18.3.2021

A more precise statement concerning generalizations of the question is the following.

Fix $q \geq 1$ ("the modulus")

[Ex : $q = 4$]

$\Omega_X = [1, X]$, $X \geq 1$

$(X \longrightarrow +\infty)$

$\mathbb{P}_X = \frac{1}{\log X} \frac{dt}{t}$ on Ω_X

$(\mathbb{Z}/q\mathbb{Z})^\times$ invertible classes modulo q

$$C_{\mathbb{R}}((\mathbb{Z}/q\mathbb{Z})^\times) = \{ \text{functions } f : (\mathbb{Z}/q\mathbb{Z})^\times \longrightarrow \mathbb{R} \}$$
$$\simeq \mathbb{R}^{\varphi(q)}$$

We define arithmetic r.v. on Ω_X with values in $C_{\mathbb{R}}((\mathbb{Z}/q\mathbb{Z})^\times)$

$\in (\mathbb{Z}/q\mathbb{Z})^\times$

by

$$\underline{N}_x(x)(a) = \frac{\log x}{\sqrt{x}} \left(\varphi(q)\, \pi(x; q, a) - \pi(x) \right)$$

$\in \Omega_x$

(recall: $\pi(x; q, a) = \sum_{\substack{p \le x \\ p \equiv a \bmod q}} 1$

$\pi(x) = \sum_{p \le x} 1$)

[Rubinstein-Saunak distribution]

Theorem 1 (Rubinstein – Saunak)

Assume GRH [modulo q].

Then $\underline{N}_x \xrightarrow{\text{law}} N_q$ $(= N)$

where N is a $C\left((\mathbb{Z}/q\mathbb{Z})^\times\right)$-valued r.v., supported on

$$H_q = \left\{ f \;\middle|\; \sum_a f(a) = 0 \right\}.$$

Remarks: (1) The second conjecture will allow us to write N_q

as a sum of independent random variables ($\Rightarrow$ tools to compute various probabilities for N_q, such as for $q = 4$

$$\mathbb{P}\left(N_4(3) > N_4(1) \right)$$

$$\left[= \lim_{x \to \infty} \frac{1}{\log x} \int_1^x \left(\pi(t;4,3) > \pi(t;4,1) \right) \frac{dt}{t} \right]$$

(2) In principle, knowing N_q lead, to answers for "all" Chebychev-type questions.

Outline:

(1) Discuss primes in arithmetic progressions, through the Dirichlet L-functions (includes discussion of discrete Fourier

analysis on finite abelian groups)

(2) Deduce Theorem 1 using Th. B.4.4 and the Kronecker-Weyl Th.

(3) Go beyond Th. 1 by studying N_q

2- Primes in arithmetic progressions

The study of $\pi(x; q, a)$ is really the most important tool in the study of the distribution of primes (e.g. gaps between primes; Zhang; Maynard; ....)

First Th. (Dirichlet, ≃ 1837)

$q \geq 1$; $(a, q) = 1$

$$\sum_{\substack{p \leq x \\ p \equiv a\,(q)}} \frac{1}{p} = \frac{1}{\varphi(q)} \left(\sum_{p \leq x} \frac{1}{p} \right) + O(1)$$

$\sim \log\log x$

This is a first confirmation that all residue classes $a \bmod q$ with $(a,q) = 1$ contain approximately the same number of primes.

Idea: represent the characteristic function of $n \equiv a\,(q)$ in a way compatible with multiplicative questions.

This includes finding a basis for functions on $(\mathbb{Z}/q\mathbb{Z})^\times$ which

is "multiplicative", i.e. the basis elements respect multiplication.

[[[Digression: discrete Fourier analysis

Def. A: finite abelian group.

A character on A is a group homomorphism

$$\chi : A \longrightarrow \mathbb{C}^\times$$

The set $\hat{A}$ of all characters is an abelian group with

$$(\chi_1 \chi_2)(a) = \chi_1(a)\,\chi_2(a),$$

$$(\chi^{-1})(a) = \frac{1}{\chi(a)}.$$

($\hat{A}$: dual group)

We will use mostly $A = (\mathbb{Z}/q\mathbb{Z})^\times$.

Remarks:

(1) A finite $\Rightarrow a^{|A|} = 1_A$

for all $a \in A \Rightarrow \chi(a)^{|A|} = 1 \in \mathbb{C}$

$\Rightarrow$ every value of $\chi \in \hat{A}$ is a root of unity (esp. $|\chi(a)| = 1$)

(2) $\chi^{-1}(a) = \overline{\chi(a)}$ for $\begin{cases} \text{all } a \\ \text{all } \chi \end{cases}$

(so one writes $\overline{\chi}$ instead of $\bar{\chi}^{-1}$)

(3) χ takes real values if and only if $\chi^2 = 1$ ~ neutral element of $\hat{A}$

$\Leftrightarrow \chi(a) \in \{\pm 1\}$ for all a.

(4) For A infinite, (1), (2), (3) can fail: $A = \mathbb{R}^\times$

$\chi(t) = t$

Examples:

(1) $A = \mathbb{Z}/d\mathbb{Z}$ for $d \geq 1$ (finite cyclic group)

$1 \in A$ generator

$\chi \in \hat{A} \Rightarrow \chi(1)^d = 1$

$\Rightarrow \exists\, \alpha \in \mathbb{Z}, \quad \chi(1) = e^{\frac{2i\pi\alpha}{d}}$

$= e\left(\frac{\alpha}{d}\right)$

Definition: for $z \in \mathbb{C}$,

$e(z) = \exp(2i\pi z)$

(so $e(z_1+z_2) = e(z_1)e(z_2)$

$e(m) = 1$ for $m \in \mathbb{Z}$)

but then

$$\chi(a) = \chi(1)^a = e\left(\frac{a\alpha}{d}\right)$$

and conversely, putting

$$\chi(a) = e\left(\frac{a\alpha}{d}\right)$$

gives an element of $\hat{A}$ for any $\alpha \in \mathbb{Z}$.

Note that $e\left(\frac{a(\alpha+d)}{d}\right) = e\left(\frac{a\alpha}{d}\right) e(a) = e\left(\frac{a\alpha}{d}\right)$

so only α mod d matters. For $0 \le \alpha < d$, we get distinct characters and moreover

$$e\left(\frac{a\alpha_1}{d}\right) e\left(\frac{a\alpha_2}{d}\right) = e\left(\frac{a(\alpha_1+\alpha_2)}{d}\right)$$

so in other words:

$$\begin{cases} \alpha \longmapsto \left(a \longmapsto e\left(\frac{a\alpha}{d}\right)\right) \\ \mathbb{Z}/d\mathbb{Z} \longrightarrow \hat{A} \end{cases}$$

is an isomorphism.

So: $\begin{cases} \hat{A} \text{ finite} \\ \hat{A} \text{ is isomorphic to } A \end{cases}$

Recall:

Th. Any finite abelian group A is of the form

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$$

for some integers $d_i \ge 1$.

Moreover:

Prop: For $A_1 \times \dots \times A_k$

The morphism

$$(\chi_1, \dots, \chi_k) \longmapsto \left(\chi(x_1, \dots, x_k) = \chi_1(x_1) \cdots \chi_k(x_k) \right)$$

gives an isomorphism

$$\widehat{A_1} \times \dots \times \widehat{A_k} \longrightarrow \widehat{A_1 \times \dots \times A_k}$$

Cor. For any finite abelian group A, $\widehat{A}$ is isomorphic to A.

Orthogonality Relations

A finite abelian group

(1) For a, b in A

$$\frac{1}{|\hat{A}|} \sum_{\chi \in \hat{A}} \chi(a) \overline{\chi(b)} = \begin{cases} 1, & a = b \\ 0, & a \neq b \end{cases}$$

[gives the characteristic function of $\{b\}$ in terms of χ's]

(2) For χ_1, χ_2 in $\widehat{A}$

$$\frac{1}{|A|}\sum_{a\in A}\chi_1(a)\,\overline{\chi_2(a)} = \begin{cases} 1, & \chi_1=\chi_2 \\ 0, & \text{else} \end{cases}$$

Proof - (2):

$$\frac{1}{|A|}\sum_{a\in A}\chi_1(a)\,\overline{\chi_2(a)}$$

$$= \frac{1}{|A|}\sum_{a\in A}(\chi_1\bar{\chi}_2)(a)$$

If $\chi_1 \neq \chi_2$ then $\chi_1\bar{\chi}_2 \neq 1$, so we can fix an element $b \in A$ s.t. $(\chi_1\bar{\chi}_2)(b) \neq 1$; then make the change of variable $a \longrightarrow bc$ to get

$$\sum_{a\in A}(\chi_1\bar{\chi}_2)(a) = \sum_{c\in A}(\chi_1\bar{\chi}_2)(bc)$$

$$= \underbrace{(\chi_1\bar{\chi}_2)(b)}_{\neq 1}\sum_{c\in A}(\chi_1\bar{\chi}_2)(c)$$

$$\Rightarrow \sum_{a\in A}(\chi_1\bar{\chi}_2)(a) = 0.$$

Moreover if $\chi_1 = \chi_2$ then the sum is

$$\frac{1}{|A|} \sum_{a \in A} \underbrace{|\chi_1(a)|^2}_{=1} = 1$$

(1) Observe that (2) states that the characters $\chi \in \hat{A}$, as elements of $C(A) = \{ f : A \longrightarrow \mathbb{C} \}$, are orthonormal vectors for the inner product

$$\langle f_1, f_2 \rangle = \frac{1}{|A|} \sum_{a \in A} f_1(a) \overline{f_2(a)}$$

By the Cor., $|\hat{A}| = |A| = \dim_{\mathbb{C}} C(A)$ so the characters form an orthonormal basis of $C(A)$.

So for any $f : A \longrightarrow \mathbb{C}$, we get:

Fourier expansion

$$\forall a \in A, \quad f(a) = \sum_{\chi \in \hat{A}} \langle f, \chi \rangle \chi(a)$$

where $$\langle f, \chi \rangle = \frac{1}{|A|} \sum_{a \in A} f(a) \overline{\chi(a)}$$

↳ discrete Fourier coefficients

Plancherel formula

$$\frac{1}{|A|} \sum_{a \in A} |f(a)|^2 = \sum_{\chi \in \hat{A}} |\langle f, \chi \rangle|^2$$

Apply this to

$$f_b(a) = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{if } a \neq b \end{cases}$$

to get

RHS of (1)

$$f(a) = \sum_{\chi \in \hat{A}} \langle f, \chi \rangle \chi(a)$$

where $$\langle f, \chi \rangle = \frac{1}{|A|} \overline{\chi(b)}$$

so $$f(a) = \frac{1}{|A|} \sum_{\chi \in \hat{A}} \overline{\chi(b)} \chi(a)$$

Application

$$A = \left(\mathbb{Z}/q\mathbb{Z}\right)^{\times}$$

$$|A| = \varphi(q)$$

The characters of A are called Dirichlet characters modulo q. In addition, we also call Dirichlet char. mod q the functions

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

defined by

$$\begin{cases} a \longmapsto \chi(a \bmod q) & \text{if } (a,q)=1 \\ a \longmapsto 0 & \text{if } (a,q) \neq 1 \end{cases}$$

Ex: $q = 4$, $\varphi(q) = 2$

Two characters:

χ_0 $\begin{cases} a \longmapsto 1 & \text{if } a \text{ odd} \\ a \longmapsto 0 & \text{if } a \text{ even} \end{cases}$

$$\chi_1 \begin{cases} a \longmapsto \begin{cases} 1 & \text{if } a \equiv 1 \bmod 4 \\ -1 & \text{if } a \equiv 3 \bmod 4 \end{cases} \\ a \longmapsto 0 \quad \text{if } a \text{ even} \end{cases}$$

Orthogonality relation

For $(a, q) = 1$, $b \in \mathbb{Z}$, we have

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\, \chi(b) = \begin{cases} 1, & b \equiv a \bmod q \\ 0, & \text{otherwise} \end{cases}$$

sum over all Dirichlet char. mod q

[indeed if $(b, q) \neq 1$, both sides are equal to zero].

So for any $f : \mathbb{Z} \longrightarrow \mathbb{C}$

$$\sum_{\substack{1 \le n \le N \\ n \equiv a \,(q)}} f(n) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \sum_{n \le N} f(n)\, \chi(n)$$

Since $\chi(ab) = \chi(a)\,\chi(b)$ for all

$a \in \mathbb{Z}$, $b \in \mathbb{Z}$ (both sides 0 if $(ab, q) \neq 1$), this formula is especially useful if f is multiplicative.

Riemann (building on Euler, Dirichlet): one can relate the characteristic of primes to multiplicative functions.

Definition: Let $\chi \bmod q$ be a Dirichlet character. The L-function of χ is

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}, \quad s \in \mathbb{C}$$

(where convergent first).

Note: $|\chi(n)| \leq 1$

$\Rightarrow L(s, \chi)$ exists for $\mathrm{Re}(s) > 1$

Theorem - (Euler product)

For all χ, $\mathrm{Re}(s) > 1$

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$