22.4.2021

Recall:

Prop. B.4.4

$\mathbb{R}^d$ $\quad d \geq 1$

$(X_n)_{n\geq 1}$ $\mathbb{R}^d$-valued random variables

$(X_{n,m})_{n\geq m\geq 1}$ " " "

$E_{n,m} = X_n - X_{n,m}$

If (1) $X_{n,m} \xrightarrow[n\to\infty]{\text{law}} Y_m$ for fixed $m \geq 1$.

(2) $\lim_{m\to\infty} \limsup_{n\to\infty} \mathbb{E}(\|E_{n,m}\|) = 0$

$\|x\| = \sqrt{x_1^2}$

then X_n and Y_m converge in law to the same limit.

We want to apply this with

$\mathbb{R}^d$

n, m

$f : (\mathbb{Z}/q\mathbb{Z})^{\times} \longrightarrow \mathbb{C}$

x, T

$(x \in \Omega_X = [1, X])$

$$X_n \quad \sum_{\chi \neq \varepsilon_q} \overline{\chi}(a) \sum_{|\gamma| \leq X} \frac{x^{i\gamma}}{1/2 + i\gamma}$$

$$X_{n,m} \quad \sum_{\chi \neq \varepsilon_q} \overline{\chi(a)} \sum_{|\gamma| \leq T} \frac{x^{i\gamma}}{1/2 + i\gamma}$$

Assumption (1) holds by Prop. 5.3.3 (Kronecker's Theorem) with

$$Y_T = \lim_{x \to \infty} \sum_{\chi \neq \varepsilon_q} \overline{\chi} \sum_{|\gamma| \leq T} \frac{x^{i\gamma}}{1/2 + i\gamma}$$

$$= \sum_{\chi \neq \varepsilon_q} \overline{\chi} \sum_{|\gamma| \leq T} \frac{I_{\chi,\gamma}}{1/2 + i\gamma}$$

where $(I_{\chi,\gamma})_{\chi, |\gamma| \leq T}$ is a r.v. uniformly distributed on the closure of $\{ (x^{i\gamma})_{\chi, |\gamma| \leq T} \mid x > 0 \}$.

Assumption (2) follows from:

Prop. (5.3.6) $k \geq 1$

$F \subset \mathbb{R}$ countable

$\alpha(t) \in \mathbb{C}^k$ for $t \in F$

Assume

(i) $\sum_t \|\alpha(t)\|^2 \sqrt{|t|} \log(1+|t|) < +\infty$

(ii) $(T>0)$ $\sum_{|t| \geq T} \frac{\|\alpha(t)\|}{t^{1/4}} \ll \frac{(\log T)^2}{T^{1/4}}$

(iii) $(t_0 \in \mathbb{R})$ $\left| \{ t \in F \mid |t - t_0| \leq 1 \} \right| \ll \log(1+|t_0|)$

Then

$$\lim_{T \to \infty} \limsup_{X \to \infty} \left\| \sum_{\substack{T \leq |t| \leq X \\ t \in F}} \alpha(t) x^{it} \right\|_{L^2(\Omega_X)} = 0$$

Application:

$F = \{ \gamma \mid \frac{1}{2} + i\gamma$ is a zero of some $L(s, \chi)$, $\chi \neq \varepsilon_q \}$

and $\alpha(t) = \sum_{\substack{\chi \neq \varepsilon_q \\ L(\frac{1}{2}+it,\chi)=0}} \overline{\chi} \; \frac{(\text{mult. of } \frac{1}{2}+it)}{\frac{1}{2}+it}$

[$\Rightarrow$ $\sum_{T \le |t| \le X, \; t \in F} \alpha(t) \, x^{it} = \sum_{\chi \neq \varepsilon_q} \overline{\chi}(a) \sum_{T \le \gamma \le X} \frac{x^{i\gamma}}{\frac{1}{2}+i\gamma}$

Hence the conclusion implies (2) of B.4.4.]

Here

$$\|\alpha(t)\| \ll \underbrace{\varphi(q)^{3/2}}_{\text{nb. of } \chi\text{'s times } \|\overline{\chi}\|} \frac{1}{|\frac{1}{2}+it|} \underbrace{\log(1+|t|)}_{\text{bound on the multiplicity}}$$

so

$$\|\alpha(t)\|^2 \sqrt{|t|} \log(1+|t|) \underbrace{\ll}_{\text{constant may depend on } q} \frac{\log(1+|t|)^2}{(1+|t|)^{3/2}}$$

so the series (i) converges

(since the the number of t's in an interval of length 1 is at most $\log(1+|H|)$)

Next:

$$\sum_{|H|\geq T} \frac{\|\alpha(H)\|}{|H|^{1/4}} \ll \sum_{|H|\geq T} \frac{\log(1+|H|)}{(1+|H|)^{5/4}}$$

same reason as before

$$\ll \frac{\log(1+T)^2}{T^{1/4}}$$

which gives (ii)

Finally:

$$|\{t \mid |t-t_0| \leq 1\}|$$

is bounded by $\ll \log(1+|t_0|)$

$\Rightarrow$ (iii).

Conclusion : [Under GRH(q)]

The Rubinstein-Saunah Theorem holds, more precisely:

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

converges in law as $X \longrightarrow +\infty$ to

$$\lim_{T\to\infty}\left(m_q(a) - \sum_{\chi \neq \varepsilon_q} \overline{\chi(a)} \sum_{\substack{|\gamma|\le T \\ L(\frac12+i\gamma,\chi)=0}} \frac{I_{\chi,\gamma}}{\frac12 + i\gamma}\right)$$

(exists in law)

where for any $T \geq 1$ the r.v.

$$\left(I_{\chi,\gamma}\right)_{\chi \neq \varepsilon_q,\ |\gamma|\le T}$$

are uniform on the closure of

$$\left\{ (x^{i\gamma})_{\chi,\,|\gamma|\le T} \;\middle|\; x>0 \right\} \subset (S^1)^{X_T}$$

with $X_T = \{(\chi,\gamma) \mid \chi \neq \varepsilon_q,\ L(\frac12+i\gamma,\chi)=0,\ |\gamma|\le T\}$

and

$$m_q(a) = \begin{cases} 1 & \text{if } a \text{ not a square mod } q \\ 1 - \left|\{x \bmod q \mid x^2 = 1\ (q)\}\right| \end{cases}$$

3 - A formula for the Rubinstein-Saunah measure

The previous formula is still unsatisfactory since the limit as $T \to \infty$ is very complicated.
We will see that under some assumption, we can formally let $T \to \infty$.

Q. What is the law of $\left(I_{x,y} \right)_{(x,y) \in X_T}$?

$$\left[X_T = \left\{ (x,y) \;\middle|\; x \neq \text{Eq}, \; L\left(\tfrac{1}{2} + iy, x\right) = 0, \; |y| \leq T \right\} \right]$$

with multiplicity

Could they be independent?

A. NO! For an obvious reason, namely

$$\overline{L(s,\chi)} = L(\bar{s},\bar{\chi})$$

$$\left[\overline{\sum_{n\geq 1}\frac{\chi(n)}{n^s}} = \sum_{n}\frac{\overline{\chi(n)}}{n^{\bar{s}}}, \quad \mathrm{Re}(s)>1,\right.$$

$$\left.\text{and then analytic continuation}\right].$$

so $$\overline{L\left(\tfrac{1}{2}+i\gamma,\chi\right)} = L\left(\tfrac{1}{2}-i\gamma,\bar{\chi}\right)$$

so if $(\chi,\gamma)\in X_T$, so is

$$(\bar{\chi},-\gamma)\in X_T$$

and $$\overline{\chi^{i\gamma}} = \chi^{-i\gamma},$$ so

$$\boxed{\overline{I_{\chi,\gamma}} = I_{\bar{\chi},-\gamma}}$$

For (χ,γ) s.t. $\gamma>0$, no such relation can be written.

Rubinstein - Sarnak then propose:

Conjecture ("Grand Simplicity Hypothesis" mod q)

The family $(I_{\chi,\gamma})_{(\chi,\gamma) \in X_T^+}$ are independent (each is S^1-valued), where ~~$X_T^+ = \{(\chi,\gamma) \in X_T \mid \gamma \geq 0\}$~~ with multiplicity.

More precisely: the ordinates γ for $(\chi,\gamma) \in X_T^+$ are $\mathbb{Q}$-linearly independent.

("More precisely" implies first statement by Kronecker's Theorem, since then

$$\{(x^{i\gamma})_{(\chi,\gamma) \in X_T^+} \mid x > 0\}$$

is dense in $(S^1)^{X_T^+}$, so the $(I_{\chi,\gamma})$ are the coordinates of

the Haar measure on $(S^1)^{X_T^+}$, which are independent (S^1)-valued random variables).

If we make this assumption, then we get:

Th. (Rubinstein-Sarnak; 5.4.4)

Assume GRH(q) and GSH(q).

Then

$$\frac{N_X^{(a)}}{X} \xrightarrow[X \to +\infty]{\text{law}} N_q = m_q(a) - \sum_{\chi \neq \varepsilon_q} \overline{\chi(a)} \sum_{\substack{\gamma > 0 \\ L(\frac{1}{2}+i\gamma, \chi)=0}} \left(\frac{I_{\chi,\gamma}}{1/2+i\gamma} + \frac{\overline{I_{\chi,\gamma}}}{\frac{1}{2}-i\gamma} \right)$$

$(I_{\chi,\gamma})_{\gamma>0}$ are i.i.d on S^1

$$2\,\mathrm{Re}\left(\frac{I_{\chi,\gamma}}{1/2+i\gamma} \right)$$

where the series converges almost surely (and in L^2), and the summands are independent.

Idea: check using Kolmogorov's 3 series theorem that the RHS is almost surely convergent, hence also in law, and compare with the previous formula

$$\lim_{\substack{T\to\infty \\ \text{(in law)}}} \left(m_q(a) - \sum_{\chi \neq \xi_q} \overline{\chi}(a) \sum_{|\gamma|\leq T} \frac{I_{\chi,\gamma}}{\frac{1}{2}+i\gamma} \right).$$

and use the relation between $\overline{I_{\chi,\gamma}}$ and $I_{\overline{\chi},-\gamma}$ to see that the two limits are the same.

□

Why should we believe in GSH(q)?

Skepticism might be because it implies many very strong facts on zeros of Dirichlet L-functions:

(1) $L(\frac{1}{2}, \chi) \neq 0$ for $\chi \neq \varepsilon_q$

[because $\{\alpha_j\}$ is not $\mathbb{Q}$-linearly independent] [conjectured previously by Chowla]

(2) No zero of $L(s, \chi)$ has multiplicity ≥ 2

[because $1 \cdot \gamma - 1 \cdot \gamma = 0$ would $\mathbb{Q}$-linear relation]

mult. 1 mult. 2

(3) For $\chi_1 \neq \chi_2$, both $\neq \varepsilon_q$, $L(s, \chi_1)$ and $L(s, \chi_2)$ have no common zero.

Very little is known about this!

Believing in GSH(q) is mostly about using the most reasonable

assumption with our current knowledge !

"Small" deviations could be very easily incorporated (e.g. a finite number of relations) in another formula.

Example:

$q = 4$; assuming GRH(4), GSH(4)

→ only one L-function

$$L(\chi_4, s) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \dots$$

$-1, \ a=3$
$1, \ a=1$

$$N_4(a) = m_4(a) - \overline{\chi}(a) \sum_{\substack{\gamma>0 \\ L(\frac{1}{2}+i\gamma, \chi_4)=0}} 2\,\mathrm{Re}\left(\frac{I_\gamma}{\frac{1}{2}+i\gamma}\right)$$

$m_4(a) = \begin{cases} 1, & \text{for } a=3 \\ -1, & \text{" } a=1 \end{cases}$

where (I_γ) are i.i.d on $\mathbb{S}^1$.

The quantity for the Chebychev Bias is

$$N_4(3) - N_4(1) = 2 + 4 \sum_{\gamma > 0} \mathrm{Re}\left(\frac{I_\gamma}{1/2 + i\gamma}\right)$$

(series with indep. terms).

Q: How do we get from this a numerical quantification of the fact that $N_4(3) - N_4(1)$ is "usually" > 0 ?

Note that by convergence in L^2 we have

$$\mathbb{E}\left(N_4(3) - N_4(1)\right) = 2 + 0$$

because $\mathbb{E}\left(\mathrm{Re}\left(I_\gamma\right)\right) = 0$, for each γ.