Irreducibility and the distribution of some exponential sums

Joint work with Fernando Chamizo and Jaime Gutierrez.

HRI, Allahabad, February, 2017

$$R(x) = \sum_{n \geq 1} \frac{\sin(2\pi n^2 x)}{n^2}$$

$$R(x) = \sum_{n\geq 1} \frac{\sin(2\pi n^2 x)}{n^2}$$

It is a continuous function differentiable only at infinitely many rational points. Hardy 1916 and Gerver, 1970

$$R(x) = \sum_{n \geq 1} \frac{\sin(2\pi n^2 x)}{n^2}$$

It is a continuous function differentiable only at infinitely many rational points. Hardy 1916 and Gerver, 1970

In fact it is multifractal (Jaffard, 1997)

The spectrum of singularities of the function f is the function

$$d_f(\beta) = \dim_H\{x : \beta_f(x) = \beta\}$$

where $\qquad \beta_f(x) = \sup\{\gamma : f(x+h) - P(h) = O(|h|^{\gamma})\}$

for $P \in \mathbb{C}[X], \deg P \leq \gamma$.

Recall that

$$\dim_H(C) = \inf\{d \geq 0 : \inf_{C \subset \cup_i B_{r_i}} \sum_i r_i^d = 0\}.$$

The spectrum of singularities of the function f is the function

$$d_f(\beta) = \dim_H\{x : \beta_f(x) = \beta\}$$

where $\qquad \beta_f(x) = \sup\{\gamma : f(x+h) - P(h) = O(|h|^\gamma)\}$

for $P \in \mathbb{C}[X], \deg P \leq \gamma$.

Recall that

$$\dim_H(C) = \inf\{d \geq 0 : \inf_{C \subset \cup_i B_{r_i}} \sum_i r_i^d = 0\}.$$

$d_f(\beta)$ is not defined when the set is empty.

The spectrum of singularities of the function f is the function

$$d_f(\beta) = \dim_H\{x : \beta_f(x) = \beta\}$$

where $\qquad \beta_f(x) = \sup\{\gamma : f(x+h) - P(h) = O(|h|^\gamma)\}$

for $P \in \mathbb{C}[X], \deg P \leq \gamma$.

Recall that

$$\dim_H(C) = \inf\{d \geq 0 : \inf_{C \subset \cup_i B_{r_i}} \sum_i r_i^d = 0\}.$$

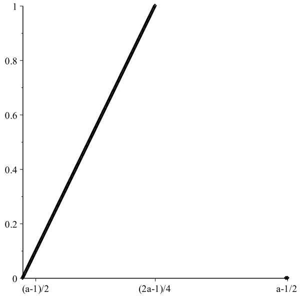
$d_f(\beta)$ is not defined when the set is empty.

A multifractal function is a function such that $d_f(\beta)$ is defined in infinitely many points.

Jaffard found the spectrum of singularities for the function

$$R_a(x) = \sum_{n \geq 1} \frac{\sin(2\pi n^2 x)}{n^a}$$

for any $a > 1$.



Our interest focuses on the function

$$F(x) = \sum_{n\geq 1} \frac{e^{2\pi i P(n)x}}{n^{\alpha}},$$

for $P \in \mathbb{Z}[x]$, $\deg P = k$.

Our interest focuses on the function

$$F(x) = \sum_{n \geq 1} \frac{e^{2\pi i P(n) x}}{n^{\alpha}},$$

for $P \in \mathbb{Z}[x]$, $\deg P = k$. For the case $k = 2$, there is theta function behind.

Our interest focuses on the function

$$F(x) = \sum_{n \geq 1} \frac{e^{2\pi i P(n) x}}{n^{\alpha}},$$

for $P \in \mathbb{Z}[x]$, $\deg P = k$. For the case $k = 2$, there is theta function behind.

Since, $\gamma \leq 1$ so we need to control

$$F(a/p + h) - F(a/p),$$

for $1 \leq a \leq p$, (periodic) and p prime (most interesting).

Our interest focuses on the function

$$F(x) = \sum_{n\geq 1} \frac{e^{2\pi i P(n)x}}{n^\alpha},$$

for $P \in \mathbb{Z}[x]$, $\deg P = k$. For the case $k = 2$, there is theta function behind.

Since, $\gamma \leq 1$ so we need to control

$$F(a/p + h) - F(a/p),$$

for $1 \leq a \leq p$, (periodic) and p prime (most interesting).

By Poisson formula

$$F(a/p + h) - F(a/p) = Ap^{-1} S_a h^{(\alpha-1)/k} + O(h^{\alpha/k} p^{1/2}),$$

for

$$S_a = \sum_{n=1}^{p} e^{2\pi i P(n) a/p}$$

The formula is valid only for very small $h \approx p^{-k}$, but the convergents goes to p^{-1}.

The formula is valid only for very small $h \approx p^{-k}$, but the convergents goes to p^{-1}. We need to make an average on x and p.

The formula is valid only for very small $h \approx p^{-k}$, but the convergents goes to p^{-1}. We need to make an average on x and p.

The goal is to prove that for $S_a = \sum_{n=1}^{p} e^{2\pi i P(n) a/p}$

$$C_1\sqrt{p} \leq S_a \leq C_2\sqrt{p},$$

for $\mu p \leq a \leq \nu p$, $0 < \mu < \nu < 1$.

The formula is valid only for very small $h \approx p^{-k}$, but the convergents goes to p^{-1}. We need to make an average on x and p.

The goal is to prove that for $S_a = \sum_{n=1}^{p} e^{2\pi i P(n)a/p}$

$$C_1\sqrt{p} \leq S_a \leq C_2\sqrt{p},$$

for $\mu p \leq a \leq \nu p$, $0 < \mu < \nu < 1$.

Chamizo- Ubis proved for $P(x) = x^k$ and $k|p-1$,

$$\sum_{p\alpha \leq a \leq p\beta} |S_a|^2 \sim (k-1)(\beta - \alpha)p^2$$

The formula is valid only for very small $h \approx p^{-k}$, but the convergents goes to p^{-1}. We need to make an average on x and p.

The goal is to prove that for $S_a = \sum_{n=1}^{p} e^{2\pi i P(n) a/p}$

$$C_1\sqrt{p} \leq S_a \leq C_2\sqrt{p},$$

for $\mu p \leq a \leq \nu p$, $0 < \mu < \nu < 1$.

Chamizo- Ubis proved for $P(x) = x^k$ and $k|p-1$,

$$\sum_{p\alpha \leq a \leq p\beta} |S_a|^2 \sim (k-1)(\beta-\alpha)p^2$$

An easy application of Jacobi sums gives in this case

$$|S_a| \leq (k-1)\sqrt{p}$$

which implies the previous inequality for $C_1 = \frac{1}{2}$ for at least $\frac{p}{k}(\beta-\alpha)$ values of a and $p \equiv 1 \pmod{k}$

This is not true in general. For example, $(k, p-1) = 1$ and $P(x) = x^k$, then $x \to x^k$ is an isomorphism of $\mathbb{F}_p^*$ and so $S_a = 0$.

This is not true in general. For example, $(k, p-1) = 1$ and $P(x) = x^k$, then $x \to x^k$ is an isomorphism of $\mathbb{F}_p^*$ and so $S_a = 0$.

This is one example of a permutation polynomial on $\mathbb{F}_p$.

This is not true in general. For example, $(k, p-1) = 1$ and $P(x) = x^k$, then $x \to x^k$ is an isomorphism of $\mathbb{F}_p^*$ and so $S_a = 0$.

This is one example of a permutation polynomial on $\mathbb{F}_p$.

The only polynomials which are permutation polynomials for infinitely many primes are the composition of linear and Dickson polynomials (Schur's conjecture).

$$D_n(x, \alpha) = \sum_{l=0}^{[n/2]} \frac{n}{n-l} \binom{n-l}{l} (-\alpha)^l x^{n-2l}$$

$$D_k(x + \alpha/x, \alpha) = x^k + (\alpha/x)^k.$$

Theorem

If P is not composition of linear and Dickson polynomials then for every large enough p

$$\sum_{a=1}^{p-1} |S_a|^2 \geq p^2 + O(p^{3/2}).$$

Theorem

If P is not composition of linear and Dickson polynomials then for every large enough p

$$\sum_{a=1}^{p-1} |S_a|^2 \geq p^2 + O(p^{3/2}).$$

Theorem

The same is true in general for a positive proportion of primes.

(This is the best one can hope. Dickson polynomial's are permutation polynomials for a set of primes of density $\prod_{p|n}(1-2/(p-1))$)

To go from the complete to the incomplete sums we have

Theorem

Given $0 < \mu < \nu < 1$, *we have*

$$\sum_{\mu p \le a \le \nu p} |S_a|^2 = (\mu - \nu) \sum_{a=1}^{p-1} |S_a|^2 + O(p^{3/2} \log p).$$

To go from the complete to the incomplete sums we have

Theorem

Given $0 < \mu < \nu < 1$, *we have*

$$\sum_{\mu p \leq a \leq \nu p} |S_a|^2 = (\mu - \nu) \sum_{a=1}^{p-1} |S_a|^2 + O(p^{3/2} \log p).$$

Corollary

Given $0 < \mu < \nu < 1$ *and* $\log p = o((\nu - \mu)p^{1/2})$, *for any* C *there exist* Δ *such that for a positive proportion of primes we have* $C\sqrt{p} < |S_a| < (\deg P - 1)\sqrt{p}$ *for at least* $\Delta(\nu - \mu)p$ *values of* a *in the interval* $\mu p \leq a \leq \nu p$.

$$f_a = \frac{1}{p} \sum_{n=1}^{p} \sum_{\mu p \le m \le \nu p} e\left(\frac{n}{p}(a-m)\right)$$

$$|S_a|^2 = \sum_{x,y=1}^{p} e^{2\pi i (P(x)-P(y))a/p}$$

$$\sum_{\mu p \le a \le \nu p} |S_a|^2 = \sum_{\mu p \le m \le \nu p} \sum_{n=0}^{p-1} e\left(\frac{-mn}{p}\right) T_n = p(\nu-\mu) T_0 + O(p^{3/2} \log p)$$

where

$$T_n = \#\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : P(x) - P(y) + n = 0\} - p.$$

The proof relies in the following lemma.

Lemma

Let K be a field. If $charK = 0$, for any non constant polynomial $P \in K[x]$ and any $r \neq 0$ in K, the polynomial $P(x) - P(y) + r$ is irreducible over K. If char $K = p$ the same is true whenever $p \nmid degP$.

The proof relies in the following lemma.

Lemma

Let K be a field. If $\mathrm{char} K = 0$, for any non constant polynomial $P \in K[x]$ and any $r \neq 0$ in K, the polynomial $P(x) - P(y) + r$ is irreducible over K. If char $K = p$ the same is true whenever $p \nmid \deg P$.

It is not true for $P(x) + P(y) + r$.

The proof relies in the following lemma.

Lemma

Let K be a field. If char$K = 0$, for any non constant polynomial $P \in K[x]$ and any $r \neq 0$ in K, the polynomial $P(x) - P(y) + r$ is irreducible over K. If char $K = p$ the same is true whenever $p \nmid \deg P$.

It is not true for $P(x) + P(y) + r$.

Take for example $P(x) = x^3 - 1$, $r = 2$. Then
$P(x) + P(y) + 2 = x^3 + y^3 = (x + y)(x^2 - xy + y^2)$.

The proof relies in the following lemma.

Lemma

Let K be a field. If $\mathrm{char}K = 0$, for any non constant polynomial $P \in K[x]$ and any $r \neq 0$ in K, the polynomial $P(x) - P(y) + r$ is irreducible over K. If $\mathrm{char}\, K = p$ the same is true whenever $p \nmid \deg P$.

It is not true for $P(x) + P(y) + r$.

Take for example $P(x) = x^3 - 1$, $r = 2$. Then
$P(x) + P(y) + 2 = x^3 + y^3 = (x + y)(x^2 - xy + y^2)$.

Corollary

Let $P \in \mathbb{Z}[x]$ with degree and leading coefficient odd numbers. Then, $P(x) + P(y) + r$ is absolutely irreducible for any r odd

Proof of the lemma.

$P(x) - P(y) + r = f(x,y)g(x,y)$, with
$f(y,y) = u, g(y,y) = ru^{-1}$.

Hence, $f(x,y) - u$ and $g(x,y) - ru^{-1}$ are divisible by $(x-y)$.
Then,

$$P(x) - P(y) + r =$$
$$= (x-y)^2 B(x,y)C(x,y) + (x-y)(ru^{-1}B(x,y) + uC(x,y)) + r$$

Evaluating the formal derivative of $P(x)$ at y we get

$$P'(y) = ru^{-1}B(y,y) + uC(y,y)$$

Proposition

Let p be and odd prime. If $P(x) = x^{2p} - 2x^{p+1} + x^2 + x$, then $P(x) - P(y) + r$ is reducible over $\mathbb{F}_p$ for every $r \in \mathbb{F}_p$.

Proposition

Let p be and odd prime. If $P(x) = x^{2p} - 2x^{p+1} + x^2 + x$, then $P(x) - P(y) + r$ is reducible over $\mathbb{F}_p$ for every $r \in \mathbb{F}_p$.

Proof.

$$P(x) - P(y) + r = (x - y + r) + H(x, y),$$

where

$$H(x,y) = \prod_{a=0}^{p-1}(x+y-a)(x-y-a) = ((x+y)^p-(x+y))((x-y)^p-(x-y)).$$

Additional tools

Davenport Lewis conjecture.

Lemma

If the polynomial $(P(x) - P(y))/(x - y)$ has an absolutely irreducible factor over $\mathbb{F}_p$, then $T_0 \geq 2p + O(p^{1/2})$

Lemma

Let k, d positive integers. There are forms $g_1, g_2 \ldots$ in $\left(\binom{k+d-1}{k}\right)$ variables with integral coefficients such that for any field K, a polynomial $P \in K[x_1, \ldots, x_k]$ of degree d is not absolutely irreducible over K if and only if all the forms evaluated at the coefficients of P vanish.

Some elementary Galois theory.

Theorem

If $p(x)$ has two simple roots, then $p(x)y + q(x)$ is hereditary for any $(q, p) = 1$.

Theorem

If $p(x)$ has two simple roots, then $p(x)y + q(x)$ is hereditary for any $(q, p) = 1$.

Lemma

Let K be a field of char$K \neq 2$. Then for any $p(x) \in K[x]$, and $a \neq b \in \overline{K}$, $(p(x) - a)(p(x) - b)$ has two simple roots over $\overline{K}$.

Proof. Enough for $a = -1$, $b = 1$. Then, if it is not true, then

$$a(x)^2 = 1 + q(x)$$

, where $q(x) = \prod_{i=1}^{d}(x - x_i)^{e_i}$, $e_i \geq 2$, for $i \geq 2$ and $e_1 = 1$.

$$a(x)a'(x) = q'(x)$$

But $(a(x), q(x)) = 1$, while $\deg(q, q') \geq \deg\,(q) - d$

$$\frac{\deg(q)}{2} - 1 \geq \deg q - d$$

$$2d - 2 \geq \deg q \geq 2d - 1.$$