(J. w. K. Soundararajan)

Twisted - multiplicativity:

$V(a\,;q)$

$a \to \mathbb{Z}/q\mathbb{Z}$, $q \to q \geq 1$ (squarefree)

s.t.

$V(a\,;q_1q_2) = V(a\overline{q_2}\,;q_1)\,V(a\overline{q_1}\,;q_2)$

$(q_1,q_2)=1$ $\qquad [\,q_1\overline{q_1} \equiv 1 \bmod q_2\,]$

Ex. If $U(a\,;q)$

$$U(a\,;q_1q_2) = U(a\,;q_1)\,U(a\,;q_2)$$

$$(\,(q_1,q_2)=1\,)$$

Then

$$V(a\,;q) = \sum_{x \bmod q} U(x\,;q)\,e\left(\frac{ax}{q}\right)$$

$\left[e(z) = e^{2i\pi z} \right]$

is twisted-mult.

[Abstractly: $\widehat{\mathbb{Z}/q\mathbb{Z}} \xleftrightarrow{\sim} \mathbb{Z}/q\mathbb{Z}$

$\left(x \longmapsto e\left(\frac{ax}{q}\right)\right) \longleftarrow\!\!| \; a$

is not compatible with C.R.T]

Ex. 1 - $U(x;q) =$ (norm.) char. function of $A_q \subset \mathbb{Z}/q\mathbb{Z}$

with $A_q = \{ x \bmod q \mid x \bmod p^n \in A_{p^n}, \; \forall p^n \| q \}$

$\rightsquigarrow \; U(a;q) = \frac{1}{|A_q|} \sum_{x \in A_q} e\left(\frac{ax}{q}\right)$

$\rightsquigarrow$ equidistribution of $\left\{ \frac{x}{q} \right\}_{x \in A_q}$

[Hooley: 60's, $A_q = \{x \mid f(x) \equiv 0\ (q)\}$
$f \in \mathbb{Z}[X]$, monic]

K. - Sound

Ex. 2 - $f \in \mathbb{Z}[X]$, $\deg f = d \geq 2$

$$U(x;q) = \frac{1}{\sqrt{q}}\Bigg(\sum_{\substack{y \in \mathbb{Z}/q\mathbb{Z} \\ f(y) = x}} 1 - 1\Bigg)$$

$\rightsquigarrow$

$$V(a;q) = \frac{1}{\sqrt{q}} \sum_{y \bmod q} e\left(\frac{a f(y)}{q}\right)$$

and if $(a,q) = 1$

$$V(0;q) = 0$$

Question: can one estimate (non-trivially)

$$\sum_{q \leq x} V(1;q) \quad ?$$

<u>Theorem</u> (Fouvry - Michel, 2003)

If f is "suitably generic" then

$$\Big|\sum_{\substack{q \le x \\ q \text{ sqf}}} V(1;q)\Big| \le \sum_{q \le x} |V(1;q)|$$

$$\ll x (\log\log x)^{k_f}$$

<u>Note.</u> <u>Weil</u>: if f mod p ~~q~~
 und constant for all $p|q$ then

$$\frac{1}{\sqrt{q}} \Big| \sum e\Big(\frac{af(x)}{q}\Big) \Big| \le (d-1)^{\omega(q)}$$

$[a \not\equiv 0 \bmod q]$

$$\Rightarrow \sum_{q \le x} |V(1;q)| \ll x (\log x)^{A_d}$$

Theorem (K.-Sound)

$f \neq g \circ h$, $\deg \geq 2$

(1) If

$$\boxed{(*) \quad \frac{f(x)-f(y)}{x-y} \in \bar{\mathbb{Q}}[x,y] \text{ is irreducible}}$$

Then $\exists$ $\gamma = \gamma(d) > 0$ s.t.

$$\boxed{\frac{x}{\log x}(\log\log x)^B} \ll \sum_{q \leq x} |V(1;q)| \ll \frac{x}{(\log x)^\gamma}$$

for $x \geq 2$.

In particular

$$\lim_{x \to \infty} \frac{1}{x} \sum_{q \leq x} |V(1;q)| = 0.$$

(2) Under the same assumption

$$\sum_{q \leq x} |V(1;q)|^2 \ll x (\log\log x)^{B_d}$$

Ideas of the proof:

Part 1: (analytic: reduce the problem to $V(a;p)$)
a varying, p prime

[Hooley]

Prop. We have (for any $V(a;q)$)

$$\sum_{\substack{q \leq x \\ q \text{ sqf}}} |V(1;q)| \ll \frac{x}{\log x} \prod_{p \leq z} \left(1 + \frac{g(p)}{p}\right) \prod_{z < p \leq x} \left(1 + \frac{G(p)}{p}\right)$$

where

$$\begin{cases} |V(a;p)| \leq G(p) \ll 1 \\ \dfrac{1}{p} \displaystyle\sum_{\substack{a \bmod p \\ (a,p)=1}} |V(a;p)| \leq g(p) \end{cases}$$

and $z = x^{1/\alpha \log\log x}$, α depends on $\max G(p)$

To get our Th. we need:
under (*), we need to find a positive proportion of primes p s.t.

$$\boxed{\frac{1}{p}\sum_{(a,p)=1}\left|V_f(a;p)\right| \leq 1-\delta}$$

for some $\delta>0$, depending only on d.

(compare with a paper of Katz in Iwasawa Proceedings)

To get the 1^{st} absolute moment, we use a trick:

if 2^{nd} moment is 1

and the 4^{th} ______ is > 1 (unif.)

$\longrightarrow$ the 1^{st} is moment is < 1 (unif)

Th. 2 - For $d \geq 2$ (for f mod p) we have a positive proportion of p with

$$M_4 = \frac{1}{p} \sum_{(a,p)=1} |V_f(a;p)|^4 \geq 2 + O\left(\frac{1}{\sqrt{p}}\right).$$

The proof of Th. 2 is pure algebraic geometry using results of Katz.

① First we may assume (*) mod p (otherwise get "easily" $M_4 \geq 4$) [RH for curves]

②

Katz: The distribution of $V(a;p)$ is "controlled" by a subgroup G_p^f of GL_{d-1}, which implies that

$$M_4 = \mathrm{Tr}\left(f_p \mid E\right) + O\left(\frac{1}{\sqrt{p}}\right)$$

"Frob at p"

where $E = \mathrm{End}\left(\mathrm{End}\left(K^{d-1}\right)\right)^{G_p^g}$

$\mathbb{C}, \overline{\mathbb{Q}_\ell}$

for some group $G_p^g \triangleleft G_p$, $f_p \in G_p / G_p^g$

Generic: $SL_{d-1} = SL_{d-1}$ Id

If $f_p = \mathrm{Id}_E$ then $\mathrm{Tr}(f_p \mid E) = \dim(E)$

Representation th (Schur's Lemma):

E = space of G_p^g - linear maps $\mathrm{End}(K^{d-1})$

and

$\dim E = 1 \iff$ This action of G_p^g

on $\mathrm{End}(K^{d-1})$ is irreducible.

$G_p^g = SL_{d-1}$: this space has two stable subspaces

$\mathbb{C}\,\mathrm{Id}_{\mathbb{C}^{d-1}}$; matrices of Tr. 0

$\neq$ $\{0\}$ $\qquad$ $\neq$ $\{0\}$ for $d \geq 2$

$\Rightarrow$ $\dim E \geq 2$

Our challenge : do this without using knowledge of G_p^g, G_p.

Key ingredients:

(1) show that f_p is also Frobenius for a Galois action over $\mathbb{Q}$

(2) so if the Galois action is finite, any totally split

prime in the kernel has $f_p = 1$.

deduced from a lemma in a previous paper by Michel-Sawin-K.