__Last time__ $(a_n)_n$ equidistr.

$$\Updownarrow$$

a) $\lim\limits_{N\to\infty} \frac{1}{N} \#\{1\le n\le N : a_n \in I\} = \text{length}(I) \qquad \forall I$

$$\Updownarrow$$

c) $\lim\limits_{N\to\infty} \frac{1}{N} \sum\limits_{n=1}^{N} e(t a_n) = 0 \qquad \forall t \neq 0$

Often, c) is easier to show, but we're more interested in a), and in fact in a quantitative version: how fast is the convergence? (for some finite N)

Given upper bounds on $\left|\frac{1}{N}\sum e(t a_n)\right|$, can we derive upper bounds on $\left|\frac{1}{N}\#\{1\le n\le N : a_n\in I\} - \text{length}(I)\right|$ (for the same N)?

__Def__ The __discrepancy__ of $a_1,\dots,a_N$ is

$$D_N := D(a_1,\dots,a_N) := \sup_{\substack{I\subseteq \mathbb{R}/\mathbb{Z} \\ \text{interval}}} \left|\frac{1}{N}\#\{1\le n\le N : a_n\in I\} - \text{length}(I)\right|.$$

[If you know $\frac{1}{N}\sum_n e(t a_n)$ __exactly__ for __all__ t, you could recover the values a_n. But that's not so useful. Instead, we want to bound D_N using just the values for $|t|\le T$. This is a little like in sieves, where we only considered small (squarefree) numbers.]

Thm 13.5 (Erdős–Turán inequality)

For any $a_1, \ldots, a_N \in \mathbb{R}/\mathbb{Z}$ and any $T \geq 1$,

$$\cancel{D_N = \frac{1}{M+1} + 3 \sum_{m=1}^{M} \frac{1}{Nm} \left| \sum_{n=1}^{N} e(m a_n) \right|}$$

$$D_N \leq \frac{1}{T+1} + \frac{3}{N} \sum_{t=1}^{T} \frac{1}{t} \left| \sum_{n=1}^{N} e(t a_n) \right| .$$

For example:

Cor 13.6 Let $\lambda \in \mathbb{R}$, $a_n = \{\lambda n\}$, $T \geq 1$. Then,

$$D_N \ll \frac{1}{T} + \frac{1}{N} \sum_{t=1}^{T} \frac{1}{t \cdot \|t\lambda\|_{\mathbb{R}/\mathbb{Z}}}$$

(if $t\lambda \notin \mathbb{Z}$ for all $1 \leq t \leq T$).

"If λ is not close to a rat. nr. with small denominator, D_N is small."

Pf of Cor

$$\sum_{n=1}^{N} e(t\lambda n) = e(t\lambda) \cdot \frac{e(t\lambda N) - 1}{e(t\lambda) - 1} \ll \frac{1}{|e(t\lambda) - 1|} \ll \frac{1}{\|t\lambda\|_{\mathbb{R}/\mathbb{Z}}} . \quad \square$$

Rmk You can get nice estimates in many other cases. For example, try the sequence $a_n = \{\lambda n^2\}$ or $a_n = \{\lambda p_n\}$ where p_n is the n-th prime number or $a_n = \{\log(n!)\}$ or ...

The theorem follows immediately from the following way of approximating $1_I(x)$ by a sum of the form $\sum_{-T\le t\le T} b_t e(tx)$:

Lemma 13.7 (Selberg) Let $I \subseteq \mathbb{R}/\mathbb{Z}$. There are real-valued functions $f^+, f^- \in L^1(\mathbb{R}/\mathbb{Z})$ such that:

a) $f^-(x) \le 1_I(x) \le f^+(x)$ for all $x \in \mathbb{R}/\mathbb{Z}$

b) $\widehat{f^\pm}(t) = 0$ unless $-T \le t \le T$

c) $\Big|\underbrace{\widehat{f^\pm}(0)}_{(=\int f^\pm(x)dx)} - \text{length}(I)\Big| = \frac{1}{T+1}$.

d) $|\widehat{f^\pm}(t)| \le \frac{3}{2|t|}$ for $t \neq 0$.

Pf of Thm

$$\frac{1}{N}\sum_{n=1}^{N} 1_I(a_n) \le \frac{1}{N}\sum_n \underbrace{f^+(a_n)}_{\hat{\hat{f}}^+(-a_n)} = \frac{1}{N}\sum_n \sum_t \widehat{f^+}(t)e(-ta_n)$$

$$= \frac{1}{N}\sum_t \widehat{f^+}(t)\underbrace{\sum_{n=1}^{N} e(-ta_n)}_{=N \text{ if } t=0}$$

$$= \widehat{f^+}(0) + \frac{1}{N}\sum_{t\neq 0}\underbrace{\widehat{f^+}(t)}_{=\widehat{f^+}(-t)}\sum_n e(-ta_n)$$

$$\le \text{length}(I) + \frac{1}{T+1} + \frac{2}{N}\sum_{t=1}^{T}\frac{3}{2|t|}\Big|\sum_n e(-ta_n)\Big|$$

The lower bound works the same way, using f^-. □

~~The lemma follows from Lemma 13.8 There is a~~

<u>Pf of Lemma</u>

~~Recall that~~ Recall from complex analysis that

$$\left(\frac{\pi}{\sin(\pi z)}\right)^2 = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2}. \qquad (\mathrm{I})$$

Let $\operatorname{sgn}(x) = \begin{cases} 1 & , \operatorname{Re}(x) \geq 0, \\ -1 & , \operatorname{Re}(x) < 0, \end{cases}$ (!)

$$B(z) = \left(\frac{\sin(\pi z)}{\pi}\right)^2 \left(\sum_{n\in\mathbb{Z}} \frac{\operatorname{sgn}(n)}{(z-n)^2} + \frac{2}{z} \right).$$

This defines an entire function (as $\frac{\sin(\pi z)}{\pi}$ has a zero at $z = n \in \mathbb{Z}$).

$$(\mathrm{I}) \Rightarrow B(z) - \operatorname{sgn}(z) = \left(\frac{\sin \pi z}{\pi}\right)^2 \Bigg(\underbrace{\sum_{n\in\mathbb{Z}} \frac{\operatorname{sgn}(n) - \operatorname{sgn}(z)}{(z-n)^2}}_{\substack{\sum_{n=1}^{\infty} \frac{-2}{(z+n)^2} \text{ if } z \geq 0 \\ \sum_{n=0}^{\infty} \frac{2}{(z-n)^2} \text{ if } z < 0}} + \frac{2}{z} \Bigg) \geq 0 \quad \forall z \qquad (\mathrm{II})$$

(with equality for $z \in \mathbb{Z}$).

Also,

$$\int_{\mathbb{R}} (B(z)-\operatorname{sgn}(z))\,dz = \lim_{A\to\infty}\int_{-A}^{A}\cdots = \lim_{A\to\infty}\int_{0}^{A}(B(z)+B(-z))\,dz$$

(at least in the principal value)

$$= \int_0^\infty \left(\frac{\sin(\pi z)}{\pi}\right)^2 \cdot \frac{2}{z^2}\,dz = \int_{\mathbb{R}}\left(\frac{\sin(\pi z)}{\pi z}\right)^2 dz = 1$$

(III)

Moreover, $B(z)-\operatorname{sgn}(z) \ll \frac{e^{2\pi|\Im z|}}{1+|z|^2}$. (IV)

Note: $B \notin L^1(\mathbb{R})$!

Let $I = [a,b]$, $a \le b \in \mathbb{R}$.

Take $F^+(x) = \frac{1}{2}(B(x-a)+B(b-x))$.

$F^-(x) = -\frac{1}{2}(B(a-x)+B(x-b))$.

(II) $\Rightarrow$ $F^+(x) \geq \frac{1}{2}(\operatorname{sgn}(x-a)+\operatorname{sgn}(b-x)) = \begin{cases} 0, & b<x, \\ 1, & a\le x\le b, \\ 0, & x<a, \end{cases}$

$= \mathbb{1}_{[a,b]}(x)$.

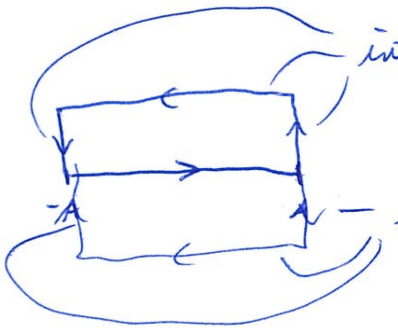
and $F^-(x) \le \dots = \mathbb{1}_{[a,b]}(x)$.

(III) $\Rightarrow$ $\int_{\mathbb{R}}(F^\pm(x) - \mathbb{1}_{[a,b]}(x))\,dx = \pm 1$

Moreover, quite surprisingly,

$$\widehat{F^{\pm}}(t) = 0 \quad \text{if } |t| \geq 1 :$$

$$\widehat{F^{+}}(t) = \int_{\mathbb{R}} F^{+}(x)\, e(xt)\, dx = \lim_{A \to \infty} \int_{-A}^{A} \cdots \qquad = 0$$



integrals go to 0 for $t > 0$ by (IV)

integrals go to 0 for $t < 0$ by (IV)

To finish the proof, rescale and then take

$$f^{\pm}(x) = \sum_{n \in \mathbb{Z}} F^{\pm}(x+n)$$

$\vdots$

(for details, see Murty / Elkies) $\square$

Outlook:

The Sato-Tate Conjectures:

Ese For any prime p, let

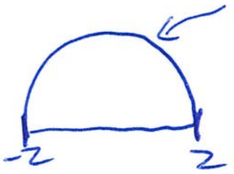
$$k_p = \# \{ (x,y) \in \mathbb{F}_p : y^2 = x^3 + x + 1 \}.$$

Let $t_p = p - k_p$.

Hasse's thm $\Rightarrow$ $|t_p| \leq 2\sqrt{p}$ for (suff. large) p.

$\rightsquigarrow$ Let $a_p = \frac{t_p}{\sqrt{p}} \in [-2,2]$.

The sequence $(a_p)_p$ is equidistributed w.r.t. the measure $\frac{1}{2\pi}\sqrt{4-x^2}\,dx$.

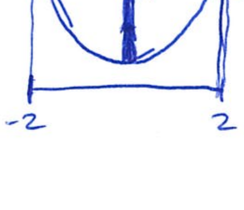


density function ("histogram")

If you do the same for the equation $y^2 = x^3 + 1$, the sequence is equidistributed w.r.t. the measure

$$\frac{1}{2\pi} \cdot \frac{1}{\sqrt{4-x^2}}\,dx + \frac{1}{2}\delta_0(x)\,dx$$

counting measure (dirac delta) at 0



for half the primes, $a_p = 0$

What's going on?

$a_p = tr(M_p)$ for a particular 2×2-matrix $M_p \in G$,

where $G = \begin{cases} SU(2) , & y^2 = x^3 + x + 1 \text{ case} \\ N(U(1)) , & y^2 = x^3 + 1 \text{ case} \end{cases}$

$$N(U(1)) = \left\{ \begin{pmatrix} u & 0 \\ 0 & \bar{u} \end{pmatrix} \middle| u \in \mathbb{C}^\times, |u| = 1 \right\} \cup \left\{ \begin{pmatrix} 0 & u \\ -\bar{u} & 0 \end{pmatrix} \middle| \ldots \right\}$$

"The matrix M_p is equidistr. in G w.r.t. the Haar measure!"