Nick Katz June 4, 2007 AIM

Weil conjectures, étale cohomology and what we can do with them.

1. From $X/\mathbb{C}$ to $X/\mathbb{F}_q$.

"spreading out"

$X/\mathbb{C}$; finite # equations & variables hence finite # of coefficients. These coefficients lie in a f.g. $\mathbb{Z}$-algebra. Hence equations for X have coefficients in R. For example, take

$$R = \mathbb{Z}[\text{coeffs}] \subseteq \mathbb{C}$$

E.g. all coefficients are in $\mathbb{Z}$, take $R = \mathbb{Z}$.

Key fact Every maximal ideal of R has a finite residue field. Moreover, almost every prime p occurs as a characteristic.

Always allowed to increase R as necessary; actual ring is mostly immaterial.

2. Zeta functions of $X/\mathbb{F}_q$

$\# X(\mathbb{F}_q)$ is finite

Unique extension of each of deg n: $\mathbb{F}_{q^n}$

$$\{\# X(\mathbb{F}_{q^n})\}_{n\geq 1}$$

$$Z(X/\mathbb{F}_q, T) := \exp\left(\sum_{n\geq 1} \frac{T^n}{n} \# X(\mathbb{F}_{q^n})\right)$$

a priori $\in \mathbb{Q}[[T]]$

e.g. 1) $X/\mathbb{F}_q = \cdot$ a point, $\mathrm{Spec}(\mathbb{F}_q) = \mathbb{A}^0$

$$Z(\cdot, T) = \exp\left(\sum_{n\geq 1} \frac{T^n}{n}\right) = \frac{1}{1-T}$$

2) $X = \mathbb{A}^d$, $\# X(\mathbb{F}_{q^n}) = q^{nd}$

$$Z(\mathbb{A}^d, T) = \frac{1}{1-Tq^d}$$

3) $X = \mathbb{P}^1$, $\# X(\mathbb{F}_{q^n}) = q^n + 1$

$$Z(\mathbb{P}^1, T) = \frac{1}{(1-T)(1-qT)}$$

Historical aside Less intuitive notion

"closed point" of X := orbit of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ in $X(\overline{\mathbb{F}}_q)$

degree := # orbit (deg of smallest field of definition of a point in the orbit)

B_r := # closed points of degree r

$$\# X(\mathbb{F}_{q^n}) = \sum_{r \mid n} r B_r$$

With this we have

$$Z(X/\mathbb{F}_q, T) = \prod_{\substack{\text{closed} \\ \text{pts} \\ \mathfrak{p}}} \left(\frac{1}{1 - T^{\deg \mathfrak{p}}} \right)$$

$$\left(\overset{\text{OR}}{=} \prod_{r \geq 1} (1 - T^r)^{-B_r} \right)$$

In particular: $Z(X/\mathbb{F}_q, T) \in 1 + T\mathbb{Z}[\![T]\!]$

Replace T by q^{-s}

$$\prod_{\substack{\text{closed} \\ \text{point} \\ \mathfrak{p}}} \frac{1}{1 - N\mathfrak{p}^{-s}}$$

This is analogous to the definition of the zeta function of a number field.

<u>Artin's thesis</u> (1923) Computes Z for some hyperelliptic curves.

(1931) F.K. Schmidt X = proj. nonsing. geom. connected curve

$$Z(X/\mathbb{F}_q, T) = \frac{P_{2g}(T)}{(1-T)(1-qT)}$$

$$P_{2g}(T) = \prod_{i=1}^{2g} (1-\alpha_i T)$$

$\alpha_i \mapsto q/\alpha_i$ permutes the α's. (in $T = q^{-s}$ variable this corresponds to $s \longleftrightarrow 1-s$).

Riemman hypothesis here would mean

$$|\alpha_i| = \sqrt{q}$$

(proved later by Weil).

(1949) Weil counting points of X over finite fields $\rightsquigarrow$ Weil conjectures.

<u>1st breakthrough</u>: (50's) Dwork Z is a ratnl fctn for any $X/\mathbb{F}_q$,

$$Z(X/\mathbb{F}_q, T) = \frac{P(T)}{Q(T)}$$

$$P, Q \in 1 + T\mathbb{Z}[T]$$

$$P(T) = \prod (1 - \alpha_i T)$$

$$Q(T) = \prod (1 - \beta_j T)$$

$$\rightsquigarrow \quad \# X(\mathbb{F}_{q^n}) = \sum_j \beta_j^n - \sum_i \alpha_i^n$$

In particular:

If we have an a priori bound ~~on~~ $m \geq \deg P + \deg Q$ then the finitely many

$\# X(\mathbb{F}_{q^k}) \quad k = 1, 2, \dots, m$

determine all the rest.

E.g. $\quad Z(E/\mathbb{F}_q, T) \qquad E =$ elliptic curve

is determined by $\# E(\mathbb{F}_q)$

THM (Grothendieck et al) $\quad X/\mathbb{F}_q$

for every prime number $\ell \neq p := \mathrm{char}(\mathbb{F}_q)$

There exists a theory of "cohomology w/ compact support for varieties $/\overline{\mathbb{F}}_q$ with coefficients in $\mathbb{Q}_\ell$

$$X \rightsquigarrow H^j_c(X \underset{\mathbb{F}_q}{\otimes} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$$

finite dimension vector space $/\mathbb{Q}_\ell$

0 for $i<0$ and $i>2\dim X$

w/ all "expected properties"

e.g. excision sequence

$$U \subseteq X \quad Y := X \setminus U$$

$$\cdots H_c^i(U) \to H_c^i(X) \to H_c^i(Y) \to H_c^{i+1}(U) \to \cdots$$

$$X \circlearrowleft \mathrm{Frob}_q$$

$X(\overline{\mathbb{F}}_q) \circlearrowleft$ fixed points are $X(\mathbb{F}_q)$

and in general

$$X(\overline{\mathbb{F}}_q)^{\mathrm{Frob}_q^n} = X(\mathbb{F}_{q^n})$$

<u>Lefschetz Trace Formula</u>

1) $$\sum_i (-1)^i \operatorname{tr}\left(\mathrm{Frob}_q^n \,\middle|\, H_c^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)\right) = \# X(\mathbb{F}_{q^n})$$

2) $$Z(X/\mathbb{F}_q, T) = \prod_{i=0}^{2\dim X} \det\left(1 - T\,\mathrm{Frob}_q \,\middle|\, H_c^i\right)^{(-1)^{i+1}}$$

(these are equivalent)

For each $\ell \neq p$ we have an ℓ-adic "factorization" of Z.

Let $P_{i,\ell} := \det(1 - T\,\mathrm{Frob}_q \mid H^i_c)$

surely it has coeff. in $\mathbb{Z}$ and is independent of ℓ. This however is still open. In fact, we don't even know that $\deg P_{i,\ell} = \dim_{\mathbb{Q}_\ell} H^i_c$

Why do we need ℓ at all?

(Serre) If there was a cohomology over $\mathbb{Q}$ we'd have End acting on it. For a super singular elliptic curve over $\mathbb{F}_q$, $\mathbb{Q}\otimes\mathrm{End}$ is a quaternion algebra non-split at p, ∞ (i.e. it's a division algebra after tensoring w/ $\mathbb{Q}_p$ or $\mathbb{R}$) By functoriality $\mathrm{End}(E)\otimes\mathbb{Q}$ would act on the 2-diml space $\tilde{H}(E,\mathbb{Q})$ which would mean the algebra is split for every prime $*$. No problem with $\tilde{H}(E,\mathbb{Q}_\ell)$ for $\ell \neq p, \infty$.

3. Deligne Weil II results

Fix $X/\mathbb{F}_q$, $\ell \neq p$.

$H^i_c \circlearrowleft \mathrm{Frob}_q$

ℓ-adic

eigenvalues $\{ \alpha_{\nu,i} \}$ $\nu = 1, \dots, \dim H^i_c$
$\in \overline{\mathbb{Q}}_\ell$

1) These $\alpha_{\nu,i}$'s are algebraic integers.

2) For each $\alpha_{\nu,i}$ there is an integer $w = w(\alpha_{\nu,i})$ (weight of $\alpha_{\nu,i}$)

$0 \leq w \leq i$

$$|\alpha_{\nu,i}^{\sigma}|_{\mathbb{C}} = q^{\frac{1}{2}w}$$

all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

3) If $X/\mathbb{F}_q$ is proper & smooth then each $\alpha_{\nu,i}$ has weight i

($\Rightarrow$ "independence of ℓ" question is true for smooth & projective X)

4. Back to $X/\mathbb{C}$

$$X/\mathbb{C} \xrightarrow[\text{spread out}]{\rightsquigarrow} \mathcal{X}/R$$

$R \subseteq \mathbb{C}$

f.g. $\mathbb{Z}$-algebra

THM (Grothendieck)

$\mathcal{X}/R$ There exits $r \in R$, $r \neq 0$

s.t. replacing R by $R[\frac{1}{r}]$

For every prime ℓ and maximal ideal m of $R[\frac{1}{r\ell}]$ with residue field k

$$H^i_c((\mathcal{X} \bmod m) \otimes_k \bar{k}, \mathbb{Q}_\ell)$$

$$\underset{\uparrow}{\simeq} \quad H^i_c(X(\mathbb{C})^{an}, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$$

as $\mathbb{Q}_\ell$-vector spaces.

Cor. The dim of $H^i_c((\mathcal{X} \bmod m) \otimes_k \bar{k}, \mathbb{Q}_\ell)$

$= \deg P_{i,\ell} = h^i_c(\mathbb{Q})$ indep of ℓ

Don't know that $P_{i,\ell}$ are indep of ℓ.

Remark

If $\mathcal{X}/R$ is smooth & projective then we can take $r = 1$.

Example (Independence of ℓ)

$X/\mathbb{F}_q$ projective & smooth

$Y \subseteq X$ closed smooth subvariety

$$\cdots \to H_c^{i-1}(Y) \to H_c^i(X \setminus Y, \mathbb{Q}_\ell) \to H_c^i(X) \to H_c^i(Y) \to \cdots$$

$$0 \to H_c^{i-1}(Y)/H_c^{i-1}(X) \to H_c^i(X \setminus Y) \to \mathrm{Ker}\left(H_c^i(X) \to H_c^i(Y)\right) \to 0$$

If we start with $X/\mathbb{C}$ the dimension of 2 terms each is indep of ℓ . themw don't know indep. of ℓ even of dim.

We never know the eigenvalues are indep of ℓ.

5. (Fontaine-Messing, Faltings)

$X/\mathbb{C}$ proper & smooth

$\rightsquigarrow \mathcal{X}/R$ proper & smooth

Ditto $Y/\mathbb{C} \rightsquigarrow \mathcal{Y}/R$ proper & smooth

Assume $\mathcal{X} \bmod \mathfrak{m}$ & $\mathcal{Y} \bmod \mathfrak{m}$ have the <u>same</u> zeta function for all maximal. $\mathfrak{m}$ of R

Then $X/\mathbb{C}$ and $Y/\mathbb{C}$ have the same $h^{p,q}$ (D. Wang)

Say $R = \mathbb{Z}[\frac{1}{N}]$

$\mathcal{X} \bmod p$, $\mathcal{Y} \bmod p$ $\quad p \nmid N$

$P_i(\mathcal{X} \bmod p) = P_i(\mathcal{Y} \bmod p)$

indep of ℓ, $\mathbb{Z}$-coeff.

given $\{P_i(\mathcal{X} \bmod p)\} \rightsquigarrow h^{a,b}$ $\quad a+b=i$?

<u>Conjectural answer</u>

$$P_i(\mathcal{X} \bmod p) = \prod_{j=1}^{b_i(X)} (1 - \alpha_{j,p} T)$$

$\alpha_{j,p}$ alg integers indep of ℓ

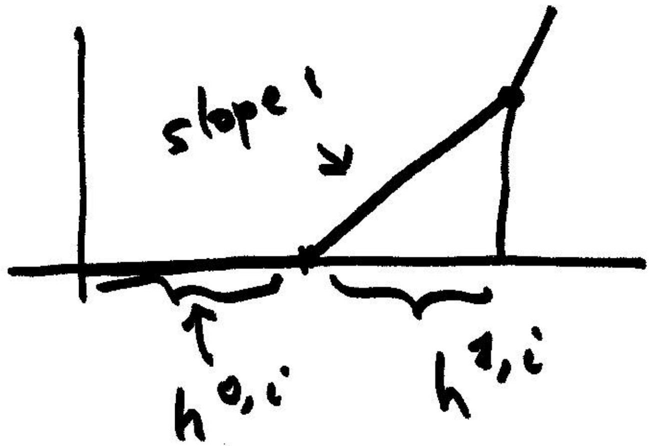
View this over $\mathbb{Q}_p \subseteq \overline{\mathbb{Q}}_p$

<u>Newton polygon</u> at p for $P_i(\mathcal{X} \bmod p)$

arrange $\alpha_{i,p}$ according to ord_p (increasing order)

slopes are $\mathrm{ord}_p(\alpha_{1,p}) \ldots$

Hodge polygon of $H^i(X)$



THM (Mazur) Newton $\geq$ Hodge
(i.e. one polygon is above the other)

CONJ Newton = Hodge for infinitely many reductions.

Some restrictions on Newton polygon
- slope $1/s$ occurs an s multiple of times
- if s is a slope $1-s$ also.