VARIATIONS ON THE CHEBYCHEV BIAS PHENOMENON

FLORENT JOUVE

① CLASSICAL SETTING

$$x \longmapsto \sum_{p \le x} \left(\frac{-1}{p}\right) \qquad \text{SIGN?}$$

p: PRIME; $\left(\frac{-1}{p}\right)$: LEGENDRE SYMBOL

i.e COMPARE $\#\{p \le x : p \equiv 1\ (4)\}$

WITH $\#\{p \le x : p \equiv 3\ (4)\}$

CHEBYSHEV (1853): "FOR MOST" $x \ge 2$

$$\sum_{p \le x} \left(-\frac{1}{p}\right) < 0$$

MORE PRECISELY AND MORE GENERALLY:

$q \ge 1$, $a_1, \dots, a_n$ INVERTIBLE CLASSES MOD q

$$\pi(x, q, a_i) = \#\{p \le x : p \equiv a_i\ (q)\}$$

CONSIDER

$$P_{q, a_1 \dots a_n} = \{x \ge 2 : \pi(x, q, a_1) > \pi(x, q, a_2) > \dots > \pi(x, q, a_n)\}$$

CHEBYCHEV CASE: $q = 4$, $a_1 = 3$, $a_2 = 1$

QUESTIONS: $P_{q; a_1, \dots, a_n} \neq \emptyset$?

MEASURE?

WINTNER ($\approx$ 1940): USE log. DENSITY TO MEASURE SUCH SETS

DEF: $P \subset \mathbb{R}_{\ge 2}$

$$\underline{\delta}(P) = \varliminf_{x \to \infty} \frac{1}{\log x} \int_{[2, x] \cap P} \frac{dt}{t}$$

WRITE $\delta(P)$ WHEN BOTH LIMITS COINCIDE.

RUBINSTEIN - SARNAK:

GET RESULTS CONDITIONAL ON GRH + LI FOR $L(\Delta, \chi)$

χ IS A CHAR. OF CONDUCTOR q.

TH: (R-S, '94) UNDER GRH + LI

$\delta(P_{q,a_1,\dots,a_n})$ EXISTS AND IS >0 (SO $P_{q,a_1,\dots,a_n} \neq \emptyset$)

$\delta(P_{4;3,1}) \approx 0.99590\ldots$ $\delta(P_{3;2,1}) \approx 0.9990\ldots$

DISSIPATION OF THE BIAS:

r fixed

$$\max_{\substack{a_1,\dots,a_n \\ \text{inv. mod } q}} \left| \delta(P_{q,a_1,\dots,a_n}) - \frac{1}{n!} \right| \xrightarrow[q\to\infty]{} 0$$

CONJ LI: MULTISET

$$\{\gamma \geq 0 ;\ L(\tfrac{1}{2} + i\gamma, \chi) = 0,\ \chi \text{ RUNNING OVER PRIM. CHAR. MOD } q\}$$

is LIN. INDEP. OVER $\mathbb{Q}$.

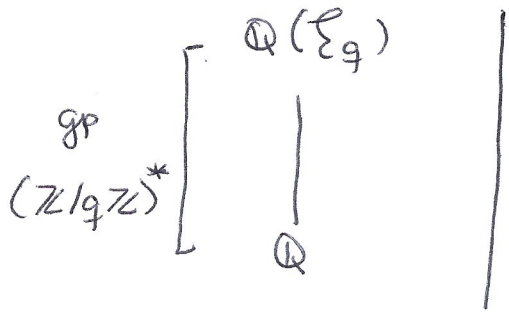
Rem: implies · $L(\frac{1}{2}, \chi) \neq 0$

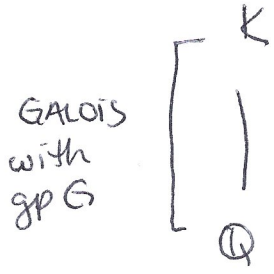
· SIMPLICITY OF CRITICAL ZEROS FOR EACH χ

(2) VARIANT 1: MORE GENERAL GALOIS GROUPS

CLASSICAL SETTING: PNT IN AP'S IS THE UNDERLYING EQUIDISTRIBUTION STATEMENT.

CORRESPONDS TO





PRIME EQUIDIST. IN CLASSES OF $(\mathbb{Z}/q\mathbb{Z})^\times$

Frob. elements equidist. in CONJ. CLASSES OF G.

EX: WHY NOT COMPARE:

$\#\{p \le x : 2 \text{ IS A CUBE MOD } p \text{ AND } p \equiv 1 \ (3)\}$

AND $\#\{p \le x : 2 \text{ IS A NON-CUBE MOD } p \text{ AND } p \equiv 1 \ (3)\}$.

HERE $K = \mathbb{Q}(2^{1/3}, \zeta_3)$ AND $G = Gal(K/\mathbb{Q}) \simeq S_3$

FIRST OF THE TWO SETS: p SUCH THAT $Frob_p$ is id. in S_3

SECOND ——— : p SUCH THAT $Frob_p$ is IN $\{(1\,2\,3), (1\,3\,2)\}$

ANALOGUE OF CHEBYCHEV QUESTION:

C_1, C_2 INV. UNDER CONJ. IN $G = Gal(K/\mathbb{Q})$

LOOK AT $P_{C_1,C_2} := \left\{ n \ge 1 : \dfrac{\pi(n, C_1)}{|C_1|} > \dfrac{\pi(n, C_2)}{|C_2|} \right\}$

WHERE $\pi(n, C) = \#\{p \le n : Frob_p \in C\}$

DENSITY TO BE STUDIED:

$$\underline{\delta}(P_{C_1,C_2}) = \varliminf_{N\to\infty} \frac{1}{\log N} \sum_{n=1}^{N} \frac{1}{n}$$

RESULTS (OBTAINED IN JOINT WORK WITH D. FIORILLI)

ARE CONDITIONAL ON (*): { GRH; ARTIN; SOME VARIANT OF LI } | FOR ARTIN L-FUNCTIONS OF IRRED. REPS. OF G

THEOREM 1: UNDER (*):

LET $K_n/\mathbb{Q}$ WITH GALOIS GROUP S_n

ONE HAS

$$\max_{C_1, C_2} \left| \delta(P_{C_1, C_2}) - \frac{1}{2} \right| \leq (n!)^{-\frac{1}{4}+o(1)}$$

$\downarrow$

no bias appears

TO HAVE HIGHLY BIASED EXAMPLES

REMEMBER IN THE CLASSICAL CASE:

"BIAS IN PRIMES mod 4 IS TOWARDS NONSQUARES" (3 mod 4)

CONSIDER: $\pi(x, NR) = \{ p \leq x : \mathrm{Frob}_p \text{ IS NOT A SQUARE IN } G \}$

$$\pi(x, R) = \sum_{\substack{p < x \\ \pi_p \neq 0}} (\pi_p - 1) \quad \text{WHERE} \quad \pi_p := \#\{ g \in G : g^2 = \mathrm{Frob}_p \}$$

THEOREM 2: UNDER (*)

THERE EXISTS $(K_\ell/\mathbb{Q})$ INDEXED BY PRIMES $\ell \geq 7$ SO THAT $\mathrm{Gal}(K_\ell/\mathbb{Q}) \simeq D_\ell$ (DIHEDRAL ORDER 2ℓ)

A CONSTANT $c > 0$

SUCH THAT $\delta(P_{NR,R}) \geq 1 - \exp\left(-c \frac{\ell}{\log \ell}\right)$

EXTREME BIAS TOWARDS POSITIVE VALUES

REM: BUILDING ON THE SAME IDEA

real $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$

K_d: HILBERT CLASS FIELD OF $\mathbb{Q}(\sqrt{d})$

ONE HAS $Gal(K_d/\mathbb{Q}(\sqrt{d})) \simeq \mathcal{C}_d$: the class group of $\mathbb{Q}(\sqrt{d})$

ALSO $K_d/\mathbb{Q}$ GALOIS WITH gp $\mathcal{C}_d \rtimes \mathbb{Z}/2\mathbb{Z}$

AND IF $\sigma \in \mathcal{C}_d$, $\tau \in \mathbb{Z}/2\mathbb{Z} \setminus \{0\}$

THEN $\tau\sigma\tau = \sigma^{-1}$

KEY POINT: IN BOTH THESE CASES $Gal(K/\mathbb{Q})$ CONTAINS MANY ELEMENTS OF ORDER 2.

③ VARIANT 2: ELLIPTIC CURVES / $\mathbb{Q}$

$E/\mathbb{Q}$: $y^2 = x^3 + ax + b$, $\Delta \neq 0$ + 1 POINT AT INFINITY

LET p BE A PRIME OF GOOD RED. MEANING "E OVER $\mathbb{F}_p$" IS STILL AN ELLIPTIC CURVE

mod p POINTS : $|E(\mathbb{F}_p)| = 1 + \sum_{x \bmod p} \left(\left(\frac{x^3+ax+b}{p} \right) + 1 \right)$

GET $|E(\mathbb{F}_p)| = p + 1 + \underbrace{\sum_{x \bmod p} \left(\frac{x^3+ax+b}{p} \right)}_{-a_p(E)}$

$x \longmapsto \left(\frac{x^3+ax+b}{p} \right)$ IS A TRACE FUNCTION

BY GROTHENDIECK - LEFSCHETZ:

$$a_p(E) = \mathrm{Tr}(\mathrm{Fr} \mid H_c^{\cdot}(\bar{E}, \bar{\mathbb{Q}}_\ell))$$

HASSE: $|a_p(E)| \leq 2\sqrt{p}$

CAN WRITE $a_p(E) = 2\sqrt{p}\cos(\theta_p)$, $\theta_p \in [0, \pi]$

ASSUME THAT E IS NOT CM : THE θ_p's

EQUIDIST. IN $[0, \pi]$ wrt the SATO-TATE LAW

ANALOGUE PNT IN AP'S, Čebotarov ...)

CHEBYSHEV TYPE QUESTION:

$$S: t \longmapsto \#\{p \leq t : a_p(E) > 0\} - \#\{p \leq t : a_p(E) < 0\}$$

sign?

(QUESTION RAISED BY MAZUR)

SARNAK ANSWERS: LOOK FIRST AT THE SIGN OF

$$x \longmapsto -\frac{\log x}{\sqrt{x}} \underbrace{\sum_{p \leq x} \frac{a_p(E)}{\sqrt{p}}}_{\Sigma \cos \ldots}$$

SARNAK, FIORILLI HAVE STUDIED THAT QUESTION:

CONDITIONALLY ON RH AND A WEAK FORM OF LI ON $L(E,S)$ (Hasse-Weil) THEY UNCOVER A LINK BETWEEN HIGH BIAS AND HIGH ANALYTIC RANK.

④ VARIANT 3: GEOMETRIC ANALOGUE / UNCONDITIONAL RESULTS

INSTEAD OF DIRICHLET CHARACTERS,

LOOK AT $\chi : (\mathbb{F}_q[t]/(m))^\times \longrightarrow \mathbb{C}^\times$

↑ FIXED $\neq 0$ ELEMENT OF $\mathbb{F}_q[t]$

THE RELEVANT L FUNCTION IS A POLYNOMIAL IN $1 + T\mathbb{Z}[T]$ THANKS TO THE WEIL CONJECTURES.

RH HOLDS THANKS TO WEIL'S THEOREM IN THIS SETTING.

B. Cha: DEVELOPED THIS ANALOGY AND OBTAINED EXACT SAME STATEMENTS AS RUBINSTEIN – SARNAK (UNDER LI)

⑤ VARIANT 3 (CONTINUED):

FUNCTION FIELD ANALOGUE FOR ELLIPTIC CURVES

$E/\mathbb{F}_q(t) : y^2 = x^3 + a(t)x + b(t)$

$a(t), b(t) \in \mathbb{F}_q[t]$

PRIMES $\longleftrightarrow$ PLACES v OF $\mathbb{F}_q(t)$

v IS A PLACE OF GOOD RED, $E_v/\mathbb{F}_v$ IS AN ELLIPTIC CURVE OVER $\mathbb{F}_v := \mathbb{F}_q[t]/(v)$

HASSE: $a_v(E) \leq 2\, q^{\deg v/2}$

WHERE $|E_v(\mathbb{F}_v)| = q^{\deg v} + 1 - a_v(E)$

CHEBYSHEV TYPE QUESTION "SARNAK STYLE"

$$T_E(X) = \frac{-X}{q^{\deg X/2}} \sum_{\substack{V \text{ good} \\ \deg X \le X}} \frac{a_V(E)}{q^{\deg V/2}}$$

SIGN OF T_E?

LOOK AT — PARTICULAR ELL. CURVES
TYPICAL BEHAVIOR

A WAY TO ADDRESS THE SECOND QUESTION:
COMPUTATIONS ON AVERAGE

FAMILY: $f \in \mathbb{F}_q[t] \setminus \{0\}$

$E_f: y^2 = x^3 + a(t) f(t)^2 x + b(t) f(t)^3$

QUAD. TWIST OF E BY f

IT HAS DISC $f^6 \Delta(E)$

INDEX SET THAT WE CHOOSE:

$F \supset \mathbb{F}_q$: $\mathcal{F}_d(\mathbb{F}) = \{f \in \mathbb{F}[t] : \deg f = d, (f, \Delta(E)) = 1$
f sq f$\}$

$d \ge 1$ FIXED

DEFINED AND STUDIED BY KATZ:

REM: $\deg\left(L(E_f \mid \mathbb{F}_{q^n}(t), T)\right) \in \mathbb{Q}[T]$ DEPENDS ON d and q, BUT NOT ON m

$f \in \mathbb{F}_{q^n}[t]$

DEF: $\overline{\delta}(E) = \overline{\lim_{N\to\infty}} \frac{1}{N} \sum_{\substack{x\le N \\ T_E(x)>0}} 1$

THM: (Cha - Fiorilli - J) THERE EXISTS $c>0$ SUCH THAT THE PROPORTION OF $f \in \mathcal{F}_d(\mathbb{F}_{q^n})$ FOR WHICH $\delta(E_f)$ EXISTS AND $|\delta(E_f) - \frac{1}{2}| \le c/\sqrt{d}$

IS AT LEAST $1 - O_{d,E}\left(\frac{n \log q}{q^n c_E d^{-2}}\right)$ WHERE

$c_E > 0$ ONLY DEPENDS ON E

Ulmer: $E_d : y^q + xy = x^3 - t^d \,/\, \mathbb{F}_q(t)$

$q = p^r$, $d \mid p^n + 1$ FOR SOME n