A NOTE ON RH FOR CURVES AND HYPERSURFACES OVER FINITE FIELDS

NICHOLAS M. KATZ

Abstract. We give what is arguably a simple (though certainly not elementary, cf. [Sch]) proof of the Riemann Hypothesis for (projective, smooth, geometrically connected) curves and hypersurfaces over finite fields, by an argument which reduces us to checking a few examples.

1. The rules of the game

We give ourselves some basic facts about ℓ-adic cohomology. We then combine them with an incarnation of Deligne's breakthrough idea in his Weil I paper, his transposition to the ℓ-adic context of Rankin's "squaring" method.

2. Deligne's version of the Rankin method

Let $U_0/\mathbb{F}_q$ be an affine, smooth, geometrically connected curve. Ignoring base points, the open curve U_0 has a profinite fundamental group, $\pi_1^{arith} := \pi_1(U_0)$, its extension of scalars $U/\overline{\mathbb{F}_q}$ has a profinite fundamental group $\pi_1^{geom} := \pi_1(U)$, and we have a short exact sequence

$$1 \to \pi_1^{geom} \to \pi_1^{arith} \to Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to 1.$$

An ℓ-adic local system (also called a lisse $\overline{\mathbb{Q}_\ell}$-sheaf) $\mathcal{F}$ on U_0 is simply a continuous, finite-dimensional $\overline{\mathbb{Q}_\ell}$-representation of π_1^{arith}.

For each closed point $\wp$ of U_0 we have an element $Frob_\wp$ in π_1^{arith}, well defined up to conjugacy. So it makes sense to form the reversed characteristic polynomial $\det(1 - TFrob_\wp|\mathcal{F})$ of its action in the given representation. The L function $L(U_0/\mathbb{F}_q, \mathcal{F}, T)$ is the element of $1 + T\overline{\mathbb{Q}_\ell}[[T]]$ defined by the Euler product

$$L(U_0/\mathbb{F}_q, \mathcal{F}, T) := \prod_{\text{closed points } \wp} \frac{1}{\det(1 - T^{\deg(\wp)}Frob_\wp|\mathcal{F})}.$$

Suppose now and henceforth that the prime ℓ is not the characteristic p of $\mathbb{F}_q$. Grothendieck's theory allows one to speak of the cohomology groups $H^i_c(U, \mathcal{F})$, on which $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ operates. These are finite dimensional $\overline{\mathbb{Q}_\ell}$ vector spaces, which vanish for i outside the range $[1, 2]$. Of the two possibly nonzero groups, we know one of them exactly: $H^2_c(U, \mathcal{F})$ is the Tate twist $(\mathcal{F})_{\pi_1^{geom}}(-1)$ of the coinvariants $(\mathcal{F})_{\pi_1^{geom}}$, the largest quotient of $\mathcal{F}$ on which π_1^{geom} acts trivially. What this means concretely is that we have the formula

$$\det(1 - TFrob_q|H^2_c(U, \mathcal{F})) = \det(1 - qTFrob_q|(\mathcal{F})_{\pi_1^{geom}}).$$

Grothendieck's cohomological formula for the L function is

$$L(U_0/\mathbb{F}_q, \mathcal{F}, T) = \frac{\det(1 - TFrob_q|H^1_c(U, \mathcal{F}))}{\det(1 - TFrob_q|H^2_c(U, \mathcal{F}))},$$

cf. [Gr-Lef, Thm. 5.1], [Ka-GKM, 2.3.2].

The local systems we are interested in are the $R^i := R^i f_\star \mathbb{Q}_\ell$ for proper smooth morphisms $f : \mathcal{X} \to U_0$. A fundamental compatibility for these R^i is this, cf. [SGA 4, Exp. XV, Cor. 2.2]. Let $\wp$ be a closed point of U_0. The residue field $\mathbb{F}_\wp$ at $\wp$ is the field $\mathbb{F}_{\mathbb{N}\wp}$ with $\mathbb{N}\wp$ elements. The fibre of f over $\wp$ is a proper smooth scheme $X_{0,\wp}/\mathbb{F}_{\mathbb{N}\wp}$, whose extension of scalars to $\overline{\mathbb{F}_{\mathbb{N}\wp}}$ we denote $X_\wp$. The fundamental compatibility is that

$$\det(1 - TFrob_\wp | R^i) = \det(1 - TFrob_{\mathbb{N}\wp} | H^i(X_\wp, \mathbb{Q}_\ell)).$$

We now come to two notions due to Deligne. Given a field embedding $\iota : \overline{\mathbb{Q}_\ell} \hookrightarrow \mathbb{C}$, an ℓ-adic local system $\mathcal{F}$ on U_0 is said be ι-pure of some integer weight w if, for all closed points $\wp$ of U_0, all the eigenvalues of $Frob_\wp$ on $\mathcal{F}$ have, via ι, complex absolute value $\mathbb{N}\wp^{w/2}$. An ℓ-adic local system $\mathcal{F}$ is said to be ι-real if, via ι, for all closed points $\wp$ of U_0, the reversed characteristic polynomial $\det(1 - TFrob_\wp|\mathcal{F})$ has coefficients in $\mathbb{R}$, the field of real numbers.

By means of the identity

$$1/\det(1 - TFrob_\wp|\mathcal{F}) = \exp(\sum_{n \geq 1} \mathrm{Trace}(Frob_\wp^n|\mathcal{F})T^n/n),$$

we see that ι-reality is the condition that for each closed point $\wp$ of U_0, and each $n \geq 1$, $\iota(\mathrm{Trace}((Frob_\wp^n|\mathcal{F}))$ is real. The key point now is that if $\mathcal{F}$ ι-real, then any even tensor power $\mathcal{F}^{\otimes 2k}$ of $\mathcal{F}$ is not only ι-real, but each of its Euler factors

$$1/\det(1 - T^{\deg(\wp)}Frob_\wp|\mathcal{F}^{\otimes 2k}) = \exp(\sum_{n \geq 1}(\mathrm{Trace}(Frob_\wp^n|\mathcal{F}))^{2k}T^{n\deg(\wp)}/n)$$

is a power series, via ι, in $1 + T\mathbb{R}_{\geq 0}[[T]]$, i.e., it has constant term 1 and all its coefficients are nonnegative real numbers.

Theorem 2.1. (Deligne, compare [De-Weil I, 3.2] and [De-Weil II, 1.5.2]) *Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that every even tensor power $\mathcal{F}^{\otimes 2k}$ of $\mathcal{F}$ satisfies the following condition: every eigenvalue β_{2k} of $Frob_q$ on the coinvariants $((\mathcal{F})^{\otimes 2k})_{\pi_1^{geom}}$ has $|\iota(\beta_{2k})| \leq 1$. Then for each closed point $\wp$, every eigenvalue $\alpha_{i,\wp}$ of $Frob_\wp$ on $\mathcal{F}$ has $|\iota(\alpha_{i,\wp})| \leq 1$.*

Proof. From the Euler product expression for the L-function of $\mathcal{F}^{\otimes 2k}$, we see that, via ι,

1. The power series for the L-function has nonnegative real coefficients.
2. The power series of each Euler factor $1/\det(1 - T^{\deg(\wp)}Frob_\wp|\mathcal{F}^{\otimes 2k})$ has nonnegative real coefficients.
3. The power series for the L-function dominates, coefficient by coefficient, the power series of each Euler factor $1/\det(1 - T^{\deg(\wp)}Frob_\wp|\mathcal{F}^{\otimes 2k})$.

By the hypothesis on coinvariants, the denominator in the cohomological expression of the L-function of $\mathcal{F}^{\otimes 2k}$, namely

$$\det(1 - qTFrob_q|((\mathcal{F})^{\otimes 2k})_{\pi_1^{geom}}),$$

has all its reciprocal zeros of absolute value, via ι, at most q. So the L-function is certainly, via ι, holomorphic in $|T| < 1/q$.

Choose a closed point $\wp$ of U_0. By the coefficientwise domination (3) above, it follows that each Euler factor $1/\det(1 - T^{\deg(\wp)}Frob_\wp|\mathcal{F}^{\otimes 2k})$ must be holomorphic in $|T| < 1/q$. This in turn means that each eigenvalue of $Frob_\wp|\mathcal{F}^{\otimes 2k}$ has, via

ι, absolute value $\leq q^{\deg(\wp)}$. But if α is an eigenvalue of $Frob_\wp|\mathcal{F}$, then α^{2k} is an eigenvalue of $Frob_\wp|\mathcal{F}^{\otimes 2k}$. Thus we get the inequality $|\iota(\alpha)^{2k}| \leq q^{\deg(\wp)}$, for each $k \geq 1$. Thus we get

$$|\iota(\alpha)| \leq q^{\deg(\wp)/2k}$$

for every integer $k \geq 1$. Letting $k \to \infty$, we get

$$|\iota(\alpha)| \leq 1.$$

□

Corollary 2.2. *Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $\wp_0$, every eigenvalue $\alpha_{i,\wp_0}$ of $Frob_{\wp_0}$ on $\mathcal{F}$ has $|\iota(\alpha_{i,\wp_0})| \leq 1$. Then for every closed point $\wp$, every eigenvalue $\alpha_{i,\wp}$ of $Frob_\wp$ on $\mathcal{F}$ has $|\iota(\alpha_{i,\wp})| \leq 1$.*

Proof. In view of the theorem, it suffices to show that for every tensor power $\mathcal{F}^{\otimes 2k}$ of $\mathcal{F}$, every eigenvalue β_{2k} of $Frob_q$ on the coinvariants $((\mathcal{F})^{\otimes 2k})_{\pi_1^{geom}}$ has $|\iota(\beta_{2k})| \leq 1$. For $d := deg(\wp_0)$, β_{2k}^d is an eigenvalue of $(Frob_q)^d$ on the coinvariants $((\mathcal{F})^{\otimes 2k})_{\pi_1^{geom}}$. Viewing these coinvariants as a quotient representation of $(\mathcal{F})^{\otimes 2k}$, the action of $(Frob_q)^d$ is just the action of $Frob_{\wp_0}$ on this quotient. In other words, β_{2k}^d is among the eigenvalues of $Frob_{\wp_0}$ on $(\mathcal{F})^{\otimes 2k}$, cf. [De-Weil II, 1.4.4]. These last eigenvalues are $2k$-fold products of eigenvalues of $Frob_{\wp_0}$ on $\mathcal{F}$, each of which has absolute value, via ι, ≤ 1. Thus the same estimate holds for each eigenvalue of $Frob_{\wp_0}$ on $(\mathcal{F})^{\otimes 2k}$. Since β_{2k}^d is among these, we get $|\iota(\beta_{2k}^d)| \leq 1$, hence $|\iota(\beta_{2k})| \leq 1$. □

3. RH for curves

Fix a characteristic $p > 0$ and a genus $g \geq 1$. There are standard examples of (projective, smooth, geometrically connected) curves of genus g over the prime field $\mathbb{F}_p$ for which RH is “easy”, in the sense that, at least over a suitable finite extension $\mathbb{F}_q/\mathbb{F}_p$, the Frobenius eigenvalues on H^1 are explicit Jacobi sums or Gauss sums, which are well known to have the correct absolute value $q^{1/2}$. For example, if $p \neq 2$, we can take the (complete nonsingular model of the) hyperelliptic curve

$$y^2 = x^{2g+1} - 1,$$

if p does not divide $2g + 1$, or

$$y^2 = x^{2g+2} - 1,$$

if p does divides $2g + 1$. These examples give rise to Jacobi sums. In characteristic two, we have the (complete nonsingular model of) the curve

$$y^2 - y = x^{2g+1},$$

which gives rise to Gauss sums.

We have the following “connect by curves” lemma.

Lemma 3.1. *Suppose given two (projective, smooth, geometrically connected) curves of genus $g \geq 1$ over $\mathbb{F}_q$, say C_0 and C_1. Then there exists a finite extension $E/\mathbb{F}_q$, an affine, smooth, geometrically connected curve U_0/E, a proper smooth morphism $f : \mathcal{C} \to U_0$ with geometrically connected fibres which are curves of genus g, and two E-valued points $u_0, u_1 \in U_0(E)$ such that the fibres $\mathcal{C}_{u_i}/E$, for $i = 0, 1$, are E-isomorphic to the given curves $C_i \otimes_{\mathbb{F}_q} E/E$.*

Proof. For genus one, choose an integer $n \geq 4$ prime to p. Extending scalars, we may assume first that both of the given curves have a rational point. Then the curves become groupschemes, with a chosen rational point as origin. Over a further finite extension $E/\mathbb{F}_q$, we may choose a point of order n on each curve. Then we use the modular curve $Y_1(n)/E$ as our U_0, and the universal family it carries as our $f : \mathcal{C} \to U_0$.

For $g \geq 2$, the moduli space $H_g^0/\mathbb{F}_p$ classifying tricanonical embedded genus g curves is quasiprojective, smooth and geometrically connected, cf. [De-Mum, &3] and [Mum, Ch. 5,&2], and every genus g curve over an $\mathbb{F}_q$ underlies an $\mathbb{F}_q$-valued point of $H_g^0/\mathbb{F}_p$. Here it is enough to pull back the universal family over $H_g^0/\mathbb{F}_p$ to a spacefilling curve $\pi : U_0 \to H_g^0$ which is bijective on $\mathbb{F}_q$-points, cf. [Ka-SFC, Thm. 8] and [Ka-SFC Corrections]. [We could instead use the moduli space $\mathcal{M}_{g,3K}/\mathbb{F}_p$ classifying genus g curves together with a basis of $H^0(C, (\Omega^1)^{\otimes 3})$, which is a $\mathbb{G}_m$ bundle over $H_g^0/\mathbb{F}_p$, so is itself quasiprojective, smooth and geometrically connected, cf. [Ka-Sar, 10.6.5].]

□

Theorem 3.2. *Let $C_0/\mathbb{F}_q$ be a (projective, smooth, geometrically connected) curve of genus $g \geq 1$ over $\mathbb{F}_q$. Then RH holds for $C_0/\mathbb{F}_q$.*

Proof. Choose a genus g curve $C_1/\mathbb{F}_q$ for which we know RH. Making a finite extension of scalars if necessary, connect C_0 to C_1 in a one parameter family $f : \mathcal{C} \to U_0$ over an affine, smooth, geometrically connected curve U_0/q. We will prove that the local system $R^1 f_\star \mathbb{Q}_\ell$ on U_0 is pure of weight one, i.e., that RH holds for every curve in the family, in particular it holds for C_0. Choose a square root $q^{1/2}$ of q in $\overline{\mathbb{Q}_\ell}$, so that we can speak of the one half Tate-twisted local system

$$\mathcal{F} := R^1 f_\star \overline{\mathbb{Q}_\ell}(1/2),$$

on which $Frob_\wp$ is now divided by $(q^{1/2})^{deg(\wp)}$. For any ι, $\mathcal{F}$ is ι-real; indeed for$R^1 f_\star \overline{\mathbb{Q}_\ell}$ the traces of all powers of all $Frob_\wp$ are integers. Because RH holds for C_1, $Frob_{u_1}|\mathcal{F}$ has all eigenvalues of absolute value one (via any ι). So by Corollary 2.2, all eigenvalues of any $Frob_\wp$ have, via ι, absolute value ≤ 1. This means that on $R^1 f_\star \mathbb{Q}_\ell$ itself, all eigenvalues of any $Frob_\wp$ have, via ι, absolute value $\leq \mathbb{N}\wp^{1/2}$. But the functional equation tells us that $\alpha \mapsto \mathbb{N}\wp/\alpha$ is an involution of the eigenvalues, so in fact this inequality is an equality; $R^1 f_\star \mathbb{Q}_\ell$ is ι-pure of weight one for every ι. □

4. The persistence of purity

We have the following variant of Corollary 2.2.

Theorem 4.1. *Let $\mathcal{F}$ be an ℓ-adic local system on U_0 which is ι-real. Suppose that for some closed point $\wp_0$, every eigenvalue $\alpha_{i,\wp_0}$ of $Frob_{\wp_0}$ on $\mathcal{F}$ has $|\iota(\alpha_{i,\wp_0})| = 1$. Then for every closed point $\wp$, every eigenvalue $\alpha_{i,\wp}$ of $Frob_\wp$ on $\mathcal{F}$ has $|\iota(\alpha_{i,\wp})| = 1$, i.e., $\mathcal{F}$ is ι-pure of weight zero as soon as some $Frob_{\wp_0}$ is ι-pure of weight zero.*

Proof. By Corollary 2.2, each $Frob_\wp$ has all its eigenvalues of absolute value, via ι, ≤ 1. So it will have all its eigenvalues of absolute value, via ι, $= 1$, if and only if $\det(Frob_\wp)$ has, via ι, absolute value $= 1$. So we are reduced to proving that $\det(\mathcal{F})$ is ι-pure of weight zero if $\det(Frob_{\wp_0})$ is. To prove this purity, we may replace the rank one local system $\det(\mathcal{F})$ by any tensor power $(\det(\mathcal{F}))^{\otimes n}, n \geq 1$, of itself. It then suffices to apply the following lemma to the rank one local system $\det(\mathcal{F})$, and compute the ι-absolute value of the α there. □

Lemma 4.2. *Let $\mathcal{L}$ be an ℓ-adic local system on U_0 of rank one. Then some tensor power $\mathcal{L}^{\otimes n}$ of $\mathcal{L}$ is geometrically constant, i.e., there exists $\alpha \in \overline{\mathbb{Q}_\ell}^\times$ such that*

$$Frob_\wp|\mathcal{L}^{\otimes n} = \alpha^{deg(\wp)}.$$

Proof. Because we know RH for the complete nonsingular model of U_0, we know that in $H^1_c(U, \overline{\mathbb{Q}_\ell})$, every eigenvalue of $Frob_q$ has absolute value $\leq q^{1/2}$ for every ι. By duality, every eigenvalue of $Frob_q$ on $H^1(U, \overline{\mathbb{Q}_\ell})$ has absolute value $\geq q^{1/2}$. In particular, 1 is not an eigenvalue of of $Frob_q$ on $H^1(U, \overline{\mathbb{Q}_\ell})$.

Now consider a rank one local system $\mathcal{L}$ on U_0. It is a homomorphism from $\pi_1^{arith} := \pi_1(U_0)$ to the group $\mathcal{O}^\times_{\overline{\mathbb{Q}_\ell}}$ of ℓ-adic units in $\overline{\mathbb{Q}_\ell}$. Because its image is compact, this homomorphism lands in $\mathcal{O}^\times_{E_\lambda}$, for some finite extension $E_\lambda/\mathbb{Q}_\ell$. The residue field $\mathbb{F}_\lambda$ of $\mathcal{O}_{E_\lambda}$ is finite, so replacing $\mathcal{L}$ by its n'th tensor power for $n = \#\mathbb{F}^\times_\lambda$, we reduce to the case where the homomorphism in question takes values in the group $1 + \lambda\mathcal{O}_{E_\lambda}$ of principal units. Now raising to the ℓ'th power, we reduce to the case where our homomorphism takes values in the group $1 + \ell\lambda\mathcal{O}_{E_\lambda}$. This group is isomorphic, by the logarithm, to the additive group $\ell\lambda\mathcal{O}_{E_\lambda}$, which is a subgroup of $E_\lambda \subset \overline{\mathbb{Q}_\ell}$. Thus we have a homomorphism from $\pi_1^{arith} := \pi_1(U_0)$ to $\overline{\mathbb{Q}_\ell}$. Its restriction to $\pi_1^{geom} := \pi_1(U)$ is then an element of $H^1(U, \overline{\mathbb{Q}_\ell})$ which is **fixed** by $Frob_q$. But as remarked above, there are no such nonzero elements. Therefore the corresponding tensor power of our $\mathcal{L}$ is trivial when restricted to π_1^{geom}. This means exactly that it is of the asserted form. □

5. RH FOR HYPERSURFACES

For $X_0 \subset \mathbb{P}^{n+1}$ a smooth hypersurface of degree d and dimension $n \geq 1$ over $\mathbb{F}_q$, and $X/\overline{\mathbb{F}_q}$ its extension of scalars to $\overline{\mathbb{F}_q}$, we define $Prim^n(X, \mathbb{Q}_\ell)$ to be $H^n(X, \mathbb{Q}_\ell)$ if n is odd, and to be $H^n(X, \mathbb{Q}_\ell)/ < L^{n/2} >$, for $< L^{n/2} >$ the one-dimensional span of the $n/2$ power of the hyperplane class $L \in H^2(X, \mathbb{Q}_\ell)$.

One knows (weak Lefschetz for $X \subset \mathbb{P}^{n+1}$) that for $i < n$, the restriction map gives an isomorphism $H^i(\mathbb{P}^n, \mathbb{Q}_\ell) \cong H^i(X, \mathbb{Q}_\ell)$. Thus for $i < n$, we have $H^i(X, \mathbb{Q}_\ell) = 0$ unless i is even, in which case $H^i(X, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-i/2)$, the one dimensional space on which $Frob_q$ acts as $q^{i/2}$. By Poincaré duality on X, these same statements hold for $H^i(X, \mathbb{Q}_\ell)$ for i in the range $n < i \leq 2n$. So for $X_0/\mathbb{F}_q$, its Zeta function has the form

$$P(T)/\prod_{i=0}^{n}(1 - q^iT), \quad n \text{ odd},$$

$$1/P(T)\prod_{i=0}^{n}(1 - q^iT), \quad n \text{ even},$$

with

$$P(T) = \det(1 - TFrob_q|Prim^n(X, \mathbb{Q}_\ell)).$$

From the formula for Zeta, we see that $P(T)$ has integer coefficients. Thus RH for $X_0/\mathbb{F}_q$ is the assertion that $Prim^n(X, \mathbb{Q}_\ell)$, or equivalently $H^n(X, \mathbb{Q}_\ell)$, is ι-pure of weight n (for some ι, or equivalently for every ι, since the only possible ambiguity in what ι does to our characteristic polynomials is which square root of q it chooses, and even this is only a problem when n is odd). The functional equation asserts that $\alpha \mapsto q^n/\alpha$ is an involution on the eigenvalues of $Frob_q$, so RH is equivalent to the assertion that every eigenvalue of $Frob_q$ on $Prim^n(X, \mathbb{Q}_\ell)$, or equivalently on $H^n(X, \mathbb{Q}_\ell)$, has ι-absolute value $\leq q^{n/2}$. If we extend scalars from $\mathbb{F}_q$ to some $\mathbb{F}_{q^e}$, we simply replace $Frob_q$ by its e'th power, so it is enough to prove RH after such an extension of scalars.

From the point count formula

$$\#X_0(F_{q^r}) = \#\mathbb{P}^n(F_{q^r}) + (-1)^n \mathrm{Trace}((Frob_q)^r | Prim^n(X, \mathbb{Q}_\ell)),$$

we see the well known equivalence of RH for $X_0/\mathbb{F}_q$ with the existence of an estimate

$$\#X_0(F_{q^r}) = \#\mathbb{P}^n(F_{q^r}) + O(q^{rn/2})$$

as $r \geq 1$ varies.

Theorem 5.1. *Given (p, d, n), suppose there exists a projective smooth hypersurface $X_0/\mathbb{F}_p$ of dimension n and degree d for which RH holds. Then for every finite extension $\mathbb{F}_q/\mathbb{F}_p$, and every projective smooth hypersurface $X_1/\mathbb{F}_q$ of dimension n and degree d, RH holds.*

Proof. Say we wish to prove RH for $X_1/\mathbb{F}_q$. Denote by $X_0/\mathbb{F}_q$ the extension of scalars from $\mathbb{F}_p$ to $\mathbb{F}_q$ of the $X_0/\mathbb{F}_p$ for which we know RH. Choose homogeneous equations F_0 and F_1 for these two hypersurfaces. Then use the one parameter family $tF_0 + (1-t)F_1$ over the dense open set of the affine t-line where this equation defines a nonsingular hypersurface, and apply Theorem 4.1 to its $R^n f_\star(\overline{\mathbb{Q}_\ell})(n/2)$. □

6. Example hypersurfaces with RH

When the degree d is prime to p, then as Weil showed, RH holds for the Fermat hypersurface of equation $\sum_{i=1}^{n+2} X_i^d = 0$. So Theorem 5.1 gives RH when the degree d is prime to p.

Suppose now that p divides d. We first treat the special case $d = 2$, for which $p = 2$ is the only problematic prime. If n is odd, then $Prim^n$ vanishes, so there is nothing to prove. If $n = 2m$ is even, then $Prim^n$ is one-dimensional. We take as example the hypersurface of equation $\sum_{i=1}^{m+1} X_i X_{m+1+i} = 0$, which over **any** finite field $\mathbb{F}_q$ is projective and smooth with $\#P^{2m}(\mathbb{F}_q) + q^m$ rational points (i.e., $Prim^n$ in this case is $\mathbb{Q}_\ell(-n/2)$, on which $Frob_q$ acts as $q^m = q^{n/2}$).

Suppose now that $d \geq 3$ and that p divides d. Then Gabber's hypersurface

$$X_1^d + \sum_{i=1}^{n+1} X_i X_{i+1}^{d-1} = 0$$

is nonsingular in characteristic $\mathbb{F}_p$, cf. [Ka-Sar, 11.4.6].

Proposition 6.1. *If $d \geq 3$ and $p|d$, Gabber's hypersurface over $\mathbb{F}_p$ satisfies RH.*

We will prove this in the next two sections, using Delsarte's method.

7. Delsarte's method and RH

Suppose we are given a homogeneous form $F(X_1, ..., X_{n+2})$ over $\mathbb{F}_q$ whose vanishing defines a smooth hypersurface H_0 in projective space $\mathbb{P}^{n+1}$. Denote by $H_0^{\mathrm{aff}} \subset \mathbb{A}^{n+2}$ the affine hypersurface defined by the same equation. Then we have the elementary relation, for each finite extension $E/\mathbb{F}_q$, with $q_E := \#E$,

$$\#H_0^{\mathrm{aff}}(E) = 1 + (q_E - 1)\#H_0(E).$$

As noted above, H_0 satisfies RH if and only if, as $E/\mathbb{F}_q$ varies over all finite extensions, we have

$$\#H_0(E) = \#\mathbb{P}^n(E) + O(q_E^{n/2}).$$

or, equivalently, if and only if, as as $E/\mathbb{F}_q$ varies over all finite extensions, we have

$$\#H_0^{\mathrm{aff}}(E) = q_E^{n+1} + O(q_E^{(n+2)/2}).$$

We will show that Gabber's hypersurface $X_1^d + \sum_{i=1}^{n+1} X_i X_{i+1}^{d-1} = 0$ satisfies this last estimate, and hence satisfies RH.

For this, we need some preliminaries. Fix an integer $N \geq 1$. Given an N-tuple $W = (w_1, ..., w_N)$ of nonnegative integers, we write X^W for the N-variable monomial $\prod_{i=1}^N X_i^{w_i}$. We say that a nonempty collection of N-variable monomials $\{X^{W_v}\}_v$ is linearly independent if the vectors $\{W_v\}_v$ are linearly independent in $\mathbb{Q}^N$. [Notice that in both Gabber's homogeneous form $X_1^d + \sum_{i=1}^{n+1} X_i X_{i+1}^{d-1}$ and the Fermat form $\sum_{i=1}^{n+2} X_i^d$ in $N = n+2$ variables, the monomials that occur are linearly independent.]

Theorem 7.1. *Let $N \geq 1$, and let $X^{W_1}, ..., X^{W_N}$ be N linearly independent monomials in N variables. Suppose that each variable X_i occurs in at most two of these monomials. Then for the affine hypersurface V of equation $\sum_i X^{W_i} = 0$ in $\mathbb{A}^N$, and variable finite fields $\mathbb{F}_q$, we have*

$$\#V(\mathbb{F}_q) = q^{N-1} + O(q^{N/2}).$$

We will prove this by counting, for each subset $S \subset [1, 2, ..., N]$, the points where the variables $X_s, s \in S$ take nonzero values, and the other variables vanish. The key result, essentially due to Delsarte [Dels], is this.

Theorem 7.2. (Delsarte) *Let $N > k \geq 0$, and suppose given $N-k$ linearly independent monomials $X^{W_1}, ..., X^{W_{N-k}}$ in N variables. Consider the hypersurface $V : \sum_i X^{W_i} = 0$ in $\mathbb{A}^N$. Denote by $V^\star \subset V$ the open set of V where all variables are invertible (i.e., $V^\star$ is the hypersurface in $\mathbb{G}_m^N$ defined by $\sum_i X^{W_i} = 0$). Then for variable finite fields $\mathbb{F}_q$, we have*

$$\#V^\star(\mathbb{F}_q) = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

Granting the truth of Delsarte's theorem, let us prove Theorem 7.1. Thus $X^{W_1}, ..., X^{W_N}$ are N linearly independent monomials in N variables. If we put all but $d \geq 1$ of the variables to 0, say $X_{d+1}, ..., X_N$, some of the monomials X^{W_i} will vanish (those in which any of $X_{d+1}, ..., X_N$ occurs), and the remaining ones (if any), those which involved only $X_1, ..., X_d$, will be linearly independent monomials in those d variables.

For each subset $S \subset [1, ..., N]$, we denote by $V^\star(S)(\mathbb{F}_q)$ the set of points on V for which precisely the variables $X_s, s \in S$ take nonzero values.

Lemma 7.3. *For each subset $S \subset [1, ..., N]$, we have*

$$\#V^\star(S)(\mathbb{F}_q) = \frac{(q-1)^{\#S}}{q} + O(q^{N/2}).$$

Proof. If $S = \emptyset$, $V^\star(\emptyset)(\mathbb{F}_q)$ consists of one point, namely $(0, ..., 0)$, and the assertion is trivially true with the $O(q^{N/2})$ term alone.

If $1 \leq \#S \leq N/2$, there are at most $\#S \leq N/2$ variables, each of which assumes at most $q-1$ values. So the assertion is trivially true with the $O(q^{N/2})$ term alone.

If $\#S > N/2$, we have set fewer than half (namely $N - \#S$) of the variables to zero. As each variable occurs in at most two of the monomials, we have killed at most $2(N-\#S)$ variables, so we are left with at least $N-2(N-\#S)$ monomials, i.e., we have at least $2\#S - N$ monomials. The number of surviving monomials is thus at least $\#S-(N-\#S)$. Applying Theorem 7.2 (with its N and k now $\#S$ and $k \leq (N - \#S)$, the error term $O(q^{(N+k)/2})$ in Theorem 7.2 is now $O(q^{(\#S+(N-\#S))/2})$, i.e. it is $O(q^{N/2})$. $\square$

With this lemma in hand, we prove Theorem 7.1. Indeed, we have

$$\#V(\mathbb{F}_q) = \sum_{S\subset[1,2,\ldots,N]} \#V^\star(S)(\mathbb{F}_q) =$$

$$= (\sum_{S\subset[1,2,\ldots,N]} \frac{(q-1)^{\#S}}{q}) + O(q^{N/2}).$$

The numerator of the sum is just the binomial expansion of $((q-1)+1)^N$.

8. proof of Delsarte's Theorem 7.2

We view the $N-k$ linearly independent monomials X^{W_i} in N variables as an f.p.p.f. surjective homomorphism of split tori over $\mathbb{Z}$,

$$\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}, \quad X = (X_1, ..., X_N) \mapsto (X^{W_1}, ..., X^{W_{N-k}}).$$

We will prove the following (slightly more general) version of Theorem 7.2.

Theorem 8.1. *Let $N > k \geq 0$, and suppose given an f.p.p.f. surjective homomorphism of split tori over $\mathbb{Z}$,*

$$\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}.$$

Denote by

$$\sigma : \mathbb{G}_m^{N-k} \to \mathbb{A}^1$$

the function "sum of the coordinates". Then for variable finite fields $\mathbb{F}_q$, we have the estimate

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) | \sigma(\phi(x)) = 0\} = \frac{(q-1)^N}{q} + O(q^{(N+k)/2}).$$

Proof. The homomorphism ϕ corresponds to the injective group homomorphism $\phi^\vee : \mathbb{Z}^{N-k} \subset \mathbb{Z}^N$ which sends the i'th basis vector of the source to W_i. The kernel $Ker(\phi)$ is the group whose character group is the cokernel of $\phi^\vee$. This cokernel is a finitely generated abelian group, say M, with $M \otimes \mathbb{Q}$ of dimension k. Thus M sits in a short exact sequence

$$0 \to M_{tors} \to M \to M/M_{tors} \cong \mathbb{Z}^k \to 0,$$

with M_{tors} a finite abelian group. Dually, we have an f.p.p.f. short exact sequence of groupschemes over $\mathbb{Z}$

$$0 \to \mathbb{G}_m^k \to Ker(\phi) \to \mu_{M_{tors}} \to 0,$$

with $\mu_{M_{tors}} := Hom(M_{tors}, \mathbb{G}_m)$ a finite flat groupscheme of multiplicative type. The composite closed immersion

$$\mathbb{G}_m^k \subset Ker(\phi) \subset \mathbb{G}_m^N$$

sits in a short exact sequence

$$0 \to \mathbb{G}_m^k \to \mathbb{G}_m^N \xrightarrow{\pi} \mathbb{G}_m^{N-k} \to 0.$$

By Hilbert's Theorem 90, this gives a short exact sequence of $\mathbb{F}_q$-valued points

$$0 \to \mathbb{G}_m^k(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\pi} \mathbb{G}_m^{N-k}(\mathbb{F}_q) \to 0.$$

Our homomorphism $\phi : \mathbb{G}_m^N \to \mathbb{G}_m^{N-k}$ factors through this quotient map π as

$$\begin{tikzcd} \mathbb{G}_m^N \arrow[r, "\pi"] \arrow[dr, "\phi"'] & \mathbb{G}_m^{N-k} \arrow[d, "\overline{\phi}"] \\ & \mathbb{G}_m^{N-k} \end{tikzcd}$$

So

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) | \sigma(\phi(x)) = 0\} = (q-1)^k \#\{x \in \mathbb{G}_m^{N-k}(\mathbb{F}_q) | \sigma(\overline{\phi}(x)) = 0\}.$$

It remains to treat the case of the f.p.p.f. surjective homomorphism

$$\overline{\phi} : \mathbb{G}_m^{N-k} \to \mathbb{G}_m^{N-k},$$

which is a "$k = 0$" case of the theorem. For then we will have

$$\#\{x \in \mathbb{G}_m^{N-k}(\mathbb{F}_q) | \sigma(\overline{\phi}(x)) = 0\} = \frac{(q-1)^{N-k}}{q} + O(q^{(N-k)/2}),$$

and multiplying through by $(q-1)^k$ gives the assertion.

Thus we are reduced to treating universally the case $k = 0$ of the theorem. In this case, we have an f.p.p.f. short exact sequence

$$0 \to \mu_{M_{tors}} \to \mathbb{G}_m^N \xrightarrow{\phi} \mathbb{G}_m^N \to 0,$$

which gives a four term exact sequence of finite groups

$$0 \to \mu_{M_{tors}}(\mathbb{F}_q) \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\phi} \mathbb{G}_m^N(\mathbb{F}_q) \to H^1(Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q), \mu_{M_{tors}}(\overline{\mathbb{F}_q})) \to 0.$$

We rewrite this simply as

$$0 \to Ker \to \mathbb{G}_m^N(\mathbb{F}_q) \xrightarrow{\phi} \mathbb{G}_m^N(\mathbb{F}_q) \to Coker \to 0.$$

In terms of coordinates $(t_1, ..., t_N)$ on the target $\mathbb{G}_m^N(\mathbb{F}_q)$, we have

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) | \sigma(\phi(x)) = 0\} =$$

$$= \#Ker\#\{t \in \mathbb{G}_m^N(\mathbb{F}_q) | \sum_i t_i = 0 \text{ and } t \in \phi(\mathbb{G}_m^N(\mathbb{F}_q))\}.$$

We count the set $\{t \in \mathbb{G}_m^N(\mathbb{F}_q) | \sum_i t_i = 0 \text{ and } t \in \phi(\mathbb{G}_m^N(\mathbb{F}_q))\}$ as follows. To determine if a point $t \in \mathbb{G}_m^N(\mathbb{F}_q)$ lies in the image $\phi(\mathbb{G}_m^N(\mathbb{F}_q))$, i.e. to see if its image in $Coker$ vanishes, we sum all $\mathbb{C}^\times$-valued characters of $Coker$ over t; we will get $\#Coker$ if t lies in the image, and zero otherwise. [We view characters of $Coker$ as characters of $\mathbb{G}_m^N(\mathbb{F}_q)$ which are trivial on the subgroup $\phi(\mathbb{G}_m^N(\mathbb{F}_q))$.] But $\#Ker = \#Coker$, so we have

$$\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) | \sigma(\phi(x)) = 0\} =$$

$$= \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q) | \sum_i t_i = 0} \quad \sum_{\chi \in Coker^\vee} \chi(t).$$

For $t \in \mathbb{G}_m^N(\mathbb{F}_q)$, we determine whether or not $\sum_i t_i = 0$ by choosing a nontrivial $\mathbb{C}^\times$-valued additive character ψ of $\mathbb{F}_q$, and using the fact that $\sum_{a \in \mathbb{F}_q} \psi(a \sum_i t_i)$ will be q if $\sum_i t_i = 0$, and zero if not. Thus our count is

$$= (1/q) \sum_{a \in \mathbb{F}_q} \sum_{\chi \in Coker^\vee} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t)\psi(a \sum_i t_i).$$

The $a = 0$ term is $(1/q) \sum_{\chi \in Coker^\vee} \sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t)$, and the innermost sum vanishes except for $\chi = \mathbb{1}$. So the $a = 0$ term is $(1/q)(q-1)^N$. For each $a \neq 0$ term, and each χ, the sum $\sum_{t \in \mathbb{G}_m^N(\mathbb{F}_q)} \chi(t)\psi(a \sum_i t_i)$ is a product of N Gauss sums, some possibly trivial, so this sum has absolute value at most $q^{N/2}$. The number of such summands is $(q-1)\#Coker$, so we get the explicit estimate

$$|\#\{x \in \mathbb{G}_m^N(\mathbb{F}_q) | \sigma(\phi(x)) = 0\} - \frac{(q-1)^N}{q}| \leq \frac{q-1}{q}(\#Coker)q^{N/2}.$$

As $\#Coker = \#Ker \leq \#M_{tors}$, we have the asserted uniform estimate.

$\square$

References

[De-Mum] Deligne, P., Mumford, D., The irreducibility of the space of curves of given genus. Publ. Math. IHES 36 (1969), 75-109.

[De-Weil I] Deligne, P., La conjecture de Weil I. Publ. Math. IHES 43 (1974), 273-307.

[De-Weil II] Deligne, P., La conjecture de Weil II. Publ. Math. IHES 52 (1981), 313-428.

[Dels] Delsarte, J., Nombre de solutions des équations polynomiales sur un corps fini. Séminaire Bourbaki, Vol. 1, Exp. No. 39, 321-329, Soc. Math. France, Paris, 1995.

[Gr-Lef] Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L. Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41-55, Soc. Math. France, Paris, 1995.

[Ka-GKM] Katz, N.,. Gauss sums, Kloosterman sums, and monodromy groups. Annals of Mathematics Studies, 116. Princeton University Press, Princeton, NJ, 1988. x+246 pp.

[Ka-Sar] Katz, N., and Sarnak, P., Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. xii+419 pp.

[Ka-SFC] Katz, N., Space filling curves over finite fields. Math. Res. Lett. 6 (1999), no. 5-6, 613-624.

[Ka-SFC Corrections] Katz, N., Corrections to: "Space filling curves over finite fields" [Math. Res. Lett. 6 (1999), no. 5-6, 613624]. Math. Res. Lett. 8 (2001), no. 5-6, 689-691.

[Mum] Mumford, D., Geometric invariant theory. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 34 Springer-Verlag, Berlin-New York 1965 vi+145 pp.

[Ran] Rankin, R. A., Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. Proc. Cambridge Philos. Soc. 35, (1939). 351-372.

[Sch] Scholl, A., Hypersurfaces and the Weil conjectures. Int. Math. Res. Not. (2011), no. 5, 1010-1022.

[SGA 4] Séminaire de Géometrie Algebrique du Bois Marie 1963/64 (SGA 4), Springer Lecture Notes in Mathematics 269-270-305.

[Weil] Weil, A., Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. 55, (1949). 497-508.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu