AMSI VACATIONRESEARCH SCHOLARSHIPS 2020–21

*Get a Thirst for Research this Summer*

# Arithmetic Algebraic Geometry of Curves

Iulian Pavel Stoilescu

Supervised by A/Prof James Borger

Australian National University

Vacation Research Scholarships are funded jointly by the Department of Education, Skills and Employment and the Australian Mathematical Sciences Institute.

**Abstract**

We sketch the large field of arithmetic algebraic geometry, focusing on the simpler case of curves. We build up the commutative algebra theory of Dedekind domains and ideal factorisation, then we talk about the class group and apply it to study the $\mathbb{Z}$ solutions of Diophantine equations. We then proceed to geometry using non-singular complete curves and the theory of valuations. Then we finish with zeta-functions and the Riemann hypothesis over finite field curves.

# 1 Introduction

There exists a series of analogies between algebraic geometry and algebraic number theory. In particular, there are many similarities between the integers and polynomials over finite fields. In Lorenzini's textbook this idea is developed by studying their integral extensions and observing how they can both be understood using the theory of Dedekind domains. The failure of these extensions to be principal is reflected in their ideal class group, and this group assists us in studying Diophantine equations, following Conrad's notes.

Another analogy between these two rings is that we can formulate a Riemann hypothesis for curves over finite fields. This is proved in Lorenzini using the Riemann-Roch theorem and in Hartshorne using the Hodge index theorem, both theorems that originated in the classical algebraic geometry of polynomials.

# 2 Statement of Authorship

None of the results or ideas in this report are original, it is simply a recollection of my readings of the work of innumerably many other authors. I thank Olin Gao for his help spotting a myriad of typos in the original draft.

# 3 Unique Facorisation Domains

Recall that the fundamental theorem of arithmetic states that any integer can be uniquely factorised into primes. For any ring, a prime is any non-unit element such that for all factorisations one factor is a unit.

We call an integral domain an unique factorisation domain (UFD) if any element can be uniquely factored into primes, up to the primes differing by units. Examples include $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-2}]$, and $k[x]$ for any field $k$.

# 4 Dedekind Domains

A integral domain is a Dedekind domain if it's

- integrally closed in its field of fractions (the solution of any monic polynomial in the field of fractions is in the ring)
- of dimension 1 (all non-zero prime ideals are maximal)

- Noetherian

**Theorem 1.** *The integral closure of $\mathbb{Z}$ inside a number field (called a number ring) is a Dedekind domain.*

**Theorem 2.** *The integral closure of $\mathbb{F}_q[x]$ inside a finite extension of $\mathbb{F}_q[x]$ (called a function field) is a Dedekind domain.*

Let $K$ be a finite extension of $\mathbb{Q}$ or $k(x)$ then $\mathcal{O}_k$ is defined to be the integral closure of $\mathbb{Z}$ or $k[x]$ in $K$, respectively.

**Theorem 3.** *If $I' \subset I$ are ideals of a Dedekind domain $A$ then there exists a unique ideal $J$ such that $IJ = I'$.*

*Proof.* It suffices to show it in the case that $I$ is a prime ideal $P$. Suppose that $IJ \subset P$, then $I \subset P$ or $J \subset P$; since otherwise we have $x \in P \backslash I$ and $y \in P \backslash J$ but then $xy \in IJ$ so is also in $P$, contradicting primality. The proof then proceeds by induction on the number of primes in the factorisation of $I'$ counting multiplicity. □

**Theorem 4.** *Let $d \in \mathbb{N} \backslash \{1, 3\}$, then the units of $\mathcal{O}_{\mathbb{Q}[\sqrt{-d}]}$ are $\{\pm 1\}$.*

## 5 Ideal Factorisation

**Theorem 5.** *Dedekind domains have the property that any ideal factorises uniquely into the product of prime ideals.*

The number ring associated to $\mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[(1+\sqrt{d})/2) & if\ d \equiv 1\ (mod 4) \\ \mathbb{Z}[\sqrt{d}] & otherwise. \end{cases}$$

As an example of factorisation into primes in the number ring $\mathbb{Z}[(1+\sqrt{-51})/2]$ we have that

$$\begin{aligned} (2) &\text{ is prime,} \\ (5) = (5, \sqrt{-51}+5)&(5, \sqrt{-51}-5), \\ (51) &= (\sqrt{-51})^2. \end{aligned}$$

## 6 Ideal Class Group

Let $M$ be the monoid of non-zero ideals of an integral domain $R$. We define an equivalence class on $M$ by defining $I \sim J$ if there exists $\alpha, \beta \in R$ such that $(\alpha)I = (\beta)J$.

**Theorem 6.** *This is an equivalence relation.*

**Theorem 7.** *Multiplication gives a well-defined operation on this equivalence relation*

**Theorem 8.** *If $R$ is a Dedekind domain then the monoid of the equivalence classes form a group.*

*Proof.* We need to prove that there are inverses in our monoid. Given $I \in M$ we need to find an $J \in M$ such that $IJ \sim (1)$. Let $\alpha \in I$ be a non-zero element, then by theorem 3 there exists a $J$ such that $IJ = (\alpha)$, hence by transitivity $IJ \sim (1)$. □

*We denote the class group of $R$ by $Cl(R)$.*

**Theorem 9.** *$R$ is a PID iff its class group is trivial.*

*Proof.* Suppose $R$ is a PID, then for any ideal $I$, there exists a $\alpha \in R$ such that $I = (\alpha)$, but then $(\alpha)(1) = (1)(\alpha)$ so $I \sim (1)$, meaning that the class group is trivial.

Now suppose that the class group is trivial, then for any ideal $I$, $I \sim (1)$; but this means that there exists $\alpha, \beta \in R$ such that $(\alpha)I = (\beta)$. Hence there exists a $\gamma \in I$ such that $\alpha\gamma = \beta$. But then $(\alpha)I = (\alpha)(\gamma)$, so unique factorisation into prime ideals implies that $I = (\gamma)$. Therefore $R$ is a PID. □

We can calculate the "size" of an ideal in a ring a norm on ideals, called so because of the multiplicative property it posesses. It turns out that in the integral closure $A$ of any of the aforementioned fields, quotients by non-zero ideals are finite, hence we may define, for any non-zero ideal $I$

$$\|I\|_A = |A/I|.$$

**Theorem 10.** *There exists a $\lambda \in R$ such that all elements of the ideal class group can be represented by ideals $I$ such that $\|I\|_{\mathcal{O}_K} < \lambda$*

*Proof.* When $K$ is the number field there exits a number called the discriminant $d_K$, where if $\mathbb{Q}(\sqrt{d})$ and $d$ is a squarefree integer then $d_K = d$. If $\{a_i\}$ are a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and $\{\sigma_i\}$ the elements of $Gal(K/\mathbb{Q})$. Then we define it to be the square of

$$\det \begin{pmatrix} \sigma_1(a_1) & \dots & \sigma_1(a_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(a_1) & \dots & \sigma_n(a_n) \end{pmatrix}$$

Then there is the following bound, due to Minkowski,

$$\lambda := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{d_k}.$$

Where $r_2$ is the number of pairs of embeddings $K \to \mathbb{C}$ where the image is not strictly real and two embedding are considered part of a pair if they are conjugates of each other.

There also exists a bound for function fields over finite fields. □

**Theorem 11.** *The ideal class group of $\mathcal{O}_K$ is finite.*

*Proof.* This is a consequence of the previous theorem and the fact that $\mathcal{O}_K$ is Noetherian. □

The cardinality of the class group of $\mathcal{O}_K$ where $K$ is a number or function field is referred to as the class number of the $K$.

**Theorem 12.** *Let $d$ be the product of $n$ distinct primes. Then there is a subgroup of $Cl(\mathcal{O}_K)$ isomorphic to $(\mathbb{Z}/2)^{n-1}$, where $K = \mathbb{Q}(\sqrt{-d})$.*

*Proof.* Suppose that $\{p_i\}$ are the prime factors of $d$. We will show that $(p_i, \sqrt{-d})$ generate the desired subgroup. Note that $(p_i, \sqrt{-d})^2 = (p_i^2, p_i\sqrt{-d}, -d)$, but because $d$ is the product of distinct primes $\gcd(p_i, d) = p_i$, so $(p_i, \sqrt{-d})^2 = (p_i)$ is a principal ideal. Now we will show that

$$\prod_i (p_i, \sqrt{-d}) = (\sqrt{-d}).$$

Note that if we take the product of the generators of our ideals on the left, all are divisible by $\sqrt{-d}$, so the left ideal includes into the right one. Now we will show that the left ideal contains $\sqrt{-d}$: without loss of generality we may assume $n \geq 2$, hence we observe that (because the primes are distinct)

$$gcd(d/p_1, d/p_2, \ldots, d/p_n) = 1$$

hence since we have $d/p_1\sqrt{-d}, d/p_2\sqrt{-d}, \ldots, d/p_n\sqrt{-d}$ as products of generators we have that the $\mathbb{Z}$-linear combination $\sqrt{-d}$ in in our product ideal.

Now we will show that if $I \subsetneq \{1, \ldots, n\}$ is proper and non-empty, then $\prod_{i\in I}(p_i, \sqrt{-d})$ is non-principal. Suppose that it is principal, let it be generated by $\alpha \in \mathcal{O}_K$. Then there exists $a, b \in \mathbb{Z}$ such that

$$\alpha = \frac{a + b\sqrt{-d}}{2}$$

Then $(\alpha^2) = (\prod_{i\in I} p_i)$ by our previous calculation of the squares of our ideals. Since theorem 4 we know that our two principal generators differ by $\{\pm 1\}$, hence $|\alpha^2| = \prod_{i\in I} p_i$ (this line of attack can be generalised to the theory of norms, which we omit for brevity). But

$$|\alpha^2| = \frac{a^2 + b^d}{4}$$

so we have that $a^2 + bd^2 = 4\prod_{i\in I} p_i$. Now observe that $a^2 | \prod_{i\in I} p_i$, but because the latter is squarefree we have that $a | \prod_{i\in I} p_i$. This implies that $\prod_{i\in I} p_i + p_j \leq 4$ where $p_j \notin I$. Now if $p_j$ is odd then we have a contradiction since $p_j \geq 3$ and $\prod_{i\in I} p_i \geq 2$. Otherwise $p_j = 2$, so since our primes are distinct $\prod_{i\in I} p_i \geq 3$, leading to another contradiction. Hence the our ideal is non-principal, meaning it doesn't represent the trivial element in the class group.

Thus we can construct the following exact sequence

$$0 \to \mathbb{Z}/2 \to (\mathbb{Z}/2)^n \to Cl(\mathcal{O}_K)$$

meaning that the kernel of the $(\mathbb{Z}/2)^n \to Cl(\mathcal{O}_K)$ map sending $I$ (identifying subsets of $\{1, \ldots, n\}$ with elements of the domain) to the equivalence class of $\prod_{i\in I}(p_i, \sqrt{-d})$ has kernel $I = \{\phi, \{1, \ldots, n\}\}$. But this means that the image of this map is a subgroup isomorphic to $(\mathbb{Z}/2)^{n-1}$. □

**Theorem 13.** *The class number of* $\mathbb{Q}(\sqrt{-51})$ *is 2.*

*Proof.* Note that the Minkowski bound of $\mathbb{Q}(\sqrt{-51})$ is less than 8. Hence the factors in the following ideals generate the class group, because the norm of a prime ideal in the factorisation of a prime number of $\mathbb{Z}$ is a power of that prime.

$$(2) \text{ is prime}$$
$$(3) = (3, \sqrt{-51})^2$$
$$(5) = \left(5, 2+\sqrt{-51}\right)\left(5, 2-\sqrt{-51}\right)$$
$$(7) \text{ is prime}$$

Hence to show that the class group is isomorphic to $\mathbb{Z}/2$, by theorem 12 (since 51=3*17) it suffices to show that the three non-principal primes appearing in our factorisations are in the same equivalence class. Now observe that

$$\left(\frac{3+\sqrt{-51}}{2}\right)\left(\frac{3-\sqrt{-51}}{2}\right) = (15) = (5)(3) = (3, \sqrt{-51})\left(5, 2+\sqrt{-51}\right)(3, \sqrt{-51})\left(5, 2-\sqrt{-51}\right)$$

Because we have that the conjugate ideal of $\left(\frac{3+\sqrt{-51}}{2}\right)$ is $\left(\frac{3-\sqrt{-51}}{2}\right)$, and these are distinct ideals, we must have that

$$\left(\frac{3+\sqrt{-51}}{2}\right) = (3, \sqrt{-51})\left(5, 2+\sqrt{-51}\right), \quad \left(\frac{3-\sqrt{-51}}{2}\right) = (3, \sqrt{-51})\left(5, 2-\sqrt{-51}\right)$$

or vice versa (the first ideal equal to the fourth and the third equal to the the second). But this implies that $(3, \sqrt{-51}) \sim \left(5, 2+\sqrt{-51}\right)$ and $(3, \sqrt{-51}) \sim \left(5, 2-\sqrt{-51}\right)$ since our ideals have 2-torsion in the ideal class group. Therefore we only have one equivalence class of non-principal ideal. Note that if the equalities were the other way around we could perform the same argument. Therefore the class group of $\mathbb{Z}[(1+\sqrt{-51})/2]$ is $\mathbb{Z}/2$, so the class number of its field of fractions is 2. □

## 7 Diophantine Applications

Since Fermat number theorists have been studying the integer solutions $(x, y)$ to

$$x^3 + k = y^2$$

for some $k \in \mathbb{Z}$.

By rearranging and factoring we see that this is equivalent to

$$x^3 = (y - \sqrt{k})(y + \sqrt{k})$$

Hence, by studying rings which contain $\mathbb{Z}[\sqrt{k}]$ we may obtain information about integer solutions.

**Theorem 14.** *If* $(x, y)$ *was a solution for* $k = -2$, $(y \pm \sqrt{-2})$ *would be coprime.*

*Proof.* First, note that $y$ cannot be even, since this would imply $x$ is even but 2 is not a square mod 8. Now suppose, for a contradiction, that $p$ is a common prime divisor, then $p$ divides their difference, which is $2\sqrt{-2}$. But then WLOG $p = \sqrt{-2}$ which implies that $\sqrt{-2} \mid y$, so y is even, a contradiction. □

**Theorem 15.** *When $k = -2$ the equation has no solutions.*

*Proof.* Suppose that we have $x, y \in \mathbb{Z}$ such that $x^3 = (y - \sqrt{-2})(y + \sqrt{-2})$. By our previous theorem our factors are coprime, so since $Z[\sqrt{-2}]$ is an UFD and all of our units are cubes (by theorem 4, $\{y \pm \sqrt{-2}\}$ are cubes. Let $a, b \in \mathbb{Z}$ such that $y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 - 6ab + (3a^2b - 2b^2)\sqrt{-2}$. But by $\mathbb{Z}$-linear independence we have that $1 = 3a^2b - 2b^2$, which implies that $a^2 = b^2 = 1$, but beacuse $y = a^3 - 6ab$ we have a contradiction. □

It turns out $\mathcal{O}_{\mathbb{Q}(\sqrt{-k})}$ is not a UFD for large $k$. But we can generalise our argument using unique factorisation of prime ideals.

**Theorem 16.** *When $k = -51$, $x^3 + k = y^2$ has no integer solutions.*

*Proof.* Let us assume that $x, y \in \mathbb{Z}$ is a solution. Since -51 is not a square mod 8, as before, we see that x must be odd. Similarly, $gcd(51, x) = 1$. We will show that the ideals $\{(y \pm \sqrt{-51})\}$ of $\mathbb{Z}[(1 + \sqrt{-51})/2]$ are coprime, suppose that there is a common prime ideal factor $\varphi$ (equivalent to containing both ideals). Then $\varphi$ contains $2\sqrt{-51}$, which means that $\varphi$ divides $(2)(\sqrt{-51})$. But since these are both prime ideals, by unique factorisation we have that $\varphi$ equals one of the two. But this implies that $x$ is even or divisible by 51, contradicting our previous observations.

Hence, because $(x)^3 = (y + \sqrt{-51})(y - \sqrt{-51})$ as ideals we have that $\{(y \pm \sqrt{-51})\}$ are the cubes of ideals. However since our class number is 2, we can deduce that these ideals are principal. And since our only units are $\{\pm 1\}$, we have that $\{y \pm \sqrt{-51}\}$ are cubes. Hence we have $a, b \in \mathbb{Z}$ such that $y - 1 + 2(1 + \sqrt{-51})/2 = (a + b(1 + \sqrt{-51})/2)^3$, from which we can obtain a contradiction. □

# 8 Valuations

Let L be a field. Then a (integer valued) valuation of $L$ is a group homomorphism $L^* \to \mathbb{Z}$ satisfying the inequality $v(x + y) \geq \min(v(x), v(y))$.

## 8.1 Examples

1. Trivial valuations

   The zero map $L^* \to \mathbb{Z}$ is called the trivial valuation of $L$.

2. $p$-adic valuations

   Let $p \in \mathbb{Z}$ be a prime, then we define the $p$-adic valuation, $v_p : \mathbb{Q}^* \to \mathbb{Z}$ by $v_p(x) = ord_p(x)$ where the order of $x$ at $p$ is the exponent of p in the unique factorisation of $x$ into the product of integer powers of distinct primes, up to a sign.

Now we will generalise this valuation to an arbitrary Dedekind domain.

3. $P$-adic valuations Let L be any field which is the field of fractions of a integral domain $R$ which has the property of unique factorisation of prime ideals (e.g. a Dedekind domain), and let $P$ be a prime ideal of $R$. Then we define the $P$-adic valuation $v_P : L^* \to \mathbb{Z}$, first on $R\{0\}$ as $v_P(x) = ord_P((x))$, i.e. the power of $P$ of the factorisation of $(x)$ into prime ideals. This uniquely extends to $L^*$ since valuations the homomorphisms, more precisely for any $x \in L^*$ there exists $a, b \in R\backslash\{0\}$ such that $x = a/b$, and we define $v_P(x) = v_P(a) - v_P(b)$. This is well defined since if $a/b = a'/b'$ then $ab' - a'b = 0$, which by the homomorphism property of $v_P$ means that $v_P(a) + v_P(b') = v_P(a') + v_P(b)$.

4. Let $L = k(x)$ for any field k, then any element $a \in L$ can be represented as $f(x)/g(x)$ for some $f(x), g(x) \in k[x]$. Hence, we can define $v_\infty(a) = \deg(f) - \deg(g)$.

5. Order of a zero/pole valuation

   Let $L$ be the field of meromorphic functions on a Riemann surface $X$, then for any $P \in X$ and $x \in L^*$, $v_P(x)$ is defined to be the order of zero or pole of $x$ at $P$, where poles are negative and zeros postitive.

## 9 Non-Singular Complete Curves

Let $\mathcal{V}(L/k)$ denote the surjective valuations of $L$ that restrict to the trivial extension on $k$. We will give $\mathcal{V}(L/k)$ the structure of a curve.

Let us first endow $\mathcal{V}(L/k)$ with the cofinite topology, meaning that the closed sets are the finite subsets and the whole set. We give it a sheaf structure. for any $P \in X$, represented by the valuation $v \in \mathcal{V}(L/k)$ let us define the discrete valuation rings to be the subring with nonnegative valuation at P

$$\mathcal{O}_P := \{x \in L^* | v(x) \geq 0\} \cup \{0\}$$

For any open set $U$ we define the sections at U to be $\mathcal{O}(U) = \cap_{P \in U} \mathcal{O}_P$. As seen in our example we have a valuation $L^*$ for every prime ideal of a subring which is a Dedekind domain whose field of fractions is $L$, if this subring contains $k$, then any ideal generated by an element of $k^*$ will generate the unit ideal, the trivial product of ideals. Hence, for any Dedekind domain A where $k \subset A \subset L$ and such that the field of fractions of $A$ is $L$ we have a function $Max(A) \to V(L/k)$. This is an injection, we will prove this when the class group is purely torsion, since then if $P \in Max(A)$ then there exists a $n \in \mathbb{N}$ and a $\alpha \in L^*$ such that $P^n = (\alpha)$ hence $v_Q(\alpha) = n$ if $Q = P$ and 0 otherwise.

We call a curve non-singular if its local rings are PIDs.

**Theorem 17.** *Let $v \in \mathcal{V}(L/k)$, then $\mathcal{O}_v$ is a PID.*

*Proof.* Let $x \in \mathcal{O}_v$ be such that $v(x) = 1$. Then for any $\alpha \in \mathcal{O}_v$ there exists a $n \in \mathbb{N}$ such that $v(\alpha/x^n) = 0$, hence $\alpha/x^n \in \mathcal{O}_v^*$. This $n$ must be the value of $v(\alpha)$ and hence is unique. Thus any element of $\mathcal{O}_v$ can be uniquely expressed as the product of a unit and a power of x. Hence, any non-zero ideal $I$ is equal to $(x^n)$,

where $n$ is the minimal power of x in the factorisation of all the non-zero elements of $I$. Therefore $\mathcal{O}_v$ is a PID. □

Therefore $\mathcal{V}(L/k)$ is a non-singular curve.

The non-singular complete curve associated with $k(x)/k$ is isomorphic to $\mathbb{P}^1(k)$. Note that $v_\infty$ corresponds to the point at infinity. Also, for a homogeneous polynomial $F$ in three variables with the projective curve $X_F(k)$ being non-singular, with dehomogenisation $f$ we have that the curve $\mathcal{V}(K/k)$ is isomorphic to $X_F(k)$ where $K$ is the field of fractions of $k[x,y]/(f)$. We call $V(K/k)$ complete since it completes the affine curve by adding the point at infinity. Note that if we look at the non-singular complete curve corresponding to the function field of a singular curve then we get a resolution of singularities of our curve.

## 10 Zeta-functions

Recall that the Riemann zeta function is the meromorphic function defined by the analytic continuation of the following series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It can be shown that for all $n \in \mathbb{N}$, $-2n$ is a zero. The Riemann hypothesis is then the conjecture that all other zeros are contained in the line $\{z \mid \mathrm{Re}(z) = 1/2\}$. Now, the well-known Euler product formula says

$$\zeta(s) = \prod_{p \ prime} \frac{1}{1-p^{-s}}.$$

For any ring $A$ where quotients by maximal ideals are finite, we can generalise this formula using the set of maximal ideals $Max(A)$

$$\zeta(A,s) := \prod_{M \in Max(A)} \frac{1}{1-\|M\|^{-s}}$$

Note that letting $A = \mathbb{Z}$ recovers the Riemann zeta function. Let $f \in \mathbb{F}_q[x_0, x_1]$ be a non-zero, absolutely irreducible (irreducible over the algebraic closure of the field of coefficients) polynomial.

**Theorem 18.** *The coefficient of $n^{-s}$ of the series expansion of $\zeta(\mathbb{F}_q[x_0,x_1]/(f),s)$ is zero unless $n$ is a power of $q$. Hence, if we let $T = q^{-s}$ we get a power series in $T$. Then the coefficient of $T^m$ is the number of points with $\mathbb{F}_{q^m}$ coefficients in the affine plane curve defined by $f$, divided by $m$.*

Let $F \in \mathbb{F}_q[X_0, X_1, X_2]$ be a non-zero, absolutely irreducible (irreducible over the algebraic closure of the field of coefficients), homogenous polynomial. This defines a curve in projective space with $\mathbb{F}_{q^n}$ coefficients for all $n \in \mathbb{N}$. Now let this curve by denoted by $X_F(\mathbb{F}_{q^n})$. We then define $N_n := |X_F(\mathbb{F}_{q^n})|$. The previous theorem then prompts us to define the zeta function of the curve $X_F/\mathbb{F}_q$ as the formal power series

$$Z(X_F/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} N_n/n \ T^n\right).$$

The reason for post-composing the previous zeta functions with a exponential will become clear in the next section, where we show that our new zeta function is a rational function.

## 11 Riemann Hypothesis

We will generalise the Riemann hypothesis for curves over finite fields, and show that this gives us a non-trivial bound on the number of points on such curves defined over a finite field extension of the field of coefficients. This is analogous to how the Riemann zeta function gives us bounds on the number of primes (both are points of schemes).

Suppose $T = q^{-s}$, then since the Riemann hypothesis (another formulation, obviously equivalent) says if $0 \leq \mathrm{Re}(s) \leq 1$, $\zeta(s) = 0$ only if $\mathrm{Re}(z) = 1/2$, if we assume the same property for $Z(q^{-s})$ this would imply that if $Z(q^{-s})$ and $1/q \leq q^{-\mathrm{Re}(s)} \leq 1$ then $q^{-} = q^{-1/2}$. But since $q^{-} = |q^{-s}|$, this implies that for any zero $T \in \mathbb{C}$ with $1/q \leq |T| \leq 1$, $|T| = 1/\sqrt{q}$.

Let $F' \in \mathcal{O}_K[X_0, \ldots X_2]$ reduce to $F$ by modding out by some prime ideal, where $K$ is a number field. Then if we choose an embedding $K \to \mathbb{C}$ we get a Riemann surface. Using algebraic topology we can compute its genus, the number of "holes". It turns out that this number does not depend on the representative $F'$ or the embedding of $K$ into $\mathbb{C}$. Note that we could alternatively define genus via an obfuscating elementary method or sheaf cohomology, they would all give the same integer. Also using the Riemann-Roch theorem we can show that if $F$ is of degree $d$, and the genus is $g$ then

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

**Theorem 19.** *Let $g$ be the genus of $X_F/\mathbb{F}_q$. There exists a polynomial $f(T) \in \mathbb{Z}[T]$ of degree $2g$ such that*

$$Z(X_F/\mathbb{F}_q, T) = \frac{f(T)}{(1-T)(1-qT)}.$$

*Thus $Z(X_F/\mathbb{F}_q, T)$ is a rational function in $\mathbb{Z}(T)$ with $2g$ zeros (counting multiplicity) and 2 poles.*

Using this rational expression we can obtain the following functional equation

**Theorem 20.**

$$Z(1/qT) = (qT^2)^{1-g} Z(T)$$

Now our previous Riemann hypothesis is equivalent to the following stronger Riemann hypothesis

**Theorem 21.** *Suppose that for some $T \in \mathbb{C}$ $Z(X/\mathbb{F}_q, T) = 0$, then $|T| = 1/\sqrt{q}$.*

*Proof.* The Riemann hypothesis for curves over finite fields was originally proven by Andre Weil using abeilian varieties. The most elementary proof is due to Bombieri and only uses the Riemann-Roch theorem. There also exists a elegant proof using the Hodge Index Theorem which can be found as an exercise in Hartshorne's textbook. □

It is easy to see that the number of points on a projective line defined over $\mathbb{F}_q$ is $q + 1$. Now the Riemann hypothesis is equivalent to the following bound on how the number of points on an plane projective curve differ from the number of points on a projective line

**Theorem 22.** *Let $X/\mathbb{F}_q$ be defined by the aforementioned $F$, and suppose it has genus $g$. Then*

$$|N_n - (q^n + 1)| \leq 2g\sqrt{q^n}.$$

## 12 Discussion and Conclusion

We can just as easily state the Riemann Hypothesis for varieties over finite fields; this and the other properties of the zeta-functions are called the Weil conjectures, however the proofs are much harder than in the curve case. Grothendieck developed étale cohomology to prove the rationality of the zeta-function (Dwork proved rationality first, using $p$-adic analysis) and the functional equation, he then made a series of general conjecture, the standard conjectures on algebraic cycles, which would imply the Riemann hypothesis. However, his student Deligne proved the Riemann hypothesis, bypassing the standard conjectures. The standard conjectures remain open to this day.

## 13 References

Dini Lorenzini. *An Invitation to Arithmetic Geometry.* American Mathematical Society, 1997.

Robin Hartshorne *Algebraic Geometry.* Springer, 1977.

Ravi Vakil. *Foundations of Algebraic Geometry.* 2017.
http://math.stanford.edu/ vakil/216blog/FOAGnov1817public

Brian Conrad. *Diophantine applications of class groups.*
http://virtualmath1.stanford.edu/ conrad/154Page/handouts/unitPicex.pdf