# Riemann Hypothesis for curves

Sasha Yom Din

June 23, 2014

## 1 Warning

There might be errors, inaccuracies, and unpleasancies in the following text. I will be happy if you let me know about it.

## 2 Convention

Whenever we say "nice variety over $F$", we mean a geometrically connected, smooth and projective scheme over $F$.

## 3 The problem

Let $k_0$ be a finite field with $q = |k_0|$ elements. We will denote $k_0^n$ an exetnsion field of $k_0$ with $q^n$ elements. Let $X_0$ be a nice curve over $k_0$, of genus $g$.

We let $a_n$ $(n \geq 0)$ be the number of effective divisors of degree $n$ on $X_0$. That is, formal non-negative integer combinations of closed points of the scheme $X_0$, $\sum c_p \cdot p$, such that $\sum c_p[\kappa(p) : k_0] = n$. We let $b_n$ $(n \geq 1)$ be the number of points of $X_0$ with values in $k_0^n$. That is, $b_n = |X_0(k_0^n)|$.

We define the zeta series:

$$z = \sum_{n \geq 0} a_n t^n.$$

Then we have also (Euler product formula):

$$z = \prod_p \frac{1}{1 - t^{[\kappa(p):k_0]}}$$

where the product runs over closed points $p$ of the scheme $X_0$. Also, it is easy to calculate:

$$t \cdot dlog(z) = \sum_{n \geq 1} b_n t^n.$$

Using Riemann-Roch formula, it is not hard to find that $z$ has the following form:

$$z = \frac{p}{(1-t)(1-qt)}$$

where $p$ is a polynomial whose free coefficient is 1, and which is of degree $\leq 2g$. Let us interpret $p$ as a polynomial over the complex numbers, and decompose $p = \prod_i (1 - \alpha_i t)$. We remark that it is possible to show using Serre duality that $\alpha \mapsto q/\alpha$ preserves the set of $\alpha_i$'s. We can calculate:

$$t \cdot dlog(z) = \sum_{n \geq 1} (1 + q^n + \sum_i \alpha_i^n) t^n.$$

The Riemann hypothesis for curves over finite fields then says:

**Theorem 3.1.** *The two following equivalent statments do hold:*

- *We have $|\alpha_i| = q^{1/2}$ for all $i$.*
- *We have $b_n = q^n + O(q^{n/2})$.*

The equivalence between the two statements is elementary, but one needs to use the fact mentioned above, that $\alpha \mapsto q/\alpha$ preserves the set of $\alpha_i$'s.

Actually, a slightly better statement can be made:

**Theorem 3.2.** *We have $|b_n - (1 + q^n)| \leq 2gq^{n/2}$.*

We will prove in this text the Riemann hypothesis for curves over finite fields, using intersection theory on the square of the curve.

# 4 Intersection theory on surfaces

## 4.1 Divisors

Let $S$ be a nice variety over an algebraically closed field $k$. We denote by $k(S)$ the function field of $S$ (i.e. the stalk of the structure sheaf at the generic point). We recall that smoothness implies that for $p \in |S|$ of codimension one (we write $p \in |S|^1$), $\mathcal{O}_{S,p}$ is a discrete valuation ring (DVR).

We will offer several descriptions of the divisor class group $Cl(S)$.

### 4.1.1 first description

By a prime divisor on $S$ we will mean a point of $|S|$ of codimension one. Those are in bijection with closed and integral subschemes of $S$ of codimension one.

We denote by $Div(S)$ the free abelian group generated by the prime divisors on $S$. It has a positive structure - divisors all of whose coefficients are non-negative are called effective.

We have a morphism $k(S)^\times \to Div(S)$, given as follows: For a function $f \in k(S)^\times$ and a prime divisor $p \in |S|^1$, we can consider $f$ as an element in the fraction field $k(S)$ of the DVR $\mathcal{O}_{S,p}$, and so take its valuation. I.e., $f \mapsto \sum_{p \in |S|^1} v_p(f) \cdot p$.

The image of the morphism above is said to consist of princiapl divisors. We will denote the cokernel of this morphism by $Cl(S)$ (divisor class group).

### 4.1.2 second description

Let $\mathcal{M}$ be a coherent sheaf on $S$, whose support is not $|S|$. Then $M_p$ is a finite-length $\mathcal{O}_{S,p}$-module, for every $p \in |S|^1$. Hence, we get a (effective) divisor by associating to each $p \in |S|^1$ the length of $M_p$. This construction gives in fact a morphism $K_0(Coh_S^{\leqq 1}/Coh_S^{<1}) \to Div(S)$, where $Coh_S^{\leqq 1}$ is the abelian category of coherent sheaves on $S$ whose support is not $|S|$ and $Coh_S^{<1}$ is the Serre subcategory of $Coh_S^{\leqq 1}$ consisting of coherent sheaves whose stalks at points of $|S|^1$ are zero. One can see that this morphism is an isomorphism. This gives another description of divisors.

In this picture, the morphism $k(S)^\times \to K_0(Coh_S^{\leqq 1}/Coh_S^{<1})$ can be described locally (on affines) by sending a regular function $f$ to $\mathcal{O}/(f)$, and one can extend this definition to non-affines by gluing.

Via this description, we see that given a closed subscheme of $S$, which is not equal to $S$, we get naturally a (effective) disivor; Consider the structure sheaf of this subscheme as a coherent sheaf on $S$. Of course, this is compatible with the identification with the first description, when prime divisors are considered as closed integral subschemes.

### 4.1.3 third description

The morphism above $k(S)^\times \to Div(S)$ can be naturally sheafified (considered as a morphism between obvious sheaf versions). It then gives rise to an isomorphism $\Gamma(k(S)^\times/\mathcal{O}_S^\times) \to Div(S)$. The principal divisor morphism is then interpreted as $\Gamma(k(S)^\times) \to \Gamma(k(S)^\times/\mathcal{O}_S^\times)$. Thus, it is easy to see that $Cl(S)$ is then identified with $H^1(S, \mathcal{O}_S^\times)$.

### 4.1.4 fourth description

Inspired by the third description, we recall that $H^1(S, \mathcal{O}_S^\times)$ classifies line bundles on $S$. How to describe divisors in this geometric language? Consider the symmetric monoidal groupoid $\mathcal{P}ic(S)$ of line bundles on $S$, and the symmetric monoidal groupoid $\mathcal{P}ic_{rigid}(S)$ of line bundles on $S$, together with a fixed non-zero rational section. We have a forgetful morphism $\mathcal{P}ic_{rigid}(S) \to \mathcal{P}ic(S)$. Then it is easy to see that he have isomorphisms of abelian groups $\pi_0(\mathcal{P}ic_{rigid}) \to Div(S)$ and $\pi_0(\mathcal{P}ic) \to Cl(S)$, such that the forgetful morphism corresponds to the canonical projection $Div(S) \to Cl(S)$.

## 4.2 Pull and Push

Here, we consider nice varieties $S, T$ and a finite surjective morphism $\phi : S \to T$.

Consider a point $q \in |S|^1$. Then $\phi(q) \in |T|^1$. We define $e(q)$ as the length of the $\mathcal{O}_{S,q}$-module $\mathcal{O}_{S,q}/\mathcal{O}_{S,q}\mathfrak{m}_{T,\phi(q)}$. Also, we define $f(q)$ as $[\kappa(q) : \kappa(\phi(q))]$. It is known that for every $p \in |T|^1$, $\sum_{\phi(q)=p} e(q)f(q) = [k(S) : k(T)]$.

### 4.2.1 pull

We define $\phi^* : Div(T) \to Div(S)$ on prime divisors by $\phi^*(p) = \sum_{\phi(q)=p} e(q) \cdot q$ , and extend by additivity.

This factors through to give $\phi^* : Cl(T) \to Cl(S)$. How does it look in the different interpretations?

In the second one, it is given by pullback of coherent sheaves. In the third one, it is given by pullback of functions. In the fourth one, it is given by pulback of line bundles.

### 4.2.2 push

We define $\phi_* : Div(S) \to Div(T)$ on prime divisors by $\phi_*(q) = f(q) \cdot \phi(q)$, and extend by additivity.

This factors through to give $\phi_* : Cl(S) \to Cl(T)$. How does it look in the different interpretations?

In the second one, it is given by pushforward of coherent sheaves. In the third one, it is given by the norm map in field extensions. In the fourth one? I stil did not figure out completely.

### 4.2.3 monad

The following property holds: $\phi_*\phi^* : Div(T) \to Div(T)$ is equal to multiplication by $[k(S) : k(T)]$.

## 4.3 Intersection pairing

### 4.3.1 characterization

We assume here that $S$ is a nice surface over an algebraically closed field $k$. We want to characterize a symmetric biadditive pairing $(\cdot, \cdot) : Cl(S) \times Cl(S) \to \mathbb{Z}$, called the intersection pairing, in different ways.

In the first description: Let $C, D$ be simple divisors on $S$ (considered as closed integral curves). Assume that $C$ and $D$ intersect transversally. This means that the intersection is zero-dimensional, and at every point of the intersection, local equations of $C$ and $D$ generate the ideal of local vanishing functions at that point. Then $(C, D)$ is equal to the number of intersection points of $C$ and $D$.

In the second description: Let $\mathcal{M}_1, \mathcal{M}_2 \in Coh_S^{\leq 1}$. Assume that $\mathcal{M}_1 \otimes_{\mathcal{O}_S} \mathcal{M}_2 \in Coh_S^{\leq 1}$. Then $(\mathcal{M}_1, \mathcal{M}_2) = dim\Gamma(S, \mathcal{M}_1 \otimes_{\mathcal{O}_S} \mathcal{M}_2)$. In particular, this includes information about how to count intersection of curves which intersect non-transversally (but zero-dimensionally).

In the third description: I still did not figure out completely.

In the fourth description: Let $\mathcal{L}_1, \mathcal{L}_2$ be two line bundles on $S$. Then $(\mathcal{L}_1, \mathcal{L}_2) = \chi(\mathcal{O}_S) - \chi(\mathcal{L}_1^{-1}) - \chi(\mathcal{L}_2^{-1}) + \chi(\mathcal{L}_1^{-1} \otimes_{\mathcal{O}_S} \mathcal{L}_2^{-1})$.

We also have some "mixed" characterizations. The intersection of a line bundle and a simple divisor, for example, can be calculated as the degree of the pullback of the line bundle to the divisor, considered as a nice curve. As an application of that, let $X$ be a nice curve and $S = X \times X$. Then we claim that $(\Delta, \Delta) = 2\chi(X)$, where $\Delta$ is the diagonal in $S$ (a simple divisor), and $\chi(X)$ is the algebraic Euler characteristic of $X$ (the dimension of the space of regular differential forms). Indeed, $\mathcal{O}_S(-\Delta)$ restricts to the sheaf of differentials on $\Delta$, and so $(-\Delta, \Delta) = deg(\Omega_X) = -2\chi(X)$.

#### 4.3.2 ample divisors

Let $D \in Div(S)$ be a very ample divisor. This means that for some embedding of $S$ into projective space, $D$ is the (scheme-theoretical) intersection of some hyperplane with $S$. Then $D$ is "very" positive - for every non-zero effective divisor $E$, we have $(D, E) > 0$ (in particular, $(D, D) > 0$). This is not hard to understand, as most hyperplanes do not contain $E$, so intersect $E$ properly (i.e. with zero-dimensional intersection), and the result follows.

#### 4.3.3 Hodge index theorem

Consider the subgroup $Cl_{num\sim 0}(S) \subset Cl(S)$ which is the kernel of the intersection pairing. Write $Cl_{num}(S) = Cl(S)/Cl_{num\sim 0}(S)$. Finally, set $\mathcal{H}_S = \mathbb{Q} \otimes_{\mathbb{Z}} Cl_{num}(S)$. Thus, $\mathcal{H}_S$ is a vector space over $\mathbb{Q}$, which admits a non-degenerate symmetric bilinear pairing $(\cdot, \cdot)$.

The Hodge Index theorem claims that the positive index of $\mathcal{H}_S$ is 1. This means that there exists $v$ such that $(v, v) > 0$ and $(w, w) \leq 0$ for every $w$ such that $(v, w) = 0$. It then follows that for every $v$ such that $(v, v) > 0$ we have $(w, w) \leq 0$ for every $w$ such that $(v, w) = 0$.

Let us see how to establish it. Fix a very ample divisor $D$ (recall that $(D, D) > 0$), and let $E$ be a divisor such that $(E, E) > 0$. It will be enough to show that $(D, E) \neq 0$. The Riemann-Roch theorem for surfaces tells us that, since $(E, E) > 0$, $\chi(nE)$ tends to $+\infty$ as $n$ tends to $+\infty$. As $\chi(nE) = h^0(nE) - h^1(nE) + h^2(nE)$, this implies that either $h^0(nE) > 0$ for arbitrarly big $n > 0$, or $h^2(nE) > 0$ for arbitrarly big $n > 0$. In the first case, $nE$ will be equivalent to an effective divisor, and hence $(D, nE) > 0$, which implies $(D, E) > 0$. In the second case, recalling $h^2(nE) = h^0(K - nE)$, $K - nE$ will be equivalent to an affective divisor, and hence $(D, K - nE) > 0$, which implies (taking $n$ big) that $(D, E) < 0$.

### 4.3.4 flat families

Suppose that $P$ is a nice variety and $\mathcal{M}$ is a coherent sheaf on $S \times P$, which is flat over $P$ and whose fiber at any $S$-section is in $Coh_S^{\leq 1}$. Thus, we get a $P$-family of divisors on $S$. The constancy of Euler characteristic in flat families easily shows that all these divisors are in fact the same when considered in $Cl_{num}(S)$.

For example, if we consider two nice curves $X, Y$ and $S = X \times Y$, then the $X$-sections of $S$ all give rise to the same element in $Cl_{num}(S)$.

### 4.3.5 unitarity-like

If $T$ is another nice surface over $k$ and $\phi : S \to T$ is a finite surjective morphism, then it is not hard to see that $(\phi^*(\cdot), \phi^*(\cdot)) = [k(S) : k(T)](\cdot, \cdot)$.

I did not completely figure out whether $\phi^*$ is adjoint (up to scalar) to $\phi_*$ or not.

### 4.3.6 counting fixed points

Suppose now that $S = X \times X$, where $X$ is a nice curve over $k$. For every morphism $\psi : X \to X$, we can consider its graph $Gr(\psi)$, a closed subscheme of $S$, which is isomorphic to $X$. In particular, $Gr(\psi)$ can be also considered as a (prime) divisor on $S$. We also note for later convinience that $(id \times \psi)^* Gr(id) = Gr(\psi)$.

Suppose that a morphism $\psi : X \to X$ is not equal to the identity morphism $id$. So, $\psi$ has a finite number of fixed points. Suppose that all of its fixed points are non-degenerate. It means that the endomorphism which $\psi$ generates of the tangent line at the fixed point is not equal to one.

Then we claim that the number of fixed points of $\psi$ is equal to $(Gr(\psi), Gr(id))$. Indeed, that $\psi \neq id$ garantuees the intersection to be zero-dimensional. That all the fixed points of $\psi$ are non-degenerate garantuees the intersection to be transversal. So $(Gr(\psi), Gr(id))$ equals just the naive number of intersection points, which is clearly the number of fixed points of $\psi$.

# 5 Proof of the Riemann hypothesis for curves over finite fields

Let $X_0$ be a nice curve over the finite field $k_0$; $|k_0| = q$. Let $k$ be an algebraic closure of $k_0$, and set $X = X_0 \times_{k_0} k$ (it is considered as a nice curve over $k$). We denote by $k_0^n$ the subfield of $k$ consisting of $q^n$ elements.

Let us note that when we write $X_0(k)$ (or $X_0(k_0^n)$), we mean the $k$ (or $k_0^n$) points of $X_0$ **over** $k_0$. Similarly, when we write $X(k)$, we mean the $k$ points of $X$ **over** $k$. Note that we have an identification $X_0(k) \cong X(k)$.

### 5.1 the miracle of Frobenius

The Galois group $Gal(k/k_0)$ acts on $X_0(k) \cong X(k)$. In particular, the inverse of $Frob \in Gal(k/k_0)$ acts. It is crucial that the action of this element is actually induced by a morphism $X_0 \to X_0$!

Considering the category of schemes over $k_0$, we have a unique endomorphism of its identity fucntor, which on affine schemes $Spec(A) \to Spec(k_0)$ is given by $A \to A : a \mapsto a^q$. We denote it by $F$. Then considering the map $F : X_0(k) \to X_0(k)$ induced by $F : X_0 \to X_0$, we easily see that it is equal to the map induced by the inverse of $Frob \in Gal(k/k_0)$. In particular, $X_0(k_0^n)$ is the fixed point set of $F^n : X_0(k) \to X_0(k)$.

We continue our abuse of notation, and denote by $F : X \to X$ the base change of $F : X_0 \to X_0$.

So, to summarize the miracle, we now have a completely geometric data - a nice variety $X$ over $k$ and a morphism $F : X \to X$, which captures the arithmetic data - the points of $X_0$ with values in finite extensions of $k_0$.

### 5.2 the end

We set $S = X \times_k X$ (it is a nice surface).

Let us notice that $F^n : X \to X$ induces zero on all tangent lines. Hence, all of its fixed points are non-degenerate. We thus deduce:

$$b_n := |X_0(k_0^n)| = |\{\alpha \in X(k) | F^n(\alpha) = \alpha\}| = (Gr(F^n), Gr(id)) = ((\Phi^n)^*(\Delta), \Delta)$$

where we set $\Phi = id \times F$ and $\Delta = Gr(id)$.

We will now be able to estimate $b_n$ by decomposing $\Delta$ into positive definite and non-negative definite parts.

Except $\Delta$, we have two more special elements in $\mathcal{H}_S$: $H = X \times pt$ and $V = pt \times X$.

The following relations are clear:

$$(H, H) = 0, (V, V) = 0, (H, V) = 1.$$

Let us write $\mathcal{H}_S = Sp\{H, V\} \oplus G$, where $G$ is the orthogonal complement to $Sp\{H, V\}$. Notice that the positive index of $Sp\{H, V\}$ is 1, so that $G$ is non-positive definite. The relations:

$$(\Delta, H) = 1, (\Delta, V) = 1$$

show that we can decompose $\Delta = H + V + \Gamma$, with $\Gamma \in G$.

It is not hard to see that $\Phi^* H = H$ and $\Phi^* V = qV$ (and that the degree of $\Phi$ is $q$). In particular, from the almost-unitarity of the pullback, we also see that $\Phi^*$ preserves $G$.

Thus, we can calculate=:

$$((\Phi^n)^* \Delta, \Delta) = 1 + q^n + ((\Phi^n)^* \Gamma, \Gamma)$$

and by Cauchy-Schwartz the last term is estimated as being $\leq q^{n/2}(\Gamma, \Gamma)$. We can also compute $(\Gamma, \Gamma) = -2g$ where $g$ is the genus of $X$. This finishes the proof.

## References

[1] http://www.math.lsa.umich.edu/ mityab/beilinson/SamREU07.pdf

[2] http://amathew.wordpress.com/2013/01/28/the-riemann-roch-and-hodge-index-theorems-on-surfaces/