \tau >$ induce the same endomorphisms on the k-algebra B. In a natural way this allows us to put a new A module structure on B by any homomorphism $\rho : A \to k < \tau >$.

Definition 2.2.3. A Drinfeld module for A defined over k will be an $\mathbb{F}_q$-algebra homomorphism $\rho : A \to k < \tau >$ such that for all $f \in A$ the constant term of $\rho(f)$ is f and for at least one f in A, $\rho(f) \notin k$.

The last condition is to guarantee that this A-module action is different from the one induced by A as a k-algebra.

There is a natural way to interpret the previous results in terms of group schemes. Namely let G_a/k be the additive group scheme over k. Given a commutative k-algebra B, G_a/k assigns the underlying additive group structure B_+. From the previous discussion we know every additive polynomial gives rise to an endomorphism of B_+. Drinfeld managed to show that $\text{End}(G_a/k) \cong k < \tau >$. Thus the module structure induced on B from a Drinfeld module is a canonical way to make B an A-module.

2.2.1 The Carlitz Module and Cyclotomic Extensions

The Carlitz module is a concrete example of Drinfeld modules.

Since A is generated freely by one element t over k, for each element $g \in k < \tau >$ with constant term t and $g \notin k$ we can determine a unique homomorphism from

A to $k < \tau >$ by mapping t to g. Thus any Drinfeld module is determined by it's action on t.

The simplest choice of $g = \tau + t \in k < \tau >$ gives the Carlitz module denoted by C. For example

$$\begin{aligned} C(t^2) &= C(t)^2 \\ &= (t+\tau)^2 \\ &= t^2 + t\cdot\tau + \tau\cdot t + \tau^2 \\ &= t^2 + (t+t^q)\tau + \tau^2. \end{aligned}$$

In general we can let the Drinfeld module ϕ be determined by

$$\phi(t) = t + c_1\tau + c_2\tau^2 + \cdots + c_r\tau^r$$

where $c_r \neq 0$. We say that r is the rank of the Drinfeld module ϕ. Note that in general the constant term of $\phi(t^n)$ is t^n and the degree in τ is nr. Thus for any polynomial $a \in A$, the constant term of $\phi(a)$ is a and the degree in τ is $r\deg(a)$.

One way to view the Carlitz module is as a function field analogue of the unit group of $\mathbb{Z}/m\mathbb{Z}$ for an integer m. The analogous structure to $\mathbb{Z}/m\mathbb{Z}$ in function fields is A/fA for some polynomial $f \in A$. Under this identification we can consider $\mathbb{Z}/m\mathbb{Z}$ as a $\mathbb{Z}$-module analogous to A/fA as an A-module. However $(\mathbb{Z}/m\mathbb{Z})^*$ is also a $\mathbb{Z}$-module under exponentiation with no clear analogy in the function field case, since 'exponentiation' by A is not defined in A/fA. The solution to this is the Carlitz module $C(A/fA)$. This discussion is summarized in the table below.

Table 2.1: Analogy between the Carlitz Module and Classical cases

Classical	**Function Field**
$\mathbb{Z}$-module	A-module
$m \in \mathbb{Z}$	$f \in A$
$\frac{\mathbb{Z}}{m\mathbb{Z}}$	$\frac{A}{fA}$
$\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^*$	$C\left(\frac{A}{fA}\right)$

Let the action of a Drinfeld module ϕ on $\overline{k}$ be denoted as $\overline{k_\phi}$. Given $f \in A$ the torsion submodule of $\overline{k_\phi}$ is

$$\phi[f] = \{\lambda \in \overline{k} | \phi(f)(\lambda) = 0\}.$$

Following the discussion above, the equation $\phi(f)(\lambda) = 0$ is analogous to $x^l - a = 0$ for $a \in \mathbb{Z}$ for $x \in \mathbb{C}$ and l an integer. We can precisely determine the structure of $\phi[f]$.

Lemma 2.2.4. *Let $f \in A$ be nonzero. Let M be an A module and suppose for each $d|f$ the submodule $M[d] = \{m \in M | dm = 0\}$ has $q^{r \deg d}$ elements. Then*

$$M[f] \cong \left(\frac{A}{fA}\right)^r.$$

Proof. Consider the prime decomposition of $f = uP_1^{e_1}P_2^{e_2}\cdots P_n^{e_n}$, where u is a constant and the P_i are primes dividing f. Clearly

$$M[f] = M[P_1^{e_1}] \oplus M[P_2^{e_2}] \oplus \cdots \oplus M[P_n^{e_n}].$$

Using the Chinese Remainder Theorem we have

$$\frac{A}{fA} \cong \frac{A}{P_1^{e_1}A} \oplus \frac{A}{P_2^{e_2}A} \oplus \cdots \frac{A}{P_n^{e_n}A}$$

so it suffices to establish the result for the case of $f = P^e$ for P a prime.

Since p is a prime A/PA is a field and $M[P]$ is a vector space of degree r over A/PA with $q^{r \deg P}$ elements. We can apply the structure theorem of modules over principle ideal domains to see that

$$M[P^e] \cong \frac{A}{P^{k_1}A} \oplus \frac{A}{P^{k_2}A} \oplus \cdots \oplus \frac{A}{P^{k_r}A}$$

for some $k_1 \cdots k_r \in A$. The number of elements in $M[P^e]$ is $q^{re \deg P}$ but this must be equal to $q^{(k_1+k_2+\cdots+k_r)\deg P}$. Since $k_i \leq e$ we have that $k_i = e$ for each i, $1 \leq i \leq r$. □

Theorem 2.2.5. *Let ϕ be a Drinfeld module of rank r. Then for each nonzero $f \in A$, we have*

$$\phi[f] \cong \left(\frac{A}{fA}\right)^r.$$

Proof. We begin by showing that for each $f \in A$, $\phi[f]$ has $q^{r \deg f}$ elements. Note that

$$\phi(f)(X) = fX + a_1X^q + a_2X^{q^2} + \cdots + a_{r \deg f}X^{q^{r \deg f}}$$

where the $a_i \in k$ and $a_{r \deg f} \neq 0$. The derivative of $\phi(f)(X)$ is nonzero so it is separable and has $q^{r \deg f}$ roots in $\overline{k}$. Thus applying the previous lemma with $M = \overline{k_\phi}$ gives the result.

□

We can adjoin the elements of $\phi[f]$ to k to form the Galois extension $k(\phi[f])/k$. This gives an injection $\Phi_f : \mathrm{Gal}(k(\phi[f])/k) \to \mathrm{Aut}_{A/aA}(\phi[f])$ where $\mathrm{Aut}_{A/aA}(\phi[f])$ denotes the automorphisms of $\phi[f]$ as an A/fA module. However from the previous result we see that

$$\mathrm{Aut}_{A/aA}(\phi[f]) \cong \mathrm{GL}(r, A/fA).$$

This gives us a representation of the Galois group which will be crucial in translating Koblitz's conjecture to function fields.

Chapter 3

Generalizing the Lower Bound Sieve

3.1 Bombieri's Lower Bound Sieve

In this section we will reformulate the lower bound sieve in the context of polynomials over a finite field. Our exposition will be based on the proof of the lower bound sieve given in [2]. Fix a finite field $\mathbb{F}_q$ and following the notation from Section 1.2.3 let $\mathcal{A}$ be a finite set of monic polynomials from $A = \mathbb{F}_q[t]$, $\mathcal{P}$ a set of monic irreducible polynomials also from A, g be a function $g : \mathcal{A} \to A$, and let $\mathcal{A}_l = \{a \in \mathcal{A} : l | g(a)\}$ for monic irreducible polynomials l. We will write $P(z)$ to denote the product of all monic irreducibles in $\mathcal{P}$ with degree less than or equal to z. Let X be a close approximation to $|A|$ and $\delta(d)$ a multiplicative function so that

$$|\mathcal{A}_d| = \frac{1}{\delta(d)} X + r_d$$

for some error term r_d. In general, sieving is concerned with finding the following quantity:

$$S(\mathcal{A}, \mathcal{P}, z) = \left| \mathcal{A} \setminus \bigcup_{\substack{l \in \mathcal{P} \\ \deg l \leq z}} \mathcal{A}_p \right| .$$

Remark 3.1.1. Throughout the rest of the thesis all sums will be taken over monic polynomials in A.

Define the Möbius function μ on $A \setminus \{0\}$ as

$$\mu(f) = \begin{cases} (-1)^{\omega(f)} & \text{if } f \text{ squarefree,} \\ 1 & \text{if } f = 1, \\ 0 & \text{otherwise} \end{cases}$$

where $\omega(f)$ is the number of distinct irreducible factors of f

Selberg's sieve relies on the inequality

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &= \sum_{a \in \mathcal{A}} \sum_{\substack{d | P(z) \\ a \in \mathcal{A}_d}} \mu(d), \\ &\le \sum_{a \in \mathcal{A}_d} \left(\sum_{\substack{d | P(z) \\ a \in \mathcal{A}_d}} \lambda_d \right)^2 \end{aligned}$$

where λ_d is a sequence indexed by polynomials such that $\lambda_1 = 1$, and λ_d supported only on squarefree polynomials of degree less than z.

Bombieri modified this sieve by adding weights to each term in the sum on the right hand side of the above inequality. In the function field case we have a result analogous to Theorem 1.2.5.

Theorem 3.1.2. *In the general sieving situation set up above, let δ be a multiplicative function defined for d squarefree, and let $\delta_1(n)$ be the Dirichlet convolution $\delta * \mu$. Then for any $y, z > 0$ and any sequence of real numbers α_t, λ_d supported only at squarefree monic polynomials composed of primes of $\mathcal{P}$, we have*

$$\sum_{a \in \mathcal{A}} \left(\sum_{\substack{\deg t \le y \\ t | P(y) \\ a \in \mathcal{A}_t}} \alpha_t \right) \left(\sum_{\substack{\deg d \le z \\ d | P(z) \\ a \in \mathcal{A}_d}} \lambda_d \right)^2 = \Delta X + E, \tag{3.1}$$

where

$$E = \mathrm{O}\left(\sum_{\substack{\deg m \le yz^2 \\ m | P(yz)}} \left(\sum_{\substack{\deg t \le y \\ t | m}} |\alpha_t| \right) \left(\sum_{\substack{\deg d \le z \\ d | m}} |\lambda_d| \right)^2 |r_m| \right)$$

and

$$\Delta \;=\sum_{\substack{\deg t\le y,\deg s\le z\\ t|P(y),s|P(z)\\ (t,s)=1}}\frac{\alpha_t}{\delta(t)\delta_1(t)}\left(\sum_{\substack{\deg r\le z-\deg s\\ r|P(z),r|t}}\mu(r)z_{sr}\right)^2,$$

with

$$z_r \;=\mu(r)\delta_1(r)\sum_{\substack{\deg s\le z-\deg r\\ s|P(z)}}\frac{\lambda_{sr}}{\delta(sr)}$$

for any positive squarefree integer r composed of primes from $\mathcal{P}$.

Note that the above expression for z_r yields

$$\lambda_d=\mu(d)\delta(d)\sum_{\substack{\deg r\le z-\deg d\\ r|P(z)}}\frac{1}{\delta_1(rd)}z_{rd},$$

so a choice for z_r gives a choice for λ_d.

In order to prove this theorem, we need several technical lemmas. We fix the notation $\delta(a,b)=\delta((a,b))$.

Lemma 3.1.3. *For any multiplicative function δ, and squarefree polynomials t,d_1,d_2,*

$$\delta\left([t,d_1,d_2]\right)=\frac{\delta(t)\delta(d_1)\delta(d_2)\delta\left(t,d_1,d_2\right)}{\delta\left(t,d_1\right)\delta\left(t,d_2\right)\delta\left(d_1,d_2\right)}.$$

Proof. See Lemma 10.1.3 in [2]. □

Define

$$\delta_{-1}(n)=\sum_{d|n}\frac{\mu(d)}{\delta(\frac{n}{d})}.$$

By Möbius inversion,

$$\frac{1}{\delta(n)}=\sum_{d|n}\delta_{-1}(d).$$

Lemma 3.1.4. *If a,b are squarefree, monic polynomials, then*

$$\sum_{\substack{[r,s]=b\\ s|a}}\delta_1(r)\delta_{-1}(s)=\begin{cases}\delta_1(b), & \textit{if } (a,b)=1,\\ 0, & \textit{otherwise.}\end{cases}\tag{3.2}$$

Proof. Let $\tau = [r,s]$, $\rho = (r,s)$. Since a,b are squarefree and δ_1 is multiplicative,then from Lemma 3.1.3

$$\delta_1(r) = \frac{\delta_1(\rho)\delta_1(\tau)}{\delta_1(s)}.$$

We will sum over s,ρ instead of r,s. If $[r,s] = b$ and $s|a$ then $s|(a,b)$; for each such s any ρ which divides s uniquely determines an r such that $[r,s] = b$ and $(r,s) = \rho$, namely $r = \frac{\tau b}{s}$. Thus

$$\begin{aligned}\sum_{\substack{[r,s]=b\\ s|a}} \delta_1(r)\delta_{-1}(s) &= \sum_{\substack{s|(a,b)\\ \rho|s}} \frac{\delta_1(b)\delta_{-1}(s)\delta_1(\tau)}{\delta_1(s)},\\ &= \sum_{s|(a,b)} \frac{\delta_1(b)\delta_{-1}(s)}{\delta_1(s)} \sum_{\rho|s} \delta_1(\rho),\\ &= \delta_1(b) \sum_{s|(a,b)} \frac{\delta_{-1}(s)\delta(s)}{\delta_1(s)}.\end{aligned}$$

Since $\delta, \delta_1, \delta_{-1}$ are multiplicative for all irreducibles l,

$$\frac{\delta_{-1}(l)\delta(l)}{\delta_1(l)} = \frac{\left(\frac{1}{\delta(l)} - 1\right)\delta(l)}{\delta(l) - 1} = -1$$

So $\frac{\delta_{-1}(s)\delta(s)}{\delta_1(s)} = \mu(s)$. Thus,

$$\begin{aligned}\sum_{\substack{[r,s]=b\\ s|a}} \delta_1(r)\delta_{-1}(s) &= \delta_1(b) \sum_{s|(a,b)} \mu(s)\\ &= \begin{cases} \delta_1(b), & \text{if } (a,b) = 1,\\ 0, & \text{otherwise.}\end{cases}\end{aligned}$$

□

By expanding and applying the definition of $\mathcal{A}_d$,

$$\sum_{a\in\mathcal{A}} \left(\sum_{\substack{\deg t\le y\\ t|P(y)\\ a\in\mathcal{A}_d}} \alpha_t\right)\left(\sum_{\substack{\deg d\le z\\ d|P(z)\\ a\in\mathcal{A}_d}} \lambda_d\right)^2 = \sum_{a\in A} \sum_{\substack{\deg t\le y\\ \deg d_1,d_2\le z\\ t|P(y)\\ d_1,d_2|P(z)\\ a\in\mathcal{A}_{[t,d_1,d_2]}}} \alpha_t\lambda_{d_1}\lambda_{d_2}$$

$$= \sum_{\substack{\deg t \le y \\ \deg d_1, d_2 \le z \\ t | P(y) \\ d_1, d_2 | P(z)}} \sum_{a \in \mathcal{A}_{[t, d_1, d_2]}} \alpha_t \lambda_{d_1} \lambda_{d_2}$$

$$= \left(\sum_{\substack{\deg t \le y \\ \deg d_1, \deg d_2 \le z \\ t | P(y) \\ d_1, d_2 | P(z)}} \frac{\alpha_t \lambda_{d_1} \lambda_{d_2}}{\delta([t, d_1, d_2])} \right) |\mathcal{A}| + \sum_{\substack{\deg t \le y \\ \deg d_1, \deg d_2 \le z \\ t | P(y) \\ d_1, d_2 | P(z)}} \alpha_t \lambda_{d_1} \lambda_{d_2} r_{[t, d_1, d_2]}.$$

Let the coefficient of $\mathcal{A}$ be Δ' and let E be the second summand.

Using the identity in Lemma 3.1.3, rearranging the terms inside the sum, and applying the definitions of δ_1 and δ_{-1} to $\delta(d_1, d_2)$ and $1/\delta(t, d_1, d_2)$, we have

$$\Delta' = \sum_{\substack{\deg t \le y; \deg d_1, \deg d_2 \le z \\ t | P(z); d_1, d_2 | P(z)}} \frac{\alpha_t \lambda_{d_1} \delta(t, d_1) \lambda_{d_2} \delta(t, d_2)}{\delta(t) \delta(d_1) \delta(d_2)} \left(\sum_{r | (d_1, d_2)} \delta_1(r) \right) \left(\sum_{s | (t, d_1, d_2)} \delta_{-1}(s) \right). \tag{3.3}$$

We can rearrange the summation signs by summing over r, s with $s | t$ and then for each r, s, summing over d_1, d_2 such that $r | (d_1, d_2)$ and $s | (t, d_1, d_2)$. Since $s | t$, this occurs precisely when $[r, s] | d_1$ and $[r, s] | d_2$.

$$\Delta' = \sum_{\substack{\deg t \le y; \deg r, \deg s \le z \\ t | P(y); r, s | P(z) \\ s | t}} \frac{\alpha_t}{\delta(t)} \delta_1(r) \delta_{-1}(s) \sum_{\substack{\deg d_1, \deg d_2 \le z \\ d_1, d_2 | P(z) \\ [r, s] | d_1 \\ [r, s] | d_2}} \frac{\lambda_{d_1} \delta(t, d_1) \lambda_{d_2} \delta(t, d_2)}{\delta(d_1) \delta(d_2)}$$

$$= \sum_{\substack{\deg t \le y; \deg r, \deg s \le z \\ t | P(y); r, s | P(z) \\ s | t}} \frac{\alpha_t}{\delta(t)} \delta_1(r) \delta_{-1}(s) \left(\sum_{\substack{\deg d \le z \\ d | P(z) \\ [r, s] | d}} \frac{\lambda_d \delta(t, d)}{\delta(d)} \right)^2, \text{ by symmetry in } d_1, d_2.$$

Define

$$\eta_{t,u} = \sum_{\substack{\deg d \le z \\ d | P(z) \\ u | d}} \frac{\lambda_d \delta(t, d)}{\delta(d)}, \tag{3.4}$$

or

$$\frac{\lambda_u \delta(t,u)}{\delta(u)} = \sum_{\substack{\deg d \le z \\ d|P(z) \\ u|d}} \mu\left(\frac{d}{u}\right) \eta_{t,d}$$

by dual Möbius inversion.

If $d = su$, then by summing over su such that $s|P(z), \deg su \le z, (s,u) = 1$ we are summing over su such that $s|P(z), \deg su \le z$, since $\lambda_{su} = 0$ if $(s,u) \ne 1$.

$$\frac{\lambda_u \delta(t,u)}{\delta(u)} = \sum_{\substack{\deg s \le z - \deg u \\ s|P(z)}} \mu(s) \eta_{t,su}. \tag{3.5}$$

If $t = 1$, (3.5) yields

$$\frac{\lambda_{su}}{\delta(su)} = \sum_{\substack{\deg t \le z - \deg su \\ t|P(z)}} \mu(t) \eta_{1,stu}. \tag{3.6}$$

So by (3.5) and (3.6),

$$\eta_{t,u} = \sum_{\substack{\deg s \le z - \deg u \\ s|P(z)}} \delta(t,su) \sum_{\substack{\deg t \le z - \deg su \\ t|P(z)}} \mu(t) \eta_{1,stu}. \tag{3.7}$$

But λ is supported only on squarefree polynomials. Thus (3.6) is zero unless $(s,u) = 1$. Say $r = st$, if $s|P(z), t|P(z)$, and $r \nmid P(z)$, then r has repeated factors and (3.6) is zero. Thus,

$$\eta_{t,u} = \sum_{\substack{\deg r \le z - \deg u \\ r|P(z)}} \sum_{s|r} \mu\left(\frac{r}{s}\right) \delta\left(\frac{r}{s}, su\right) \eta_{1,ru}.$$

Analyzing the inner sum, if $r|t$, then

$$\begin{aligned}\sum_{s|r} \mu\left(\frac{r}{s}\right) \delta\left(\frac{r}{s}, su\right) &= \sum_{s|r} \mu\left(\frac{r}{s}\right) \delta(s) \\ &= \delta_1(s).\end{aligned}$$

If $r \nmid t$, let $v = (r,t) \neq r$, then as $\deg r/v > 0$.

$$\begin{aligned}\sum_{s|r} \mu\left(\frac{r}{s}\right) \delta\left(\frac{r}{s}, su\right) &= \sum_{s|r/v} \mu\left(\frac{r}{s}\right) \sum_{s|v} \mu\left(\frac{r}{s}\right) \delta(s) \\ &= 0.\end{aligned}$$

So,

$$\begin{aligned}\eta_{t,u} &= \sum_{\substack{\deg r \leq z - \deg u \\ r|P(z), r|t}} \delta_1(r) \eta_{1,ru} \\ &= \sum_{\substack{\deg r \leq z - \deg u \\ r|P(z), r|t}} \delta_1(r) \sum_{\substack{\deg s \leq z - \deg rs \\ s|P(z)}} \frac{\lambda_{rsu}}{\delta(rsu)}, \text{ by (3.4)} \\ &= \frac{\mu(u)}{\delta_1(u)} \sum_{\substack{\deg r \leq z - \deg u \\ r|P(z), r|t}} \mu(r)\mu(ru)\delta_1(ru) \sum_{\substack{\deg s \leq z - \deg ru \\ s|P(z)}} \frac{\lambda_{rsu}}{\delta(rsu)}. \qquad (3.8)\end{aligned}$$

Substituting (3.4) and (3.8) into (3.3) gives

$$\Delta' = \sum_{\substack{\deg t \leq y; \deg r, \deg s \leq z \\ t|P(y); r,s|P(z) \\ s|t}} \frac{\alpha_t}{\delta(t)} \delta_1(r) \delta_{-1}(s) \eta^2_{t,[r,s]}.$$

By moving the sum over s inside, and indexing by $u = [r,s]$, we have

$$\begin{aligned}\Delta' &= \sum_{\substack{\deg t \leq y; \deg u \leq z \\ t|P(y); u|P(z)}} \frac{\alpha_t}{\delta(t)} \eta^2_{t,u} \sum_{\substack{[r,s]=u \\ s|t}} \delta_1(r)\delta_{-1}(s) \\ &= \sum_{\substack{\deg t \leq y; \deg u \leq z \\ t|P(y); u|P(z) \\ (t,u)=1}} \frac{\alpha_t}{\delta(t)} \delta_1(u) \eta^2_{t,u} \text{ by lemma 1.} \\ &= \sum_{\substack{\deg t \leq y; \deg u \leq z \\ t|P(y), u|P(z) \\ (t,u)=1}} \frac{\alpha_t}{\delta(t)\delta_1(u)} \left(\sum_{\substack{r \leq z - \deg u \\ r|P(z), r|t}} \mu(r)\mu(ru)\delta_1(ru) \right) \left(\sum_{\substack{\deg s \leq z - \deg ru \\ s|P(z)}} \frac{\lambda_{rsu}}{\delta(rsu)} \right)^2 \\ &= \sum_{\substack{\deg t \leq y; \deg u \leq z \\ t|P(y); u|P(z) \\ (t,u)=1}} \frac{\alpha_t}{\delta(t)\delta_1(t)} \left(\sum_{\substack{\deg r \leq z - \deg u \\ r|P(z), r|t}} \mu(r)\alpha_{ru} \right)^2, \text{ by substituting the definition of } z_r \text{ in (3.2).} \\ &= \Delta. \qquad (3.9)\end{aligned}$$

This is the coefficient of $|\mathcal{A}|$ in Bombieri's lower bound sieve.

Returning to the error term, by summing over $m = [t, d_1, d_2]$ we have

$$E = \sum_{\substack{t \le y; d_1, d_2 \le z \\ t|P(y); d_1, d_2|P(z)}} \alpha_t \lambda_{d_1} \lambda_{d_2} r_{[t,d_1,d_2]} \tag{3.10}$$

$$= \mathrm{O}\left(\sum_{\substack{\deg m \le yz^2 \\ m|P(\max\{y,z\})}} \left(\sum_{\substack{\deg t \le y \\ t|P(y)}} |\alpha_t| \right) \left(\sum_{\substack{\deg d \le z \\ d|m}} |\lambda_d| \right)^2 |r_m| \right). \tag{3.11}$$

This concludes the proof of the function field analogue of the lower bound sieve.

□

Chapter 4

Koblitz's Conjecture for Function Fields

4.1 The Euler Characteristic

Our ultimate goal is to present a version of Koblitz's conjecture for Drinfeld modules. The starting point is to understand the respective module structures between elliptic curves over finite fields and Drinfeld modules defined over quotients of A by irreducible monic polynomials.

Drinfeld modules are the function field analogues of elliptic curves. In this thesis we will only consider the rank two case. Though this will become clearer in the next section, as an example note that given an elliptic curve over $\mathbb{C}$, $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ and for a Drinfeld module ϕ and a polynomial $f \in A$, $\phi[f] \cong (A/fA)^2$.

Fix an elliptic curve over a finite field $E(\mathbb{F}_l)$. This has a natural $\mathbb{Z}$–module structure induced by the additive group of the elliptic curve. Similarity by fixing an irreducible polynomial $f \in A$, A/fA has a natural A-module structure.

In the elliptic curve case we are interested in studying the quantity $\omega(|E(\mathbb{F}_l)|)$, where $\omega(n)$ denotes the number of distinct prime factors of n. In our case $\omega\left(|A/fA|\right) = 1$ regardless of f, thus is not a very interesting quantity to study. However from the discussion in Chapter 2 we can construct a new A-module structure on A/fA through a Drinfeld module ϕ. However $\omega\left(|\phi\left(A/fA\right)|\right) = \omega\left(|A/fA|\right) = 1$, still an unenlightening quantity to study.

Given an elliptic curve E and a prime l, for sufficiently divisible $m \in \mathbb{Z}$ we have

$E(\mathbb{F}_l) \subseteq E(\mathbb{F}_l)[m]$, and

$$E(\mathbb{F}_l) \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m_2\mathbb{Z}}$$

where $|E(\mathbb{F}_q)| = m_1 m_2$ for some $m_1, m_2 \in \mathbb{Z}$.

Given a cyclic $\mathbb{Z}$-module, $\mathbb{Z}/m\mathbb{Z}$ we denote the *Euler characteristic* of $\mathbb{Z}/m\mathbb{Z}$ as $\chi(\mathbb{Z}/m\mathbb{Z}) = m$. Extending this definition multiplicatively to $E(\mathbb{F}_l)$ we see that $|E(\mathbb{F}_l)| = m_1 m_2 = \chi(E(\mathbb{F}_l))$.

Using the decomposition theorem for finite modules over principle ideal domains, we see that

$$\phi\left(\frac{A}{fA}\right) \simeq \frac{A}{f_1 A} \oplus \frac{A}{f_2 A} \ldots \oplus \frac{A}{f_s A}$$

where the $f_i \in A$ and $f_i | f_{i-1}$ for $2 \leq i \leq s$. Since the Euler characteristic of A/fA is f, we can decompose

$$\begin{aligned}
\chi\left(\phi\left(\frac{A}{fA}\right)\right) &\simeq \chi\left(\frac{A}{f_1 A} \oplus \frac{A}{f_2 A} \ldots \oplus \frac{A}{f_s A}\right) && (4.1)\\
&= \chi\left(\frac{A}{f_1 A}\right) \oplus \chi\left(\frac{A}{f_2 A}\right) \ldots \oplus \chi\left(\frac{A}{f_s A}\right) && (4.2)\\
&= f_1 f_2 \cdots f_s. && (4.3)
\end{aligned}$$

This quantity is the natural analogue of the size of $E(\mathbb{F}_l)$ for function fields. We may now ask how often $\chi(\phi(A/fA))$ is prime for an irreducible polynomial f. From now on we adopt the notation $\chi_\phi(f) = \chi(\phi(A/fA))$. Note that unlike the elliptic curve case, our Euler characteristic is not an integer but a polynomial. We can now formulate Koblitz's conjecture for function fields.

Theorem 4.1.1 (Koblitz's Conjecture for Function Fields.)**.** *Let ϕ be a Drinfeld module of rank two with every A-isogeny having no A-torsion points and with $End_{\overline{k}}(\phi) = A$. Furthermore assume that for each monic irreducible $l \in A$, $k(\phi[l])/k$ is a geometric extension. Then given $x \in \mathbb{Z}_+$ there exists a real positive constant C_ϕ depending on ϕ so that there are asymptotically*

$$C_\phi \frac{q^x}{x^2}$$

monic irreducible polynomials p with degree at most x such that $\chi_\phi(p)$ is prime.

We can also prove the following analogue of Miri and Murty's result given in Chapter 1.

Theorem 4.1.2. *Let ϕ be a Drinfeld module of rank two with every A-isogeny having no A-torsion points and with $End_{\overline{k}}(\phi) = A$. Furthermore assume that for each monic irreducible $l \in A$, $k(\phi[l])/k$ is a geometric extension. Then given $x \in \mathbb{Z}_+$ there exists a real positive constant C_ϕ depending on ϕ so that there are at least*

$$C_\phi \frac{q^x}{x^2}$$

monic irreducible polynomials p with degree at most x such that $\chi_\phi(p)$ has at most 13 prime factors.

Remark 4.1.3. Through an abuse of notation, we are going to use p to denote a prime in A. Also prime and monic irreducible will be used interchangeably.

The various requirements we need will be explained.

4.2 Some Algebra

Before we begin a proof of Theorem 4.1.2 we need a proper algebraic formulation of the divisibility properties of $\chi_\phi(p)$ for $p \in A$ prime analogous to those established for N_p in Section 1.2.1. Throughout this section, we assume that ϕ is a Drinfeld module of rank 2.

Fix a prime $l \in A$ and recall Theorem 2.2.5 gives,

$$\phi[l^n] \cong \left(\frac{A}{l^n A}\right)^2.$$

Let $\phi[l^\infty]$ denote the direct limit of the $\phi[l^n]$, namely

$$\phi[l^\infty] = \bigcup_{n \geq 1} \phi[l^n].$$

If we allow A_l and k_l to be the completions of A and k at l then we can define the *l-adic Tate module of* ϕ, $T_l(\phi)$ as

$$T_l(\phi) = \mathrm{Hom}_{A_l}(k_l/A_l, \phi[l^\infty])$$

which is a free A_l-module of rank r.

For all but finitely many irreducibles $p \in A$, ϕ has good reduction at A/pA. By an analogue of the Ogg-Neron-Shafarevich theorem for Drinfeld modules, ϕ has good reduction at p if and only if p is unramified in the extension $k(\phi[l^\infty])/k$ for all primes $l \in A$ coprime to p. In this situation let σ_p denote the Artin symbol of p in $\mathrm{Gal}(k(\phi[l^\infty])/k)$. By choosing an appropriate basis for $T_l(\phi)$ there is an action

$$\rho_{l,\phi} : \mathrm{Gal}(\bar{k}(\phi[l^\infty])/k) \to \mathrm{Aut}(T_l(\phi)) \cong \mathrm{GL}(2, A_l).$$

In particular the characteristic polynomial $P_{p,\phi}$ of σ_p under this action is independent of l and we have the following result:

Theorem 4.2.1 ([5]). *As ideals of A,*

$$\chi_\phi(p) = P_{p,\phi}(1)A.$$

Since ϕ has rank 2 we know that $P_{p,\phi} = x^2 - \mathrm{tr}(\sigma_p) + \det \sigma_p$ so if $l | \chi_\phi(p)$ then $1 - \mathrm{tr}(\sigma_p) + \det \sigma_p \equiv 0 \mod l$ implying that σ_p has an eigenvalue of one.

Now recall the representation given in Section 2.2.1

$$\Phi_f : \mathrm{Gal}(k(\phi[l])/k) \to \mathrm{GL}(2, A/lA).$$

In particular we have the following result:

Theorem 4.2.2. *If ϕ has good reduction over p then $\chi_\phi(p)$ is divisible by l if and only if $\Phi_l(\sigma_p)$, where σ_p is the Artin symbol of p in the extension $k(\phi[l])/k$, has eigenvalue one.*

In general since ϕ has rank 2 then for all but finitely many primes, we have that Φ_l is an isomorphism provided $\mathrm{End}_k(\phi) = A$. Let the set of exceptional primes be denoted by L'_ϕ.

This is a specific case of the more general open image conjecture for which we refer the reader to [14].

Now define

$$\pi_\phi(x, l) = \{p \in A : \deg p = x, l | \chi_\phi(p), p \nmid l, p \text{ unramified}\}.$$

From the above discussion we see that

$$\pi_\phi(x, l) = \{p \in A : \deg p = x, p \nmid l, \Phi_l(\sigma_p) \text{ has eigenvalue } 1\},$$

a quantity that we will now compute using the Tchebotarev density theorem.

Let C denote the conjugacy class of matrices in $\mathrm{GL}(2, A/lA)$ which have eigenvalue 1. We will use Theorem 2.1.7 with $L = k(\phi[l])$, under the assumption that this extension is geometric ($r_L = 1$). In addition we have the following theorem.

Theorem 4.2.3 ([4])**.** *Let $l \in A$ and let $g_{k(\phi[l])}$ be the genus of the extension $k(\phi[l])/k$. Then there exists a constant $D(\phi)$ depending on ϕ only, such that*

$$g_{k(\phi[l])} \leq D(\phi)[k(\phi[l]) : k] \deg l.$$

Applying Theorem 2.1.7 gives

$$\pi_\phi(x, l) = \frac{|C|}{|G|}\pi_q(x) + \mathrm{O}\left(\frac{2|C|}{x} q^{x/2} \deg l\right). \tag{4.4}$$

Since A/lA is a finite field of size $|l|$, $|\mathrm{GL}(2, A/lA)| = (|l|^2 - |l|)(|l|^2 - 1)$ and $|C| = |l|^3 - 2|l|$. Thus we see that for $l \notin L'_\phi$,

$$\begin{aligned}
\pi_\phi(x, l) &= \frac{|l|^2 - 2}{(|l|^2 - 1)(|l| - 1)}\pi_q(x) + \mathrm{O}\left(\frac{|l|^3}{x} q^{x/2} \deg l\right) && (4.5)\\
&= \frac{1}{\delta(l)}\pi_q(x) + \mathrm{O}\left(\frac{|l|^3}{x} q^{x/2} \deg l\right) && (4.6)
\end{aligned}$$

where we define $\delta(l)$ to be

$$\delta(l) = \frac{(|l|^2 - 1)(|l| - 1)}{|l|^2 - 2}.$$

Since L'_ϕ is finite we can extend the definition of $\delta(l)$ to these primes also so that (4.5) holds with $\delta(l) = |G|/|C|$. The only issue in doing this is to guarantee $\delta(l) > 1$. However this is a direct consequence of the following analogue of Katz's theorem ([7]) for Drinfeld Modules.

Theorem 4.2.4. *Let ϕ be a Drinfeld module and $m \in A \smallsetminus \mathbb{F}_q$. For each prime p of k at which ϕ has good reduction, if*

$$\chi_\phi(p) \equiv 0 \mod m$$

for a set of primes of density one in k, then there exists a k-isogenous Drinfeld module ϕ' over K for which

$$|\mathit{Torsion\ of}\ \phi'| \equiv 0 \mod m.$$

The proof is identical to the elliptic curve case.

In particular from our formula for $\delta(l)$ when $l \notin L'_\phi$ and the fact that L'_ϕ is finite, for each $l \in A$, monic irreducible, we have that

$$\delta(l) = |l| - a_l \tag{4.7}$$

for some constant a_l. Furthermore we can find a positive constant C such that the $|a_l|$ are uniformly bounded by C.

Let $d = p_1 p_2$ be the prime decomposition of a squarefree polynomial (in general the number of factors is irrelevant to this discussion), and let G_d (respectively G_{p_1}, G_{p_2}) be the Galois group of the field $k(\phi[d])$ (respectively $k(\phi[p_1]), k(\phi[p_2])$) over k. By our previous discussion we know that G_d can be embedded in $GL(2, A/mA)$. By the analogue of Ogg-Neron-Shafarevich for Drinfeld modules, the reduction of $\mathrm{GL}(2, A/dA)$ to $\mathrm{GL}(2, A/p_1A)$ (or $\mathrm{GL}(2, A/p_2A)$) is compatible with the Galois action for G_d restricted to $k(\phi[p_1])$ (or $k(\phi[p_2])$). In particular a matrix in $\mathrm{GL}(2, A/dA)$ has eigenvalue 1 if and only if it's reductions on $\mathrm{GL}(2, A/p_1A)$ and $\mathrm{GL}(2, A/p_2A)$ have eigenvalue 1. Since $d|\chi_\phi(p)$ if and only if $p_1|\chi_\phi(p)$ and $p_2|\chi_\phi(p)$, δ is multiplicative and by the Tchebotarev Density theorem

$$\begin{aligned}\pi_\phi(x,d) &= \{p \in A : \deg p = x, d|\chi_\phi(p), p \nmid d, p \text{ unramified}\} && (4.8)\\ &= \frac{1}{\delta(d)}\pi_q(x) + \mathrm{O}\left(\frac{|d|^3}{x} q^{x/2} \deg d\right). && (4.9)\end{aligned}$$

We summarize the analogy between elliptic curves and Drinfeld modules in the following table.

Table 4.1: Analogy between the Drinfeld module and elliptic curves.

Classical	**Function Field**
$\mathbb{Z}$-module	A-module
elliptic Curve E	Drinfeld Module ϕ
$p \in \mathbb{Z}$	$p \in A$
$E(\mathbb{F}_p)$	$\phi\left(\frac{A}{fA}\right)$
N_p	$\chi_\phi(p)$
Tate Module $T_l(E)$	Tate Module $T_l(\phi)$
$\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$	$\mathrm{End}_{\overline{k}}(\phi) = A$

4.3 Applying the Sieve

We are now at the point that we can apply the lower bound sieve developed in Chapter 3 to the situation at hand. Fix a Drinfeld module ϕ of rank 2 with the assumptions in Theorem 4.1.2.

Let $\mathcal{A} = \{p \in A : \deg p = x, \phi \text{ has good reduction over } p\}$ and for d squarefree let $\mathcal{A}_d = \{p \in A : \chi_\phi(p) \equiv 0 \mod d\}$. In this case $X = \pi_q(x)$ and from the previous section

$$|\mathcal{A}_d| = \frac{1}{\delta(d)}X + r_d$$

where

$$r_d \ll \frac{|d|^3}{x} q^{x/2} \deg d.$$

As was done in the elliptic curve case, we will make two different choices of α_t and λ_d and allow y, z to be constants we will choose later.

The lower bound sieve, Section 3.1.2, tells us that

$$\sum_{p \in \mathcal{A}} \left(\sum_{\substack{\deg t \le y \\ t | P(y) \\ t | \chi_\phi(p)}} \alpha_t \right) \left(\sum_{\substack{\deg d \le z \\ d | P(z) \\ d | \chi_\phi(p)}} \lambda_d \right)^2 = \Delta X + E. \tag{4.10}$$

We divide the rest of this chapter into the computations of the error and the main term respectively.

4.4 The Error Term

From above,

$$r_m \ll \frac{|m|^3}{x} q^{x/2} \deg m, \tag{4.11}$$

thus

$$E = \mathrm{O}\left(\sum_{\substack{\deg m \le y+2z \\ m | P(y+z)}} \left(\sum_{\substack{\deg t \le y \\ t | m}} |\alpha_t| \right) \left(\sum_{\substack{\deg d \le z \\ d | m}} |\lambda_d| \right)^2 |r_m| \right).$$

Using (4.11), we see that this reduces to

$$
\begin{aligned}
E &\ll \sum_{\deg m \le y+2z} d(m)^3 \frac{|m|^3}{x} q^{x/2} \deg m \\
&\ll \frac{q^{x/2}}{x} \sum_{1 \le n \le y+2z} \sum_{\deg m = n} n^4 q^{3n} \\
&\ll \frac{q^{x/2}}{x} \sum_{1 \le n \le y+2z} n^4 q^{4n} \\
&\ll \frac{q^{x/2}}{x} (y+2z)^5 q^{4(y+2z)} \\
&\ll q^{(1-\epsilon)x}
\end{aligned}
$$

provided that

$$y + 2z \ll \left(\frac{1}{8} - \epsilon\right) x. \tag{4.12}$$

4.5 The Main Term

Now we tackle the computation of Δ present in the main term of (4.10) for two different choices of sequences α_t and λ_d.

We begin with a series of lemmas. The following result is crucial to our proof and also interesting in its own right. A detailed proof is presented in Appendix A.

Lemma 4.5.1. *For any positive integer z there exists a positive constant A_1 and a real number A_2 such that*

$$\sum_{\substack{\deg u \le z \\ u \textit{ squarefree}}} \frac{1}{\delta_1(u)} = A_1 z + A_2 + \mathrm{O}\left(\frac{1}{q^{z/2}}\right). \tag{4.13}$$

The sum (4.13) will be referred to as $V(z)$. This lemma is the analog of Lemma 10.2.3 in [2]. If z is an integer, then restricting the sum (4.13) to a single degree yields:

$$
\begin{aligned}
\sum_{\substack{\deg u = z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} = &\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} - \sum_{\substack{\deg u \le z-1 \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \\
&= A_1 + \mathrm{O}\left(\frac{1}{q^{z/2}}\right).
\end{aligned} \tag{4.14}
$$

The function δ_1 also satisfies the following lemma:

Lemma 4.5.2.

$$\sum_{\substack{\deg u \le z \\ u \textit{ squarefree}}} \frac{1}{\delta_1(u)} \log\left(\frac{1+y}{1+z-\deg u}\right) = V(z)\left(1+\log\left(\frac{1+y}{z}\right)\right) + \mathrm{O}\left(\log z\right).$$

Proof.

$$\begin{aligned}
&\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \log\left(\frac{1+y}{1+z-\deg u}\right) \\
&\qquad = \log(1+y) \sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} - \sum_{1\le n\le z}\left(A_1 + \mathrm{O}\left(\frac{1}{q^{n/2-\epsilon}}\right)\right)\log(1+z-n), \text{ by (4.14)} \\
&\qquad = V(z)\log(1+y) - A_1 \sum_{1\le k\le z} \log k + \mathrm{O}\left(\sum_{1\le k\le z} \frac{\log k}{q^{k/2-\epsilon}}\right).
\end{aligned}$$

By partial summation,

$$\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \log\left(\frac{1+y}{1+z-\deg u}\right) \tag{4.15}$$

$$= V(z)\log(1+y) - A_1\left([z]\log z - \int_1^z \frac{[t]}{t}dt\right) + \mathrm{O}(\log z) \tag{4.16}$$

$$= V(z)\log(1+y) - A_1 z\log z + A_1 z + \mathrm{O}(\log z)$$

$$= V(z)\left(1+\log\left(\frac{1+y}{z}\right)\right) + \mathrm{O}(\log z), \text{ by (4.13).} \tag{4.17}$$

The error term in (4.16) comes from summing $\log k/q^{k/2-\epsilon}$. □

Lemma 4.5.3 (Mertens' Formula)**.** *There exists a positive constant C such that*

$$\sum_{\deg l \le x} \frac{1}{\delta(l)} = \log(1+x) + C + \mathrm{O}\left(\frac{1}{1+x}\right). \tag{4.18}$$

Firstly note that from our discussion of $\delta(l) = |l| - a_l$ above, $\delta(l) \asymp |l|$. Now

$$\left|\sum_{\deg l \le z} \frac{1}{|l|} - \sum_{\deg l \le z} \frac{1}{\delta_1(l)}\right| = \left|\sum_{\deg l \le z} \frac{a_l}{|l|\delta(l)}\right|.$$

This sum converges absolutely, so there exists a constant C such that

$$\begin{aligned}\left|\sum_{\deg l\leq z}\frac{1}{|l|}-\sum_{\deg l\leq z}\frac{1}{\delta_1(l)}\right| &= C+\left|\sum_{\deg l\geq z}\frac{a_l}{|l|\delta(l)}\right|\\ &= C+\mathrm{O}\left(\frac{1}{q^z}\right),\end{aligned}$$

using the fact that the a_l are uniformly bounded.

By the prime number theorem for irreducibles in A,

$$\begin{aligned}\sum_{\deg l\leq x}\frac{1}{|l|} &= \sum_{n\leq x}\frac{q^n}{nq^n}+\mathrm{O}\left(\frac{q^{n/2}}{nq^n}\right)\\ &= \sum_{n\leq x}\frac{1}{n}+\mathrm{O}(\frac{1}{nq^{n/2}})\\ &= \log x+\gamma+\mathrm{O}(1/x).\end{aligned}$$

But $\log x = \log(1+x)+\mathrm{O}(1/x)$, and $\mathrm{O}(1/x) = \mathrm{O}(1/(1+x))$, so the result follows.

We also have the following two lemmas.

Lemma 4.5.4.

$$\sum_{\substack{\deg u\leq z\\ u\ \textit{squarefree}}}\frac{1}{\delta_1(u)(1+z-\deg u)} = \mathrm{O}(\log z). \tag{4.19}$$

Proof. From Lemma 4.5.1

$$\sum_{\substack{\deg u\leq z\\ u\ \text{squarefree}}}\frac{1}{\delta_1(u)(1+z-\deg u)} = \sum_{1\leq n\leq z}\sum_{\deg u=z}\frac{1}{\delta_1(u)(1+z-n)} \tag{4.20}$$

$$= \sum_{1\leq n\leq z}\frac{1}{1+z-n}\left(A_1+\mathrm{O}\left(\frac{1}{q^{z/2}}\right)\right). \tag{4.21}$$

$$\ll \log z \tag{4.22}$$

□

Lemma 4.5.5.

$$\sum_{\substack{\deg u\leq z\\ u\ \textit{squarefree}}}\frac{1}{\delta_1(u)}\sum_{\substack{z-\deg u<\deg l\leq y\\ l\ \textit{irreducible,}\\ l\nmid u}}\frac{1}{\delta(l)} = \mathrm{O}(1). \tag{4.23}$$

These last two lemmas are analogs of Lemmas 10.2.4, and 10.2.5 in [2]. Recalling the discussion from Section 3.1 on making a choice for λ_d through implicitly choosing z_r we make the following first choices of α_t and z_r as:

$$\alpha_t = \begin{cases} 1, & \text{if } \deg t = 0 \\ 0, & \text{otherwise} \end{cases} \tag{4.24}$$

and

$$z_r = \begin{cases} z_1, & \text{if } \deg r < z \text{ and } r \text{ is squarefree} \\ 0, & \text{otherwise} \end{cases} \tag{4.25}$$

If $\deg t \le z - \deg u$ and $t|P(z)$, then $\deg r \le z - \deg u$ and $r|P(z)$ for all $r|t$, so

$$\left(\sum_{\substack{\deg r \le z - \deg u \\ r|P(z), r|t}} \mu(r) \right)^2 = 0. \tag{4.26}$$

Also, if t is a prime,

$$\left(\sum_{\substack{\deg r \le z - \deg u \\ r|P(z), r|t}} \mu(r) \right)^2 = \begin{cases} 1, & \text{if } \deg t > z - \deg u \\ 0, & \text{otherwise.} \end{cases} \tag{4.27}$$

The first choice for α_t yields the following main term:

$$\begin{aligned} \Delta_1 &= z_1^2 \sum_{\substack{\deg t \le y, \deg u \le z \\ t|P(y), u|P(z) \\ (t,u)=1}} \frac{\alpha_t}{\delta(t)\delta_1(u)} \left(\sum_{\substack{\deg r \le z - \deg u \\ r|P(z), r|t}} \mu(r) z_{ur} \right)^2 \\ &= z_1^2 \sum_{\substack{\deg u \le z \\ u|P(z)}} \frac{1}{\delta_1(u)}, \text{ by (4.26) and because } t = 1, \\ &= z_1^2. \end{aligned} \tag{4.28}$$

The second choice for α_t is

$$\alpha_t = \begin{cases} 1, & \text{if } t \text{ irreducible} \\ 0, & \text{otherwise} \end{cases} \tag{4.29}$$

with z_r remaining the same. This yields for the main term:

$$\begin{aligned}
\Delta_2 &= z_1^2 \sum_{\substack{\deg t \le y, \deg u \le z \\ t | P(y), u | P(z) \\ (t,u)=1}} \frac{\alpha_t}{\delta(t)\delta_1(u)} \left(\sum_{\substack{\deg r \le z - \deg u \\ r | P(z), r | t}} \mu(r) \right)^2 \\
&= z_1^2 \sum_{\substack{\deg u \le z \\ z - \deg u < \deg l \le y \\ u \text{ squarefree} \\ l \nmid u}} \frac{1}{\delta(l)\delta_1(u)}, \text{ by (4.29).}
\end{aligned}$$

$$\begin{aligned}
&= z_1^2 \sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \sum_{\substack{z - \deg u < \deg l \le y \\ l \nmid u}} \frac{1}{\delta(l)} \\
&= z_1^2 \sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \left(\sum_{z - \deg u < \deg l \le y} \frac{1}{\delta(l)} - \sum_{\substack{z - \deg u < \deg l \le y \\ l | u}} \frac{1}{\delta(l)} \right).
\end{aligned}$$

By Mertens' formula,

$$\Delta_2 = z_1^2 \sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \left(\log\left(\frac{1+y}{1+z-\deg u} \right) + \mathrm{O}\left(\frac{1}{1+z-\deg u} \right) - \sum_{\substack{z - \deg u < \deg l \le y \\ l | u}} \frac{1}{\delta(l)} \right). \tag{4.30}$$

By appealing to Lemma 4.5.2,

$$\begin{aligned}
\Delta_2 &= z_1^2 \left(1 + \log\left(\frac{1+y}{z} \right) \right) V(z) + \mathrm{O}\left(z_1^2 \log z \right) \\
&+ z_1^2 \sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta_1(u)} \left(\mathrm{O}\left(\frac{1}{1+z-\deg u} \right) - \sum_{\substack{z - \deg u < \deg l \le y \\ l | u}} \frac{1}{\delta(l)} \right).
\end{aligned}$$

By Lemmas 4.5.4 and 4.5.5,

$$\Delta_2 = z_1^2 \left(1 + \log\left(\frac{1+y}{z}\right)\right) V(z) + \mathrm{O}\left(z_1^2 \log z\right). \tag{4.31}$$

Substituting (4.28) and using our respective choices of α_t into the main theorem of the lower bound sieve gives the following.

$$\sum_{\substack{\deg p \le x \\ p \text{ irreducible}}} \left(\sum_{\substack{d \mid P(z) \\ d \mid \chi_\phi(p)}} \lambda_d \right)^2 = z_1^2 V(z) \pi_q(x) + E, \tag{4.32}$$

$$\sum_{\substack{\deg p \le x \\ p \text{ irreducible}}} \left(\sum_{\substack{\deg l \le y \\ l \text{ irreducible} \\ l \mid \chi_\phi(p)}} 1 \right) \left(\sum_{\substack{\deg d \le z \\ d \mid P(z) \\ d \mid \chi_\phi(p)}} \lambda_d \right)^2 = z_1^2 \left(\left(1 + \log\left(\frac{1+y}{z}\right)\right) V(z) + \mathrm{O}\left(\log z\right) \right) \pi_q(x) + E. \tag{4.33}$$

Taking a linear combination of (4.32) and (4.33) yields the following:

$$\sum_{\substack{\deg p \le x \\ p \text{ irreducible}}} \left(2 - \sum_{\substack{\deg l \le y \\ l \text{ irreducible} \\ l \mid \chi_\phi(p)}} 1 \right) \left(\sum_{\substack{\deg d \le z \\ d \mid P(z) \\ d \mid \chi_\phi(p)}} \lambda_d \right)^2 = z_1^2 \left(1 - \log\left(\frac{1+y}{z}\right)\right) \cdot V(z) \cdot \frac{q^x}{x} + E. \tag{4.34}$$

Say that for large x,

$$1 + \log\left(\frac{1+y}{z}\right) > 0. \tag{4.35}$$

This would imply that for infinitely many monic irreducible polynomials p

$$2 - \sum_{\substack{\deg l \le y \\ l \text{ irreducible} \\ l \mid \chi_\phi(p)}} 1$$

will be positive. These primes will contain at most one irreducible factor with degree less then y and since $\deg \chi_\phi(p) = \deg p \le x$ they can have at most $\lfloor 1/y \rfloor \cdot x - 1$ prime factors other then y. So for infinitely many primes p, $\chi_\phi(p)$ contains at most $\lfloor 1/y \cdot \rfloor$ prime factors. To minimize this quantity we must maximize y subject to the constraints (4.35) and the constraint from our error term, (4.12). Let

$$y = (k+\epsilon)\cdot x \quad \text{and} \tag{4.36}$$

$$z = (l+\epsilon)\cdot x \tag{4.37}$$

for $k, l, \epsilon > 0$. After some simplification, (4.35) is equivalent to

$$\frac{k}{l} < e.$$

and (4.12) becomes

$$k + 2l < \frac{1}{8}.$$

Combining these gives

$$k < .0720$$

and thus we see that for infinitely many primes p, $\chi_\phi(p)$ has at most 13 prime factors.

Now we can count the number of such primes we have identified with the use of equation (4.32) and Lemma 4.13. From the definition of z_r and Möbius inversion we know that

$$\lambda_d = \mu(d)\delta(d) \sum_{\substack{\deg r \le z - \deg d \\ r | P(z)}} \frac{1}{\delta_1(rd)} z_{rd}.$$

Thus

$$\sum_{\substack{\deg d \le z \\ d | P(z) \\ d | \chi_\phi(p)}} \lambda_d \ll \sum_{\deg d < z} \delta(d) \sum_{\deg r \le z - \deg d} \frac{1}{\delta_1(rd)} |z_{rd}| \tag{4.38}$$

$$\ll z \tag{4.39}$$

$$\ll x \tag{4.40}$$

Thus equation (4.32) along with the prime number theorem gives that the number of primes with $\chi_\phi(p)$ having at most 13 prime factors is at least

$$C_\phi \frac{q^x}{x^2}$$

for some real positive constant C_ϕ depending only on ϕ.

Figure 4.1: A Drinfeld module of rank 2, such that the reduction at every prime is geometric.

As a final tribute to the elusive, monstrous and certainly mysterious Drinfeld module, we present an artist's rendition of a Drinfeld module of rank 2, such that the reduction at every prime is geometric.

Appendix A

A.1 A Sum

The goal of this appendix is to prove Lemma 4.5.1. We restate it here.

Lemma A.1.1. *Let δ be a multiplicative function on A whose support is the set of monic squarefree polynomials, and for any irreducible l,*

$$\delta(l) = |l| - a_l > 0$$

for some real number a_l. Furthermore, we assume that

$$a_l = \mathrm{O}(1),$$

i.e., there exist a positive constant c such that $|a_l| \leq c$ for all irreducible l. Then, for any $z \in \mathbb{Z}^+$, there exists a positive constant C_1 and a real number C_2 such that

$$\sum_{\substack{\deg u \leq z \\ u \text{ squarefree}}} \frac{1}{\delta(u)} = C_1 z + C_2 + \mathrm{O}\left(q^{-z/2}\right).$$

Remark A.1.2. In the notation of chapter 4, the function δ_1, defined $\delta_1(l) = \delta(l) - 1$ for l monic irreducible satisfies these properties by the discussion in Section 4.2. This proves Lemma 4.5.1.

For any integer $z \in \mathbb{Z}$, we have

$$\sum_{\deg f \leq z} 1 = \frac{q^{z+1}}{q-1} + \mathrm{O}(1).$$

For any $f \in A$, let $\omega(f)$ be the number of distinct irreducible factors of f. Then we have

$$\omega(f) = \mathrm{O}\left(\frac{\deg f}{\log \deg f}\right).$$

Let $\varphi(f)$ be the cardinality of the unit group $(A/fA)^*$ of A/fA. From Theorem 2.1.4,

$$\varphi(f) = |f| \cdot \prod_{\substack{l|f \\ l \text{ irreducible}}} \left(1 - \frac{1}{|l|}\right) = |f| \cdot \sum_{s|f} \frac{\mu(s)}{|s|}.$$

The following lemma is the key step to prove our main lemma.

Lemma A.1.3. *Let δ be a multiplicative function on A with the properties in Lemma A.1.1. For any $z \in \mathbb{Z}^+$, there exists positive constant A such that*

$$\sum_{\substack{\deg u \leq z \\ u \text{ squarefree}}} \frac{|u|}{\delta(z)} = Aq^z + \mathrm{O}\left(q^{z/2}\right).$$

Proof. First of all, we can rewrite $|u|/\delta(u)$ as follows:

$$\begin{aligned} \frac{|u|}{\delta(u)} &= \prod_{\substack{l|u \\ l \text{ irreducible}}} \frac{|l|}{\delta(l)} \\ &= \prod_{\substack{l|u \\ l \text{ irreducible}}} \frac{1}{1 - a_l/|l|} \\ &= \prod_{\substack{l|u \\ l \text{ irreducible}}} \left(1 + (a_l/|l|) + (a_l/|l|)^2 + \cdots\right) = \prod_{\substack{l|u \\ l \text{ irreducible}}} \left(1 + \frac{a_l'}{|l|}\right), \end{aligned}$$

for some a_l' which also has the property $a_l' = \mathrm{O}(1)$. By abuse of notation, we still use a_l to denote them. Then

$$\frac{|u|}{\delta(u)} = \prod_{\substack{l|u \\ l \text{ irreducible}}} \left(1 + \frac{a_l'}{|l|}\right) = \sum_{d|u} \frac{a_d}{|d|},$$

where

$$a_d = \prod_{\substack{l|d \\ l \text{ irreducible}}} a_l.$$

Thus,

$$|a_d| \leq c^{\omega(d)},$$

where the constant c is a uniform bound for the a_l. The sum in our lemma now becomes

$$\begin{aligned}\sum_{\substack{\deg u\le z\\ u \text{ squarefree}}} \frac{|u|}{\delta(z)} &= \sum_{\substack{\deg u\le z\\ u \text{ squarefree}}} \sum_{d|u} \frac{a_d}{|d|}\\ &= \sum_{\substack{\deg d\le z\\ u \text{ squarefree}}} \frac{a_d}{|d|}\left(\sum_{\substack{d|u\\ \deg u\le z, u \text{ squarefree}}} 1\right).\end{aligned}$$

Define for $z \in \mathbb{Z}^+$

$$s(z,d) := \sum_{\substack{d|u\\ \deg u\le z\\ u \text{ squarefree}}} 1.$$

Let's modify $s(z,d)$ in the following way

$$\begin{aligned}s(z,d) &= \sum_{\substack{d|u\\ \deg u\le z-\deg d, u \text{ squarefree}}} 1\\ &= \sum_{\substack{\deg u'\le z-\deg d,\\ u' \text{ squarefree}, (u',d)=1}} 1\\ &= \sum_{\deg r\le (z-\deg d)/2} \mu(r)\left(\sum_{\substack{\deg u'\le z-\deg d,\\ r^2|u', (u',d)=1}} 1\right).\end{aligned}$$

Again, we consider the inner sum. If $(r,d)\neq 1$, then the sum is zero. Hence, we may assume that $(r,d)=1$. Then

$$\begin{aligned}\sum_{\substack{\deg u'\le z-\deg d\\ r^2|u', (u',d)=1}} 1 &= \sum_{s|d} \mu(s) \sum_{\deg u''\le z-\deg(d\cdot r^2\cdot s)} 1\\ &= \sum_{s|d} \mu(s)\left(\frac{q^{z-\deg d-2\deg r-\deg s+1}}{q-1} + \mathrm{O}(1)\right)\\ &= \frac{q^{z+1}}{q-1}\cdot\frac{1}{|d|\cdot|r|^2}\left(\sum_{s|d}\frac{\mu(s)}{|s|}\right) + \mathrm{O}(\sum_{s|d} 1)\\ &= \frac{q}{q-1}q^z\cdot\frac{\varphi(d)}{|r|^2\cdot|d|^2} + \mathrm{O}\left(2^{\omega(d)}\right).\end{aligned}$$

Thus, the original inner sum $s(z,d)$ is

$$s(z,d) = \sum_{\substack{(r,d)=1 \\ \deg r \le (z-\deg d)/2}} \mu(r) \left(\frac{q}{q-1} q^z \cdot \frac{\varphi(d)}{|r|^2 \cdot |d|^2} + \mathrm{O}(2^{\omega(d)}) \right) \tag{A.1}$$

$$= \frac{q}{q-1} q^z \cdot \frac{\varphi(d)}{|d|^2} \cdot \sum_{\substack{(r,d)=1 \\ \deg r \le (z-\deg d)/2}} \frac{\mu(r)}{|r|^2} + \mathrm{O}\Big(2^{\omega(d)} \cdot \sum_{\deg r \le (z-\deg d)/2} 1\Big) \tag{A.2}$$

$$= \frac{q}{q-1} q^z \cdot \frac{\varphi(d)}{|d|^2} \cdot \sum_{\substack{(r,d)=1 \\ \deg r \le (z-\deg d)/2}} \frac{\mu(r)}{|r|^2} + \mathrm{O}\Big(2^{\omega(d)} \cdot q^{(z-\deg d)/2}\Big). \tag{A.3}$$

Note that the sum

$$\sum_{\substack{(r,d)=1 \\ \deg r \le (z-\deg d)/2,}} \frac{\mu(r)}{|r|^2}$$

is absolute convergent as z goes to infinity. Hence, there exists a positive constant $c_d = \mathrm{O}(1)$ such that

$$\sum_{\substack{(r,d)=1 \\ \deg r \le (z-\deg d)/2,}} \frac{\mu(r)}{|r|^2} = c_d - \sum_{\substack{(r,d)=1 \\ \deg r > (z-\deg d)/2,}} \frac{\mu(r)}{|r|^2} = c_d + \mathrm{O}\Big(q^{-(z-\deg d)/2}\Big).$$

Since $\frac{\varphi(d)}{|d|} < 1$ and $c_d = \mathrm{O}(1)$, substituting this in (A.1) gives

$$s(z,d) = c_d \frac{q}{q-1} q^z \cdot \frac{\varphi(d)}{|d|^2} + \mathrm{O}\Big(2^{\omega(d)} \cdot q^{(z-\deg d)/2}\Big).$$

Now we come back to our original sum.

$$\begin{aligned}
\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{|u|}{\delta(z)} &= \sum_{\substack{\deg d \le z, \\ u \text{ squarefree}}} \frac{a_d}{|d|} \cdot s(z,d) \\
&= \sum_{\substack{\deg d \le z, \\ u \text{ squarefree}}} \frac{a_d}{|d|} \cdot \left(c_d \cdot \frac{q}{q-1} q^z \cdot \frac{\varphi(d)}{|d|^2} + \mathrm{O}\Big(2^{\omega(d)} \cdot q^{(z-\deg d)/2}\Big) \right) \\
&= q^z \cdot \sum_{\substack{\deg d \le z, \\ u \text{ squarefree}}} \left(a'_d \cdot \frac{\varphi(d)}{|d|^3} \right) + \mathrm{O}\left(q^{z/2} \cdot \sum_{\deg d \le z} \frac{a_d \cdot 2^{\omega(d)}}{|d|^{3/2}} \right),
\end{aligned}$$

where $a'_d = a_d \cdot c_d \cdot q/(q-1)$. Since $|a_d| \le c^{\omega(d)}$, $\omega(d) = \mathrm{O}(\deg d / \log \deg d)$, and $c_d = \mathrm{O}(1)$, for any $\epsilon > 0$,

$$a_d = \mathrm{O}(|d|^\epsilon), \quad a'_d = \mathrm{O}(|d|^\epsilon), \quad 2^{\omega(d)} = \mathrm{O}(|d|^\epsilon).$$

Therefore, the sums

$$\sum_{\substack{\deg d \le z, \\ u \text{ squarefree}}} a'_d \cdot \frac{\varphi(d)}{|d|^3} \ll \sum_{x \le z} \frac{1}{q^{(1-\epsilon)x}}$$

and

$$\sum_{\deg d \le z} \frac{|a_d| \cdot 2^{\omega(d)}}{|d|^{3/2}} \ll \sum_{x \le z} \frac{1}{q^{(1/2-\epsilon)x}}$$

are convergent. Furthermore, there exists a constant C such that

$$\begin{aligned}\sum_{\substack{\deg d \le z, \\ u \text{ squarefree}}} a'_d \cdot \frac{\varphi(d)}{|d|^3} &= C - \sum_{\substack{\deg d > z, \\ u \text{ squarefree}}} a'_d \cdot \frac{\varphi(d)}{|d|^3} \\ &= C + \mathrm{O}(1/q^{(1-\epsilon)z}).\end{aligned}$$

Putting all together, we get

$$\begin{aligned}\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{|u|}{\delta(z)} &= q^z \cdot (C + \mathrm{O}(1/q^{(1-\epsilon)z})) + \mathrm{O}(q^{z/2}) \\ &= C \cdot q^z + \mathrm{O}(q^{z/2}).\end{aligned}$$

To justify the positivity of C, we come back to the original sum. The limit $|u|/\delta(u)$ is 1. Therefore, as z goes to infinity, the original sum is bounded below by

$$\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{2} \asymp q^z.$$

Therefore, C must be positive.

Proof of Lemma A.1.1. By the Abel summation formula and Lemma A.1.3

$$\begin{aligned}\sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{1}{\delta(u)} = \sum_{\substack{\deg u \le z \\ u \text{ squarefree}}} \frac{|u|}{\delta(u)} \cdot |u|^{-1} \\ =& \left(C \cdot q^z + \mathrm{O}(q^{z/2})\right) q^{-z} - \sum_{x \le z-1} \left(C \cdot q^x + \mathrm{O}(q^{x/2})\right) \cdot \left(\frac{1}{q^{x+1}} - \frac{1}{q^x}\right) \\ =& C + \mathrm{O}(q^{-z/2}) + (1 - 1/q) \cdot \sum_{x \le z-1} \left(C + \mathrm{O}(q^{-x/2})\right) \\ =& C_1 z + C_2 + \mathrm{O}(q^{-z/2}), \qquad \text{since } \sum_x q^{-x/2} \text{ converges,}\end{aligned}$$

where $C_1 = (1 - 1/q) \cdot C > 0$. It completes the proof. ∎

List of References

[1] Enrico Bombieri. Le grand crible dans la théorie analytique des nombres. *Astérisque*, (18):103, 1987.

[2] A. C. Cojocaru and M. R. Murty. *An Introduction to Sieve Methods and their Applications.* Cambridge University Press, 2005.

[3] Michael D. Fried and Moshe Jarden. *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, second edition, 2005.

[4] F. Gardeyn. Une borne pour láction de línertie sauvage sur la torsion dún module de Drinfeld. *Arch. Math.*, 79:241–251, 2002.

[5] Ernst-Ulrich Gekeler. On Finite Drinfeld Modules. *J. Algebra*, 141(1):187–203, 1991.

[6] G. H. Hardy and J. E. Littlewood. Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes. *Acta Math.*, 44(1):1–70, 1923.

[7] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[8] Neal Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math.*, 131(1):157–165, 1988.

[9] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[10] D. A. Marcus. *Number Fields.* Springer-Verlag, New York Inc., 1977.

[11] S. Ali Miri and V. Kumar Murty. An application of sieve methods to elliptic curves. In *Progress in cryptology—INDOCRYPT 2001 (Chennai)*, volume 2247 of *Lecture Notes in Comput. Sci.*, pages 91–98. Springer, Berlin, 2001.

[12] M. R. Murty. *Problems in Analytic Number Theory.* Springer-Verlag, New York Inc., 2001.

[13] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag Berlin Heidelberg, 1999.

[14] Richard Pink. The Mumford-Tate conjecture for Drinfeld-modules. *Publ. Res. Inst. Math. Sci.*, 33(3):393–425, 1997.

[15] Michael Rosen and Joseph H. Silverman. On the independence of Heegner points associated to distinct quadratic imaginary fields. *J. Number Theory*, 127(1):10–36, 2007.

[16] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[17] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[18] Jörn Steuding and Annegret Weng. On the number of prime divisors of the order of elliptic curves modulo p. *Acta Arith.*, 117(4):341–352, 2005.