

Some aspects and applications of the Riemann Hypothesis over finite fields

E. Kowalski

April 24, 2009

What is the Riemann Hypothesis over finite fields?

Although it is can be stated in a way quite precisely analogous to the original Riemann Hypothesis, the version over finite fields can take surprising forms in applications.

What is the Riemann Hypothesis over finite fields?

Although it can be stated in a way quite precisely analogous to the original Riemann Hypothesis, the version over finite fields can take surprising forms in applications.

This is particularly the case when the *second form* of the theorem is invoked.

History: P. DELIGNE:
La conjecture de Weil: I,
Publ. Math. IHÉS 43 (1974),

What is the Riemann Hypothesis over finite fields?

Although it can be stated in a way quite precisely analogous to the original Riemann Hypothesis, the version over finite fields can take surprising forms in applications.

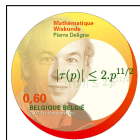
This is particularly the case when the *second form* of the theorem is invoked.

History: P. DELIGNE:

La conjecture de Weil: I,
Publ. Math. IHÉS 43 (1974),

La conjecture de Weil: II,
Publ. Math. IHÉS 52 (1980).

(see <http://www.numdam.org>)



Some examples

Example 1. (Gauss sums) For any prime number p and a integer not divisible by p , we have

$$\left| \sum_{x=1}^p e\left(\frac{ax^2}{p}\right) \right| = \sqrt{p}$$

where $e(z) = e^{2i\pi z}$.

Example 2. (Hasse bound) For any prime $p \neq 2, 3$, any a, b with $4a^3 + 27b^2$ not divisible by p , we have

$$\left| \left| \{(x, y) \in (\mathbf{Z}/p\mathbf{Z})^2 \mid y^2 = x^3 + ax + b\} \right| - p \right| \leq 2\sqrt{p}.$$

Example 2. (Hasse bound) For any prime $p \neq 2, 3$, any a, b with $4a^3 + 27b^2$ not divisible by p , we have

$$\left| \left| \{(x, y) \in (\mathbf{Z}/p\mathbf{Z})^2 \mid y^2 = x^3 + ax + b\} \right| - p \right| \leq 2\sqrt{p}.$$

Example 3. (Hyper-Kloosterman sums) For any p , any $n \geq 1$, any a not divisible by p , we have

$$\left| \sum_{\substack{1 \leq x_1, \dots, x_n \leq p-1 \\ x_1 x_2 \cdots x_n = a}} e\left(\frac{x_1 + \cdots + x_n}{p}\right) \right| \leq np^{(n-1)/2}$$

(Weil for $n = 2$, Deligne for $n \geq 3$).

Definition

Finite sets $X_n \subset X$ become equidistributed in a locally compact metric space X with respect to the measure μ if for all functions $f : X \rightarrow \mathbf{C}$ continuous and bounded, we have

$$\frac{1}{|X_n|} \sum_{x \in X_n} f(x) \longrightarrow \int_X f(x) d\mu(x).$$

Definition

Finite sets $X_n \subset X$ become equidistributed in a locally compact metric space X with respect to the measure μ if for all functions $f : X \rightarrow \mathbf{C}$ continuous and bounded, we have

$$\frac{1}{|X_n|} \sum_{x \in X_n} f(x) \longrightarrow \int_X f(x) d\mu(x).$$

Example 4. (“Average” Sato-Tate law) The sets of angles $(\theta_{p,a})$ in $[0, \pi]$ defined for p prime and $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ by

$$\sum_{x=1}^{p-1} e\left(\frac{x + ax^{-1}}{p}\right) = 2\sqrt{p} \cos \theta_{p,a}$$

become equidistributed, as $p \rightarrow +\infty$, for $\mu = 2/\pi \sin^2 \theta d\theta$ (N. Katz).

Recognizing the hidden hand of Riemann

What corresponds to the Riemann Hypothesis, in these examples, is the presence of bounds involving $p^{m/2}$, where $m \geq 0$ is an integer. The $1/2$ is the link with zeros on the line $\text{Re}(s) = 1/2$.

Recognizing the hidden hand of Riemann

What corresponds to the Riemann Hypothesis, in these examples, is the presence of bounds involving $p^{m/2}$, where $m \geq 0$ is an integer. The $1/2$ is the link with zeros on the line $\operatorname{Re}(s) = 1/2$.

Another, more qualitative, feature is the *uniformity* of all estimates, which is a characteristic effect of using the Riemann Hypothesis.

Recognizing the hidden hand of Riemann

What corresponds to the Riemann Hypothesis, in these examples, is the presence of bounds involving $p^{m/2}$, where $m \geq 0$ is an integer. The $1/2$ is the link with zeros on the line $\text{Re}(s) = 1/2$.

Another, more qualitative, feature is the *uniformity* of all estimates, which is a characteristic effect of using the Riemann Hypothesis. (Uniformity is also characteristic of *sieve methods*...)

Recognizing the hidden hand of Riemann

What corresponds to the Riemann Hypothesis, in these examples, is the presence of bounds involving $p^{m/2}$, where $m \geq 0$ is an integer. The $1/2$ is the link with zeros on the line $\text{Re}(s) = 1/2$.

Another, more qualitative, feature is the *uniformity* of all estimates, which is a characteristic effect of using the Riemann Hypothesis. (Uniformity is also characteristic of *sieve methods*...)

Semi-philosophical point: for a fairly wide range of problems, it is the uniformity which matters.

Setting-up for the Riemann Hypothesis

We introduce the setting of the second form of the Riemann Hypothesis fairly generally, though without all details. Recall the following equivalent formulation of the Generalized Riemann Hypothesis:

$$\sum_{p \leq x} \chi(p) \leq 2\sqrt{x}(\log qx)^2,$$

for $x \geq 2$, for all primitive Dirichlet characters χ with conductor q .

The Riemann Hypothesis over finite fields allows a very detailed understanding of certain sums

$$\sum_{x \in V(\mathbf{F}_q)} \Lambda(x)$$

where V is some algebraic variety and where Λ is a function (often oscillating) of a special algebraic nature.

Although V can be quite general, we will only consider simple cases (one can think, e.g., of the affine line or some affine space, so $V(\mathbf{F}_q) = \mathbf{F}_q^n$ for a fixed $n \geq 1$). On the other hand, we will mention somewhat general choices of $\Lambda(x)$.

The Riemann Hypothesis over finite fields allows a very detailed understanding of certain sums

$$\sum_{x \in V(\mathbf{F}_q)} \Lambda(x)$$

where V is some algebraic variety and where Λ is a function (often oscillating) of a special algebraic nature.

Although V can be quite general, we will only consider simple cases (one can think, e.g., of the affine line or some affine space, so $V(\mathbf{F}_q) = \mathbf{F}_q^n$ for a fixed $n \geq 1$). On the other hand, we will mention somewhat general choices of $\Lambda(x)$.

(This is very much related to the general Langlands philosophy and to the Galois–Motivic sides of the Rosetta stone of L -functions.)

The setup

- ▶ \mathbf{F}_q is a finite field with $q = p^\nu$ elements, $\nu \geq 1$.
- ▶ V/\mathbf{F}_q is an algebraic variety (for instance $V = \mathbf{A}^n$, so $V(\mathbf{F}_q) = \mathbf{F}_q^n$); we see it often as the points $\bar{V} = V(\bar{\mathbf{F}}_q)$ over the algebraic closure, with the action of the *Frobenius automorphism* $x \mapsto x^q$. Write d for the dimension of V .

The setup

- ▶ \mathbf{F}_q is a finite field with $q = p^\nu$ elements, $\nu \geq 1$.
- ▶ V/\mathbf{F}_q is an algebraic variety (for instance $V = \mathbf{A}^n$, so $V(\mathbf{F}_q) = \mathbf{F}_q^n$); we see it often as the points $\bar{V} = V(\bar{\mathbf{F}}_q)$ over the algebraic closure, with the action of the *Frobenius automorphism* $x \mapsto x^q$. Write d for the dimension of V .

Further data provided by the theory (Grothendieck,...):

- ▶ A compact group $\Pi_1 = \Pi_1(V)$ and a normal subgroup $\Pi_1(\bar{V})$;

The setup

- ▶ \mathbf{F}_q is a finite field with $q = p^\nu$ elements, $\nu \geq 1$.
- ▶ V/\mathbf{F}_q is an algebraic variety (for instance $V = \mathbf{A}^n$, so $V(\mathbf{F}_q) = \mathbf{F}_q^n$); we see it often as the points $\bar{V} = V(\bar{\mathbf{F}}_q)$ over the algebraic closure, with the action of the *Frobenius automorphism* $x \mapsto x^q$. Write d for the dimension of V .

Further data provided by the theory (Grothendieck,...):

- ▶ A compact group $\Pi_1 = \Pi_1(V)$ and a normal subgroup $\Pi_1(\bar{V})$;
- ▶ Well-defined *Frobenius conjugacy classes* F_x in Π_1 , for every $x \in V(\mathbf{F}_q)$.

The summands

To define the summands $\Lambda(x)$, we need to first fix some prime number $\ell \neq p$. Then we consider *continuous group homomorphisms*

$$\rho : \Pi_1(V) \rightarrow GL(r, K)$$

where K is a finite extension of the ℓ -adic field \mathbf{Q}_ℓ such that:

The summands

To define the summands $\Lambda(x)$, we need to first fix some prime number $\ell \neq p$. Then we consider *continuous group homomorphisms*

$$\rho : \Pi_1(V) \rightarrow GL(r, K)$$

where K is a finite extension of the ℓ -adic field \mathbf{Q}_ℓ such that:

For all $x \in V(\mathbf{F}_{q^m})$, $m \geq 1$, the eigenvalues of $\rho(F_x)$ are algebraic numbers, and $|\alpha| = q^{mw(x)/2}$ for all eigenvalues, $w(x) \in \mathbf{Z}$ depending only (possibly) on x .

(This is called a q^m -Weil number of weight $w(x)$).

The summands

To define the summands $\Lambda(x)$, we need to first fix some prime number $\ell \neq p$. Then we consider *continuous group homomorphisms*

$$\rho : \Pi_1(V) \rightarrow GL(r, K)$$

where K is a finite extension of the ℓ -adic field \mathbf{Q}_ℓ such that:

For all $x \in V(\mathbf{F}_{q^m})$, $m \geq 1$, the eigenvalues of $\rho(F_x)$ are algebraic numbers, and $|\alpha| = q^{mw(x)/2}$ for all eigenvalues, $w(x) \in \mathbf{Z}$ depending only (possibly) on x .

(This is called a q^m -Weil number of weight $w(x)$).

Then, the general theory can analyze quite precisely the sums

$$S(V, \rho) = \sum_{x \in V(\mathbf{F}_q)} \text{Tr}(\rho(F_x)).$$

Examples

Example 1. We can always take $\rho = 1$. The stated condition is obviously true with $w(x) = 0$ for all x . The sum is just $|V(\mathbf{F}_q)|$, the number of rational points on V .

Examples

Example 1. We can always take $\rho = 1$. The stated condition is obviously true with $w(x) = 0$ for all x . The sum is just $|V(\mathbf{F}_q)|$, the number of rational points on V .

Example 2. Take $q = p$. For any regular function f on V (e.g., $f(x)$ a polynomial of n variables if $V = \mathbf{A}^n$), there exists a ρ_f with $r = 1$ such that the only eigenvalue (and the trace!) of $\rho(F_x)$ is $e\left(\frac{f(x)}{p}\right)$, so $w(x) = 0$ and the sum $S(V, \rho_f)$ is a fairly arbitrary additive exponential sum.

Examples

Example 1. We can always take $\rho = 1$. The stated condition is obviously true with $w(x) = 0$ for all x . The sum is just $|V(\mathbf{F}_q)|$, the number of rational points on V .

Example 2. Take $q = p$. For any regular function f on V (e.g., $f(x)$ a polynomial of n variables if $V = \mathbf{A}^n$), there exists a ρ_f with $r = 1$ such that the only eigenvalue (and the trace!) of $\rho(F_x)$ is $e\left(\frac{f(x)}{p}\right)$, so $w(x) = 0$ and the sum $S(V, \rho_f)$ is a fairly arbitrary additive exponential sum.

Example 3. (“Functoriality”) This comes for free: given ρ , consider any algebraic homomorphism $\pi : GL(r) \rightarrow GL(d)$ and form the composite

$$\Pi_1(V) \xrightarrow{\rho} GL(r, K) \xrightarrow{\pi} GL(d, K)$$

(e.g., symmetric powers).

Analysis of the sums

The main transformational tool here is the *Grothendieck-Lefschetz trace formula*: given the data, there are finite-dimensional K -vector spaces $H_c^i(\bar{V}, \rho)$, with an action of the global Frobenius of V , such that

$$S(V, \rho) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}(F \mid H_c^i(\bar{V}, \rho)).$$

Analysis of the sums

The main transformational tool here is the *Grothendieck-Lefschetz trace formula*: given the data, there are finite-dimensional K -vector spaces $H_c^i(\bar{V}, \rho)$, with an action of the global Frobenius of V , such that

$$S(V, \rho) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}(F \mid H_c^i(\bar{V}, \rho)).$$

Example. (Trivial) Take a 0-dimensional V defined by the equation $f(x) = 0$ where $f \in \mathbf{F}_q[X]$, $f \neq 0$. Then $\Pi_1(V)$ is the Galois group of the splitting field of f ; take $\rho = 1$, and the formula is

$$\begin{aligned} |\{x \in \mathbf{F}_q \mid f(x) = 0\}| &= \operatorname{Tr}(F \mid H_c^0(\text{zeros of } f)) \\ &= \operatorname{Tr}(\text{permutation matrix of } F \text{ on the roots of } f). \end{aligned}$$

The original Weil conjecture(s)

Take V smooth projective, $\rho = 1$. Apply the formula to q^m for all $m \geq 1$; then the formula becomes

$$|V(\mathbf{F}_{q^m})| = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}(F^m \mid H^i(\bar{V}))$$

and multiplying by T^m and summing we get

$$\exp\left(\sum_{m \geq 1} \frac{|V(\mathbf{F}_{q^m})| T^m}{m}\right) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2d}(T)},$$

with $P_i = \det(1 - TF \mid H^i(\bar{V}))$, i.e., the rationality of the zeta function of V .

The original Weil conjecture(s)

Take V smooth projective, $\rho = 1$. Apply the formula to q^m for all $m \geq 1$; then the formula becomes

$$|V(\mathbf{F}_{q^m})| = \sum_{i=0}^{2n} (-1)^i \operatorname{Tr}(F^m \mid H^i(\bar{V}))$$

and multiplying by T^m and summing we get

$$\exp\left(\sum_{m \geq 1} \frac{|V(\mathbf{F}_{q^m})| T^m}{m}\right) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2d}(T)},$$

with $P_i = \det(1 - TF \mid H^i(\bar{V}))$, i.e., the rationality of the zeta function of V .

Poincaré duality then gives the functional equation, which relates $Z(V, T)$ and $Z(V, (qT)^{-d})$.

Example: curves

For a smooth projective geometrically connected curve C/\mathbf{F}_q , we get

$$\exp\left(\sum_{m \geq 1} \frac{|C(\mathbf{F}_{q^m})| T^m}{m}\right) = \frac{P_1(T)}{P_0(T)P_2(T)},$$

where $\deg(P_1) = 2g$, $g \geq 0$ being the genus of the curve. One can show easily that $P_0(T) = 1 - T$, $P_2(T) = 1 - qT$.

Example: curves

For a smooth projective geometrically connected curve C/\mathbf{F}_q , we get

$$\exp\left(\sum_{m \geq 1} \frac{|C(\mathbf{F}_{q^m})| T^m}{m}\right) = \frac{P_1(T)}{P_0(T)P_2(T)},$$

where $\deg(P_1) = 2g$, $g \geq 0$ being the genus of the curve. One can show easily that $P_0(T) = 1 - T$, $P_2(T) = 1 - qT$. If we write

$$P_1(T) = \det(1 - TF \mid H^1(\bar{C})) = \prod_{1 \leq j \leq 2g} (1 - \alpha_j T)$$

then $|\alpha_j| = \sqrt{q}$ and $\alpha_j \alpha_{2g+1-j} = q$ (for some numbering). This was first proved by Weil, and there are now very elementary proofs (Stepanov, W. Schmidt, Bombieri).

Digression on étale topology

It can be difficult to get a good feeling of what the étale cohomology groups are. One observation that can at least give a feel-good impression is the following:

Digression on étale topology

It can be difficult to get a good feeling of what the étale cohomology groups are. One observation that can at least give a feel-good impression is the following:

- ▶ Localizing close to x in the Zariski topology amounts to allowing “new” functions $1/f$, where f is regular at x , but may vanish elsewhere;

Digression on étale topology

It can be difficult to get a good feeling of what the étale cohomology groups are. One observation that can at least give a feel-good impression is the following:

- ▶ Localizing close to x in the Zariski topology amounts to allowing “new” functions $1/f$, where f is regular at x , but may vanish elsewhere;
- ▶ “Localizing” close to x in the étale topology “allows” new functions $g(x)$ which satisfy (separable) algebraic equations, e.g., $g(x) = \sqrt{x}$ on the affine line minus 0, via the second projection $R = \{(x, y) \mid x = y^2\} \rightarrow \mathbf{G}_m$

The Deligne Riemann Hypothesis

Assume $w(x) \leq k$ for all $x \in \bar{V}$, for some fixed k . Then Deligne proved in Weil II (using L -functions, families...) that

Every eigenvalue of F acting on $H_c^i(\bar{V}, \rho)$ is a q -Weil integer of some weight $\leq k + i$, i.e., an algebraic integer with all conjugates of modulus $|\alpha| \leq q^{(i+k)/2}$.

Sometimes, if $w(x) = k$ for all x , and under relatively favorable circumstances, there is equality $|\alpha| = q^{(k+i)/2}$.

The Deligne Riemann Hypothesis

Assume $w(x) \leq k$ for all $x \in \bar{V}$, for some fixed k . Then Deligne proved in Weil II (using L -functions, families...) that

Every eigenvalue of F acting on $H_c^i(\bar{V}, \rho)$ is a q -Weil integer of some weight $\leq k + i$, i.e., an algebraic integer with all conjugates of modulus $|\alpha| \leq q^{(i+k)/2}$.

Sometimes, if $w(x) = k$ for all x , and under relatively favorable circumstances, there is equality $|\alpha| = q^{(k+i)/2}$.

For the P_i of the original Weil Conjecture for V/\mathbf{F}_q , this is the case, and it translates to

The Deligne Riemann Hypothesis

Assume $w(x) \leq k$ for all $x \in \bar{V}$, for some fixed k . Then Deligne proved in Weil II (using L -functions, families...) that

Every eigenvalue of F acting on $H_c^i(\bar{V}, \rho)$ is a q -Weil integer of some weight $\leq k + i$, i.e., an algebraic integer with all conjugates of modulus $|\alpha| \leq q^{(i+k)/2}$.

Sometimes, if $w(x) = k$ for all x , and under relatively favorable circumstances, there is equality $|\alpha| = q^{(k+i)/2}$.

For the P_i of the original Weil Conjecture for V/\mathbf{F}_q , this is the case, and it translates to

All zeros of $L_i(V, S) = P_i(q^{-s})$ satisfy $\operatorname{Re}(s) = i/2$.

Example. (Weil $n = 2$, Deligne $n \geq 3$) Take $\rho = \rho_f$ for a polynomial of degree d in n variables such that the homogeneous part of degree d , say f_d , defines a smooth hypersurface. (E.g., $f_d(x) = x_1^d + \cdots + x_n^d$). Then

$$H_c^i(\rho_f) = 0 \text{ if } i \neq n, \quad \dim H_c^n(\rho_f) = (d - 1)^n.$$

Example. (Weil $n = 2$, Deligne $n \geq 3$) Take $\rho = \rho_f$ for a polynomial of degree d in n variables such that the homogeneous part of degree d , say f_d , defines a smooth hypersurface. (E.g., $f_d(x) = x_1^d + \cdots + x_n^d$). Then

$$H_c^i(\rho_f) = 0 \text{ if } i \neq n, \quad \dim H_c^n(\rho_f) = (d-1)^n.$$

Hence we get

$$|S_f(p)| = \left| \sum_{1 \leq x_1, \dots, x_n \leq p} e\left(\frac{f(x)}{p}\right) \right| \leq (d-1)^n p^{n/2}$$

for such polynomials.

Bringing the family along

By the previous result and the Riemann Hypothesis, we can write

$$S_f(p) = p^{n/2}(\alpha_{f,1} + \cdots + \alpha_{f,b})$$

with $b = (d - 1)^n$, $|\alpha_{f,j}| = 1$. And all f over \mathbf{F}_q of degree d can be thought of as given by freely chosen coefficients, with non-vanishing conditions for the top-degree part.

Bringing the family along

By the previous result and the Riemann Hypothesis, we can write

$$S_f(p) = p^{n/2}(\alpha_{f,1} + \cdots + \alpha_{f,b})$$

with $b = (d - 1)^n$, $|\alpha_{f,j}| = 1$. And all f over \mathbf{F}_q of degree d can be thought of as given by freely chosen coefficients, with non-vanishing conditions for the top-degree part.

In other words, there is another algebraic variety D_d/\mathbf{Z} (defined by non-vanishing of some integral polynomials) such that the polynomials over \mathbf{F}_q correspond bijectively to $D_d(\mathbf{F}_q)$.

And it turns out, by the general theory, that there is a

$$\tilde{\rho}_d : \Pi_1(D_d) \rightarrow GL((d-1)^n, K)$$

for some K/\mathbf{Q}_ℓ such that for any q and $f \in D_d(\mathbf{F}_q)$

$$\mathrm{Tr}(\tilde{\rho}_d(F_f)) = \sum_{x \in \mathbf{F}_q^m} e\left(\frac{\mathrm{Tr}(f(x))}{p}\right).$$

And it turns out, by the general theory, that there is a

$$\tilde{\rho}_d : \Pi_1(D_d) \rightarrow GL((d-1)^n, K)$$

for some K/\mathbf{Q}_ℓ such that for any q and $f \in D_d(\mathbf{F}_q)$

$$\mathrm{Tr}(\tilde{\rho}_d(F_f)) = \sum_{x \in \mathbf{F}_q^m} e\left(\frac{\mathrm{Tr}(f(x))}{p}\right).$$

This is a general feature, and this is the key to understanding variations of exponential sums in families (such as the vertical Sato-Tate laws) and in particular the Katz-Sarnak philosophy and results.

Monodromy

Suppose (as in the case above) that the weight k is constant and equal to zero. The eigenvalues of $\rho(F_x)$ define a conjugacy class θ_x in $U(r, \mathbf{C})$.

Monodromy

Suppose (as in the case above) that the weight k is constant and equal to zero. The eigenvalues of $\rho(F_x)$ define a conjugacy class θ_x in $U(r, \mathbf{C})$.

Theorem (Deligne's Equidistribution Theorem)

As $q \rightarrow +\infty$, $\{\theta_x\}_{x \in V(\mathbf{F}_q)}$ become equidistributed for Haar measure in a compact subgroup $H \subset U(r, \mathbf{C})$,

Monodromy

Suppose (as in the case above) that the weight k is constant and equal to zero. The eigenvalues of $\rho(F_x)$ define a conjugacy class θ_x in $U(r, \mathbf{C})$.

Theorem (Deligne's Equidistribution Theorem)

As $q \rightarrow +\infty$, $\{\theta_x\}_{x \in V(\mathbf{F}_q)}$ become equidistributed for Haar measure in a compact subgroup $H \subset U(r, \mathbf{C})$, whose connected component is a maximal compact subgroup of the geometric monodromy group G^g of ρ , which "is" the Zariski closure of $\rho(\Pi_1(\bar{V}))$, provided $\rho(F_x) \in G^g(\bar{K})$ for all x .

Monodromy

Suppose (as in the case above) that the weight k is constant and equal to zero. The eigenvalues of $\rho(F_x)$ define a conjugacy class θ_x in $U(r, \mathbf{C})$.

Theorem (Deligne's Equidistribution Theorem)

As $q \rightarrow +\infty$, $\{\theta_x\}_{x \in V(\mathbf{F}_q)}$ become equidistributed for Haar measure in a compact subgroup $H \subset U(r, \mathbf{C})$, whose connected component is a maximal compact subgroup of the geometric monodromy group G^g of ρ , which "is" the Zariski closure of $\rho(\Pi_1(\bar{V}))$, provided $\rho(F_x) \in G^g(\bar{K})$ for all x .

This is a tremendous generalization of Dirichlet's Theorem on primes in arithmetic progressions.

The proof is not so difficult with the general formalism: consider an irreducible representation π of G^g :

$$\Pi_1(V) \rightarrow G^g(\bar{K}) \xrightarrow{\pi} GL(\dim \pi).$$

By harmonic analysis, one must show that

$$\frac{1}{|V(\mathbf{F}_q)|} \sum_{x \in V(\mathbf{F}_q)} \text{Tr } \pi \rho(F_x) \rightarrow 0$$

as q grows.

The proof is not so difficult with the general formalism: consider an irreducible representation π of G^g :

$$\Pi_1(V) \rightarrow G^g(\bar{K}) \xrightarrow{\pi} GL(\dim \pi).$$

By harmonic analysis, one must show that

$$\frac{1}{|V(\mathbf{F}_q)|} \sum_{x \in V(\mathbf{F}_q)} \text{Tr } \pi \rho(F_x) \rightarrow 0$$

as q grows. The composite is still subject to Deligne's result, and since $|V(\mathbf{F}_q)| \gg q^n$, it is only needed to show

$$H_c^{2n}(\bar{V}, \pi \rho) = 0.$$

(at least for fixed p).

The proof is not so difficult with the general formalism: consider an irreducible representation π of G^g :

$$\Pi_1(V) \rightarrow G^g(\bar{K}) \xrightarrow{\pi} GL(\dim \pi).$$

By harmonic analysis, one must show that

$$\frac{1}{|V(\mathbf{F}_q)|} \sum_{x \in V(\mathbf{F}_q)} \text{Tr } \pi \rho(F_x) \rightarrow 0$$

as q grows. The composite is still subject to Deligne's result, and since $|V(\mathbf{F}_q)| \gg q^n$, it is only needed to show

$$H_c^{2n}(\bar{V}, \pi \rho) = 0.$$

(at least for fixed ρ). A general result states this is

$$H_c^{2n}(\bar{V}, \pi \rho) = V_\pi^{\rho(\Pi_1^g)} = V_\pi^{G^g} = 0 \quad (\text{by irreducibility}).$$

Sieve

The need to select a prime $p \neq \ell$ may look like a bother since so much seems independent of it. However, this gives the possibility of controlling *reductions modulo primes*, since the ℓ -adic integers give a reduction $\mathbf{Z}_\ell \rightarrow \mathbf{Z}/\ell\mathbf{Z}$. This, and equidistribution, is the input for sieve theory but we must have control of many ℓ .

Theorem (K., 2006, 2008)

Let q be odd, $f \in \mathbf{F}_q[X]$ squarefree of degree $2g \geq 2$. Consider the family of curves of genus g given by $C_t : y^2 = f(x)(x - t)$, its L -functions

$$L(C_t) = P_1(C_t) = \prod_{1 \leq j \leq 2g} (1 - \alpha_{t,j} T), \quad |\alpha_{t,j}| = \sqrt{q}.$$

Then

$$|\{t \in \mathbf{F}_q \mid P_1(C_t) \text{ has small Galois group}\}| \ll g^2 q^{1-\gamma_g}$$

for some $\gamma_g \approx 1/4g^2$, and absolute implied constant.

Crucial input (J-K. Yu, C. Hall): the image modulo ℓ of Π_1^g is all of $Sp(2g, \mathbf{F}_\ell)$ for all $\ell \neq 2, p$.

Problems

- ▶ What happens with “short sums”, where the summation set loses algebraicity? E.g., non-trivial bounds for

$$\sum_{1 \leq x \leq p^\theta} e\left(\frac{\bar{x}}{p}\right)$$

if $\theta < 1/2$? (cf. Burgess bound).

Problems

- ▶ What happens with “short sums”, where the summation set loses algebraicity? E.g., non-trivial bounds for

$$\sum_{1 \leq x \leq p^\theta} e\left(\frac{\bar{x}}{p}\right)$$

if $\theta < 1/2$? (cf. Burgess bound).

- ▶ What happens with “larger degree”, where the degree of the L -function overwhelms the saving from Riemann Hypothesis, e.g.

$$\sum_{1 \leq x \leq p} e\left(\frac{f(x)}{p}\right)$$

if $\deg(f) > p^{1/2}$? (Bourgain, Konyagin, Heath-Brown, “sum-product”, ...)

- ▶ Katz-Sarnak for fixed q and genus/conductor growing? Here arithmetic factors like the Euler product a_k of Keating-Snaith should appear. One (easy) case known: dimension 0 (K.–Nikeghbali)!

- ▶ Katz-Sarnak for fixed q and genus/conductor growing? Here arithmetic factors like the Euler product a_k of Keating-Snaith should appear. One (easy) case known: dimension 0 (K.–Nikeghbali)!
- ▶ Variation with p : the dependency of additive exponential sums with p is not yet entirely understood (Katz: “exponential sums over \mathbf{Z} ”).

- ▶ Katz-Sarnak for fixed q and genus/conductor growing? Here arithmetic factors like the Euler product a_k of Keating-Snaith should appear. One (easy) case known: dimension 0 (K.–Nikeghbali)!
- ▶ Variation with p : the dependency of additive exponential sums with p is not yet entirely understood (Katz: “exponential sums over \mathbf{Z} ”). In particular, we have the horizontal Sato-Tate conjecture: do we have

$$\frac{1}{\pi(x)} \sum_{p \leq x} f(\theta_{p,1}) \rightarrow \frac{2}{\pi} \int_0^\pi f(\theta) \sin^2 \theta d\theta,$$

- ▶ Katz-Sarnak for fixed q and genus/conductor growing? Here arithmetic factors like the Euler product a_k of Keating-Snaith should appear. One (easy) case known: dimension 0 (K.–Nikeghbali)!
- ▶ Variation with p : the dependency of additive exponential sums with p is not yet entirely understood (Katz: “exponential sums over \mathbf{Z} ”). In particular, we have the horizontal Sato-Tate conjecture: do we have

$$\frac{1}{\pi(x)} \sum_{p \leq x} f(\theta_{p,1}) \rightarrow \frac{2}{\pi} \int_0^\pi f(\theta) \sin^2 \theta d\theta,$$

(Almost nothing known; Fouvry–Michel have some results for Kloosterman sums with ‘almost prime’ moduli, Duke–Friedlander–Iwaniec, using spectral theory for $GL(2)$ have solved the analogue for Salié sums).

- ▶ Make the theory “easier to apply”;

- ▶ Make the theory “easier to apply”; e.g., can one transparently guess the link between

$$L(1/2, \chi_d) \ll_{\varepsilon} |d|^{1/6+\varepsilon}, \quad \text{for all } \varepsilon > 0,$$

where χ_d is a real primitive character (Conrey–Iwaniec)

- ▶ Make the theory “easier to apply”; e.g., can one transparently guess the link between

$$L(1/2, \chi_d) \ll_{\varepsilon} |d|^{1/6+\varepsilon}, \quad \text{for all } \varepsilon > 0,$$

where χ_d is a real primitive character (Conrey–Iwaniec) and estimating

$$\sum_{x,y \bmod p} \chi(xy(x+1)(y+1)) e\left(\frac{xy-1}{p}\right)$$

where $\chi \neq 1$ is a multiplicative character modulo p ?