p-adic Analysis and Rational Points on Curves

Christian Hokaj

Advisor: Andrei Jorza

A senior thesis presented in supplement of the requirements of the Honors Concentration for a B.S. in Mathematics.

Mathematics
University of Notre Dame
April 20th, 2018

Contents

1 Introduction

The goal of this thesis is to provide a proof of the following theorem:

Theorem 1 (Chabauty)**.** *Let X be a curve over $\mathbb{Q}$ with genus, g, greater than 1 and let the rank of the Jacobian (the Mordell-Weil rank) of X be strictly less than g. Then $X(\mathbb{Q})$ is finite.*

In 1941, Chabauty proved Theorem 1 using p-adic analytic techniques, establishing a bound on the number of rational points, which would be the most significant progress toward Mordell's conjecture for quite some time.

A curve of genus 1 is known as an *elliptic curve*. The rational points on an elliptic curve form a finitely-generated Abelian group (this is the Mordell-Weil Theorem), and there are many such elliptic curves which are known to have infinitely many rational points. In fact, it is expected that half of all elliptic curves have finitely many rational points and the other half are of rank 1. The study of elliptic curves is a beautiful subject on its own and is one of the most fundamental and profound areas in number theory.

But in the case where $g > 1$, there are only finitely many rational points on these curves. This was originally conjectured by Mordell in 1922, without the condition on the Jacobian of X.

Theorem 2 (Faltings (Mordell's Conjecture))**.** *Let X be a curve over $\mathbb{Q}$ with genus, $g > 1$. Then $X(\mathbb{Q})$ is finite.*

In 1983, Gerd Faltings proved the Mordell Conjecture in full using techniques from algebraic geometry and was awarded the Fields Medal in 1986 for his work, but his method was not effective. The result was later generalized to hold over an arbitrary number field.

Shortly after, in 1985, while Chabauty's proof was unable to be adapted to show Faltings' Theorem in full, Coleman developed a method which improved the bound established by Chabauty in the case where the rank of the Jacobian of X is less than the genus which led to a method that enables one to explicitly compute the rational points in some special cases - a significant improvement.

More recently, number theorists have been interested in finding uniform bounds on the number of rational points on such curves, the bound dependent only on the genus (Coleman's bound involves the genus and the number of rational points of a reduction of the curve to $\mathbb{F}_p$ for a prime of good reduction). In particular, we have the result due to Katz, Rabinoff, Zureick-Brown where for a specific kind of curve of genus greater than 3 over $\mathbb{Q}$ with the rank of the Jacobian at most $g - 3$ the number of rational points is bounded above by $84g^2 - 98g + 28$, an explicit bound in terms of the genus (and their result also produced a bound for general number fields).

We will proceed to develop background in understanding of the methods of Chabauty and Coleman to prove the special case of Faltings' Theorem. In Section 2, after developing the necessary language of divisors, we need to understand the Jacobian of a curve, which we will build explicitly for curves over

$\mathbb{C}$. We will be able to show it is isomorphic to a g-dimensional torus. We will then develop an understanding of the Abel-Jacobi map which injects a curve X into its Jacobian.

In Section 3, we will build the background of elementary p-adic analysis and the theory of Newton Polygons, which will be used to bound the number of zeros of particular p-adic analytic functions whose zeros which lie in $p\mathbb{Z}_p$ correspond to the rational points on the curve.

In Section 4, we will continue expanding upon the theory of divisors to prove the Riemann-Roch Theorem for curves over arbitrary (algebraically closed) fields, which is a major tool used in the bound of the goal theorem, leading to an understanding of what 1-forms look like on curves over fields other than $\mathbb{C}$ or $\mathbb{R}$.

Then in the remaining sections we will outline the methods of Chabauty and Coleman used to deduce the special case of Faltings' Theorem. We will conclude by stating the results of current research efforts in finding uniform bounds on the number of rational points.

2 Complex Analysis Background

Our end-goal in building up this complex analysis background is to understand the Jacobian of a curve, X, (which is an Abelian variety over the base field which has dimension g, the genus of the curve) and the associated Abel-Jacobi Map which injects a curve into is Jacobian. Understanding the Jacobian and Abel-Jacobi map is much more accessible when we work on a curve over $\mathbb{C}$ instead of over a general field.

We thus will be able to realize the Jacobian of our curve over $\mathbb{Q}$ as the Jacobian of the curve over $\mathbb{C}$, but considering the equations which define the Abelian variety as over $\mathbb{Q}$ instead of $\mathbb{C}$ (which can be done). We will also be able to define the Jacobian of $X(\mathbb{Q}_p)$, a curve over $\mathbb{Q}_p$, as the Jacobian of $X(\mathbb{Q})$ but considering the equations defining the Abelian variety as over $\mathbb{Q}_p$ instead of $\mathbb{Q}$.

The Jacobian can be constructed over an arbitrary base scheme, but this is a much more intensive procedure; taking the complex approach to understanding the Jacobian will suffice for our purposes.

2.1 Divisors

Divisors are a convenient way of analyzing the zeros and poles of a meromorphic function or 1-form.

Definition 3. *Let X be a compact Riemann Surface. A divisor on X is a function $D : X \to \mathbb{Z}$ whose support is a discrete subset of X.*

Proposition 4. *The set of divisors form a group under pointwise addition (Div(X)). Ths group is exactly the free Abelian group on the points of X.*

Remark 5. *A divisor can be represented as a (formal) sum*

$$D = \sum_{p \in X} D(p) \cdot p$$

which is necessarily finite by our definition of divisor.

Definition 6. *The degree of a divisor, D, is:*

$$\mathrm{Deg}(D) = \sum_{p \in X} D(p).$$

Definition 7. *Let f be a meromorphic function (which is not identically zero) on X a Riemann Surface. The divisor of f, div(f) is the divisor defined by:*

$$\mathrm{div}(f) = \sum_{p \in X} \mathrm{ord}_p(f) \cdot p$$

where $\mathrm{ord}_p(f)$ denotes the order of the zero at f if f has a zero at p, the negative order of the pole of f at p if f has a pole at p, and is 0 if f does not have a zero or pole at p. Such a divisor is called a ***principal divisor***

Definition 8. *Similarly, let ω be a meromorphic 1-form on a Riemann Surface X which is not identically zero. Then the divisor of ω, $\mathrm{div}(\omega)$ is the divisor:*

$$\mathrm{div}(\omega) = \sum_{p \in X} \mathrm{ord}_p(\omega) \cdot p.$$

Where $\mathrm{ord}_P(\omega)$ denotes the order of the zero or negative order of the pole pole of the meromorphic 1-form ω (and is 0 if ω has no zero or pole at p).

A divisor of this form is referred to as a ***canonical divisor****.*

Definition 9. *Two divisors are linearly equivalent if they differ by a principal divisor.*

We wish to prove a theorem relating the degree of a canonical divisor to the genus of the surface, but we will need to recall a few standard results from complex analysis:

Lemma 10. *Let $F : X \to Y$ be a holomorphic map between Riemann Surfaces and let ω be a (nonconstant) meromorphic 1-form. Let $F^*\omega$ denote the pullback of ω via F. Fix a point $p \in X$. Then we have:*

$$\mathrm{ord}_p(F^*\omega) = (1 + \mathrm{ord}_{F(p)}(\omega))\mathcal{C}_p(F) - 1.$$

where $\mathcal{C}_p(F)$ denotes the ramificaction index of F at p. In other words, this is the number, n, such that F can be represented locally as z^n in a neighborhood of P.

Proof. Choose coordinates z on X and w on Y to write F locally as $z \mapsto w^n$ in a neighborhood of P. We can also write ω locally as $[cz^{\mathrm{ord}\ \omega} + O(z^{\mathrm{ord}\ \omega+1})]dz$.

By basic results about pullbacks, we have:

$$F^*(\omega) = [cz^{n\cdot\mathrm{ord}\ \omega} + O(z^{n\cdot\mathrm{ord}\ \omega+1})](nz^{n-1})dz.$$

From such an expansion it is clear that the order of $F^*(\omega)$ is as in the statement of the lemma. □

Theorem 11. *Hurwitz' Formula Let $F : X \to Y$ be a (nonconstant) holomorphic map between (compact) Riemann Surfaces. Let g_X denote the genus of X and g_Y denote the genus of Y. Then:*

$$2g_X - 2 = \deg(F)(2g_Y - 2) + \sum_{p \in X}(\mathcal{C}_p(F) - 1).$$

We recall from complex analysis that there are finitely many ramification points, so there are only finitely many $p \in X$ where $(\mathcal{C}_p(F) - 1)$ is nonzero.

The degree of F, where p is a point on Y is:

$$\deg(F) = \sum_{x \in F^{-1}(p)} \mathcal{C}_p(F).$$

It is well known that this sum is independent of the choice of p.

Proof. This relies on much elementary complex analysis whose knoweldge we assume. See reference [10] p. 52, by Miranda. □

Theorem 12. *Let X be a compact Riemann Surface. Then there exists a canonical divisor on X of degree $2g - 2$ where 2 is the genus of X.*

Proof. Let f be a (nonconstant) meromorphic function on X. Realize f as a function $f : X \to \mathbb{C}_\infty$ where $\mathbb{C}_\infty$ denotes the Riemann Sphere. This can be done for every meromorphic function.

Consider then the meromorphic 1-form on the Riemann Sphere given by dz. Let $f^*(dz)$ be the pullback of dz under f. Recall that dz is meromorphic of degree -2; it has a pole of order 2 at infinity and no other zeros or poles. We have:

$$\begin{aligned}
\deg(\operatorname{div}(f^*(dz))) &= \sum_{p \in X} \operatorname{ord}_p(f^* dz) \\
&= \sum_{p \in X} [(1 + \operatorname{ord}_{f(p)} dz))\operatorname{ord}_p(f) - 1] \\
&= \sum_{p \in X - f^{-1}(\{\infty\})} (\operatorname{ord}_p(f) - 1) + \sum_{p \in f^{-1}(\{\infty\})} (-\operatorname{ord}_p(f) - 1) \\
&= 2g - 2 + 2\deg(f) - 2\deg(f). \\
&= 2g - 2.
\end{aligned}$$

The second equality comes from Lemma 10, the third by recognizing the zeros and poles of dz and splitting up the sum over different points of X, and the fourth from Hurwitz' formula.

□

We note that one could define the genus in the above way - . Riemann-Roch, which will be proven later in this thesis over arbitrary (algebraically closed) fields will imply the equivalence of the many possible definitions of the genus.

Remark 13. *It is nontrivial that every compact Riemann Surface has a nonconstant meromorphic function, which we used for this proof. Finding such meromorphic functions often occupies much of a graduate level complex analysis course; nevertheless, this is a well known result.*

Remark 14. *In fact, more is true here than Theorem 10 suggests. The degree of* ***any*** *canonical divisor on X must be $2g-2$, as we will show later.*

We can define a partial ordering on divisors which is necessary for introducing a vector space of meromorphic functions of critical importance. We could begin the trek to proving Riemann Roch here, but we will only state what is necessary and we will provide a proof in Section 4.

Definition 15 (A Partial Ordering on Divisors)**.** *Let D be a divisor on a Riemann Surface, X. Say $D \geq 0$ if $D(p) \geq 0$ for all p. Say $D > 0$ if $D \geq 0$ and $D \neq 0$. Finally, say $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.*

Definition 16. *Define $L(D)$ as the space of meromorphic functions with poles bounded by D. i.e.*

$$L(D) = \{f \in \mathcal{M}(X) | \operatorname{div}(f) \geq -D\}.$$

Notice that this condition means that for each p, $\operatorname{ord}_p(f) \geq -D(p)$.

We state here a theorem that we will prove in Section 4 in a more general setting.

Theorem 17 (Riemann-Roch)**.** *Let K be a canonical divisor on X. Then for any divisor, D, we have:*

$$l(D) = deg(D) + 1 - g + l(K - D),$$

where $l(D)$ denotes the dimension (as a vector space) of $L(D)$.

2.2 The First Homology Group

Here we construct the first homology group on a Riemann Surface.

Definition 18. *Let X be a Riemann Surface. Definethe set of chains as the free Abelian group on the set of paths of X. I.e. if C is a chain, we can write:*

$$C = \sum_{i=0}^{n} a_i \gamma_i.$$

with $a_i \in \mathbb{Z}$ and each γ_i is a path on X.

Proposition 19. *We define a homomorphism from the group of chains on X to the free Abelian group generated by the points of X as follows. On a path, define $F(\gamma_i)$ as the formal sum $\gamma_i(0) - \gamma_i(1)$. On a $\mathbb{Z}$-linear combination of paths, define:*

$$F(\sum_{i=0}^{n} a_i \gamma_i) = \sum_{i=0}^{n} a_i F(\gamma_i)$$

where the sum is formal. It is clear that this is a homomorphism.

Definition 20. *Where F is as above, define the set (which is also a group) of* ***closed chains*** *of X as the kernel of F.*

Definition 21. *We call a chain a* ***boundary chain*** *if its paths comprise the boundary of a (triangulizable) closed set of X.*

Definition 22. *The* ***first homology group*** *is the quotient group of the closed chains modulo the boundary chains. We will denote it by $H_1(X)$ or $H_1(X, \mathbb{Z})$.*

Remark 23. *The first homology group can also be defined as the abelianization of the fundamental group of X. These two definitions are equivalent.*

Theorem 24. *If X is a (compact) 2-manifold of genus g, then $H_1(X)$ is a free Abelian group of rank $2g$.*

2.3 Some background on 1-forms

Definition 25. *A* ***closed*** *1-form ω is a 1-form such that $d\omega = 0$.*

Proposition 26. *Every holomorphic 1-form is closed.*

Proof. Write ω locally as fdz, which can be done since ω is holomorphic.

$$d\omega = \partial\omega + \overline{\partial}\omega = \left(\frac{\partial f}{\partial \overline{z}}\right) dz \wedge d\overline{z}.$$

$\frac{\partial f}{\partial \overline{z}} = 0$ is equivalent to the Cauchy Riemann equations, and we are done. □

Proposition 27. *Let ω be a holomorphic 1-form. Then the integral of ω along any boundary chain is 0.*

Proof. This is an application of Stoke's Theorem. Let D be a triangulizable set such that the boundary chain we are interested in is ∂D. By Stokes, we get:

$$\int_{\partial D} \omega = \int\int_D d\omega = 0.$$

□

Corollary 28. *For any $\gamma \in H_1(X, \mathbb{Z})$, let δ be another representative of the same homology class (i.e. γ and delta differ only by a boundary chain). We have that*

$$\int_\gamma \omega = \int_\delta \omega$$

where ω is holomorphic. Hence, the integral of a holomorphic 1-form over a homology class is well-defined.

Proof. We can break up over the paths which comprise γ and δ, and the integrals will differ only by the integral of ω over a boundary chain which is 0 by the previous proposition. □

Corollary 29. *Let $\gamma \in H_1(X, \mathbb{Z})$. There exists a linear functional from $\Omega^1(X)$, the space of holomorphic 1-forms, into $\mathbb{C}$ given by:*

$$\omega \mapsto \int_\gamma \omega.$$

Definition 30. *$\phi \in \Omega_1(X)^*$ (the dual space, the space of linear functionals on $\Omega_1(X)$) is a **period** if it can be written as:*

$$\phi(\omega) = \int_\gamma \omega$$

for some $\gamma \in H_1(X, \mathbb{Z})$.

2.4 The Jacobian and the Abel-Jacobi Map

Definition 31. *A compact Riemann Surface, X, is an **algebraic curve** if $\mathcal{M}(X)$, the field of (global) meromorphic functions on X separates points and tangents.*

Theorem 32. *Every compact Riemann Surface (including a projective plane curve or projective curve) is an algebraic curve.*

Proof. This is a rather deep result. A construction can be found in Narasimhan's book, *Complex Analysis in One Variable* [8]. □

Definition 33. *The **Jacobian** of a (compact) Riemann Surface X, denoted $J(X)$ is the quotient group given by $\Omega^1(X)^*$ modulo the group of periods.*

We can also characterize the Jacobian in a different way in terms of bases.

Let $\omega_1, ..., \omega_g$ be a basis of $\Omega^1(X)$ (recall g is the genus of X). We can define an isomorphism of vectors spaces $\Omega^1(X)^* \to \mathbb{C}^g$ given by:

$$\phi \mapsto \begin{bmatrix} \phi(\omega_1) \\ \vdots \\ \phi(\omega_g) \end{bmatrix}.$$

Remark 34. *While we constructed the Jacobian of a curve for a curve over $\mathbb{C}$, Weil has shown that one can analogously construct the Jacobian of a curve over an arbitrary field [12].*

Proposition 35. *We thus have that $\mathrm{Jac}(X)$ is isomorphic to $\mathbb{C}_g$ modulo the group of periods. In fact, it is true that the group of periods forms a lattice and we have:*

$$J(X) \cong \frac{\mathbb{C}^g}{\mathbb{Z}^{2g}}$$

which is a g-dimensional complex torus.

We will have a proof of the isomorphism after we establish that the group of periods forms a lattice of $\mathbb{C}^g$. We will prove this later on in this section.

Our next goal is to develop the Abel-Jacobi Map, which injects a Riemann surface, X, into its Jacobian.

Definition 36. *Define A, the Abel-Jacobi Map, as follows:*

Fix a base point, $P_0 \in X$. For every $P \in X$, select a path, γ from P to P_0. Send P to the linear functional on $\Omega^1(X)$ given by integration along γ. In other words, for every P, $A(P)$ is the map:

$$A(P)(\omega) = \int_\gamma \omega.$$

We must verify that many aspects of this map are well defined.

We will first show that the choice of path from P to P_0 doesn't matter. Choose another path, call it δ, which goes from P to P_0. Let δ^{-1} be the path δ traversed in reverse. Then $\gamma + \delta^{-1}$ (concatenate the path γ with the path δ^{-1}) forms a boundary chain which tells us that:

$$\int_{\gamma+\delta^{-1}} \omega = \int_{\gamma} \omega + \int_{\delta^{-1}} \omega.$$

This gives us that:

$$-\int_{\delta^{-1}} \omega = \int_{\gamma} \omega - \int_{\gamma+\delta^{-1}} \omega$$

for every $\omega \in \Omega^1(X)$. Which is the same as:

$$\int_{\delta} \omega = \int_{\gamma} \omega - \int_{\gamma+\delta^{-1}} \omega.$$

So while the Abel-Jacobi map is not well defined as a map into $\Omega^1(X)$, it is well defined up to integration around a closed chain. But this is exactly a period, so it is well defined as a map into $\mathrm{Jac}(X)$.

Proposition 37. *We can also write a more explicit form of the Abel Jacobi map into $\mathbb{C}^g$ modulo periods as follows:*

$$A(P) = \begin{bmatrix} \displaystyle\int_{P_0}^{P} \omega_1 \\ \vdots \\ \displaystyle\int_{P_0}^{P} \omega_g \end{bmatrix}$$

where $\omega_1, ..., \omega_g$ is a basis of $\Omega^1(X)$. This form can be achieved by composing the original Abel-Jacobi map with the isomorphism of $\Omega^1(X)^* \to \mathbb{C}^g$

We should note, though, that as a map from X to $\mathrm{Jac}(X)$, the Abel-Jacobi Map does depend on the base point.

However, we can remove this dependency on the base point if we choose to work over the divisors of X instead of X itself. Divisors are discussed at length later in this thesis, but we will develop the Divisor-form of the Abel-Jacobi map now.

Proposition 38. *We can extend A linearly to a map on divisors of X in the obvious way. I.e. If $D = \sum_{P \in X} D(P) \cdot P$ then we have a map $A : \mathrm{Div}(X) \to \mathrm{Jac}(X)$ given by:*

$$A(D) = A\left(\sum_{P\in X} D(P)\cdot P\right) = \sum_{P\in X} D(P)\cdot A(P).$$

This is obviously a group homomorphism, as we extended the map linearly.

Theorem 39. *Let A_0 be the restriction of A to the group of divisors of degree 0. Then A_0 is independent of a choice of base point, P_0.*

Proof. Let $D = \sum_{P \in X} D(P) \cdot P$ be a divisor of degree 0. Let Q_0 be a second base point. Let δ be a path from Q_0 to P_0, and let A_P and A_Q be the Abel-Jacobi Maps induced by these base points.

Notice, first, that $A(P_0) = 0$ as this is integration on the constant loop. Now, let $P \in X$ and let γ_P be a path from P to P_0 and let γ_Q be a path from P to Q_0. Notice that:

$$\int_{\gamma_P} \omega = \int_{\gamma_Q} \omega + \int_\delta \omega$$

so we have:

$$A_P(P) = A_Q(P) + \begin{bmatrix} \int_\delta \omega_1 \\ \vdots \\ \int_\delta \omega_g \end{bmatrix}.$$

Then

$$\begin{aligned}
A(\sum_{P \in X} D(P) \cdot P) &= \sum_{P \in X} D(P) \cdot A_P(P) \\
&= \sum_{P \in X} \left(D(P) \cdot \left(A_Q(P) + \begin{bmatrix} \int_\delta \omega_1 \\ \vdots \\ \int_\delta \omega_g \end{bmatrix} \right) \right) \\
&= \sum_{P \in X} (D(P) \cdot A_Q(P)) + \sum_{P \in X} D(P) \cdot \begin{bmatrix} \int_\delta \omega_1 \\ \vdots \\ \int_\delta \omega_g \end{bmatrix} \\
&= \sum_{P \in X} (D(P) \cdot A_Q(P)) + \begin{bmatrix} \int_\delta \omega_1 \\ \vdots \\ \int_\delta \omega_g \end{bmatrix} \cdot \sum_{P \in X} D(P) \\
&= \sum_{P \in X} (D(P) \cdot A_Q(P)) + 0
\end{aligned}$$

where the last equality holds since D is a divisor of degree 0. Hence A_0, which is A restricted to divisors of degree 0 is independent of the base point. □

As our goal is to show that we can embed the curve X into its Jacobian, we will build up to the result that the Abel-Jacobi map is injective. In order to do this, we will prove an intermediate theorem about divisors.

2.5 Abel's Theorem

This section will seek to prove the following theorem:

Theorem 40 (Abel)**.** *Let X be a compact Riemann surface of genus g. Let D be a divisor of degree 0. Then if $A_0(D) = 0$, D is a principal divisor; in other words, there exists a meromorphic function f on X such that $D = \operatorname{div}(f)$.*

We will first develop the tools necessary to prove the reverse direction, which will use trace operations. Then, we will develop the tools needed for the forward direction.

Definition 41. *Let F be a nonconstant holomorphic map $X \to Y$ of degree d and let g be a meromorphic function on X. Let q be a point in Y which is not a branch point of F. If none of the poles of g are in the preimage of q, we define the Trace of g as:*

$$\operatorname{Tr}(g)(q) = \sum_{p \in F^{-1}(q)} g(p).$$

It is easy to check that $\operatorname{Tr}(g)$ is a well-defined meromorphic function everywhere in Y which is not a branch point, and is holomorphic at a point in the preimage of q if g is, as long as none of the poles of g are at the preimage of q.

If this condition on the poles is not met, it is not necessarily true that this gives a well-defined meromorphic function, and we construct the trace as follows:

If F has degree d, there are d preimages of $q \in Y$ under F, which we can call $p_1, ..., p_d$. About q we can find a chart U where $F^{-1}(U) = \bigsqcup V_i$ where each V_i is a chart containing p_i. As the multiplicity of the p_i is 1, the chart map $U \to V_i$ is a biholomorphism F_i with inverse F_i^{-1}. Then we can define:

$$\operatorname{Tr}(g)(q) = \sum_{i=1}^{d} g(F_i^{-1}).$$

It is easy to see that these two definitions agree.

Remark 42. *Considering ω as a 1-form we can define $\operatorname{Tr}(\omega)$ in the analogous way.*

Now, let F be a nonconstant holomorphic function between compact Riemann surfaces, let γ be a path on Y, and let ω be a meromorphic 1-form on X whose poles avoid $F^{-1}(\gamma)$. In this case, we can integrate $\operatorname{Tr}(\omega)$ since it is just a meromorphic 1-form. We wish to relate this to the integral of ω.

As long as γ does not pass through the branch points of F, every q in Y has d preimages under F where d is the degree of F. So, at all but finitely many branch points of Y we can lift γ to d paths $\gamma_1, ..., \gamma_d$ which may intersect at ramification points of F (lying above branch points). By taking the closure of these lifted paths, we get d lifts $\overline{\gamma_i}$. We will denote $F^*(\gamma) = \sum_{i=1}^{d} \gamma_i$.

From this discussion, we conclude the following lemma.

Lemma 43. *Let $F : X \to Y$ be a (nonconstant) holomorphic map between (compact) Riemann surfaces. Let $\omega \in \Omega^1(X)$ and let γ be a chain on Y. Then:*

$$\int_{F^*(\gamma)} \omega = \int_\gamma \mathrm{Tr}(\omega).$$

We can now show the reverse direction of Abel's Theorem.

Theorem 44 (Abel's Theorem, reverse direction)**.** *Let X be a compact Riemann surface of genus g. Let D be a divisor of degree 0. If there exists a meromorphic function f on X such that $D = \mathrm{div}(f)$ (if D is principal), then $A_0(D) = 0$.*

Proof. Let D be the divisor of a (nonconstant) meromorphic function $F : X \to \mathbb{C}_\infty$ on X, a compact Riemann Surface.

Let γ be a path from ∞ to 0 on $\mathbb{C}_\infty$ which does not pass through any branch points of the map F except for possibly 0 or ∞. Write $F^*(\gamma)$ to denote pulling back the path under F, and note that this chain is:

$$F^*(\gamma) = \sum_{i=1}^{\mathrm{ord}(F)} \gamma_i$$

where each γ_i connects a zero of F to a pole of F (or vice-versa) and $\mathrm{ord}(F)$ denotes the number of zeros and poles of F (counted without multiplicity).

Write $\mathrm{div}(f) = D = Z + P$ where Z is the divisor of zeros, $Z = \sum_i z_i = \sum_i \gamma_i(1)$ and P is the divisor of poles of f $P = \sum_i q_i = \sum_i \gamma_i(0)$. Write $\omega_1, ..., \omega_g$ as a basis of $\Omega^1(X)$ and select a base point $x \in X$. For every i, write α_i as a path from x to p_i and β_i as a path from x to q_i.

Now that we're done with our setup, we can finally do some math. We will apply the Abel-Jacobi map (on divisors) to get:

$$A_0(D) = \sum_{i=1}^{d} \left(\begin{bmatrix} \int_{\alpha_1} \omega_1 \\ \vdots \\ \int_{\alpha_g} \omega_g \end{bmatrix} - \begin{bmatrix} \int_{\beta_1} \omega_1 \\ \vdots \\ \int_{\beta_g} \omega_g \end{bmatrix} \right)$$

up to periods.
Notice that we can write a period:

$$\begin{bmatrix} \int_{\alpha_1 - \gamma_1 - \beta_1} \omega_1 \\ \vdots \\ \int_{\alpha_g - \gamma_g - \beta_g} \omega_g \end{bmatrix}$$

as $\alpha_i - \gamma_i - \beta_i$ is a closed path. So we can rewrite $A_0(D)$ as:

$$A_0(D) = \sum_{i=1}^{d} \left(\begin{bmatrix} \displaystyle\int_{\gamma_1} \omega_1 \\ \vdots \\ \displaystyle\int_{\gamma_g} \omega_g \end{bmatrix} \right)$$

$$= \begin{bmatrix} \displaystyle\int_{F^*(\gamma)} \omega_1 \\ \vdots \\ \displaystyle\int_{F^*(\gamma)} \omega_g \end{bmatrix}$$

which holds because $F^*(\gamma) = \sum_i \gamma_i$.

Our previous lemma allows us to write $\displaystyle\int_{F^*(\gamma)} \omega_j = \int_\gamma \mathrm{Tr}(\omega_j)$.

As ω_j is holomorphic, so is $\mathrm{Tr}(\omega_j)$. But there are no holomorphic 1 forms on the Riemann Sphere. (This can be proven independently, or one could remark that the Riemann sphere is of genus 0 and this gives the number of linearly independent holomorphic 1-forms.)

So this vector is the zero vector and $A_0(D) = 0$ in $J(X)$ as desired. So we have shown that if D is a principal divisor then $A_0(D) = 0$.

□

We can now work toward proving the other direction of Abel's Theorem. Approaching this in such a way will also allow us to show that the group of periods forms a lattice.

Definition 45 (The Standard Polygon)**.** *Let X be a Riemann Surface of genus g. Then we can identify such a surface with a polygonal presentation which has $4g$ sides $\{a_i, b_i, a_i', b_i'\}_{i=1}^{g}$ (in this order) where a_i and a_i' are identified to a closed loop and b_i and b_i' are identified to a closed loop. We assign a forward direction to each a_i, b_i and a reverse direction to each a_i' and b_i'.*

Definition 46. *Let ω be a 1-form on X. We define:*

$$A_i(\omega) = \int_{a_i} \omega$$

$$B_i(\omega) = \int_{b_i} \omega$$

We call these the ***periods*** *of ω and the A_i are the a-periods and the B_i are the b-periods.*

Definition 47. *Period Matrices*

Let $\omega_1, ..., \omega_g$ be a basis for $\Omega^1(X)$. Define:

$$A = \begin{bmatrix} A_1(\omega_1) & ... & A_1(\omega_g) \\ \vdots & ... & \vdots \\ A_g(\omega_1) & ... & A_g(\omega_g) \end{bmatrix}$$

$$B = \begin{bmatrix} B_1(\omega_1) & ... & B_1(\omega_g) \\ \vdots & ... & \vdots \\ B_g(\omega_1) & ... & B_g(\omega_g) \end{bmatrix}$$

*and call these the **period matrices**.*

Lemma 48. *Both A and B are nonsingular matrices.*

Proof. We'll show this for A since the proof is the same for B. Let

$$A \begin{bmatrix} c_1 \\ \vdots \\ c_g \end{bmatrix} = 0.$$

Obviously $\sum_{i=1}^{g} c_i\omega_i$ is a nonzero holomorphic 1-form on X because it is a linear combination of ω_i which form a basis. Applying each A_i to $\sum_{i=1}^{g} c_i\omega_i$ yields 0 by the condition on the c_i (it can be read off the matrix multiplication). So we have $A_i(\sum_{j=1}^{g} c_j\omega_j) = 0$ for every i and we must have $\omega = 0$. □

Lemma 49. *We have:*

$$A^t B = B^t A.$$

Proof. This follows from matrix multiplication and a few properties of integration of 1-forms. (See [10] Chapter VIII, Section 4, Lemma 4.5) □

Lemma 50. *Let D be a divisor of degree 0 on a compact Riemann Surface X such that $A_0(D) = 0$ in $J(X)$. Then there exists a memormorphic 1-form, ω such that: ω has simple poles at each point where D is nonzero and has no other poles, $D(p)$ is the residue of ω at p for each $p \in X$, and the a and b periods are integral multiples of $2\pi i$.*

Proof. See [10] Chapter VIII, Section 4, Lemma 4.6. □

Theorem 51 (Abel)**.** *Let X be a compact Riemann surface of genus g. Let D be a divisor of degree 0. Then if $A_0(D) = 0$, D is a principal divisor.*

Proof. We have previously shown the reverse direction and now only need the forward direction.

So suppose that D is a divisor of degree 0 where $A_0(D) = 0$ in $J(X)$. Let ω be a meromorphic 1-form as described in the previous lemma. Fix a base point $q \in X$ and define:

$$f(p) = e^{\int_q^p \omega}.$$

Since the periods of ω are multiples of 2π by the previous lemma and the residues of ω are integers, f is defined independently of the path chosen from q to p and f is holomorphic where ω is.

Let p be such that $D \neq 0$. Select coordinates on D such that:

$$\omega = \frac{\mathrm{div}(f)(p)}{z} + g(z) = \frac{\mathrm{ord}_p(f)}{z} + g(z)$$

for a holomorphic g (recall a principal divisor is defined such that $\mathrm{div}(f)(p) = \mathrm{ord}_p(f)$). So in a neighborhood of p we can write:

$$\int_q^p \omega = \mathrm{div}(f)(p) \cdot \ln(z) + h(z)$$

for a holomorphic h. i.e.:

$$f(z) = z^{\mathrm{div}(f)(p)} e^{h(z)}$$

which is a meromorphic function which has the same order at p as D does trivially.

Hence $\mathrm{div}(f) = D$ by definition of the divisor of a function, and we have proven Abel's Theorem. □

We only need go a little further with period matrices to show that the subgroup of periods involved in the construction of the Jacobian forms a lattice.

Lemma 52 (Riemann's Bilinear Relations)**.** *There is a choice of basis of* $\Omega^1(X)$ *such that* $A = I_g$ *and* B *is symmetric with positive definite imaginary part (i.e.* $\mathrm{Im}(B)$ *is a positive definite real matrix).*

Proof. See [10] Chapter VIII, Section 4, Lemma 4.7 □

Lemma 53. *The columns of* A *and* B *are linearly independent over* $\mathbb{R}$*.*

Proof. Consider the matrix

$$M = \begin{bmatrix} I & B \end{bmatrix}.$$

The last lemma shows that the linear independence of the columns of this matrix is equivalent to the linear independence of the columns of A and B.

Consider a nonzero vector $v = \begin{bmatrix} a \\ b \end{bmatrix}$ over $\mathbb{R}$ and suppose for contradiction that $Mv = 0$. Then we must have $a + Bb = 0$. This means the imaginary part of $Bb = 0$ which allows us to conclude by the last lemma that $b = 0$. But then we also have $a = 0$, which is a contradiction. □

Theorem 54. *The subgroup of periods in* $\mathbb{C}^g$ *as in the construction of the Jacobian form a lattice.*

Proof. By the last lemma the columns of the period matrices form a basis of the subgroup of periods of $\mathbb{C}^g$. Since they are linearly independent over $\mathbb{R}$ they form a lattice in $\mathbb{C}_g$. □

Corollary 55.

$$J(X) \cong \frac{\mathbb{C}^g}{\mathbb{Z}^{2g}} \cong \left(\frac{\mathbb{R}}{\mathbb{Z}}\right)^{2g}.$$

Proof. This is obvious given the last theorem and the definition of the Jacobian. Thus the Jacobian is a complex g-dimensional torus. □

Remark 56. *Abel's Theorem gives us that the kernel of A_0, the Abel-Jacobi map on divisors of degree 0 has the set of principal divisors contained in the kernel. In fact, A_0 is actually surjective, and the first isomorpism theorem allows us to consider the quotient of degree 0 divisors by principal divisors. which is sometimes denoted $\mathrm{Pic}_0(X)$. We then have that $J(X)$ is isomorphic to this quotient.*

2.6 Consequences of Abel's Theorem

We finally can talk about why we needed to prove Abel's Theorem and how this relates to the Jacobian.

Theorem 57. *The Abel-Jacobi map, $A : X \to \mathrm{Jac}(X)$ is injective if X is a curve of genus at least 1.*

Proof. Let $P, Q \in X$ be such that $A(P) = A(Q)$ with $P \neq Q$. Consider P and Q as divisors on X so that A is a group homomorphism. I.e. we have that $A(P - Q) = 0$.

From Abel's Theorem, we know that $P - Q = \mathrm{div}(f)$ for some meromorphic function f on X. Since we know explicitly what $\mathrm{div}(f)$ is, we know that P is a zero of multiplicity 1 of f, Q is a pole of order 1 of f, and f has no other zeros or poles.

We recall that we can reinterpret a meromorphic function $X \to \mathbb{C}$ as a holomorphic function $X \to \mathbb{C}^\infty$, where $\mathbb{C}^\infty$ denotes the Riemann Sphere.

This map is nonconstant ($p \mapsto 0$ and $q \mapsto \infty$) and of degree 1 (i.e. it locally looks like $f(z) = z$). By the theory of Riemann Surfaces, this map must be an isomorphism. However, the genus of $\mathbb{C}^\infty$ is 0 and the genus of X is greater than 0, so these two surfaces cannot be isomorphic.

We reach a contradiction to conclude that A is injective. □

Theorem 58. *The Jacobian is compact.*

Proof. It is isomorphic to a g-dimensional complex torus, which is compact. □

3 p-adic analytic functions

Our goal in this section is to build up some basic p-adic analysis background. The goal result realizes particular integrals as p-adic analytic functions and then looks at the Newton Polygon of this type of function to find an upper bound on the number of zeros it has in $p\mathbb{Z}_p$ (which end up being the only zeros we care about). So it will be helpful (and fun) to become familiar with the some standard objects in p-adic analysis.

We give a brief reminder that $\mathbb{C}_p$ denotes the completion of the algebraic closure of $\mathbb{Q}_p$, which is both complete and algebraically closed. The algebraic closure of $\mathbb{Q}_p$, $\overline{\mathbb{Q}_p}$, is **not** complete.

Definition 59. *A p-adic analytic function, f, is a function $f : U \to \mathbb{C}_p$, where U is an open set of $\mathbb{C}_p$, and f can be written as a power series, i.e.*

$$f(z) = \sum_{i=0}^{\infty} a_i (z-b)^i$$

where $a_i \in \mathbb{C}_p, b \in U$, and the series converges everywhere in a neighborhood of b.

Lemma 60. *Consider the sum $\displaystyle\sum_{i=0}^{\infty} a_i$ where $a_i \in \mathbb{C}_p$. Then the series converges* ***if and only if*** $\lim_{i\to\infty} |a_i|_p = 0$.

Proof. The proof that if the series converges then $\lim_{i\to\infty} |a_i|_p = 0$ is the same as in the real and complex case, so we will omit this as it is a basic result proven in any real analysis (or even calculus) course. The interesting part of this proposition is the other direction.

We'll show that the series is Cauchy, which will show the series is convergent since $\mathbb{C}_p$ is complete.

So assume that $\lim_{i\to\infty} |a_i|_p = 0$. Let $S_N = \displaystyle\sum_{i=0}^{N} a_i$ be the Nth partial sum. For any integers j, k such that $j \geq k \geq 0$, we have that:

$$|S_j - S_k|_p = \left| \sum_{i=k+1}^{j} a_i \right|_p \leq \max_{k+1 \leq i \leq j} |a_i|_p.$$

Since $\lim\limits_{i\to\infty} |a_i|_p = 0$ then

$$\lim_{k,j\to\infty} |S_j - S_k|_p = 0.$$

Thus the sequence of partial sums is Cauchy and hence the series is convergent. □

We next show a nice convergence result about p-adic analytic functions - that they always converge in an (open) disk of radius 1 if their coefficients are in $\mathbb{Z}_p$(i.e. this disk is $D_1(b) = \{x \in \mathbb{C}_p |\ |x-b|_p < 1\}$. Making a distinction between "open" and "closed" disks is perhaps bad terminology, because both of these disks are both open and closed since $\mathbb{C}_p$ is a totally disconnected topological field.)

Proposition 61. *Let $f(z) = \displaystyle\sum_{i=0}^{\infty} a_i (z-b)^i$ be a p-adic analytic function with $a_i \in \mathbb{Z}_p$. Then f converges on $\{x \in \mathbb{C}_p : |x-b|_p < 1\}$.*

Proof. Let $x \in \mathbb{C}_p$ be such that $|x-b|_p < 1$. Notice that $|a_i(x-b)^i| = |a_i|_p|x-b|_p^i \leq |x-b|_p^i$, which goes to 0 as i goes to infinity since $|x-b|_p < 1$. The first inequality comes from the fact that $a_i \in \mathbb{Z}_p$, hence $|a_i|_p \leq 1$.

Then, the whole series must converge since the norms of the summands do, by the previous lemma. □

The notion of radius of convergence is the same as in the real and complex world.

Definition 62. *The radius of convergence, r, of a p-adic analytic function, $f(z) = \sum_{i=0}^{\infty} a_i z^i$ is*

$$r = \frac{1}{\operatorname{limsup}_{i\in\mathbb{N}}(|a_i|_p^{1/i})}.$$

As in real and complex analysis, one can show that $f(z)$ converges at c if $|c|_p < r$ and $f(z)$ does not converges at c if $|c|_p > r$. The proof of these things is the same as in real and complex analysis, so we omit it. (In fact, the ultrametric inequality makes these proofs even easier.)

Convergence on the boundary, though, is much simpler than in complex analysis.

Proposition 63. *Let $f(z) = \displaystyle\sum_{i=0}^{\infty} a_i z^i$ be a p-adic analytic function. Then the series either converges for all $x \in \mathbb{C}_p$ with $|x|_p = r$, or it diverges for all $x \in \mathbb{C}_p$ with $|x|_p = r$.*

Proof. Note that we center the series at 0 for the sake of convenience, but the proof is nearly identical if not centered at zero.

Let x be a point at which $f(x)$ converges and $|x|_p = 1$. Let y be another point where $|y|_p = 1$. Then we have:

$$\lim_{i\to\infty} |a_i x^i|_p \to 0.$$

But:

$$|a_i x^i|_p = |a_i|_p |x|_p^i = |a_i|_p |y|_p^i = |a_i y^i|_p.$$

So $\lim_{i\to\infty} |a_i y^i|_p \to 0$ and we are done.

The case of divergence is identical: the limits must take the same value. □

Proposition 64. *p-adic analytic functions are continuous.*

Proof. The proof is the same as that real and complex convergent power series are continuous, but can be made even easier with the ultrametric inequality. □

We now aim at one of the most important fundamental results of p-adic analysis, that p-adic analytic functions have finitely many zeros in $\mathbb{Z}_p$.

Lemma 65. *Let* $f(z)=\sum_{i=0}^{\infty}a_iz^i$ *be a p-adic analytic function, and let b be a point such that f converges at b. Then we can expand f about b, writing it as:*

$$f(z)=\sum_{i=0}^{\infty}c_i(z-b)^i$$

and this series has the same disk of convergence as the original series.

Proof. First, note, we mean that they converge and diverge on the same sets, necessarily to the same value: this is stronger than they just have the same radius of convergence - this a consequence of the non-Archimedean phenomenon that ”every point inside of a circle is the center of the circle.”

Then, again, this is true if the power series is not centered at 0 and the proof is the same, but we work only in the case where the initial series was centered at 0 to simplify the proof.

Write $f(z)=\sum_{i=0}^{\infty}a_i(z-b+b)^i$ and open up parentheses to deduce:

$$f(z)=\sum_{i=0}^{\infty}a_i\sum_{j=0}^{i}\binom{i}{j}(z-b)^jb^{i-j}.$$

From this formula it is clear that we can expand f as a power series about b, so we need only care about convergence. Notice:

$$\left|\binom{i}{j}(z-b)^jb^{i-j}\right|_p\leq|a_i|\max(|b|_p,|z-b|_p)^i.$$

We just got rid of the $\binom{i}{j}$ since it's an integer, and then the sum of powers to which $(z-b)$ and b appear is the same, so we just took the largest one.

But, $f(z)$ converges at b, so $|a_ib^i|_p\to 0$. So if $f(z)$ converges at z, as b is in the radius of convergence, we see that $|a_i||z-b|^i\to 0$ as well. So if $f(z)$ converges, so does this series. Rewriting this series like:

$$f(z)=\sum_{j=0}^{\infty}(z-b)^j\sum_{i=0}^{\infty}a_i\binom{i}{j}b^{i-j}$$

shows that our power series centered at b converges at z also. Switching the order of summation is justified by our discussion of convergence above.

□

Lemma 66. $\mathbb{Z}_p$ *is compact.*

Proof. We show that it is sequentially compact - that every sequence has a convergent subsequence.

Let $\{\sum_{i=0}^{\infty}a_{i,j}p^i\}_{j=0}^{\infty}$ be a sequence in $\mathbb{Z}_p$. Then since there are finitely many possible values of $a_{0,j}$ (it is in $\{0,...,p-1\}$), there must be one value of $a_{0,j}$

which appears infinitely many times. Call this value c_0, and let $\{\sum_{i=0}^{\infty} b_{i,j}p^i\}_{j=0}^{\infty}$ be a subsequence where each element in the sequence has first term c_0.

Similarly, there must be a value of $b_{1,j}$ which appears infinitely many times, call this value c_1, and take a subsequence $\{\sum_{i=0}^{\infty} d_{i,j}p^i\}_{j=0}^{\infty}$ where all terms have c_0 and c_1 in common.

We can continue this process to show that for every n there exists a subsequence $\{\sum_{i=0}^{\infty} x_{i,j,n}p^i\}_{j=0}^{\infty}$ where each p-adic integer in the sequence has the first n terms of its power series expansion in common. Taking the diagonal sequence gives us a subsequence that converges to $\sum_{i=0}^{\infty} c_i p^i$, a p-adic integer (noticing that two p-adic integers "sharing the first n terms in common" means that their difference begins with $c_{n+1}p^{n+1}$ and hence the norm of their difference is less than or equal to $\frac{1}{p^{n+1}}$, so we can see convergence to its claimed limit easily). □

Proof. We provide an alternate proof of this very important lemma.
It is well-known from point set topology that a metric space is compact if and only if it is complete and totally bounded. Note that $\mathbb{Z}_p$ is the ring of integers of $\mathbb{Q}_p$ which is a completion of $\mathbb{Q}$. The ring of integers of a completion is the completion of the ring of integers, hence $\mathbb{Z}_p$ is complete as it is the completion of $\mathbb{Z}$ with respect to the p-adic norm. So we need only show that $\mathbb{Z}_p$ is totally bounded.

Let $\epsilon > \frac{1}{p^n} > 0$. Then we can cover $\mathbb{Z}_p$ with balls: $a + B_{\frac{1}{p^n}}(0)$ for all a in $\mathbb{Z}/p^n\mathbb{Z}$.

It is clear from the power series expansion of p-adic integers that these balls cover all of $\mathbb{Z}_p$. Hence $\mathbb{Z}_p$ is totally bounded, complete, and compact. □

Corollary 67. *p-adic analytic functions with their domain restricted to $\mathbb{Z}_p$ are uniformly continuous, as they are continuous on a compact set. They are also bounded, because they are continuous on a compact set.*

Corollary 68. *$\mathbb{Z}_p$ is a profinite group - it is compact, totally disconnected, and Hausdorff.*

Nothing is special about $\mathbb{Z}_p$ here; the same proof used to show sequential compactness can show that $p^i\mathbb{Z}_p$ for any $i \in \mathbb{Z}$ is compact, the "power series in p" expansion would just start finitely many terms earlier or later. The second proof can be adapted in a similar way.

Notice, then, that since a p-adic analytic function would have to have finitely many zeros in $p^i\mathbb{Z}_p$ for every i, then it would have to have countably many zeros in $\mathbb{Q}_p$ which is the union of all such $p^i\mathbb{Z}_p$.

Theorem 69. *Let $f(z) = \sum_{i=0}^{\infty} a_i z^i$ be a p-adic analytic function which is not identically zero. Then $f(z)$ contains finitely many zeros in $\mathbb{Z}_p$.*

Proof. Suppose $f(z)$ has infinitely many zeros in $\mathbb{Z}_p$. Then, by compactness of $\mathbb{Z}_p$, the set of all of these zeros has a limit point, call this limit point b (If anyone asks, this limit point is also in $\mathbb{Z}_p$ as $\mathbb{Z}_p$ is complete; the operations of taking completions and rings of integers commute for algebraic number fields- as is a standard result in commutative algebra/algebraic number theory).

Expand f about this limit point, $f(z) = \sum_{i=0}^{\infty} b_i(z-b)^i$ (which is convergent on the same set because of the lemma). This form of f is not identically zero because the first form was not. So let b_N be the first nonzero coefficient of f expanded about b. i.e. we have:

$$f(z) = (z-b)^N(b_N + (z-b)g(z))$$

for some p-adic analytic function $g(z)$.

We can pick an ϵ small enough such that if $|z-b|_p < \epsilon$, then $|(z-b)g(z)|_p < |b_N|_p$, because $(z-b)g(z)$ is continuous and zero at b.

Thus f is nonzero in a small punctured disk of radius ϵ about b, because $(z-b)^N$ is only zero at b and $|(z-b)g(z)+b_N|p$ can't be zero or else $|(z-b)g(z)|_p = |b_n|_p$, which contradicts our choice of ϵ.

But b was a limit point of the set of zeros of f, meaning there must be a zero of f in this disk. We have derived a contradiction and hence have shown that f has finitely many zeros in $\mathbb{Z}_p$.

□

This can be used to prove a nice theorem (which is entirely unrelated to our main goal):

Theorem 70 (Skolem-Mahler-Lech [5]). *Let $\{a_i\}_{i=0}^{\infty}$ be a sequence of numbers (necessarily integers) which is given by an integer linear recurrence relation. Then the zero set of this sequence is given by the union of a finite set and finitely many arithmetic sequences.*

Proof. By standard results about integer linear recurrences, we can write our recurrence as:

$$a_k =< A^k v, w >$$

where A is the characteristic matrix of the linear recurrence (Say it is an n by n matrix), $v, w \in \mathbb{Z}^n$, and $< \cdot, \cdot >$ denotes the Euclidean inner product. In particular, the linear recurrence is given by multiplying the vector of initial conditions, v, by the characteristic matrix raised to a certain power, and taking the inner product with w selects a particular entry in that vector (so w is some standard basis vector). The existence of such a representation of any recurrence is a standard fact, and can be made via the coefficients of the recurrence condition.

Select a prime, p, such that A is invertible mod p. If no such p exists, the determinant of A is zero which is not possible for the characteristic matrix of a recurrence (This would mean one of the recurrence conditions is redundant (linearly dependent with the rest of the conditions), and it could be removed to form a shorter set of conditions from which a matrix could be formed). Let N

denote the order of A as an element of $GL_n(\mathbb{F}_p)$. Lifting up to the integers, we can write $A^N = I + pB$.

Define functions $f_i(n) =< A^{Nn+i}v, w >= a_{Nn+i} =< (I + pB)^n A^i v, w >=$ $< \left[\sum_k \binom{n}{k} p^k B^k\right] A^i v, w >= \sum_k \binom{n}{k} p^k < B^k A^i v, w >$. While these functions make sense for all values of i, we only need to consider the ones for $i \in \{0, ..., N-1\}$. Notice that every element in the recurrence belongs in the range of exactly one of these functions, because every element in the recurrence can be written $a_k =< A^k v, w >$ for some k, and these functions just partition the overall sequence by dividing it up into groups where the indices are grouped into finitely many arithmetic sequences with the same common difference (N), but different starting points (i).

But the useful part of such a partition is that by expanding out the binomial coefficients as a polynomial in n, each $f_i(n)$ makes sense as a p-adic analytic function convergent on $\mathbb{Z}_p$.

Then, each f_i is either identically zero or has finitely many zeros in $\mathbb{Z}_p$ and hence $\mathbb{Z}$. The ones which are identically zero correspond to an arithmetic sequence of zeros (The range of f_i restricted to $\mathbb{Z}$ gives one of these partitioned arithmetic sequences of the original recurrence, which must all be zero), and the ones with finitely many zeros in $\mathbb{Z}_p$ will yield finitely many zeros of the recurrence relation. □

3.1 Newton Polygons

Newton Polygons are a powerful tool relating the zeros and valuations of zeros of a polynomial or power series to the coefficients (and valuations of the coefficients). Particularly, the use of Newton Polygons will be allow us to bound how many zeros a particular kind of p-adic analytic function has in $p\mathbb{Z}_p$ which is integral for proving the goal theorem.

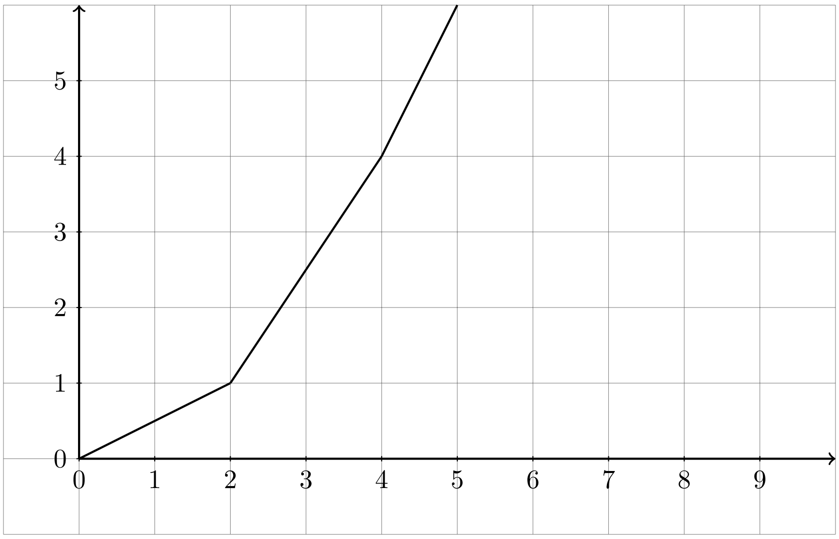
Definition 71. *Let $f(z) = \sum_{i=0}^{N} a_i z^i$ be a polynomial with coefficients in $\mathbb{Q}_{|}$. We create the Newton Polygon as follows:*

(1) Graph on the xy plane the points $(0, v_p(a_0)), (1, v_p(a_1)), ..., (n, v_p(a_n))$. (Do not graph the points with valuation ∞. It is customary to draw these points at the top of the coordinate plane and ignore them when drawing the polygon.)

(2) The Newton Polygon is the lower convex hull of these points.

As an intuitive way to think about it, imagine taking the y-axis and sticking in a pin at $(0, v_p(a_0)$. Rotate the y axis counterclockwise about the pin. When it intersects another one of the points we drew , draw a line from $(0, v_p(a_0))$ to this point. Place a pin at this point, and now rotate about this point. Repeat until we reach the last of the points (which we can do since there are finitely many).

Example 72. *Consider the polynomial* $5^6x^5 + 625x^4 + 125x^3 + 5x^2 + 5x + 1$. *It has the* 5*-adic Newton Polygon:*



Remark 73. *Some people demand that the Newton polygon begins at* $(0, 0)$ *and we must normalize our polynomial (or power series) to have constant term* 1. *We won't adopt this convention.*

We construct the Newton Polygons for power series the same way, but because there are infinitely many points we draw, one of three things could happen as we continue to rotate about each point.

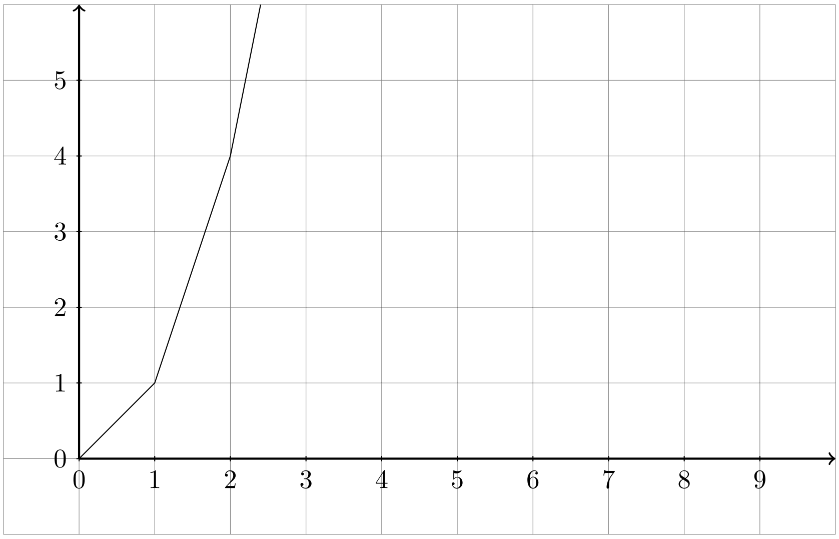
(1) There are infinitely many segments of finite length.

Example 74.

$$f(z) = \sum_{i=0}^{\infty} p^{i^2} z^i$$

.

The valuation of a_i *is* i^2. *We draw part of the Newton Polygon below. The segments will continue to increase in slope.*



(2) There are finitely many segments, and the last one is infinitely long.

Example 75.

$$f(z) = \sum_{i=0}^{\infty} z^i$$

.

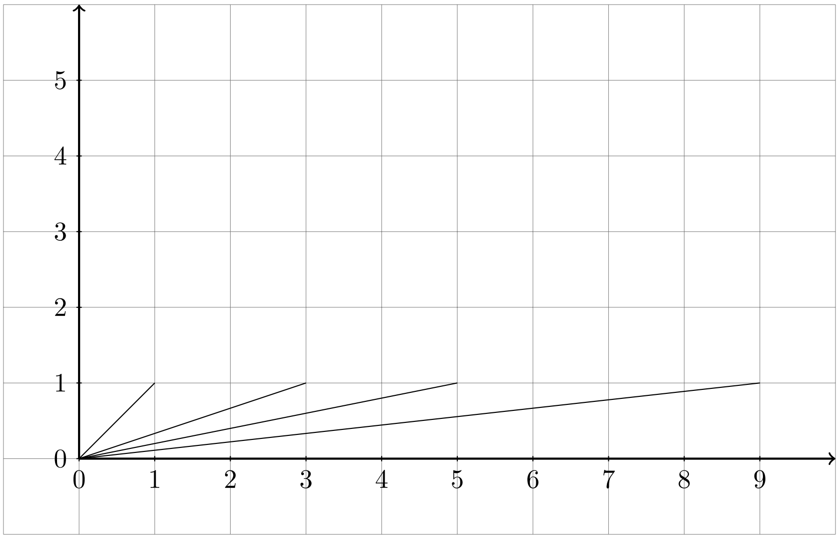
Proof. The valuation of a_i is 0 for every i. The Newton Polygon will be one slope consisting of the x-axis. □

(3) It appears that cannot draw a last segment because there is some (infinite) sequence of indices n_i such that the segment should reach $(n_{i+1}, v_p(a_{n_i+1}))$ before $(n_i, v_p(a_{n_i}))$ for all i. In this case, we take this last segment as having slope equal to the least upper bound of all of the slopes induced by these points. This is best illustrated through an example.

Example 76.

$$f(z) = 1 + \sum_{i=0}^{\infty} pz^i$$

The valuation of each point is p. If we only consider the Newton Polygon of the nth partial sum of the power series, they will look as below (drawn for $n = 1, 3, 5, 9$).



For each n, the Newton Polygon of the nth partial sum is one slope from $(0,0)$ to $(n,1)$, hence the slope is $\frac{1}{n}$. Thus, the Newton Polygon of the whole power series will just be the x-axis, as this is the lower convex hull of the union of all of these slopes.

Remark 77. *Notice by construction, the slopes of the segments of the Newton Polygon are always increasing.*

Theorem 78. *If λ is the slope of a segment of the Newton Polygon of a polynomial of horizontal length l, then precisely l of the zeros of the polynomial (considering the zeros as in $\mathbb{C}_p$) have p-adic valuation equal to $-\lambda$.*

Proof. Write $f(x) = \sum_{i=0} a_i x^i$. Let the distinct valuations of the roots (in order from greatest to least) be $\lambda_1, ..., \lambda_m$ and say there are exactly l_i roots with valuation λ_i. Then a_i is the ith elementary symmetric polynomial in the roots. The valuation of the ith elementary symmetric polynomial, by the ultrametric inequality, will be the valuation of the product $m_1 \cdot ... \cdot m_{l_1}$ where the m_i are the roots of valuation λ_1. This product has valuation $l_1 \cdot \lambda_1$.

Similarly, for each $\left(\sum_{i=1}^{j} l_i\right)$th elementary symmetric polynomial, it has valuation determined by the term of products of the $l_1 + .. + l_j$ roots of valuations $\lambda_1, ..., \lambda_j$, which has valuation $l_1\lambda_1 + ... + l_j\lambda_j$. Notice all other terms in the polynomial will have strictly smaller valuation by the choice of the elementary symmetric polynomial we are working with.

So the line segment joining two such points on the Newton polygon, the point corresponding to the $l_1 + ... + l_j$th coefficient and the point corresponding to the $l_1 + ... + l_{j+1}$th coefficient has horizontal length l_{j+1} and slope $-\lambda_i$. So we are done (inductively) if we show that all of the points on the Newton Polygon between these two lie on or above this segment.

Any elementary symmetric polynomial in the roots between these two must necessarily have valuation lying on or above this segment, as the smallest possible valuation of a term in the elementary symmetric polynomial will be $l_1\lambda_1 + ... + l_j\lambda_j + l_{j+1}m$ for the m determined by which elementary symmetric polynomial we are working on. If the valuation is exactly determined by this term, the point on the Newton Polygon lies on the slope described before. But the valuations of the other term could equal the valuation of this term, in which the point on the Newton Polygon would lie above the aforementioned slope. □

Theorem 79. *Let $f_1, ..., f_n$ be polynomials (or you could take f_n to be a power series) such that all of the slopes of the Newton Polygon of f_i are less than or equal to all of the slopes of f_{i+1} for all i. Then the Newton Polygon of $\prod_{i=1}^{n} f_i$ is the concatenation of the Newton Polygons of $f_1, ..., f_n$. (i.e. begin the polygon of f_2 where the polygon of f_1 ends, etc.)*

Proof. This is a direct application of the last theorem, as the slopes are the negatives of the valuations of the roots. Having them in increasing order determines that the slopes, which must appear in increasing order in the Newton Polygon, have this order match with the concatenation of the polygons of the original f_i. □

Theorem 80. *If the Newton Polygon of a polynomial, f over $\mathbb{Q}_{|}$ (which is not identically zero), consists of a single slope which contains no other lattice points (point with two integer coordinates) other than the start or end points, then it is irreducible.*

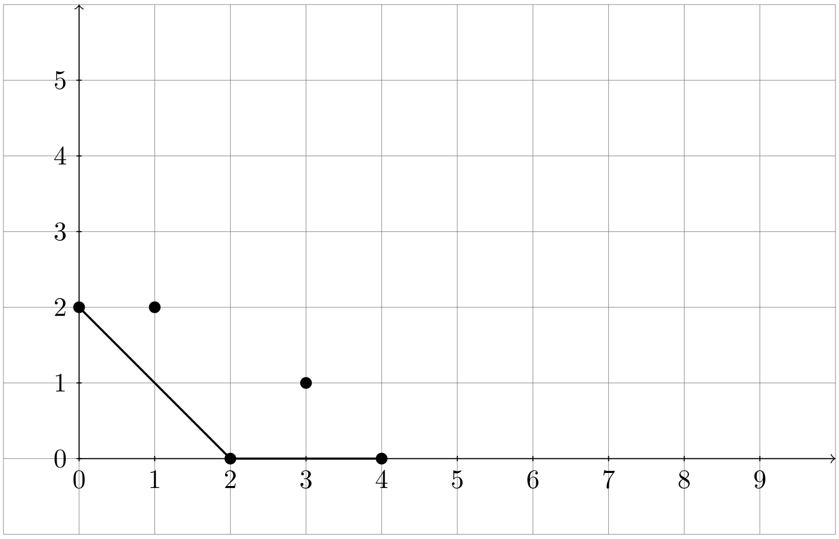
Proof. If it is reducible, write $f = gh$ where g and h are polynomials over $\mathbb{Q}_p$, neither of which is identically zero. Notice that the valuation of a p-adic number is integral (or infinity), so the Newton Polygons of g and h begin and end at a lattice point. Concatenating the two results in one segment which passes through a lattice point. This is a contradiction. □

The useful thing is that we can go in reverse over $\mathbb{Q}_p$.

Theorem 81. *Let the Newton polygon of a polynomial f (over $\mathbb{Q}_p$) consist of m segments of length l_i, $i = 1, ..., m$ where each segment has distinct slope. Then f can be written as the product of m polynomials (in $\mathbb{Q}_p$) of degrees l_i, and the Newton polygons of these polynomials consist of one segment of slope l_i.*

Proof. See [7]. □

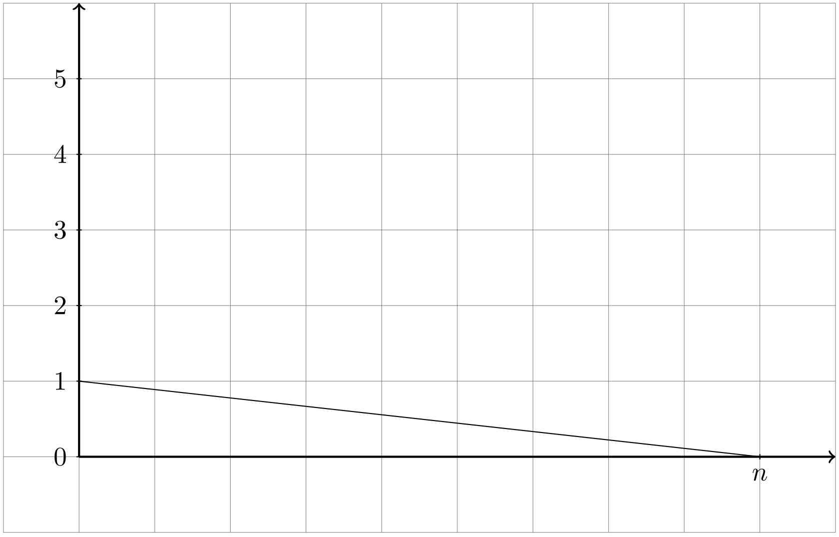
Remark 82. *It is not necessarily true that each of these segments correspond to an irreducible polynomial. Some of the Newton Polygons of the factors could pass through lattice points, and then we know nothing. We have the example where $f(x) = (x-1)^2(x-2)^2 = x^4 - 6x^3 + 13x^2 - 12x + 4$ which clearly cannot be split into two irreducibe quadratics. The 2-adic Newton Polygon of this polynomial is as follows:*



So, the two slopes in the Newton Polygon do correspond to irreducible quadratic factors of $f(x)$.

Theorem 83. *Eisenstein Irreducibility Criterion Let $f = \sum_{i=0}^{n} a_i x^i$ be a monic polynomial over $\mathbb{Q}$ where p divides a_i for $i = 0, ..., n-1$ and p^2 does not divide a_0. Then f is irreducible over $\mathbb{Q}$.*

We draw here the Newton Polygon of an Eisenstein Polynomial:



Proof. The Newton Polygon consists of one segment which begins at $(0, 1)$ and ends at $(n, 0)$ as p divides the constant term, p does not divide the leading coefficient of 1, and p divides every other term. So we consider the point $(0, 1), (n, 0)$, and each other point is on or above the line $y = 1$, hence the polygon is one segment as described.

This clearly does not pass through any lattice points, hence is irreducible over $\mathbb{Q}_p$ and hence $\mathbb{Q}$. □

We are now ready to prove the result(s) about Newton Polygons we need for the goal theorem.

Theorem 84. *Suppose that $f(x) \in \mathbb{Q}_p[[x]]$ is such that $f'(x) \in \mathbb{Z}_p[[x]]$. Let m be the least integer such that the coefficient of z^m in $f'(x)$ is not divisible by p. If $m < p - 2$, then f has at most $m + 1$ zeros in $p\mathbb{Z}_p$.*

Proof. Write $f(x) = \displaystyle\sum_{i=0}^{\infty} a_i x^i$. Then we have $f'(x) = \displaystyle\sum_{i=0}^{\infty} a_i \cdot i \cdot x^{i-1}$. We must have $v_p(a_{m+1}) = 0$, as m is the order of vanishing of $0 \equiv p$ of $f'(t) \pmod{p}$. For $i > m + 1$, we must have $v_p(a_i) \geq -v_p(i)$ as $i \cdot a_i \in \mathbb{Z}_p$. Then, we have obviously $v_p(i) < i$ but since $m + 1 < p - 1$, we get $v_p(i) < i - (m + 1)$ or $-v_p(i) > (m + 1) - i$. So we see that the slope from $(m + 1, 0)$ to (i, x) where $x > m + 1 - i$is greater than $-\frac{m+1-i}{m+1-i} = -1$. We also see that the slope from $(i, m + 1 - i)$ to $(j, m + 1 - j)$ is greater than $-\frac{m+1-j-(m+1-i)}{j-i} = -1$. So the points to the right of $m+1$ on the Newton Polygon increase at a rate of at least -1. Hence no slope of the Newton Polygon including any points to the right of $m + 1$ can be greater than -1.

As the negative valuations of the slopes correspond to the roots of the Newton Polygon, the $f(x)$ has at most $m + 1$ zeros with valuation greater than 1 in $\mathbb{C}_p$. Hence $f(x)$ has only finitely many roots in $p\mathbb{Z}_p$. □

While the previous theorem is sufficient to showing the result, the estimates made in the previous proof can be made stronger. In fact, Coleman proved the following theorem.

Theorem 85 (Coleman - A stronger version [2])**.** *Let $f(x) \in \mathbb{C}_p[[x]]$ be such that $f'(x) \in \mathcal{O}_{\mathbb{C}_p}[[x]]$ (where $\mathcal{O}_{\mathbb{C}_p}$ denotes the ring of integers of $\mathbb{C}_p$) and let the first power of x with a nonzero coefficient in the power series expansion of $\tilde{f} = f'(x) \pmod{p}$ be denoted l. Then $f(x)$ has at most* $\max\{k : \frac{s^k}{|k|_p} \geq \frac{s^l}{|l|_p}\}$ *zeros inside $B_s(0) = \{x \in \mathbb{C}_p : |x|_p \leq s\}$.*

4 Curves over Finite Fields

The goal of this section is to develop an understanding of algebraic curves, in particular over finite fields, in order to prove the Riemann Roch Theorem over a general field. For this section, let k denote this field, which we assume is algebraically closed.

As this thesis is meant to build up the number theory, not algebraic geometry, we assume the following theorem:

Theorem 86. *Let C be a projective curve over k, an algebraically closed field. Then there is a nonsingular projective curve X (unqiue up to isomorhpism) and a birational morphism f from X onto C. We call X the **nonsingular model** of C.*

Proof. See [4] 7.5 Theorem 3. □

We will use X to denote the nonsingular model of a projective plane curve and will not distnguish between the curve and its nonsingular model.

Corollary 87. *There is a one-to-one correspondence between nonsingular projective curves and algebraic function fields in one variable $K = k(X)$. If X' and X are two such curves, dominant morphisms from X' to X correspond to homomorphisms from $k(X)$ into $k(X')$.*

Remark 88. *The points P of X are in one-to-one correspondence with discrete valuation rings $\mathcal{O}_P(X)$ of K. $f(P) = Q$ exactly when $\mathcal{O}_P(X)$ dominates $\mathcal{O}_P(C)$. The points of X are called **places** of C (or of K).*

We associate each point on the curve with a discrete valuation ring by sending P to the valuation v_P, which maps a function, f, to its order of vanishing at P.

Proof. See [4]. □

For the rest of this section, we will use K to denote this function field in one variable corresponding to the nonsingular model, X, of a projective plane curve, C over k.

4.1 Divisors

Divisors are defined over arbitrary fields the same way they were in the complex place. As expected, the set of divisors forms a group, the free abelian group on X.

Definition 89. *We call a divisor **effective** if $D(P) \geq 0$ for all $P \in X$.*

Definition 90. *Let $f \in K$. Analogous to the case of a meromorphic function in the complex case, we define:*

$$\operatorname{div}(f) = \sum_{P \in X} \operatorname{ord}_P(f) P$$

where $\operatorname{ord}_P(f)$ denotes the order of the zero or pole of f at P. Note that since a rational function has the same number of zeros and poles (counting the zeros/poles at the point at infinity) that such a divisor will always have degree 0.

*As in the complex case, we call such a divisor a **principal divisor**.*

Proposition 91. *Let $f, g \in K$ which are not zero. Then:*

$$\operatorname{div}(f) = \operatorname{div}(g) \iff f = \lambda g$$

for some $\lambda \neq 0 \in k$.

Proof. This is an obvious property of rational functions. □

We next define an ordering on the set of divisors:

Definition 92. *Let* $D = \sum_{P \in X} D(P) \cdot P$ *and* $E = \sum_{P \in X} E(P) \cdot P$ *be divisors of* X*. We say that* $D \geq E$ *if* $D(P) \geq E(P)$ *For all* $P \in X$*. We define less than, greater than, greater than or equal to, and less than or equal to in the expected ways.*

Definition 93. *Let* D *and* E *be divisors. We say they are linearly equivalent if they differ by the divisor of a function* $f \in K$*. i.e. if there exists an* $f \in K$ *such that:*

$$D = E + \operatorname{div}(f).$$

We'll write $D \sim E$ *to denote this relation.*

Proposition 94. *Linear equivalence of divisors is an equivalence relation.*

Proof. Reflexivity is trivial, as we can write D as the sum of itself plus the divisor of the constant function 1 which has no zeros nor poles.

Symmetry is also simple, as if we have $D = E + \operatorname{div}(f)$, then we have $E = D - \operatorname{div}(f)$ and we see $-\operatorname{div}(f) = \operatorname{div}\frac{1}{f}$. $\frac{1}{f}$ is in K as K is a field.

For transitivity, let D, E, F be divisors where we have $D = E + \operatorname{div}(f)$ and $E = F + \operatorname{div}(g)$. We have:

$$\begin{aligned} D &= E + \operatorname{div}(f) \\ &= F + \operatorname{div}(f) + \operatorname{div}(g) \\ &= F + \operatorname{div}(f \cdot g). \end{aligned}$$

Hence linear equivalence is an equivalence relation. □

Proposition 95. *Some easy facts about linear equivalence*
Let D *and* E *be two divisors.*
(1) $D \sim 0$ *if and only if* D *is principal*
(2) $D \sim E \implies \deg(D) = \deg(E)$

Proof. These are both immediate. For 1, we remarked already that a principal divisor has degree 0. Similarly, given a divisor with degree 0 it is trivial to find a rational function with the prescribed zeros and poles.

(2) follows immediately from (1). and the fact that the degree of divisors is an additive function. □

Definition 96. *We define a special divisor dependent on our curve* C*. We'll denote this divisor by* E *(which will unfortunately limit our choices for what letters to call divisors). So let* C *be a plane curve with only ordinary points of multiplicity greater than* 1 *(i.e. a point of multiplicty* $r > 1$ *which has* r *distinct tangents). Then we define:*

$$E = \sum_{Q \in X} (\operatorname{mult}_Q(C) - 1)Q.$$

The sum is finite since there will only be finitely many nonsingular points.

Definition 97. *An **adjoint** of C is a plane curve G in X for which* $\operatorname{div}(G) \geq E$ *(the relation as defined in definition 92), where* $\operatorname{div}(G)$ *is the divisor of a the plane curve, i.e.*

$$\operatorname{div}(G) = \sum_{P \in X} \operatorname{ord}_P(G) \cdot P.$$

Here we will define a vector space integral for the proof of Riemann-Roch

Definition 98. *Let D be a divisor of K. We define:*

$$L(D) = \{f \in K | \operatorname{div}(f) \geq -D\}.$$

We will denote dimension of this vector space as $l(D)$. Note this definition is equivalent to:

$$L(D) = \{f \in K | \operatorname{ord}_P(F) \geq -D(P) \forall P \in X\}.$$

Proposition 99. *If $D \leq D'$ then $L(D) \subset L(D')$ and* $\dim(L(D')/L(D)) \leq \deg(D' - D)$.

Proof. We can write $D' = D + \sum_{i=1}^{k} P_i$ for some k (where the P_i are not necessarily distinct - notice by the definition of the comparison operator on divisors that we must have that every P which appears in D has a smaller coefficient in D than in D').

Then, it is obvious that if $f \in L(D)$ then $f \in L(D + \sum_{i=1}^{k} P_i)$ by definition. So we've proven the first part of the statement.

We'll omit the proof of the second which involves a few more technical definitions (see [4] Chapter 8). □

Proposition 100. *$L(0) = k$; $L(D) = 0$ if* $\deg(D) < 0$.

Proof. We remarked earlier that any rational function has the same number of zeros as poles (including multiplicity and the point at infinity). Thus any rational function which has a zero also has a pole, so if the rational function f has either a zero or a pole then there exists a P such that $\operatorname{ord}_p(f) < 0$ (namely, the pole). Hence the only rational functions in $L(0)$ are the functions without zeros or poles, which are the constant functions. So $L(0) = k$.

Then, if $\deg(D) < 0$, we use similar logic. The degree of $\operatorname{div}(f) = 0$ for any $f \in K$. But then $\deg(\operatorname{div}(f) + D) < 0$ so we cannot have $\operatorname{div}(f) \geq -D$. Hence no nonzero f are in $L(D)$. □

Proposition 101. *$L(D)$ is finite dimensional for all D. In fact, if* $\deg(D) \geq 0$ *then $l(D) \leq \deg(D) + 1$. (Otherwise, $l(D) = 0$ by a previous proposition.)*

Proof. Let $\deg(D) = n \geq 0$. (By a previous proposition, it's trivial if $n < 0$, as $L(D) = 0$.) Then choose a $P \in X$ and consider the divisor $D - (n+1)P$. By a previous proposition and noting the degree of this divisor is -1, we have that $L(D - (n+1)P) = 0$ and $\dim(L(D)/L(D-(n+1)P) \leq n+1$. So we have that $l(D) \leq n + 1$ as desired. □

Proposition 102. *If $D \sim D'$ then $l(D) = l(D')$.*

Proof. Write $D = D' + \text{div}(f)$. Define a map between $L(D)$ and $L(D')$ by sending g to fg. This is a linear map and an isomorphism of vector spaces, so we have an equivalence of dimensions (as the vector spaces are finite dimensional). □

4.2 Derivations and Differentials

Before proving Riemann Roch, our main application of Riemann-Roch will be to 1-forms, so we should introduce differentials on general curves.

Definition 103. *Let R be a ring containing k and let M be a R-module. A derivation of R into M over k is a k linear map $D : R \to M$ such that $D(xy) = xD(y) + yD(x)$ for all $x, y \in R$.*

By properties of polynomial rings, it follows that such a D acts on a polynomial in $k[X_1, ..., X_n]$ as follows:

$$D(F(X_1, ..., X_n)) = \sum_{i=1}^{n} F_{X_i}(x_1, ..., x_n) D(x_i)$$

for $x_1, ..., x_n \in R$.

Proposition 104. *Let R be a domain with field of fractions K and M, a vector space over K. Then a derivation $R \to M$ extends uniquely to a derivation $\tilde{D} : K \to M$.*

Proof. Let $z = \frac{x}{y} \in K$ with $x, y \in R$. Then if such a $\tilde{D}$ exists, we must have:

$$\frac{1}{y}(D(x) - zDy) = \tilde{D}(z)$$

by the properties of a derivation, so any such $\tilde{D}$ must be this one. Plugging in $\frac{x}{1}$ shows that $\tilde{D}$ agrees with D on R, as:

$$\tilde{D}\left(\frac{x}{1}\right) = D(x) - xD(1) = D(x).$$

Applying the Liebniz rule to $D(1 \cdot 1)$ and using the fact that R is a domain makes it clear that $D(1) = 0$.

We can also verify that this is a derivation.

It is clearly k-linear because D is; this check is routine. $\tilde{D}(z)$ ends up in M since M is a K vector space and the image of D is in M. To show the Liebniz rule as satisfied, we have:

$$\begin{aligned}
\tilde{D}\left(\frac{a}{b} \cdot \frac{c}{d}\right) &= \frac{1}{bd}\Big(D(ac) - \frac{a}{b} \cdot \frac{c}{d} \cdot D(bd)\Big) \\
&= \frac{1}{bd}\Big(aD(c) + cD(a) - \frac{a}{b} \cdot \frac{c}{d} \cdot (bD(d) + dD(b))\Big) \\
&= \frac{1}{bd}\Big(cD(a) - \frac{ac}{b}D(b) + cD(a) - \frac{ac}{d}D(d)\Big) \\
&= \frac{a}{c} \cdot \frac{1}{b}\Big(D(a) - \frac{a}{b}D(b)\Big) + \frac{b}{d} \cdot \frac{1}{d}\Big(D(c) - \frac{c}{d}D(d)\Big)
\end{aligned}$$

Hence this is indeed a differential. □

We want to define differentials for these arbitrary fields just like the ones we know so well from $\mathbb{R}$ and $\mathbb{C}$.

So, let F be the free R-module with generating set R. (i.e. an element in F is a formal (finite) sum of elements in R with coefficients in R. Scalar multiplication is given by multiplication in R. As R is a ring it is obvious that this is a module.)

Let N be the submodule generated by (note: the elements are elements in the free module F, not the ring R):

$$N =< x + y - x - y, (\lambda x) - \lambda \cdot x, (xy) - x \cdot y | x, y \in R > .$$

Definition 105. *Define $\Omega^1_{R/k} = F/N$. Here k represents the underlying field k. We can call "dx" the image of x under the quotient map (take this as the definition of the map d). This set is the module of differentials of R over k and d is a derivation.*

Proposition 106. *$\Omega^1_{R/K}$ is generated by the differentials $dx_1, ..., dx_n$ given $x_1, ..., x_n \in R$ where $x_1, ..., x_n$ generate R.*

This is immediate from the action of a derivation on a polynomial in $k[X_1, ..., X_n]$ described earlier.

Definition 107. *If X is the nonsingular model of a projective curve with K its function field, then $\Omega^1_{K/k}$ is the space of differentials of K over k (we will sometimes call it Ω^1). These are analogous to the 1-forms in the case where $k = \mathbb{C}$.*

Definition 108. *Let $\omega \in \Omega^1$. Let P be a place of C (i.e. a point of X, which is in one-to-one correspondence with the discrete valuation rings $\mathcal{O}_P(X)$, hence why the definition sounds so similar (and is analogous to) the more familiar definition found in algebraic number theory). Write $\omega = f dt$ for some $f \in K$ and a uniformizing parameter t.*

We define:

$$\text{ord}_P(\omega) = \text{ord}_P(f)$$

as is analogous to the complex definition of zeros/poles of 1-forms. Change-of-variables shows that this is well-defined.

Since we have such a notion, now, like how we defined canonical divisors in the complex case, we can define canonical divisors here, too.

Definition 109. *A **canonical divisor** is a divisor of the form:*

$$\text{div}(\omega) = \sum_{P \in X} \text{ord}_p(\omega) \cdot P$$

where $\omega \in \Omega^1_k(K)$ and ω is nonzero.

Remark 110. *It is nontrivial that this is well-defined, i.e., that the specified sum is finite. We shall assume this result.*

Proposition 111. *The degree of a canonical divisor is $2g-2$, hence, $l(W) \geq g$.*

Proof. See [4] Chapter 8.4. □

4.3 Riemann-Roch

Lemma 112. *Let $f \in K$ be nonconstant. Let Z be the divisor of zeros of f and let $n = [K : k(x)]$. Then there exists a constant τ such that $l(rZ) \geq rn - \tau$ for all r.*

Proof. See [4] Chapter 8. □

Theorem 113 (Riemann's Theorem)**.** *There is an integer g such that $g \geq \deg(D) + 1 - l(D)$ for all divisors D.*

This g also happens to be the genus of X. As we know, the genus is a nonnegative integer, which can be shown using the language of divisors.

Proof. First, notice that by taking $D = 0$ then if this g exists, it must be greater than or equal to $\deg(0) + 1 - l(0)$. By Proposition 100, this is 0. Hence $g \geq 0$.

Then, it is obvious that the same g works for linearly equivalent divisors, as if $D \sim D'$, then $\deg(D) = \deg(D')$ and $l(D) = l(D')$ by our discussion of l in the last section.

This discussion shows that if $D \leq D'$, then $\deg(D) + 1 - l(D) \leq \deg(D) + 1 - l(D)$. So, a g where the inequality holds for D' will also make it hold for D.

By Lemma 112, there exists a τ such that $l(rZ) \geq rn - \tau$ for all r where $Z = \sum Z(P)P$ is the divisor of zeros for some f nonconstant in K. Then we have $\deg(rZ) + 1 - l(D) \leq \tau + 1$ for all r. As $rZ \leq (r+1)Z$, we conclude that $\deg(rZ) + 1 - l(rZ) = \tau + 1$ for all r sufficiently large. We now claim that $\tau + 1 = g$ and then we will have found a divisor which is sufficient to show that $g \geq \tau + 1$.

We will conclude this by constructing a linearly equivalent divisor, D' to any divisor $D = \sum D(P)P$ and an integer $r \geq 0$ such that $D' \leq rZ$. We seek an f such that $D(P) - \mathrm{ord}_p(f) \leq rZ(P)$. By taking r large enough, this just amounts to finding a rational function which has zeros and poles such that $D(P) - \mathrm{ord}_p(f)$ is less than an a large number, which is easy to construct.

□

Corollary 114. *There is an integer N such that for all divisors D of degree greater than N, $l(D) = \deg(D) + 1 - g$.*

Proof. Choose D_0 such that $l(D_0) = \deg(D_0) + 1 - g$ (we showed that the bound given by Riemann's Theorem can be achieved inside the proof of Riemann's Theorem). If D is a divisor such that $\deg(D) \geq \deg(D_0) + g$, then we have that $\deg(D - D_0) + 1 - g > 0$, so $l(D - D_0) > 0$ by Riemann's Theorem. So we have that $D - D_0 + \mathrm{div}(f) \geq 0$ for some f (any such f will do), so we have $D + \mathrm{div}(f) \geq D_0$. Hence $l(D) = \deg(D) + 1 - g$. □

Lemma 115 (Noether's Reduction Lemma)**.** *If $l(D) > 0$ and $l(W - D - P) \neq l(W, D)$ then $l(D + P) = l(D)$.*

Proof. See [4] Chapter 8. □

Theorem 116 (Riemann-Roch)**.** *Let W be a canonical divisor on X. Then for any divisor, D, we have:*

$$l(D) = deg(D) + 1 - g + l(W - D)$$

.

Proof. We first prove the theorem for $l(W - D) = 0$ via induction on $l(D)$.

In our base case, where $l(D) = 0$, by Riemann's Theorem we get

$$0 \geq \deg(D) + 1 - g$$
$$0 \geq \deg(W - D) + 1 - g$$

from which the theorem is immediate.

If $l(D) = 1$, we can assume $D \geq 0$.

Then $g \leq l(W)$ by the (Corollary of 8.5), $l(W) \leq l(W - D) + \deg(D)$ (lemma) and $\deg(D) \leq g$ by Riemann's Theorem. So we have $l(W) = g$ and the theorem is easy.

If $l(D) > 1$, select P such that $l(D - P) = l(D) - 1$ (which can always be done). Then Neother's Reduction Lemma gives us that $l(W - (D - P) = 0$. We see Riemann Roch is true for the divisor $D - P$ by induction, which immediately implies its truth for the divisor D.

We now consider when $l(W - D) > 0$, which can only occur if $\deg(D) \leq \deg(W) = 2g - 2$. Pick a maximal degree divisor, D, for which Riemann-Roch is false to proceed by contradiction. By maximality, Riemann-Roch must be true for $D + P$ for all P on the curve. So choose a P for which $l(W - D - P) = l(W - D) - 1$. If $l(D) = 1$, we are done by Case 1 to the divisor $W - D$. So assume $l(D) > 0$. Then Noether's Reduction Lemma gives $l(D + P) = l(D)$. As Riemann Roch is true for $D + P$, we deduce $l(D) = l(D + P) = \deg(D + P) + 1 - g + l(W - D - P) = \deg(D) + 1 - g + l(W - D)$. □

Corollary 117. *$l(K) = g$ for K a canonical divisor.*

Note this gives us an alternative characterization of the genus, analogous to the case in the finite field.

Proof. Recall that $\deg(D) = 2g - 2$ and $l(0) = 1$. This then follows immediately from Riemann Roch. □

4.4 An application of Riemann Roch

We show the equivalence of the two definitions of the genus of a curve as the dimension of $\Omega_k(K)$ and where $2g - 2$ is the degree of a canonical divisor.

Definition 118. *Analogous to $L(D)$, define:*

$$L^{(1)}(D) = \{\omega \in \Omega^1(X) | \text{div}(\omega) \geq -D\}.$$

Lemma 119. *We have $\Omega^1(X) \cong L^{(1)}(0)$, which is clear by definition.*

Theorem 120. *We have:*

$$L^{(1)}(D) \cong L(D+K)$$

for any divisor D and canonical divisor K.

Proof. Fix $K = \operatorname{div}(\omega)$. Let $f \in L(D+K)$. We claim multiplication of f by ω is the desired isomorphism.

We have $\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega)$. As $f \in L(D+K)$, we have $\operatorname{div}(f) + D + K \geq 0$, hence $\operatorname{div}(f) + \operatorname{div}(\omega \geq -D$. This is the same as saying that $\operatorname{div}(f\omega) \in L^{(1)}(D)$. So this is a well-defined map. It is clearly $\mathbb{C}$-linear. Injectivity is very clear.

Surjectivity is more involved. Given $\omega' \in L^{(1)}(D)$, we have a rational function such that $\omega' = f\omega$. Furthermore, we have $\operatorname{div}(f) + D + \operatorname{div}(\omega) = \operatorname{div}(f\omega) + D = \operatorname{div}(\omega') + D \geq 0$. □

From here it is easy to deduce the equivalence of the two definitions of genus. We have, by the previous work in this section, that $L(K) = L(K+0) \cong L^{(1)}(0) = \Omega_k^1(K)$. But by Riemann Roch we have $l(K) = g$, where this g is the g that appears in the dimension of a canonical divisor. Then as the other definition of the genus is as the dimension of $\Omega_k^1(K)$, we are done.

5 Chabauty's Approach

5.1 The Jacobian over $\mathbb{Q}_p$

Now that we have introduced the Jacobian, Abel-Jacobi Map, have shown Riemann Roch for all fields, and have a sufficient amount of background in elementary p-adic analysis, we can begin the trek toward the goal theorem.

We start with considering the Jacobian over $\mathbb{Q}_p$ which leads very quickly to an excellent way to intuitively understand the goal theorem in terms of intersections of manifolds, which Chabauty turned into a proof.

Definition 121. *We define $J(X)(\mathbb{Q}_p)$ as the same algebraic variety given by $J(X)(\mathbb{Q})$ (whose construction was described over $\mathbb{C}$ earlier) but where the equations defining it are given over $\mathbb{Q}_p$ instead of $\mathbb{Q}$.*

Remark 122. *In fact, $J(X)(\mathbb{Q}_p)$ is a p-adic Lie Group.*

We can also consider the analytic closure (with respect to the p-adic topology), which we will denote $\overline{J}$ of $J(X)(\mathbb{Q})$ as a subgroup $J(X)(\mathbb{Q}_p)$. It turns out that this is a p-adic manifold and that we have:

$$\dim(\overline{J}) \leq \operatorname{rk}(J(X)(\mathbb{Q})).$$

This allows us to get a very good intuitive grasp at why the goal result should be true in the case where $\operatorname{rk}(J(X)(\mathbb{Q})) < g$. Since $X(\mathbb{Q}_p)$ is a curve, the Abel-Jacobi map allows us to realize $X(\mathbb{Q}_p)$ as a submanifold of $J(X)(\mathbb{Q}_p)$

which has dimension g, the genus of the curve $X(\mathbb{Q}_p)$. If the genus is greater than 1, we have $X(\mathbb{Q}_p)$ residing as a proper submanifold.

However, we also have $X(\mathbb{Q}) \subset \overline{J}$, again by the injection induced by the Abel-Jacobi map. So, we have realized $X(\mathbb{Q})$ as a subset of both $\overline{J}$ and $X(\mathbb{Q}_p)$. which are both contained in the p-adic manifold $J(X)(\mathbb{Q}_p)$. In the case where we have $\dim(\overline{J}) \leq \mathrm{rk}(J(X)(\mathbb{Q}))$, we recognize that $\overline{J}$ is a proper submanifold of $J(X)(\mathbb{Q}_p)$ as well. Hence, by intersection theory, we would expect the intersection of a 1-dimensional submanifold and less-than-g-dimensional submanifold of a g-dimensional manifold to have dimension 0, which would tell us that $X(\mathbb{Q})$, which is a subset of this intersection, is discrete.

While this is not a proof, it is perhaps the most intuitive way to understand this result.

In fact, while later refined by Coleman, Chabauty did prove the result:

Theorem 123 (Chabauty)**.** *Let X be a curve of genus $g \geq 2$ over $\mathbb{Q}$. Let p be a prime and suppose that $\dim(\overline{J}) \leq \mathrm{rk}(J(X)(\mathbb{Q}))$. Then $X(\mathbb{Q}_p) \cap \overline{J}$ is finite.*

For a proof, see [1].

We will focus on Coleman's refinement instead of Chabauty's proof, but we will prove enough so that the intuitive characterization is as justified as it can be without showing this intersection is actually finite. The following theorem is sufficient to do this, the proof of which depends on one definition.

Definition 124. *We have a map:*

$$J(X)(\mathbb{Q}_p) \times H^0(J(X)(\mathbb{Q}_p, \Omega^1(X)) \to \mathbb{Q}_p$$

given by

$$(P, \omega) \mapsto \int_0^P \omega.$$

This map corresponds to a map $J(X)(\mathbb{Q}_p) \to (H^0(J(X)(\mathbb{Q}_p), \Omega^1(X))^*$ which we will denote as log.

Theorem 125. *We have:*

$$\dim(\overline{J}) \leq \mathrm{rk}(J(X)(\mathbb{Q}))$$

for a curve $X(\mathbb{Q})$.

Proof. The log function is a local diffeomorphism on $\overline{J}$. Hence we have:

$$\dim(\overline{J}) = \dim(\log(\overline{J})) = \dim(\overline{\log(J(X)(\mathbb{Q})}).$$

Then, we have $\overline{\log(J)} = \mathbb{Z}_p \cdot \log J(X)(\mathbb{Q})$, as the closure of a subgroup of a $\mathbb{Q}_p$ vector space is its $\mathbb{Z}_p$ span. We often take as a definition that the dimension of such a subgroup G of a p-adic manifold is the dimension of $\mathrm{span}(\overline{\log(G)})$ as a $\mathbb{Z}_p$-module. Then, obviously:

$$\mathrm{span}_{\mathbb{Z}_p}(\log J(\mathbb{Q})) \supset \mathrm{span}_{\mathbb{Z}}(\log J(\mathbb{Q}))$$

as $\mathbb{Z} \subset \mathbb{Z}_p$. The containment, the equivalence of dimensions described above, and the fact that log is a local diffeomorphism gives us the desired inequality of dimensions, that:

$$\dim(\overline{J}) \leq \dim(J(X)(\mathbb{Q}_p)).$$

□

6 Coleman's Approach

Throughout the following section, we will let p be a prime of good reduction.

Lemma 126. *Let $\omega \in H^0(J(X)(\mathbb{Q}_p), \Omega^1)$. If Q, Q' are two points in $X(\mathbb{Q}_p)$ which have the same reduction in $X(\mathbb{F}_p)$, then we can write $\int_Q^{Q'} \omega$ locally as a power series on X. [9]*

6.1 Residue Classes of Curves over $\mathbb{Q}_p$

Let $X(\mathbb{Q}_p)$ be a curve with good reduction at p. There is an obvious surjective map:

$$\pi : X(\mathbb{Q}_p) \to X(\mathbb{F}_p).$$

Definition 127. *We define a **residue class** as the preimage of a point in $X(\mathbb{F}_p)$ under π.*

Lemma 128. *There exists a function, t, which maps the residue class of a point $\tilde{Q} \in X(\mathbb{F}_p)$ bijectively to $p\mathbb{Z}_p$. [9]*

6.2 Some results involving 1-forms on $J(X)(\mathbb{Q}_p)$

Coleman proved the following proposition which will be instrumental to the goal result:

Theorem 129 (Coleman [2])**.** *Suppose K is a complete discretely valued subfield of $\mathbb{C}_p$. Let X be a curve over K and suppose that $j : (X, c_o) \to (A, 0)$ is a morphism over K of a pointed curve into an Abelian Variety, both with good reduction. Suppose G is a subgroup of $A(K)$. Then, $j(X(K)) \cap G$ is contained in the set of all $x \in X(K)$ such that:*

$$\int_{c_0}^{x} \omega = 0$$

for all $\omega \in j^*(H^0(A, \Omega^1_{A/K}))$ where ω is nonzero on G .

Remark 130. *We are interested in the case where A is the Jacobian of $X(\mathbb{Q}_p)$. The map j will be the Abel-Jacobi map injecting $X(\mathbb{Q}_p)$ into its Jacobian. G, the subgroup will be $X(\mathbb{Q})$ (realizing $\mathbb{Q}$ as a subfield of $\mathbb{Q}_p$). The result here will tell us that $X(\mathbb{Q})$ is contained in the zero set of the integrals $I(x) = \int_{c_0}^{x} \omega = 0$; this zero set is a subset of $X(\mathbb{Q}_p)$. The rest of the proof will involve counting the zeros of the integrals which lie in $p\mathbb{Z}_p$ (we have essentially done all of this* *work in the Newton Polygons section) and realizing these zeros which lie in $p\mathbb{Z}_p$ as points in the residue class.*

Remark 131. *This same process can be done over a general number field, L instead of just $\mathbb{Q}$, where we can take K as the completion of L at a place p, A as the Jacobian, j as the Abel-Jacobi map with any base point, and G as $X(L)$ where L realized as a subfield of K. Notice that the completion of any number field will be a discretely valued subfield of $\mathbb{C}_p$ as all valuations must be an integral multiple of the valuation of a uniformizer.*

Theorem 132. *Let ω be a 1-form on $X(\mathbb{Q}_p)$ which reduces to a nonzero 1-form on the residue class defined by a point $\tilde{Q}$. Then ω can be locally written as $w(t)dt$ where $w(t) \in \mathbb{Z}_p[[t]]$ such that $w(t)$ is nonzero mod p. Furthermore, the function $I(t) : X(\mathbb{Q}_p) \to \mathbb{Q}_p$ given by $I(t) = \displaystyle\int_Q^t \omega$ can be written as a power series in $\mathbb{Q}_p$ whose derivative is $w(t)$. [9]*

Theorem 133. *Our setup is as in the previous theorem. Such an integral $I(t)$ has at most $\mathrm{ord}_{\tilde{Q}}\tilde{\omega} + 1$ zeros in $p\mathbb{Z}_p$. This will be particularly useful due to the bijective correspondence between the zeros in $p\mathbb{Z}_p$ and the residue classes of a point $\tilde{Q} \in \mathbb{F}_p$ established in a previous lemma. [9]*

6.3 A bound on $X(\mathbb{Q})$

Lemma 134. *Let $\omega \in H^0(X_{\mathbb{Q}_p}, \Omega^1)$ such that it reduces to a nonzero 1-form in $H^0(X_{\mathbb{F}_p}, \Omega^1)$ (which can be done by multiplying by a scalar of $\mathbb{Q}_p$). Let $\tilde{Q} \in X(\mathbb{F}_p)$. If $\mathrm{ord}_{\tilde{Q}} < p - 2$, then the number of points in $X(\mathbb{Q})$ reducing to $\tilde{Q}$ is at most $m + 1$.*

Proof. Fix a point in $X(\mathbb{Q})$ which reduces to $\tilde{Q}$ (if no such point exists, then there are zero points reducing to $\tilde{Q}$ which is less than $\mathrm{ord}_{\tilde{Q}}\tilde{\omega} + 1$ as $\mathrm{ord}_{\tilde{Q}}\tilde{\omega} \geq 0$). Call this point Q.

By another previous lemma, we can write the function $I(x) = \int_Q^x \omega = 0$ for any Q' as a power series.

Our main result about zeros of power series confirms that $I(x)$ has at most $\mathrm{ord}_{\tilde{Q}}\tilde{\omega} + 1$ zeros.

By a previous lemma, we have $\int_Q^{Q'} \omega = 0$ for any Q' which reduces to $\tilde{Q}$ by a previous lemma, i.e., the rational points Q' which reduce to $\tilde{Q}$ are zeros of $I(x)$. But our bound on the zeros of $I(x)$ confirms that there are at most $\mathrm{ord}_{\tilde{Q}}\tilde{\omega} + 1$ such Q' which reduce to $\tilde{Q}$ as desired. □

Theorem 135. *If $p > 2g$, then we have:*

$$|X(\mathbb{Q})| \leq |X(\mathbb{F}_p)| + 2g - 2.$$

Proof. By Riemann-Roch, the total number of zeros of $\tilde{\omega}$ is $2g - 2$. Hence $\sum_{P \in \mathbb{F}_p} \mathrm{ord}_P \tilde{\omega} \leq 2g - 2$.

By the previous lemma, we have that the number of points in $X(\mathbb{Q})$ reducing to P is at most $\mathrm{ord}_{\tilde{P}} + 1$ for every $P \in X(\mathbb{F}_p)$. Hence we have $|X(\mathbb{Q})| \leq \sum_{P \in \mathbb{F}_p} \mathrm{ord}_P\, \tilde{\omega}_P + 1$ since every point in $X(\mathbb{Q})$ reduces to some point in $X(\mathbb{F}_p)$ and then the lemma applies for each such point. Then,

$$\sum_{P\in\overline{\mathbb{F}}_p} \mathrm{ord}_P\ \tilde{\omega}_P + 1 = |X(\mathbb{F}_{|})| + \sum_{P\in\overline{\mathbb{F}}_p} \mathrm{ord}_P\ \tilde{\omega}_P \leq |X(\mathbb{F}_p)| + 2g - 2$$

where the equality simply sums 1 over the points of $\mathbb{F}_p$ and the second is the bound established by Riemann Roch. This shows that there are finitely many rational points on such a curve. □

7 Recent Results

While we won't go into any depth of their methods, it feels pertinent to describe some of the recent results in this active area of research.

Many mathematicians were able to refine Coleman's bound and extend the result to primes of bad reduction. In fact, we have:

Theorem 136 (Stoll [11] Cor. 6.7)**.** *Let $X/\mathbb{Q}$ be a curve of genus $g \geq 2$, let the rank of $J(X)$ be r, and $p > 2g$ be of good reduction. Then we have:*

$$|X(\mathbb{Q})| \leq |X(\mathbb{F}_p)| + 2r.$$

As we required $r < g$, this could be an improvement.

Current efforts seek to find uniform bounds on the number of rational points on curves of genus greater than 1 in terms of the genus.

Theorem 137. *Katz, Rabinoff, Zureick-Brown [6]*
Let $d \geq 1$ and $g \geq 3$ be integers. There exists an explicit constant $N(g, d)$ such that for any number field F of degree d and any smooth, proper, geometrically connected genus g curve X/F where the rank of $J(X)$ is at most $g-3$, we have:

$$|X(F)| \leq N(g, d).$$

For $F = \mathbb{Q}$, we have:

$$N(g, 1) = 84g^2 - 98g + 28.$$

References

References

[1] Claude Chabauty, Sur les points rationnels des courbes algebriques de genre superieur a l'unite, C. R. Acad. Sci. Paris 212 (1941), 882–885 (French).

[2] R. Coleman: *Effective Chabauty*, Duke Math J. **52** (1985), no. 3, 765-770.

[3] R. Coleman: *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111-168.

[4] W. Fulton: *Algebraic Curves: An Introduction to Algebraic Geometry* (2008).

[5] C. Lech: *A Note on Recurring Series*, Arkiv for Mathematik (1953), no. 5, 417-421.

[6] E. Katz, J. Rabinoff, D. Zureick-Brown. *Uniform bounds for the number of rational points on curves of small Mordell-Weil rank.* Duke Math J. Vol 165, No. 16 (2016) 3189-3240.

[7] N. Koblitz: *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Graduate texts in Mathematics, Vol. 58. Springer-Verlag New York (1984).

[8] R. Narasimhan and Y. Nievergelt. Birkhauser: New York (2001).

[9] W. Mccallum, B. Poonen: *The Method of Chabauty and Coleman.*

[10] R. Miranda: *Algebraic Curves and Riemann Surfaces.* Graduate Studies in Mathematics, Volume 5 (1997).

[11] M. Stoll Independence of rational points on twists of a given curve, Compos. Math. 142 (2006), no. 5, 1201–1214.

[12] A. Weil: *Variétés abéliennes et courbes algébriques.* Hermann, Paris (1948)