18.782 Introduction to Arithmetic Geometry **Fall 2020**
Lecture #37 **12/7/2020**

Deligne's original proof of the Riemann hypothesis for arbitrary varieties over $\mathbb{F}_q$ is very difficult. Expositions [2, §6-13; 3, §28-33; 7, §6] all require substantial background and investment of time. A simplification was given by Katz in 2015 [7, §5], which proves the Riemann hypothesis for hypersurfaces of arbitrary dimension, then uses a result of Scholl to deduce the result for general varieties.

Other proofs exist for curves. In this case Weil gave two proofs in his original 1949 paper: a proof using the positivity of the Rosati involution on the Jacobian [4, Thm 1.30] and a geometric proof using Riemann-Roch and intersections on $C \times C$ [5, §3.2]. These are much more approachable, but still involve a lot of background from algebraic geometry: endomorphism rings, polarizations and the Weil pairing for abelian varieties in the first case, and Serre duality for line bundles, the Hodge index theorem and intersection theory on surfaces for the second. There is a more elementary proof due to Bombieri and Stepanov [1,8], but the argument is more intricate.

In this lecture we give a sketch of Katz' argument, following [7, §5]. We also discuss the case of curves and the relationship between the Hasse-Weil bound and the Riemann hypothesis.

37.1 The Riemann hypothesis for hypersurfaces over $\mathbb{F}_q$

Katz' idea is that we can prove the Riemann hypothesis by deforming from a hypersurface where it is easy to prove. For any hypersurface with equation $G = 0$, there is another hypersurface of the same dimension d and degree n where one can use classical Gauss sums to compute the number of points (and thus the zeta function). In particular, when $\gcd(n, q) = 1$ we can take the Fermat hypersurface

$$G_0 = \sum_{i=0}^{d} a_i x_i^n = 0$$

for any choice of nonzero a_i; when $\gcd(n, q) \neq 1$ we can take

$$G_0 = x_0^n + \sum_{i=0}^{n-1} x_i x_{i+1}^{n-1} = 0.$$

We then use the following lemma.

Lemma 37.1. *Let $U \subseteq \mathbb{P}^1$ be a nonempty open subscheme of the projective line over $\mathbb{F}_q$ and let $\mathcal{F}$ be a locally constant sheaf* [1] *of finite-dimensional $\mathbb{Q}_\ell$-vector spaces on U. Suppose that, for every closed point x, the characteristic polynomial of Frobenius*

$$P_x = \det(1 - F_x^{\deg(x)} T | \mathcal{F}_x)$$

has real coefficients and that there is some point $x_0 \in U$ so that all roots of P_{x_0} have absolute value 1. Then the same holds for all closed points of U.

The lemma requires a sheaf where the characteristic polynomial of Frobenius has roots on the unit circle, but the Weil conjectures require roots of absolute value[2] $q^{d/2}$; where

[1] A locally constant sheaf is an étale sheaf $\mathcal{F}$ on U so that there is some étale cover $f : U' \to U$ so that $f^*\mathcal{F}$ is constant. The classic example is the sheaf μ_n on a point $\operatorname{Spec}(\mathbb{Q})$: the value $\mu_n(K)$ varies over field extensions K/k, but once K contains the cyclotomic field $\mathbb{Q}(\zeta_n)$ then $\mu_n(K)$ becomes constant

[2] the middle dimension d is the only hard case by the weak Lefschetz theorem

does the difference come from? We can rescale using a technique known as a Tate twist [6, §7.5.4], which is useful since any tensor power of a sheaf with roots on the unit circle also has roots on the unit circle.

We can then apply the lemma to the dimension $d+1$ hypersurface defined by the equation $tG + (1-t)G_0 = 0$. In particular we will take U to be the complement of the singular fibers. One can check that the hypotheses of the lemma are satisfied using the fact that the zeta function is rational and that the characteristic polynomials on $H^i_{ét}(X, \mathbb{Q}_\ell)$ are rational for every $i \neq d$.

37.2 The Hasse-Weil bound

For a smooth projective curve C of genus g over $\mathbb{F}_q$ it is an easy consequence of the Weil conjectures that

$$|1 + q - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}. \tag{37.1}$$

But it turns out that the converse holds as well: the Riemann hypothesis for curves follows from this bound.

Proposition 37.2. *The Hasse-Weil bound (37.1) for a genus g curve C over $\mathbb{F}_q$ implies the Riemann hypothesis for C.*

Proof. Note first that, by the functional equation, the roots $\alpha_j := \alpha_{1,j}$ are fixed as a set by the map $x \mapsto q/x$. Thus it is enough to prove only one direction of inequality, that $\alpha_j \leq \sqrt{q}$.

To derive this inequality from (37.1), set $a_m = 1 + q^m - \#C(\mathbb{F}_{q^m}) = \sum_{j=1}^{2g} \alpha_j^m$. Consider the generating function

$$\sum_{m\geq 1} a_m T^m = \sum_{j=1}^{2g} \sum_{m\geq 1} \alpha_j^m T^m = \sum_{j=1}^{2g} \frac{\alpha_j T}{1 - \alpha_j T}.$$

As a power series around 0, this function has a pole at $t = 1/\alpha_j$. We now show that it converges for any $t \in \mathbb{C}$ with $|t| < q^{-1/2}$ and thus $q^{-1/2} \leq 1/|\alpha_j|$.

Given (37.1) we have $|a_m| \leq 2gq^{m/2}$ for all m by base change to $\mathbb{F}_{q^m}$. For $|t| < q^{-1/2}$, we have

$$|\sum_{m\geq 1} a_m t^m| \leq 2g \sum_{m\geq 1} (\sqrt{q}|t|)^m = \frac{2g\sqrt{q}|t|}{1 - \sqrt{q}|t|}.$$

□

The hard work for curves then goes into proving the Hasse-Weil bound. We close by noting that the proof is much simpler for elliptic curves, where it follows from the following result about the degree of isogenies of a special form.

Lemma 37.3. *Suppose E is an elliptic curve over $\mathbb{F}_q$, F is the Frobenius map of degree q on E and $r, s \in \mathbb{Z}$. Set $a = 1 + q - \#E(\mathbb{F}_q)$. Then*

$$\deg(rF - s) = r^2 q + s^2 - rsa.$$

Proof. See [9, §4.2] □

Proof of Hasse bound for elliptic curves. Degrees are nonnegative, so dividing the expression in the lemma by s^2 we get

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0.$$

for $r, s \in \mathbb{Z}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we get that the discriminant $a^2 - 4q$ must be nonpositive, implying $|a| \leq 2\sqrt{q}$. □

References

[1] Raymond von Bommel. *The Bombieri-Stepanov approach to the Riemann hypothesis for curves over finite fields* https://raymondvanbommel.nl/talks/BombieriStepanov.pdf

[2] Uwe Jannsen. *Deligne's Proof of the Weil Conjectures.* http://www.mathematik.uni-regensburg.de/Jannsen/home/Weil-gesamt-eng.pdf

[3] James Milne. *Lectures on étale cohomology.* https://www.jmilne.org/math/CourseNotes/LEC.pdf

[4] James Milne. *The Riemann hypothesis over finite fields: from Weil to the present day.* In "The legacy of Bernhard Riemann after one hundred and fifty years," Lizhen Ji, Frans Oort and Shing-Tung Yau (ed.), International Press, 2016. arXiv:1509.00797

[5] Mircea Mustaţă. *Zeta functions in algebraic geometry.* http://www-personal.umich.edu/~mmustata/zeta_book.pdf

[6] Bjorn Poonen. *Rational points on varieties.* Graduate Studies in Mathematics 186. Amer. Math. Soc., Providence, 2017. https://math.mit.edu/~poonen/papers/Qpoints.pdf

[7] Tamás Szamuely. *A course on the Weil conjectures.* https://www.ams.org/open-math-notes/omn-view-listing?listingId=110831

[8] Terence Tao. *The Bombieri-Stepanov proof of the Hasse-Weil bound.* https://terrytao.wordpress.com/2014/05/02/the-bombieri-stepanov-proof-of-the-hasse-weil-bound/

[9] Lawrence Washington. *Elliptic curves, number theory and cryptography.* Taylor & Francis Group, Boca Raton FL, 2008.