(82 yrs old)

Variation with p of the number $N(p)$ of solutions mod p of poly equations.

Introduction:

(1) Def of $N(p)$.

$f_\alpha(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$

$N(p) = |(x_1, \dots, x_n),\ x_i \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,\ f_\alpha(x) = 0$ in $\mathbb{Z}/p\mathbb{Z}$ for every α $|$

$A = \mathbb{Z}[X]/f$ ring of finite type over $\mathbb{Z}$.

$(x) \in \mathbb{F}_p^n$ $f(x) = 0 \iff$ hom $A \to \mathbb{F}_p$ = max ideal of A of index p

Recall: in A, every maximal ideal has finite index

$A \supset m$, A/m finite field. (eg. Bourbaki comm alg).

$q = p^e$, $e \geq 1$, $N(q)$ nb of sol in $\mathbb{F}_q$.

"vertical" $\{p, p^2, p^3, \dots$

horizontal: $p \to \infty$ (less known, our interest)

Scheme point of view:

A, $\operatorname{Spec} A$ prime ideals in A, Zariski top, sheaf of local rings.

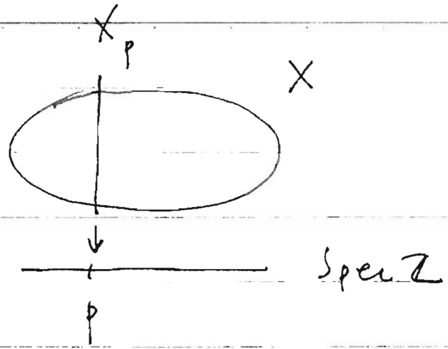
affine scheme.

$$\begin{array}{c} \operatorname{Spec} A \\ \downarrow \\ \operatorname{Spec} \mathbb{Z} \end{array}$$

Generalization: Consider $\begin{array}{c} X \\ \downarrow \pi \\ \operatorname{Spec} \mathbb{Z} \end{array}$ a scheme (always assume separated) π of finite type.

ie. X has a finite covering by open sets, of type $\operatorname{Spec}(A)$, A f.g. over $\mathbb{Z}$.
subschemes

© C.CHING



X_p scheme over $\mathbb{F}_p$ (fiber)
in scheme theory, there are 2 notions of "points". in order not go into that, consider only

$N_X(p)$ = number of closed points $x \in X$, $|k(x)| = p$.
For general case $\mathbb{F}_q$, need to consider
$X(\mathbb{F}_q) = \{(x, \varphi),\ x \in X \text{ closed},\ \varphi : k(x) \to \mathbb{F}_q\}$
eg. p^2, $k(x) : \mathbb{F}_q \to \mathbb{F}_q$ deg 2, count 2 points

② Results to be proved later:
relate $N_X(p)$ with the topology of $X(\mathbb{C})$
Ex. affine case, f_α, $X(\mathbb{C})$ = set of cpx sol.
top space, $\mathbb{C}$-analytic

Theorem 1. $X(\mathbb{C}) = \phi \Leftrightarrow N_X(p) = 0$ for all large enough p.

Theorem 2. $m \geq 0$

(a) $\dim X(\mathbb{C}) \leq m \Leftrightarrow N_X(p) = O(p^m)$ when $p \to \infty$. eg. the eq'n $\begin{cases} x = p \\ x = 0 \end{cases}$
i.e. there exists p_0, C, p_0 prime, $C > 0$
$N_X(p) \leq C p^m$ for all $p \geq p_0$.

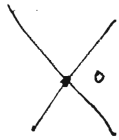
(b). Let e the number of $\mathbb{C}$-irreducible components of $X(\mathbb{C})$ of dim m, Then $\limsup_{p \to \infty} \frac{N_X(P)}{p^m} = e$
Assume $\dim X \leq m$.

Date
Note

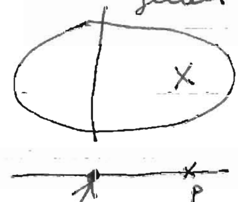
Ex. $x^2+y^2=0$ $\quad \mathbb{F}_2 \quad N(p)=2$

$\mathbb{F}_p, \quad p \equiv 1 \pmod 4; \ N_X(p) = 2p-1 \ \Big| \ i \in \mathbb{F}_p$

$p \equiv -1 \pmod 4; \ N_X(p) = 1$.



(c) Let $e_{\mathbb{Q}}$ be the number of $\mathbb{Q}$ irreducible components of dim m of $X/\mathbb{Q}$. Then



$$\sum_{p \le x} N_X(p) = e_{\mathbb{Q}} \frac{x^{m+1}}{\log(x^{m+1})} + O\left(\frac{x^{m+1}}{(\log x)^2}\right).$$

(The prime # thm!).

Rigidity property of $p \longmapsto N_X(p)$:

Theorem 3. Let X, Y be 2 schemes of finite type over $\mathbb{Z}$, Assume $N_X(p) = N_Y(p)$ for a set of primes of density 1, Then there exists p_0, st.

$$N_X(p^e) = N_Y(p^e) \text{ for every } p \geq p_0, \ e \geq 1.$$

Theorem 4. Let $n \geq 1$, $a \in \mathbb{Z}/n\mathbb{Z}$ (X f.type $/\mathbb{Z}$)

The congruence $N(p) \equiv a \pmod n$ has infinite many sol (in p) if

a = Euler characteristic of $X(\mathbb{C})$.

(They make a set of the primes with density >0, and $\in \mathbb{Q}$.)

$X(\mathbb{C})$ locally compact. //

T loc. cpt. 2 kinds of coh.

$H^i(T, \mathbb{Q})$ coh. with "arbitrary support", H^0 = set of loc. constant functions $X \to \mathbb{Q}$.

$H^i_c(T, \mathbb{Q})$ coh with "cpt support", H^0 = set of loc const fcn which are 0 outside some cpt.

If the H^i are finite dim and $= 0$ for i large, then one defines Euler-Poincaré:

$$EP(T) = \sum (-1)^i \dim H^i(T, \mathbb{Q})$$

$$EP_c(T) = \sum (-1)^i \dim H^i_c(T, \mathbb{Q})$$

Theorem (Grothendieck, Laumon)

If $T = X(\mathbb{C})$, $\subset \mathbb{R}$

$$EP(T) = EP_c(T)$$

Notice: this is not true in general, eg. $X = \mathbb{R}$ by Poincaré dual

③ Examples:

(1). $\dim X(\mathbb{C}) = 0$, $f \in \mathbb{Z}[x]$, $f \not\equiv 0$. $X = \operatorname{Spec} \mathbb{Z}[x]/(f)$

$N_X(p)$ = nb of sol of $f(x) = 0 \mod p$.

$f = x^2 + 1$,

$$N(p) = \begin{cases} 1 & \text{if } p = 2 \\ 2 & \text{if } p = 1\ (4) \\ 0 & \text{if } p = -1\ (4) \end{cases}$$

If not just count numbers, we want to "find" sol.

From the computational point of view:

$p \equiv 1 \mod 4$, $\sqrt{-1} \in \mathbb{F}_p$?

Find it in polynomial time wrt $\log p$:

- There is a "probability method" for all $f(x)$: Legendre.

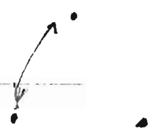
Now ask for "deterministic method" even for $\sqrt{-1}$.
J.-F. Mestre, René Schoof ~ 1985
$N_X(p)$, X elliptic curve. $O(\log p)^8$. later Atkin ...
Cor. Algorithm for computing square roots in poly time.

Rmk: # primes $p \equiv 1\ (4)$, $p \le x$ $\sim \frac{1}{2}\pi(x)$.
Sarnak + Rubinstein "Chebychev bias" a gap 0.998..
$+1 \quad -1 \quad +1 \quad \cdots$ competing primes.

(2) Cubic example: $x^3 - x - 1 = 0$, disc $= -23$.
$N(23) = 2$,

$$p \neq 23: \quad \left.\begin{array}{l} \left(\frac{p}{23}\right) = -1, \quad N(p) = 1, \quad (p \equiv \cdots) \\ \left(\frac{p}{23}\right) = 1, \quad N(p) = \begin{cases} 0: & p \text{ is not} \\ 3: & p \text{ is repr by the } a^2 + 23b^2 \end{cases} \end{array}\right\} *$$

$p \neq 23$, $\overline{\mathbb{F}_p}$, 3 sol. $X(\overline{\mathbb{F}_p})$ has 3 elements:
$x \in X \Rightarrow x^p \in X$, Frob. permutation of X



σ_p of order 2: 1 $\quad \sigma_p \in \mathrm{Sym}_X \simeq S_3 \simeq P_3$
σ_p of order 3: 0
in respected order in *
σ_p of order 1: $\underline{3}$
↑ Frob. fixed pts.

Chebotarev density thm:
each of these cases has a density: $\frac{3}{6} = \frac{1}{2}$, $\frac{2}{6} = \frac{1}{3}$, $\frac{1}{6}$.

A bit Alg. number theory:

$$\begin{tikzcd}[column sep=small] & & E \arrow[dll, dash, "3"'] \arrow[d, dash, "2"] \\ \mathbb{Q}(\sqrt{-23}) \arrow[d, dash, "2"'] & & \\ \mathbb{Q} \arrow[rr, dash, "3"'] & & \mathbb{Q}(x) \end{tikzcd}$$

$x^3 - x - 1 = 0$
E is a Galois ext of $\mathbb{Q}$
with Galois gp D_3.

$\sigma_p \in D_3 = Gal(E/\mathbb{Q})$, what do we know about it?
σ_p in $\mathbb{Q}(\sqrt{-23})/\mathbb{Q}$ is the Frob of that ext

$\Leftrightarrow$ order $\begin{matrix}1\\2\end{matrix}$ if -23 $\begin{matrix}\text{square}\\ \text{not square}\end{matrix}$ mod p $\Leftrightarrow$ $\begin{matrix}\left(\frac{p}{23}\right) = 1\\ \left(\frac{p}{23}\right) = -1\end{matrix}$.

$D_3 \longrightarrow (\pm 1)$.

Investigate the nice tower:

$$\begin{array}{c} E \\ \Big| \, 3 \\ \mathbb{Q}(\sqrt{-23}) \\ \Big| \\ \mathbb{Q} \end{array}$$

$C_3 = Gal(E/\mathbb{Q}(\sqrt{-23}))$
is unramified.

is a quotient of the class gp.
$\mathcal{O}$ = integer of $\mathbb{Q}(\sqrt{-23})$, is a Dedekind ring.
$cl(\mathcal{O}) = Pic(\mathcal{O})$.
order of $cl(\mathcal{O}) = h(-23)$, the class number.
So, E is the maximal unramified
abelian ext of $\mathbb{Q}(\sqrt{-23})$ i.e. Hilbert class field.
How do we decide the role σ_p?

$\mathfrak{p}, \bar{\mathfrak{p}}$ ideals of $\mathcal{O}$ of norm p, $\mathcal{O}/\mathfrak{p} = \mathbb{F}_p$
If $\mathfrak{p}$ is a principal ideal, then $\sigma_p = 1$
i.e. $\exists\, \pi \in \mathcal{O}$ st $\pi\bar{\pi} = Norm(\pi) = p$

if not, σ_p is of order 3.

then it is almost clear
$\pi = \lambda + \mu\sqrt{-23}$
$Norm(\pi) = \lambda^2 + 23\mu^2$.

Date

Note

Modular intepretation of $N(p)$:

$$f = q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) = \eta(z)\eta(23z)$$

[where $q = e^{2\pi i z}$, $\eta = q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)$.]

$$= \sum a_n q^n = q - q^2 - q^3 + \cdots$$

$$= \frac{1}{2}\Big\{ \underset{Ⓐ}{\sum_{a,b\in\mathbb{Z}} q^{a^2+ab+6b^2}} - \underset{Ⓑ}{\sum_{a,b\in\mathbb{Z}} q^{2a^2+ab+3b^2}} \Big\}$$ theta series.

these 2 2 forms are easy to remember, since disc = −23.

Theorem : $N(p) = 1 + a_p$.

e.g. $p=3$, $N(3) = 1-1 = 0$. ($x^3 - x - 1 = 0$, $0 - 1 = 0$ not possible.)

Also $-1 \le a_p \le 2$.

Dirichlet series : $L_f(s) = \sum_{n\geq 1} a_n n^{-s}$.

Ⓔ : highly non-obviously : $= \prod_p \dfrac{1}{1 - a_p p^{-s} + \left(\frac{p}{23}\right) p^{-2s}}$; if $p = 23$ $\left(\frac{p}{23}\right) := 0$

The a_n's are mult: $a_{nn'} = a_n a_{n'}$ if $(n, n') = 1$.

weight : k — $N = 23$, $k = 1$, ε the Legendre character mod 23.

level : N .

char mod N : ε — cusp forms, 1-dimensional

both Ⓐ, Ⓑ are modular forms, but not cusp.

after substract, cancel const get 1-dim cusp forms.

Hence by <u>Hecke</u> operators get Euler prod Ⓔ .

Modular forms = Galois representations of dim 2 :

In weight 1 ; $\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{C})$

C.CHING

Date
Note

Our case: $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(E/\mathbb{Q}) \longrightarrow GL_2(\mathbb{C})$

$\mathrm{Gal}(E/\mathbb{Q}) \cong P_3 \longrightarrow$ obvious representation.

$\rho(\sigma_p)$, $p \neq 23$	trace	a_p
	det	$\varepsilon(p)$

So it is really Artin L-series $= \prod_p \frac{1}{\det(1-\rho\sigma_p)p^{-s}}$

$$\left(= \prod_p \frac{1}{1-\mathrm{Tr}(\sigma_p)p^{-s} + \det(\sigma_p)p^{-2s}} \right)$$

$N(p)$ = nb of fixed pt of σ_p

a_p = trace of $\rho(\sigma_p)$

$\rho_3 = 1 \oplus \rho$, ρ_3 is the permutation repr of D_3 on 3 elts.

This example has many features, some extends, some don't!

$\rho_3 = 1 \oplus \rho$

$x^3 - x - 1 \qquad \Delta = -27 + 4 = -23$

$x^3 + x - 1 \qquad \Delta = -27 - 4 = -31$, play the same game. $h(-31) =$

f level 31, wt 1, Legendre char mod 31,

$$f = \frac{1}{2}\left\{ \sum q^{a^2+ab+8b^2} - \sum q^{2a^2+ab+4b^2} \right\} = \sum a_n q^n$$

$N(p) = 1 + a_p$.

Before: $p = 23$, $\eta(z)\eta(23z)$. 23 is essential since $1+23=24$ to get $q^{\frac{1}{24}} q^{\frac{23}{24}} = q$.

- Now an exercise:

$f = q + \cdots = q(1-q)^{\alpha_1}(1-q^2)^{\alpha_2}\cdots$ such exp $\exists$!

Exercise: For ~~$p=31$,~~ this case, α_i not bounded!

So No explicit prod formula.

Hint: Show that the modular form $f(e^{2\pi i t})$ has a zero in the upper half plane, hence not consist with [illegible]

About the Lectures:

N(p): Chebotarev theorem

applications of ℓ-adic coh

Next lecture will go to motives, Langlands.

③ Reminder of ℓ-adic cohomology / over a finite field $\mathbb{F}_q$ with q elements.

a) X scheme of finite type over an alg closed field k (char 0 or p all ok.)

Separated. (required). eg.

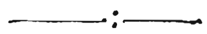
Since we do not consider cohomology of non-sep space.

line L; $U = L - \{0\}$

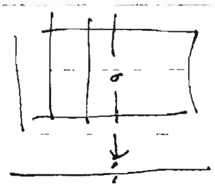
L'; $U' = L' - \{0\}$

in scheme theory, can glue freely

glue L and L' over $U \simeq U'$.

(*)  non separated even in classical top.

Even in Diff geom:



plane $\setminus \{0,0\}$

equiv: x, y are in the same conn. comp of fiber.

the quot get (*).

One can define coh étale coh gps, modules for X with coeff in a finite gp $\mathbb{Z}/m\mathbb{Z}$.

replace open sets by étale open sets.

$H^i(X, \mathbb{Z}/m\mathbb{Z})$

$H^i_c(X, \mathbb{Z}/m\mathbb{Z})$ proper support

: good properties when $(m, \mathrm{char}(k)) = 1$

$\Downarrow$

$\left\{ \begin{array}{l} \text{Finite (for given } i, m), \\ 0 \text{ if } i > 2\dim X. \end{array} \right.$

C.CHING

Next step: ℓ prime $\neq$ char k.

$$H^i(X, \mathbb{Z}_\ell) =_{def} \varprojlim_n H^i(X, \mathbb{Z}/\ell^n\mathbb{Z})$$

$\mathbb{Z}_\ell$-module of finite type.

Rmk: may have torsion, deep thm of Gabber, $\exists$ torsion only for finite many ℓ.

$H^i(X, \mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}} H^i(X, \mathbb{Z}_\ell)$. Same def'n for H^i_c.

Remarks: a) $\dim H^i(X, \mathbb{Q}_\ell)$ is conj to be indep of ℓ

known for X smooth projective.

Theorem (M. Artin)
If $k = \mathbb{C}$, these coh gps $H^i(X, \mathbb{Z}/m\mathbb{Z})$, $H^i_c(X, \mathbb{Z}/m\mathbb{Z})$ are the same as the coh gps of $X(\mathbb{C})$ in the top sense

b) k not necessarily alg. closed, $\bar{k}$ some alg. closure.

$\bar{X} = X/\bar{k}$, $H^i(\bar{X})$, $H^i_c(\bar{X})$ are well-defined

we do not use $H^i(X)$ since they are too complicate!

$$\begin{array}{l} \bar{k} \\ \mid \\ k_s \text{ : sep closure} \\ \mid \\ k \end{array}$$

$\downarrow$ they are module over $\mathrm{Gal}(\bar{k}/k)$ by "transport de structure" (by functoriality)

$X = \mathrm{Spec}\, A$
$\bar{X} = \mathrm{Spec}(A \otimes_k \bar{k})$ get $\begin{array}{c} \bar{X} \\ \downarrow \\ \mathrm{Spec}\, \bar{k} \end{array}$

$H^i(\bar{X}, \mathbb{Q}_\ell)$, $H^i_c(\bar{X}, \mathbb{Q}_\ell)$ these Galois repr's are fundamental objects.

Date
Note

c) $k = \mathbb{F}_q$, finite,

$$\begin{tikzcd} \bar{X} \arrow[r, "\pi"] \arrow[d] & \bar{X} \arrow[dl] \\ \mathrm{Spec}(\bar{\mathbb{F}}_q) & \end{tikzcd}$$

choose $\bar{\mathbb{F}}_q$

π : Frobenius morphism:

$x_1, \dots, x_n$; $\pi_q(x_1, \dots, x_n) = (x_1^q, \dots, x_n^q)$

π acts on the coh : sep. proj.

Two possible def'n of the "action of Frobenius"

Method (a) π_q acts on $H^i(\bar{X})$, $H^i_c(\bar{X})$, "geometric Frobenius" since it is a morphism, $X \to Y$, $H^i(X) \leftarrow H^i(Y)$.

Method (b) $\sigma_p \in \mathrm{Gal}(\bar{\mathbb{F}}_q / \mathbb{F}_q)$ acts on $H^i(\bar{X})$, "arithmetic Frobenius".

Thm: σ_p and π_q are inverse to each other!

geometric Frob. is not uniform in p, it grows as $p \to \infty$.

to be continued.

C.CHING

Serre's Lecture II 7/9.

3. Cohomology :

$X / \mathbb{F}_q$, $\bar{X} = X / \bar{\mathbb{F}}_q$

geometric frobenius π_q : $X \to X$, $\bar{X} \to \bar{X}$

$x \in$ pt of X in $\bar{\mathbb{F}}_q$, $x \in X(\mathbb{F}_q) \Leftrightarrow \pi_q(x) = x$.

i.e. $\mathbb{F}_q$ - rat $\Leftrightarrow$ fixed by Frob

· Weil's idea : "Lefschetz formula"

$N_X(q) = |X(\mathbb{F}_q)| =$ number of fixed pts of Frob.

· Grothendieck :

Using H_c $\pi_q : \bar{X} \to \bar{X}$ "proper"

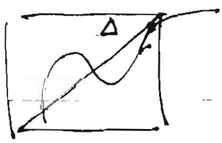
proper support $H^i(\bar{X}) \leftarrow H^i(\bar{X})$ indeed

$H^i_c(\bar{X}) \leftarrow H^i_c(\bar{X})$ "finite morphism)

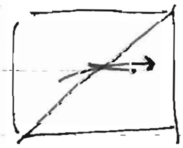
Theorem : $|\bar{X}(\mathbb{F}_q)| = \sum_{i=0}^{2\dim X} (-1)^i \operatorname{Tr}\left(\pi_q : H^i_c(\bar{X}, \mathbb{Q}_\ell)\right)$

for every $\ell \neq$ chark.

· Remarks (surprising for several reasons)

1)  top left : count pts with multiplicities

but now NO ! just count 1 !

 $x \mapsto x^q$ derivative is "0"

graph of π  ??

So π is transversal to the diagonal !

$\Rightarrow$ mult $= 1$.

2) Why H_c ? H_c has additive property

$X \supset Y$, Y closed , $U = X - Y$

$$\cdots \to H^i_c(U) \to H^i_c(X) \to H^i_c(Y) \xrightarrow{\delta} H^{i+1}_c(U) \to \cdots$$

$/\mathbb{F}_q$ π.   compati with π_q action .

$\mathrm{Tr}(\pi, H_c(\bar{X})) = \sum (-1)^i \mathrm{Tr}\, H^i$

Simple exercise $\Rightarrow$ $\chi_c(X) = \chi_c(U) + \chi_c(Y)$.

which should be same $N_X(q) = N_Y(q) + N_U(q)$.

Deligne's thm's : (pure)

CW 1. X proj sm of dim d

π_q acts on $H^i(\bar{X}, \mathbb{Q}_\ell)$, eigenvalues

Thm (Deligne, 1974), the eigenvalues of π_q are "q-Weil numbers of weight i".

Def'n: integral q-Weil number of height i

α, α : alg int. $|\alpha|_v = q^{i/2}$

for every archimedean abs value of $\mathbb{Q}(\alpha)$

$|\alpha| = q^{i/2}$, all the Galois conjugate has abs val $q^{i/2}$.

The char poly of π_q has coeff $\in \mathbb{Z}$, and is indep of ℓ.

Let $\pi_q{}^e = \pi_{q^e}$, $e \geq 1$.

Cor: Trace $(\pi_q{}^e, H^i_c(\bar{X}, \mathbb{Q}_\ell))$ is an integer, indep of ℓ and its abs val is $\leq b_i\, q^{ei/2}$

where $b_i = \dim H^i_c(\bar{X}) = H^i$.

Cor: Assume $\bar{X}$ is irred (= connected) of dim d.

$H^{2d}(\bar{X}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-d)$. (Tate twist).

canonical, compatible with Galois action.

what's that? ℓ prime

μ_{ℓ^n}, ℓ^n-th roots of unity in $\bar{k}$, $T_\ell = \varprojlim \mu_{\ell^n}$

($\simeq \mathbb{Z}_\ell$ with $\mathrm{Gal}(\bar{k}/k)$ acting by the cycl. char / χ)

$V_\ell = T_\ell[\frac{1}{\ell}] = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell = T_\ell \otimes_{\mathbb{Z}} \mathbb{Q}$

1-dim vector space with an action of Gal. (via χ).

i.e. it is a "line bundle"

C.CHING

$n \geq 0$, $V_\ell^{\otimes n} = \mathbb{Q}_\ell(n)$, $V_\ell = \mathbb{Q}_\ell(1)$.

$\mathbb{Q}_\ell(-n)$ = dual of $\mathbb{Q}_\ell(n)$, action χ^{-n}.

$M/\mathbb{Q}_\ell$, $M(n) := M \otimes \mathbb{Q}_\ell(n)$.

Then we have: $\chi(\sigma_q) = q$

arith Fr acts by q^{-d} on $H^{2d}(\bar{X}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-d)$

geom Fr " q^d

$$N_X(q) = \sum (-1)^i \, Tr(\cdot, H^i)$$

$$i = 2d \longrightarrow q^d$$

$\Rightarrow$ Cor. $\bar{X}$ proj sm, dim d, irred.

$$\Big| \underset{|X(\mathbb{F}_q)|}{\overset{\shortparallel}{N_X(q)}} - q^d \Big| \leq A\, q^{d-\frac{1}{2}}, \quad A = \sum_{i=0}^{2d-1} b_i$$

what's the next step?

Remark: $i = 2d$ is the main term: q^d

Lemma: $i = 2d-1$ is related to the Albanese variety

$X \mapsto A$ Alb. univ. property or (Picard) of X.

P Picard, essentially connected component of Groth's Pic

for alg gps:

$\mathbb{G}_m$ μ_{ℓ^n}

A $A[\ell^n] = \ker \ell^n : A \to A$

$T_\ell A = \varprojlim A[\ell^n]$, $V_\ell(A) = \mathbb{Q}_\ell \otimes T_\ell A$

π_q acts on $V_\ell(A)$ H_1 homology.

eigenvalues of char poly. $q^{1/2}$, Weil number of wt 1.

$$Tr(\pi_q, H^{2d-1}) = q^{d-1}\, Tr(\text{Frob end of } A)$$

weight $d - \frac{1}{2}$.

$$\left| N_X(q) - q^d + q^{d-1}\,\mathrm{Tr}(\pi_q, A) \right| \ll q^{d-1}$$

$\sum_{i \le 2d-2} b_i$

This is about Deligne I.

Deligne (1980) CW II. No hypo on X

(except finite type over $\mathbb{F}_q$, separated)

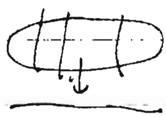
Thm: The eigenvalues of π_q acting on $H^i_c(\bar{X}, \mathbb{Q}_\ell)$ are Weil numbers, of height $\le i$.

In top dim, same as in the proj smooth case.

$$H^{2d}_c(\bar{X}, \mathbb{Q}_\ell) \xrightarrow[\text{can}]{=} \mathbb{Q}_\ell(-d).$$

Rmk: $|N_X(q) - q^d| \ll q^{d-\frac{1}{2}}$ is proved earlier 1954

by Lang-Weil, Nisnevic, using tool:



fiber = curve, then use Weil (1940-48)

dim $d-1$

For curves, eigenvalue

H^0, H^1 = Jacobian, H^2.

irreducible curves: $q+1+O(q^{1/2})$.

The general method also use fibration by curves.

4. Examples in dim 1 and 2.

4.1, $g=0$, conic$/\mathbb{F}_q$, $\mathbb{P}^1$ H^0 dim 1 $H^i = 0$ others.

i.e. top S^2. H^2 dim 1

π_q on $H^0 \to 1$, π_q on $H^2 \to q$ $\Rightarrow$ nb of pts $= q+1$.

Notice that this is also true for conic!

hence solve Chevalley-Warning prob. $\Rightarrow$ it has a pt.

4.2, $g=1$, $\dim H^1 = 2$,

π_q, α, β $|\alpha| = q^{1/2}$, $\beta = \bar{\alpha}$, $\alpha\bar{\alpha} = q$.

©C.CHING

$N(q) = q - a + 1$ $\qquad |a| \le 2\sqrt{q}$

$H^2 \quad \alpha+\beta \quad H^0 \quad \Rightarrow N(q) \ge (\sqrt{q}-1)^2 > 0$

$\Rightarrow$ elliptic curves over finite field has a point!

Examples of computation of a:

4.2.1. $y^2 = x^3 - x \subset \mathbb{P}^2$ (∞ included)

bad reduction at 2. (cond. 32)

for $p \ne 2$, $a_p = ?$

$p \equiv -1 \pmod 4 \Rightarrow a_p = 0$ nbd of pts $= 1+p$

$p \equiv 1 \pmod 4 \Rightarrow$

write $p = a^2+b^2$, st

$a+bi \equiv 1 \pmod{(1+i)^2}$

Then $a_p = 2a$.

$N(p) = 1+p-2a$

eg. $p=5$, $5 = 2^2+1^2$.

This is a CM curve since besides

$y \mapsto -y$, $x \mapsto x$, has also

$x \mapsto -x$, $y \mapsto iy$.

Q: In general it is not easy to present $p = a^2+b^2$.

$\mathbb{Z}[i]$ Gauss int.

$p = \pi\bar{\pi}$, $\pi = a+bi$ $\quad a, b \in \mathbb{Z}$

$p = a^2+b^2$.

π can be chosen in a unique way st.

$\pi \equiv 1 \mod 2(i+1)$

$\quad \text{''} \quad (1+i)^2$

or any ideal of $\mathbb{Z}[i]$ prime to $1+i$, it has a unique generator π_a $\equiv 1 \pmod{(i+1)^2}$.

Rmk: for $y^2 = f(x)$, can write

$$N \text{ of sol} = \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{f(x)}{p}\right)\right) = \text{nb of affine sol}$$

in time $O(p)$.

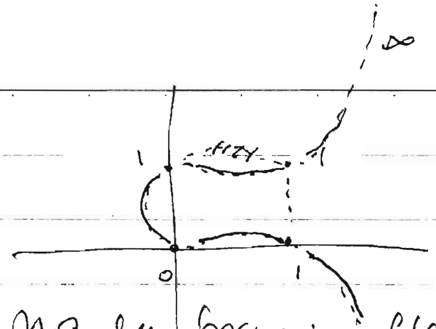
4.3.

Next example: Elliptic curve without CM.

$y^2 - y = x^3 - x^2$

Date
Note

$i\infty$ only 5 pts mod 2.



$C_5 = E(\mathbb{Q})$

good reduction outside $p=11$.

How to get a_p?

Modular form: $f(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = \eta^2(z)\,\eta^2(11z)$
$= \sum_{n=1}^{\infty} a_n q^n$

$q = e^{2\pi i z}$

Theorem: a_p = Trace of π_p acting on $H^1(\bar{E})$.

$p=2$, $a_2=-2$, $N_E(p) = p - a_p + 1$, $p \neq 11$

(for $p=2$: $2+2+1=5$)

f modular form, eigen form of wt 2, level 11, unique (starting with q). $T_p f = a_p f$. (Hecke op.)

$X_0(11)$, $X_1(11)$ happen to be isogenous

$y^2 - y = x^3 - x$

the eq'n is more complicate.

· Eichler: mod p go to X then win?

Taniyama, Weil and others: every elliptic curve $/\mathbb{Q}$ is obtained in this way. (Wiles, Taylor-Wiles)

4.4. Surfaces: a quadric $\subset \mathbb{P}^3$

$ax^2+by^2+cz^2+dt^2=0$, $a,b,c,d \neq 0$, char $\neq 2$.

it's well-known that over $\mathbb{C}$, $\cong \mathbb{P}^1 \times \mathbb{P}^1$

In general, $\cdot \longrightarrow \cdot$ require $\sqrt{abcd}$

If $abcd$ is a square, nb of pts $=(q+1)^2 = q^2+2q+1$

From top. Also easy from Frobenius. H^4 H^2 H^0

if $abcd$ is not a square,

H^2 over alg closure $\alpha \leftrightarrow \beta$, Trace $=0$.

So get q^2+1 pts. $\begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$

C.CHING

<u>Restriction of scalars</u>: F'/F variety X' over F',

$\exists$ var X/F $\dim X = \dim X' . [F':F]$ (if sm)

$X(F) = X'(F')$. (just like var$/\mathbb{C}$ to $/\mathbb{R}$).

X quadric $\Leftarrow$ k'/k quadratic extension

$X' = \mathbb{P}^1$.

$\mathbb{P}^1/\mathbb{F}_{q^2}$ à la Weil, hence get q^2+1 pts.

Rational surfaces (birat'l $\simeq \mathbb{P}^2/\bar{k}$)

1 dim $- H^0$

$H^2 = NS \otimes \mathbb{Q}_\ell(-1)$.

Néron-Severi gp

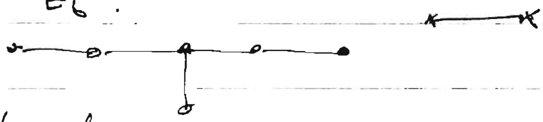
1 dim $- H^4$

Cubic surface, rk $NS = 7$ H^2 has dim 7.

27 lines gives 27 elts in H^2.

Look automorphisms of the graph of these lines:

$= \mathrm{Weyl}(E_6)$ E_6:



Every cubic surface $/k$ has

$\mathrm{Gal}(\bar{k}/k) \to \mathrm{Weyl}(E_6)$

$\mathbb{F}_q \to$ conjugacy class in Weyl.

Cubic surfaces: $N(q) - (q^2 + q + 1) = aq$

 H^4 H^2 H^0

$a =$ trace of σ_p — the part by cut hyp plane

viewed as an element

of $\mathrm{Weyl}(E_6)$, with $-3 \leq a \leq 6$.

The next interesting case will to see with odd H^i especially, Calabi-Yau varieties. But will not do it here.

5. Chebotarev Theorem (in dim 1)

E/K Galois ext (finite) of number fields.

$\mathcal{O}_E, \mathcal{O}_K$ ring of integers.

V_K set of non-archim places of K

i.e. $v \in V_K \longleftrightarrow$ prime ideal of $\mathcal{O}_K$ (instead of writing $\mathfrak{p}$) maybe $\mathfrak{p}_v$

"Nv", write $|v|$ = # of elts of the residue field $k(v)$.

$w \in V_E$ elts. $\begin{matrix} w \\ \downarrow \\ v \end{matrix}$, D_w: decomposition gp in G $g \in G$, $gw = w$

I_w: inertial gp $g \in G$, $gw = w$, g acts trivially on $k(w)/k(v)$.

$D_w/I_w = \mathrm{Gal}\left(k(w)/k(v)\right)$: finite.

$\sigma_{w/v}$ Can generator of D_w/I_w, Frob.

Rmk: I_w is almost always 1, w is ram, $I_w \neq 1$.

when v, w is unram, σ_v the conj class of $\sigma_{v/w}$ for any $w|v$.

Theorem (Cheb + Artin) Let C be a subset of G, stable under inner auto, (i.e. a union of conj classes)

Let $V_{K,C} = \{ v \mid$ unram. $\sigma_v \in C \}$.

For $X \to \infty$,

$$\left| v \in V_{K,C},\ |v| \leq x \ - \frac{|C|}{|G|} Li(x) \right| \leq \text{const.}$$

(with no hypothesis), $\leq$ cost. $x \cdot \exp(-c'\sqrt{\log x})$.

(with GRH) $\leq$ const. $x^{1/2} \log x$. $c' > 0$.

$$Li(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \quad \text{logarithmic integral.}$$

Sometimes $li(x) = \int_0^x$ (notice put 1 does not conv.)

really mean p.v. $\lim_{\varepsilon \to 0} \left[\int_0^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^{x} \frac{dt}{\log t} \right]$

$li(x) = Li(x) + li(2) = 1.045$.

CHING

$$\mathrm{Li}(x) = \frac{x}{\log x}\left(1 + \frac{1!}{\log x} + \frac{2!}{(\log x)^2} + \cdots\right)$$

asym exp.
not conv

Corollary:
The set $V_{K,C}$ has density $\frac{|C|}{|G|}$. hence is infinite if $C \neq \phi$.

To be continued.

5. Chebotarev E/K, $C \subset G$

Theorem: $\left| \sum_{\substack{v \in V_{K,C} \\ |v| \le x}} 1 - \frac{|C|}{|G|} \mathrm{Li}(x) \right| \ll \left(\begin{array}{l} x \exp(-c\sqrt{\log x}) \quad c>0 \\ x^{1/2} \log x \quad \text{(with GRH)} \end{array} \right.$

$v \in V_K$, $\sigma_v \in C$ unrami

Based on: Artin L function att to a linear cpx repr of G: ρ with char χ, called V

$$L(\rho, s) = \prod_{v \in V_K} \frac{1}{\det(1 - \sigma_w | V^{I_w} . |v|^{-s})} \quad \sigma_w \in D_w/I_w, \ w|v$$

$$= \prod_v \frac{1}{\prod_\alpha (1 - \alpha |v|^{-s})}$$

α run thr the eigenvalues of σ_v acting on V^{I_v}

$=$ finite of .. $\cdot \prod_v \frac{1}{\det(1 - \sigma_v |v|^{-s})}$

$Re(s) > 1$, $|v| = Nv$, $\mathfrak{p}$, $N\mathfrak{p}$

$$-\frac{dL/ds}{L} = \sum \chi(\sigma_v) |v|^{-s} + \dots$$

First case: for the L fun attached to abelian char of class gp (modulo ..)

Hecke ($\sim$1917), analytic conti, fun'l eq'n

$\chi \neq 1$, non-zero, $Re(s) = 1$

Next case, Artin, χ abelian char, $s=1$

reciprocity law $\sim$1926. became same as Hecke.

G, $\chi = \sum n_\alpha \operatorname{Ind} I^w \dots$ //

Complements:

1) Ch $\Rightarrow$ for every conj class C, the set $V_{K,C}$ is infinite with density $|C|/|G|$.

2) (Analytic method) $\sum_{\substack{v \in V_{K,C} \\ |v| \le x}} 1 = \frac{|C|}{|G|} \mathrm{Li}(x) + \varepsilon(x)$

$|\varepsilon(x)| \le \varepsilon_0(x) = x \exp(-c\sqrt{\log x})$

may replace this by others,

Will need 2 cases: integer $d \geq 0$

Ex. $\sum |v|^d = \frac{|C|}{|G|} \, Li(x^{d+1}) + O(x^d \varepsilon_0(x))$

$\sum |x|^{-1} = \frac{|C|}{|G|} \log\log(x) + O(1)$

eg. $\sum_{p \leq x} \frac{1}{p} = \log\log(x) + O(1)$, $x \to \infty$

so, ∂, $\sigma_v \in C$, $\sum_v \frac{1}{|v|} = \infty$

This is by Abel summation / or integration by parts.

$A_d(x) = \sum_{|v| \leq x, \, v \in V_{K,C}} |v|^d$ $\qquad A(x) = A_0(x) = \alpha \, Li(x) + \varepsilon(x)$

let $\alpha = \frac{|C|}{|G|}$ $\qquad A_d(x) = \int_0^x t^d \, dA(t)$

Stieltjes integral

in the sense of Schwartz distribution

$A_d(x) = \left[t^d A(t) \right]_2^x - d \int_2^x t^{d-1} A(t) \, dt$

$= O(1) + x^d A(x) - d \int t^{d-1} A(t) \, dt$ $\qquad$ dist cont fu

simplify: write

$A(t) = \alpha \, Li(t) + \varepsilon(t)$

$\alpha \int_2^x t^d \, d\,Li(t) = \alpha \int_2^x t^{d+1} \frac{dt/t}{\log t}$, $u = t^{d+1}$

$\frac{du}{u} = (d+1) \frac{dt}{t}$, $= \alpha \int_{2^{d+1}}^{x^{d+1}} u \, \frac{du}{u} \, \frac{1}{d+1} = \alpha \int_{2^{d+1}}^{x^{d+1}} \frac{du}{\log u}$

$\to Li(x^{d+1}) - Li(2^{d+1}) = Li(x^{d+1}) + O(1)$.

Translation to "Frobenius functions" of $v \in V_K$.

Let S be a finite subset of V_K

Ω be a set (with discrete top)

$f : V_K \setminus S \longrightarrow \Omega$

Def: We say that f is S-Frobenius, if there exists a finite Galois extension E/K, Galois gp, unramified outside S, and a map $\varphi : G \to \Omega$

inv by conjugacy ($\varphi : Cl(G) \to \Omega$) st

$f(v) = \varphi(\sigma_v)$ for all $v \in V_K - S$

Exercise: There is a smallest such E/K.

Frobenius := S-Frob for some S.

- $K = \mathbb{Q}$, $\Omega = \mathbb{Z}/m\mathbb{Z}$, $S = \{p, p \mid m\}$

$f : p \mapsto$ residue mod m, is a S-Frob fcn $\mathbb{Q}(\zeta_m)/\mathbb{Q}$

If f takes the value $w \in \Omega$ for some v, it does so for ∞-many v's (with density > 0, rat'l)

$H(X) \in \mathbb{Z}[X]$, $\not\equiv 0$

$N_H(p)$ = nb of sol mod p

S = set of primes which divides the disc(H)

$\Omega = \mathbb{Z}$, $p \mapsto N_H(p)$ is S-Frobenian

(Take E gen by roots of H).

Let $f : V_K - S \to \Omega$ be a Frobenian map.

"$f(1)$" : choose E/K, G, φ, Then define $f(1)$ as $\varphi(1)$

" $f(v) = \varphi(\sigma_v)$ "

Eg in the case H has no repeated roots;

f = number of roots, then $f(1)$ = nb of cpx roots.

$K \xrightarrow[v_\infty]{} \mathbb{R}$ $\quad C_{v_\infty}$ conj class in G, order 1 or 2

$f(v_\infty) = \varphi(C_{v_\infty})$, then $f(v_\infty)$ = nb of real roots (corr to the

Cor. There are ∞-many v's embedding $K \hookrightarrow \mathbb{R}$).

st H has deg H roots in $K(v)$.

eg. $p \mapsto p$ mod m, $\Omega = \mathbb{Z}/m\mathbb{Z}$

val at $1 \to 1$

" $\infty \to -1$

f S-Frob. $(\Psi^e f)(v) := \varphi(\sigma_v^e)$, e integer.

T_p operators in modular form theory [T_p mod m]
$N_X(p)$ for X an arbi scheme of finite type over $\mathbb{Z}$.
[$p \mapsto N_X(p)$ mod m - for all m's]

6. The Frobenius property of the T_p's:
N level, $k \geq 1$, ε char mod N.
$M(N, k, \varepsilon)$ = mod forms with these data ($\mathbb{C}$-v.s has a basis made of $\sum a_n q^n$, all $a_n \in K$ (f ext/$\mathbb{Q}$) $a_n \in O_K$.
Hecke operator T_p, $p \nmid N$.
Consider Λ = submodule $\sum a_n q^n$, $a_n \in O_K$.

$T_p \Lambda \subset \Lambda$, Choose $m \geq 1$.
Thm: $p \mapsto T_p \in \mathrm{End}(\Lambda)/m\,\mathrm{End}(\Lambda)$ is S-Frob with S = prime div of Nm (S finite?)
How to see this without Hecke op:
let $\sum a_n q^n$ be a mod form with coeff $\in O_K$, let $m \geq 1$ then the function $p \mapsto a_p \pmod m$ is Frobenius value at 1 is $2a_1$ mod m
∞ is 0 mod m

Cor. The set of p's with $a_p \equiv 0$ mod m has density > 0
$a_p \in m\, O_K$.

$\Delta = \sum \tau(n) q^n$, $\tau(n) \equiv 0 \pmod{\underline{691}}$ for n's of density 1.
f eigen form of Hecke (cusp form)
norm $a_1 = 1$. $q + a_2 q^2 + \cdots$
if n is an integer st $n = pn'$, $(n', p) = 1$, $a_p \equiv 0 \pmod n$
then $a_n \equiv 0 \pmod n$.

Fact: Let P be a set of prime which is frobenian
(= Ch f of P's is Fobenian) — characteriz funtion
of density $\alpha > 0$.

Then the set of $n \in \mathbb{N}$, div by an elt of P
(with exp 1) has density 1.

($n \equiv 0 \mod p$) density $\frac{p-1}{p^2} \sim \frac{1}{p}$

$\prod_{p \text{ in the set}} (1 - \frac{1}{p})$, $\sum \frac{1}{p} \sim c \log \log x \to \infty$.

The pf consists of taking a better basis of modular forme.
basis made up of all forms and new forms.

$F = \sum a_n q^n$ eigenform, relative to new forms, :

$= q + \cdots$ $(n, N) = 1$: a_n = eigenvalue of T_n.

a_p, Deligne, that for every ℓ, ℓ-adic repr

$\rho_\ell : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_\ell)$,

p large, $\begin{cases} Tr_{\rho_\ell}(\sigma_p) = a_p \\ det_{\rho_\ell}(\sigma_p) = p^{k-1} \varepsilon(p) \end{cases}$ $Tr(\rho_\ell(\text{upx wai})) = 0$,

$$\begin{tikzcd} Gal \arrow[r] \arrow[dr] & GL_2(\mathcal{O}_\ell) \arrow[d, "\sigma_\ell \text{ of a f. lxt.}"] \\ & GL_2(\mathcal{O}_\ell / \ell \mathcal{O}_\ell) \end{tikzcd}$$

For every m, there are ∞-many p's $a_p \equiv 2 q_1 \mod m$.

C.CHING

Date
Note

7. Back to $N_X(p)$. X f.t. sep $/\mathbb{Z}$ (or $\mathcal{O}_K$)
S finite set of primes, P set of all primes
max Galois ext of $\mathbb{Q}$ unram outside S: G_S
Profinite $G_S = \varprojlim \mathrm{Gal}(E/\mathbb{Q})$
$E/\mathbb{Q}$ unram outside S

Conti ℓ-adic repr of G_S

$\rho : G_S \longrightarrow GL_n(\mathbb{Q}_\ell)$ some n
up to conj, ρ takes values in $GL_n(\mathbb{Z}_\ell)$, cpt ℓ-adic gp
$\mathrm{Tr}(\rho(\sigma_p)) \in \mathbb{Z}_\ell$ trace of image of Frobenius
$\chi = \mathrm{char}\,\rho$, $\chi(\sigma_p)$, it is Frob mod ℓ^M for every M.
X, choose ℓ prime. Def: $\varphi : G_S \to \mathbb{Z}_\ell$ a (virtual) generalized character
Theorem: if it can be written as $\sum_\alpha n_\alpha \chi_\alpha$
There exists a finite set S, containing ℓ, finite. $\mathbb{Z}$ trace of fin rep ρ_α
a generalized char $\varphi_{X,\ell}$ of G_S, st.

$$N_X(p) = \varphi_{X,\ell}(\sigma_p) \quad \text{for all } p \notin S. \quad (\text{in } \mathbb{Z}_\ell)$$

Cor. $p \mapsto N_X(p) \bmod \ell^M$ is S-Frob. For every $M \geq 0$,

Better formula: $N_X(p^e) = \varphi_{X,\ell}(\sigma_p^e)$, $p \mapsto N_X(p^e)$, $\psi^e N_X$.

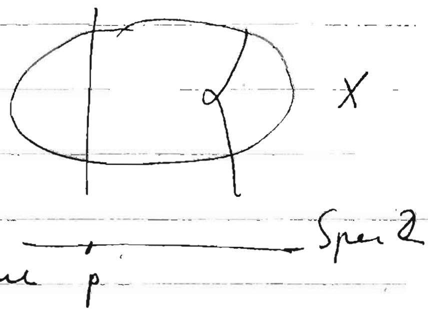
$$\begin{array}{ccc} X & : & X_{\mathbb{Q}} \\ \downarrow & & \downarrow \\ \mathrm{Spec}\,\mathbb{Z} & \supset & \mathrm{Spec}\,\mathbb{Q} \end{array}$$

$\mathbb{Q}$-alg. var.
$H^i_c(\bar{X}, \mathbb{Q}_\ell)$ has an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

SGA 4, $4\frac{1}{2}$, 5 : unr outside a finite set of primes S
assume $S \ni \ell$.

$\varphi = \sum (-1)^i \, \mathrm{Tr}\, \rho_i$, ρ_i repr. of G_S given by $H^i_c(\bar{X}, \mathbb{Q}_\ell)$.
(this is why need virtual repr, virtual character)

- need to relate (identify) the coh of the p-fiber $\bar{X}_p$ with that of $\bar{X}$ itself.



Use Grothendieck's direct image
$(R^i \pi_! \mathbb{Q}_\ell)$ "constructible"
proper support ie ① there is an open dense subscheme of the base over which it is lisse.

① The formation of $R^i \pi_! \mathbb{Q}_\ell$ is compatible with base change,
so the stalk at p of $R^i \pi_! \mathbb{Q}_\ell$ is $H^i_c(\bar{X}_p, \mathbb{Q}_\ell)$.

Then the thm is just Grothendieck's trace formula
$$N_X(p) = \sum (-1)^i \, \mathrm{Tr}(\pi_q, H^i_c(\bar{X}, \mathbb{Q}_\ell)).$$
#

Back to Thm 3 of lect 1.

X, Y finite type $/\mathbb{Z}$. If $N_X(p) = N_Y(p)$ for a set of prime of density 1, then there is a p_0 st.
$N_X(p^e) = N_Y(p^e)$ for all $p \geq p_0$, all $e \geq 1$.

pf: φ_X, φ_Y of G_S,
$\varphi_X(\sigma_p) = \varphi_Y(\sigma_p)$ $\forall$ p's in a set of density 1,
(so such σ_p's are dense in G_S)
by continuity: $\varphi_X = \varphi_Y$. #

C.CHING

28. Serre's lecture 4.

(8. Proof of the archimedean estimate for $N_X(p)$)

Erratum: $<$ geom Fr / arith Fr $\Big|$ H^i_c in last lecture ~ replace by dual

The pf is now relatively easy.

X scheme of finite type $/\mathbb{Z}$, "sep. dim $d+1$" or just "geometric fiber of dim d" is all we need.

$X_{\mathbb{Q}}$ has abs irred comp (i.e. $/\bar{\mathbb{Q}}$) of dim d

Let I be the set of such comp.

$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on I.

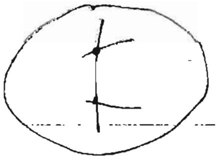
Linear repr of Gal of dim $|I|$, unr outside finite set S

$p \notin S$, σ_p will depend pan of $|I|$

G acting I, $g \in G$, $|I^g| = \mathrm{Tr}(g)$, $\mathrm{Tr}(\sigma_p)$.

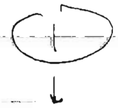
Formula:

$$N_X(p) = \mathrm{Tr}(\sigma_p)\, p^d + O(p^{d-\frac{1}{2}}) \quad \text{for } p \text{ large enough.}$$



X_p

p large, the geom irred comp of X_p are just the red mod p of the ones of $X_{\mathbb{Q}}$.

cf. EGA:  this is only true for "abs irred".

i.e. may identify $I \simeq I_p$ (large p)

$\mathrm{Tr}(\sigma_p) = \#$ of $\bar{\mathbb{F}}_p$-irred comp of X_p which are rational over $\mathbb{F}_p$

To prove the formula, we simply use that the Betti number of X_p's are constant, hence bounded.

① $\mathrm{Tr}(\sigma_p) = |I|^{\sigma_p}$, Frob func of p

$0 \le \mathrm{Tr}(\sigma_p) \le |I|$, $\mathrm{Tr}(\sigma_p) = |I|$ for a set of p's of density > 0. "value at 1" $= |I|$.

If p is choosen that $I^{\sigma_p} = I$, then
$N_X(p) = |I| \, p^d + O(p^{d-\frac{1}{2}})$
Cor. $\limsup \frac{N_X(p)}{p^d} = |I|$, Th3 B Thm2 (b).

(*) $\sum_{p \le x} N_X(p) = \sum_{p \le x} p^d \, \mathrm{Tr}(\sigma_p) + O(x^{d+\frac{1}{2}})$
f Frobenius fcn with value in $\mathbb{C}$:
$I(f) = \int f$ mean value of f $= \int_G \varphi$
$G \xrightarrow{\varphi} \mathbb{C}$, $f(p) = \varphi(\sigma_p)$, use Haar measure, now just finite gp
$$\int \varphi = \frac{1}{|G|} \sum_{g \in G} \varphi(g)$$
$\sum_{p \le X} f(p) \, p^d = I(f) \, Li(x^{d+1}) + O(\text{---})$ | $x^{d+1} \exp(-c\sqrt{\log x})$ or GRH $x^{d+\frac{1}{2}} \log x$

- G on I:

Tr: rel to the corr linear repr
$I(\mathrm{Tr}) =$ dim fixed pts $= \int \mathrm{Tr} = \#$ of G-orbits in I.
Also known as Burnside's Lemma:
$\#$ of orbits of G acting on $I = \frac{1}{|G|} \sum_{g \in G} |I^g|$

Then (*) $= e_Q \, Li(x^{d+1}) + O(\cdots)$
$e_Q =$ number of orbits of G in $I = \#$ of Q-irred comp.
Lang: 1957, Weil: curves 1948.
Can then use fibering by curves. i.e. Actually can get the result using just the Weil bound.

Date
Note

9. Prime number thm, Ch density for higher dim.

X finite type $/\mathbb{Z}$, sep.

$x \in |X|$ closed pt, $|x|$ = nb of residue field (norm of x)

Hyp: X is flat over $\mathbb{Z}$

(i.e. if $X = \operatorname{Spec} A$, A has "no torsion",

i.e. $A \to A \otimes \mathbb{Q}$ is inj.)

Ex. $A = \mathbb{Z}$, $|X|$ = set of primes, $x = p$, $|x| = p$

$A = \mathcal{O}_K$, $|X|$ = prime ideals v, $|v|$ = # residue field.

recall, $\sum_{p \le x} 1 = Li(x) + \cdots$

Theorem. (let $X = \phi$)

let δ be the dimension of X, e the number of irred comp. of X of dim δ. then

$$\circledast \quad \sum_{\substack{x \in |X| \\ |x| \le \underline{x}}} 1 = e \, Li(\underline{x}^{\delta}) + O(-) .$$

↖ a number

x closed, $k(x) = \mathbb{F}_{p^e}$, $e = \deg(x)$

$e = 1$ is of particular interest, $k(x) = \mathbb{F}_p$

$\sum_{k(x) = \mathbb{F}_p} 1 = N_X(p)$, so

$$\circledast = \sum_{p \le \underline{x}} N(p) + \sum_{\substack{x \in |X| \\ |x| \le \underline{x} \\ \deg(x) \ge 2}} 1$$

one finds this is $O(\underline{x}^{\delta - \frac{1}{2}} \log x)$

This is well-known in Alg # thy. that prime with deg ≥ 2 is of density 0

More or less the same argu.

Analogue of Chebatarev's density thm :

G finite gp acting on a scheme Y (f.t. sep), Assume that Y has a covering by affine open sets which are G-stable then $X = Y/G$ can be defined as a scheme.

Notice that G is not assumed to act faithfully.

$$\sigma_y \qquad \begin{matrix} y \in |Y| \\ \downarrow \\ x \in |X| \end{matrix}$$ will define just like Artin theory

$G \supset D_y \supset I_y$. D_y set of $g \in G$, $gy = y$

I_y " " , and g acts trivially on residue field.

$\sigma_y \in D_y/I_y = \mathrm{Gal}(k(y)/k(x))$

Let φ be a class function on G, with values in $\mathbb{C}$.

$\varphi(x) =$ mean value of $\varphi(g)$

def , for all $g \in D_y$, whose image in D_y/I_y is σ_y.

Still assume Y, X flat $/\mathbb{Z}$. Let δ be the dim of $Y = \dim X$

Then " $\displaystyle\sum_{\substack{x \in |X| \\ |x| \leq X}} \varphi(\sigma_x) = \langle \varphi, r_I \rangle \, Li(X^\delta) + O(-)$. "

scalar prod.

I_y = set of irred comp over $\bar{\mathbb{Q}}$ of $Y/\bar{\mathbb{Q}}$.

Action of G

r_I = char of the perm repr of G (acting on I)

$\langle \varphi, r_I \rangle = I(r_I \cdot \varphi) = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} r_I(g)\varphi(g)$.

Eg. $\begin{matrix} E \\ | \, G \\ \mathbb{Q} \end{matrix}$ $\qquad \begin{matrix} \mathrm{Spec}\, \mathcal{O}_E \\ | \, G \\ \mathrm{Spec}\, \mathbb{Z} \end{matrix} \rightsquigarrow \begin{matrix} \bar{\mathbb{Q}} \times \cdots \times \bar{\mathbb{Q}} \\ \\ \bar{\mathbb{Q}} \end{matrix}$?? Seems to be a contradiction!

$\delta = 1$, $d = 1$

Homework : Make it correct !! may be need to define

I = set of irred. comp of Y of dim δ.

G acts faithfully

Assume Y irred. $\sum_{\neq \phi} \varphi(\sigma_x) = I(\varphi) \cdots$ (use analytic # th on base)

For every $C \subset G$, conj class, there are ∞ many $x \in |X|$ with $\sigma_x \in C$ and they are Zar dense in X.

10. Conjectures related to Motives / Langlands

$X/\mathbb{Q}$ sm proj (not assume conn.)

Choose $\underset{X =}{X/\mathbb{Z}[\frac{1}{N}]}$ sm proj, st. $X \otimes \mathbb{Q} = X/\mathbb{Q}$

By Deligne, $N_X(p) = \sum_{i=0}^{2\dim} (-1)^i \, Tr(\pi_p | H^i_c(\bar{X}, \mathbb{Q}_\ell))$ eigenvalues has abs value $= p^{i/2}$

$= \sum (-1)^i p^{i/2} \varphi_i^X(p)$, i.e.

$-b_i \leq \varphi_i = p^{-i/2} Tr(\pi_p, H^i_c) \leq b_i$

$b_i = \dim H^i_c(\bar{X})$.

Would like to have arch analogue to ℓ-adic repr.

Take a finite family of Xs, get φ_i^X

Conj: There exists a compact Lie gp K,

and a family of conj classes $g_p \in K$

(defined for $p \geq p_0$) and char χ_i^X of K st.

(a) $\varphi_i^X(p) = \chi_i^X(g_p) \quad p \geq p_0$

(b) The g_p are equi-distribution in the cpt set $Cl(K)$

K Haar measure (total measure $=1$) $\quad Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to K/K^0$.

$\downarrow$

$Cl(K)$ direct image.

The trivial case is dim 0. then $K =$ Galois gp

(b) $=$ Ch density thm.

- Ell curve: No CM (over $\bar{\mathbb{Q}}$)

$1+p-a_p$, $a_p = \text{trace } \pi_p$ $\quad \varphi_1(p) = \frac{a_p}{p^{1/2}}$; $[-2, 2]$

In this case $K = SU_2$

$\varphi_0 = \varphi_2 = 1$. φ_1 = natural repr of SU_2.

$a_p = 2\cos\theta_p \cdot p^{1/2}$, g_p = class of $\begin{pmatrix} e^{i\theta_p} & 0 \\ 0 & e^{-i\theta_p} \end{pmatrix}$

Then (*) $\Leftrightarrow$ Sato-Tate conjecture.

$Cl\,K = [-2,2] = [0,\pi]$. Image of Haar $= \frac{2}{\pi}\sin^2\theta\, d\theta$

Sato-Tate proved recently over $\mathbb{Q}$, modulo some technical condition, by Harris, Taylor, Clozel.

- 2 ell. curves without CM, non-isog. over $\bar{\mathbb{Q}}$.

$K = SU_2 \times SU_2$ predicts indep.

Symp. Pure Math AMS: Motives.

"motivated" means cut out by alg cycles
not just some stupid l-adic cycles.

ellip curve, H^1 motive, $G_M \subset GL_2 = GL(H^1)$
motivic gp

H^1, $H^1 \otimes \cdots \otimes H^1$, dual

G_M are essentialy the gp fixes this spaces.

for non-CM, this is known.

genus g curve, $G_M \subset GSp_{2g}$, $G_M \to \mathbb{G}_m$, eg $G_M \subset GL_2 \xrightarrow{\det} \mathbb{G}_m$

$\mathbb{G}_m \nearrow$ get $\mathbb{G}_m \to \mathbb{G}_m$, $\lambda \mapsto \lambda^2$.

$$\underbrace{\mathbb{G}_m \longrightarrow G_M}_{\text{weight map}} \underbrace{\xrightarrow{T} \mathbb{G}_m}_{\text{Tate map}}$$

$G'_M = \ker G_M \to \mathbb{G}_m$, elli curve $G'_M = SL_2$. $(SL_2(\mathbb{C}))$

$K := G'_M(\mathbb{C})$ maximal cpt, should be the K.

C.CHING

There should be Frob. element

p good red., $\sigma_p \in [\mathcal{C}\ell G_M](\mathbb{Q})$

σ_p, $\quad G_M \xrightarrow{T} \mathbb{G}_m \quad$ eg. $\mathbb{G}_m \xrightarrow{inj} GL_2 \xrightarrow{det} \mathbb{G}_m$

$\quad \sigma_p \longmapsto p \qquad\qquad p^{1/2} \qquad (\alpha_p, \bar{\alpha}_p)$

$w : \mathbb{G}_m \to G_M$ is in the center

$g_p = w(p^{-1/2})\,\sigma_p$.

This is (K, g_p). and we expect equi-distribution.

Langland's theory (1966-67).

Grothendieck defines motives

Weil : Tanayama-Weil conj

Langlands : Yale Notes :

Reductive gp, root system

$G \qquad G'$ (Langlands dual)

$G = GL_n$, $G^L = GL_n$

$G = PGL_2$, $G^L = SL_2$.

B_ℓ o—o—o⇒o orth gp $2\ell+1$

C_ℓ o—o—o⇐o Symp gp 2ℓ.

Langlands dual

∞-dim rep G

"tempered" (namely satisfying the Ramanujan conj)

Action of some Hecke alg.

$\longleftrightarrow$ conjugacy classes in $G^L(\mathbb{C})$ of cpt type.

This is striking since:

start with repr/$\mathbb{Q}$, get auto repr of $G(\mathbb{A}_\mathbb{Q})$

$\to$ for each p a conj class in the dual gp
cpt

• Should have motivic g_p's be special cases of L-dual.

Rmk:

motivic gp for ellip curve / k

no CM GL_2

CM defined over ground field: T max torus of GL_2

CM not defined ..: N = normalizer of T $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$.

In general, for H^i, i odd, $2g = \dim H^i$

$-2g \leq \mathrm{Tr}(\sigma_p / p^{i/2}) \leq 2g$.

Conj ⇒ they are dense, eq. wrt a measure μ

with supp $[-2g, 2g]$

why? K, G_M, has circle gp $S_1 \to K$ q.l.t

Hodge indices p.q. $S_1 \xrightarrow{\mathrm{Trace}} [-2g, 2g]$ is onto

$\theta \mapsto 2\cos\theta$

This means that there is no way to improve the Weil bound.

$(2g-\varepsilon)^{1/2} \leq \mathrm{Tr}(\sigma_p) \leq 2g\, p^{1/2}$

Equiv. conj: many L function: ∞-many..

hol at $\mathrm{Re}(s) = 1$ and not zero

$\underline{L(s, \chi)}$ χ char. K, χ ~~mod~~ $\neq 1$.

$\quad$ Tmod

cf. Langlands A Märchen $\quad$ $\underline{\underline{\text{End}}}$

(Fairy tale)

and Arthur.

C.CHING