Remembrances of polynomial values:

Fourier's Way

[Joint with K. Soundararajan]

1. Introduction

Davenport (according to M. Fried):

\[\begin{align*}
\text{Q: If } f, g \text{ are in } \mathbb{Q}[x], \text{ monic, and } \\
\text{what can one say?}
\end{align*}\]

Obvious sol. \[g = f(ax+b), \quad a \neq 0, \quad b \in \mathbb{Q}\]

("f, g are lin. equiv., p.e.")
Classical example: $16$ is an $8^{th}$ power modulo every $p$, $(f(x^8), f(16x^8))$ satisfy $\ast$, but these are not $i.e.$

Note that these are decomposable: $goh$, where $deg(h) \geq 2$.

Th. (Fried) If $f$ and $g$ are indecomposable, then $\ast \iff f, g \text{ lin. equiv.}$

Our problem arises from the natural variant: what about
for all $a$, $N(f; a) = N(g; a)$

$$\sum 1$$

$\frac{1}{f(x) = a}$

$x \in \mathbb{F}_p$

$\Rightarrow$

Consider the discrete Fourier transforms:
\[ \hat{W}(f; h) = \frac{1}{\sqrt{p}} \sum_{a \in \mathbb{F}_p} \hat{N}(f; a) e\left(\frac{ah}{p}\right) \]

\[ e(2) = e^{2\pi i} \]

\[ = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} e\left(\frac{hf(x)}{p}\right) \]

\[ \hat{\circ} \quad \Rightarrow \quad \hat{\otimes} \]

**discrete Fourier analysis**

\[ |\hat{W}(f; h)| = |\hat{W}(g; h)| \]

\[ \hat{\otimes} \quad \Rightarrow \quad \hat{\otimes} \quad \text{holds for } p \text{ large}, \]

**Q.** [K-Sound] if \( \hat{\otimes} \) holds for \( p \) large, what can we say?
Obvious solutions:

\[ g = \bigoplus f(a \chi + b) + \psi \]

w.l.o.g. complex conjugate and multiply \( W \) by \( e(\frac{\beta h}{p}) \)

**Theorem (K - Sound)**

If \( f, g \in \mathbb{F}_p[x] \)

1. \( \deg(f) = \deg(g) = d \geq 1 \), \( p \) large w.r.t. \( d \), and \( f \) and \( g \) generic, then \( |W(f; h)| = |W(g; h)| \)

for all \( h \in \mathbb{F}_p \) implies \( f, g \) w.l.o.g. over \( \overline{\mathbb{F}_p} \).

2. If \( f, g \) are in \( \mathbb{A}[x] \), \( \deg f = \deg g = d \geq 1 \), and are "generic", then \( \bigoplus \) for \( p \) large implies \( f, g \) w.l.o.g.
Q. Can one have "indecomposable" in this statement instead of "generic"?

2. Ideas of the proof [of (1)]

Tools:
1. Deligne's $l$-adic Fourier transform
2. Katz's computation of some "monochromy" groups ($\cong$ big Galois groups)
3. Some group theory (finite groups, compact Lie groups)

Davenport problem
"Sufficiently generic": some Galois groups are "almost" as big as possible

Ideas of the proof: \( p > d \)

Classical Davenport problem

Diagram:

\[ \begin{array}{c}
\mathbb{A}^1_{\mathbb{F}_p} \\
\downarrow f \\
\mathbb{A}^1_{\mathbb{F}_p} \\
\end{array} \xrightarrow{X} \text{Galois closure} \]

\[ \mathbb{G}_d \text{ Galois group} \]

\[ \text{[ = Gal } f(Y) = X, Y \text{ indeterminates base field } \mathbb{F}_p(T)] \]

Fried proved: if \( f, g \) have the same image (over \( \mathbb{F}_p \) also) and indecomposable \((+ \varepsilon)\)
\[ \deg(f) = \deg(g) \]

Then

\[
\begin{array}{cc}
G_f & \quad \downarrow \quad G_g \\
A_1 & \quad \downarrow \quad A_1 \\
A_1 & \quad \downarrow \quad A_1 \\
\end{array}
\]

\[ \text{G}_f \text{ and } G_g \text{ are } \text{the same } \text{ group } G, \text{ moreover:} \]

1) the permutation reps. are isomorphic \( \iff \) \( f, g \) are e.t.

2) the associated linear reps. \( \boxdot \) are isomorphic.

clear under \( \otimes \) because characters are given by \( N(f; \alpha) \), \( N(g; \alpha) \)

\( \alpha \in \mathbb{F}_p^n \)
A construction of Deligne gives "a Fourier side": there exist

\( \Pi(T) = \text{Gal} \left( \overline{\mathbb{F}_p(t)} \Big/ \mathbb{F}_p(t) \right) \xrightarrow{f_g} \hat{G}_q \subset \text{GL}_{d-1} \)

\[\begin{array}{c}
\hat{G}_q \\
\cup \\
\hat{G}_q \\
\cap \\
\text{GL}_{d-1}
\end{array}\]

\[d = \text{deg}(f) = \text{deg}(g)\]

with

\[\text{Tr} \ p_g \left( \text{Frob}_h \right) = \omega(f, h) \neq \text{cong. class in } \Pi(T)\]
Why is it useful?

\[ |W(f; h)| = |W(g; h)| \quad \forall h \]

\[ |W(f; h)|^2 = |W(g; h)|^2 \]

\[ \text{Tr} (\text{Frob}_h | \text{End}(f)) = \text{Tr} (\text{Frob}_h | \text{End}(g)) \]

\[ V = \binom{d-1}{d-1} \]

R.H over finite fields: if \( p \geq p_0(d) \) then these equalities for \( a \in \overline{\mathbb{F}}_p \) (essentially) mean that \( \text{End}(f g) = \text{End}(g f) \).
Q: Given \( p_f, p_g \), if \( \text{End}(p_f) \subseteq \text{End}(p_g) \), what can we say?

We will assume the following "genericity" condition:

1. The original \( G_f, G_g \) are \( S_d \) (generic)
2. The image \( \hat{G}_f, \hat{G}_g \) are (Zariski-dense)

If \( p_f, p_g \) are irreducible, then:

Theorem (Kat2). This holds if

1. \( p > 2d + 1 \)
2. \( f \) has \( d-1 \) distinct critical values \( \left( \frac{f(\zeta)}{f'(\zeta)\zeta} > 0 \right) \)
(3) The critical values form a Sidon set

(\Rightarrow a + b = c + d \text{ with } a, b, c, d \text{ in } S

\Rightarrow a = c \text{ or } a = d)

Last ingredient

\begin{align*}
\text{Lemma. ("Goursat - Kolchin - Ribet Criterion"))} \\
\text{If } \widehat{G}_f = \widehat{G}_g = SL_{d-1} \text{ and } \text{End}(\rho_f) = \text{End}(\rho_g) \\
\text{then either}
\end{align*}

\begin{align*}
(1) \rho_f \otimes \rho_g \text{ is irreducible } (\Rightarrow \text{ not possible}) \\
(2) \rho_f \cong \rho_g \\
(3) \rho_f \cong \rho_g^{\lor} \quad \text{[contragredient]}
\end{align*}