Comparative Prime Number Theory

Greg Martin

Collaborative Research Group (CRG)
“L-functions in Analytic Number Theory”

CRG Launch Event—November 19, 2022

Banff International Research Station
for Mathematical Innovation and Discovery

PIMS UBC University of Lethbridge UNBC

Humans count primes ...

$\pi(x)$ = number of primes up to $x = \sum_{p\le x} 1$

... but nature counts prime powers

$\psi(x) = \sum_{p^k\le x} \log p = \sum_{n\le x} \Lambda(n)$, where

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \text{ for some } k \ge 1, \\ 0, & \text{otherwise.} \end{cases}$$

- $\sum_{n=1}^{\infty} \Lambda(n) n^{-s} = -\frac{\zeta'(s)}{\zeta(s)}$ is a nice meromorphic function

When going from $\psi(x)$ to $\pi(x)$, we:

1. remove the weight $\log p$ (affects things quantitatively)
2. remove the squares, cubes, 4th powers, ... of primes (affects things qualitatively)

Explicit formula

$\psi(x) = x - \sum_\rho \frac{x^\rho}{\rho} + O(\log x)$

- the sum is over nontrivial zeros ρ of $\zeta(s)$

Notation

- Write $\rho = \beta + i\gamma$, so that $x^\rho = x^\beta e^{i\gamma \log x}$
- Define $\Theta \in [\frac{1}{2}, 1]$ to be the supremum of the βs that appear
  - $\psi(x) - x = \Omega_\pm(x^{\Theta-\varepsilon})$ (Landau)

The rightmost zeros matter most

For any $\theta \in [0, \Theta)$,

$$\psi(x) = x - \sum_{\rho\colon\ \theta<\beta\le\Theta} x^\beta \frac{e^{i\gamma \log x}}{\rho} + O(x^\theta \log^2 x)$$

- analysis of main term depends on whether there exist $\beta = \Theta$ and whether there exists $\{\beta_k\} \nearrow \Theta$

Assuming the Riemann hypothesis ($\Theta = \frac{1}{2}$)

$$E^{\psi}(x) = \frac{\psi(x) - x}{\sqrt{x}} = -\sum_{\gamma\colon \zeta(\frac{1}{2}+i\gamma)=0} \frac{e^{i\gamma \log x}}{\frac{1}{2} + i\gamma} + o(1)$$

Random model

Replace $e^{i\gamma \log x}$ by a random variable X_γ that's uniform on S^1, and note that $e^{-i\gamma \log x} = \overline{e^{i\gamma \log x}}$ should force $X_{-\gamma} = \overline{X_\gamma}$:

$$X^{\psi} = \sum_{\gamma\colon \zeta(\frac{1}{2}+i\gamma)=0} \frac{X_\gamma}{|\rho|} = \sum_{\gamma>0} \frac{2\Re X_\gamma}{\sqrt{\frac{1}{4} + \gamma^2}}$$

Random model

$$X^{\psi} = \sum_{\gamma:\, \zeta(\frac{1}{2}+i\gamma)=0} \frac{X_\gamma}{|\rho|} = \sum_{\gamma>0} \frac{2\Re X_\gamma}{\sqrt{\frac{1}{4}+\gamma^2}}$$

- Linear Independence conjecture (LI): $\{\gamma > 0\}$ is linearly independent over $\mathbb{Q}$—corresponds to $\{X_\gamma\}$ being independent random variables
- Under RH and LI, we can write down the Fourier transform of the limiting distribution of $E^{\psi}(x)$ (the characteristic function of X^{ψ}), from which we can extract lots of information
- Via tail estimates, we can give heuristics for the maximal oscillations of E^{ψ} (Montgomery's conjecture):

$$\limsup \frac{\psi(x)-x}{\sqrt{x}(\log\log\log x)^2} = \frac{1}{2\pi}, \quad \liminf = -\frac{1}{2\pi}$$

Back to primes

Passing from $\psi(x)$ to $\pi(x)$ requires (a) partial summation; (b) removing squares of primes, cubes of primes, etc.

$$E^\pi(x) = \frac{\pi(x) - \mathrm{li}(x)}{\sqrt{x}/\log x} = -1 - \sum_{\gamma\colon \zeta(\frac12+i\gamma)=0} \frac{e^{i\gamma\log x}}{\frac12+\gamma} + o(1)$$

- Littlewood: the sum is $\Omega_\pm(\log\log\log x)$
  - used Diophantine approximation to find x such that lots of the $e^{i\gamma\log x}$ point in the same direction
- therefore $\pi(x) > \mathrm{li}(x)$ infinitely often (contrary to conjecture)

Rubinstein and Sarnak

The probability that $X^\pi = -1 + X^\psi$ is negative is ≈ 0.99999974. So assuming RH and LI, the set $\{x > 0\colon \pi(x) > \mathrm{li}(x)\}$ has logarithmic density ≈ 0.00000026.

Conjectures made from early numerical data

- Mertens conjecture: if $M(x) = \sum_{n \le x} \mu(n)$, then $|M(x)| \le \sqrt{x}$
- Pólya's problem: if $L(x) = \sum_{n \le x} (-1)^{\Omega(n)}$, is $L(x) \le 0$?
- Turán's problem: if $L_r(x) = \sum_{n \le x} \frac{(-1)^{\Omega(n)}}{n}$, is $L_r(x) \ge 0$?
  - If true, each of these would imply RH (and all zeros simple), but also that LI has infinitely many violations (Ingham)
  - All now known to be false (Haselgrove; Odlyzko/te Riele)
  - $M(x) \ll \sqrt{x}$ is still unresolved, but probably false

Dirichlet series

- $\sum_{n=1}^{\infty} \mu(n) n^{-s} = \frac{1}{\zeta(s)}$
- $\sum_{n=1}^{\infty} (-1)^{\Omega(n)} n^{-s} = \frac{\zeta(2s)}{\zeta(s)}$
- $\sum_{n=1}^{\infty} \frac{(-1)^{\Omega(n)}}{n} n^{-s} = \frac{\zeta(2s+2)}{\zeta(s+1)}$

Explicit formulas

- $M(x) = \sum_{\rho} \frac{x^{\rho}}{\rho \zeta'(\rho)}$
- $L(x) = \frac{x^{1/2}}{\frac{1}{2}\zeta(\frac{1}{2})} + \sum_{\rho} \frac{\zeta(2\rho) x^{\rho}}{\rho \zeta'(\rho)}$
- $L_r(x) = \frac{x^{-1/2}}{-\frac{1}{2}\zeta(\frac{1}{2})} + \sum_{\rho} \frac{\zeta(2\rho) x^{\rho-1}}{(\rho-1)\zeta'(\rho)}$

Explicit formulas

- $M(x) = \sum_{n \le x} \mu(n) = \sum_{\rho} \frac{x^\rho}{\rho \zeta'(\rho)}$
- $L(x) = \sum_{n \le x} (-1)^{\Omega(n)} = \frac{x^{1/2}}{\frac{1}{2}\zeta(\frac{1}{2})} + \sum_{\rho} \frac{\zeta(2\rho) x^\rho}{\rho \zeta'(\rho)}$
- $L_r(x) = \sum_{n \le x} \frac{(-1)^{\Omega(n)}}{n} = \frac{x^{-1/2}}{-\frac{1}{2}\zeta(\frac{1}{2})} + \sum_{\rho} \frac{\zeta(2\rho) x^{\rho-1}}{(\rho - 1)\zeta'(\rho)}$

- Results on the distribution of these sums often require RH and LI and some information/conjecture on $\sum_{\rho} \frac{1}{|\zeta'(\rho)|}$
- Mossinghoff and Trudgian have studied the interpolating sums $\sum_{n \le x} \frac{(-1)^{\Omega(n)}}{n^\alpha}$ for $0 \le \alpha \le 1$

Chebyshev observed that there seem to be more primes that are $3 \pmod 4$ than primes that are $1 \pmod 4$.

Other arithmetic progressions where we see advantages

- Primes that are $2 \pmod 3$ over primes that are $1 \pmod 3$
- Primes that are $3, 5,$ or $6 \pmod 7$ over primes that are $1, 2,$ or $4 \pmod 7$
- Primes that are $3, 5,$ or $7 \pmod 8$ over primes that are $1 \pmod 8$
- Primes that are 3 or $7 \pmod{10}$ over primes that are 1 or $9 \pmod{10}$
- Primes that are $5, 7,$ or $11 \pmod{12}$ over primes that are $1 \pmod{12}$

$\cdots$ in general, nonsquares $\pmod q$ over squares $\pmod q$

Primes in arithmetic progressions

$$\pi(x;q,a) = \text{\# of primes up to } x \text{ that are congruent to } a \pmod q$$
$$= \sum_{\substack{p\le x \\ p\equiv a \pmod q}} 1$$
$$\psi(x;q,a) = \sum_{\substack{n\le x \\ n\equiv a \pmod q}} \Lambda(n) = \sum_{\substack{p^k\le x \\ p^k\equiv a \pmod q}} \log p$$

Now when going from $\psi(x;q,a)$ to $\pi(x;q,a)$, we remove squares of primes in the residue classes whose square is $a \pmod q$.

Definition (when $(a,q)=1$)

$$c(q;a) = -1 + \#\{b \pmod q : b^2 \equiv a \pmod q\}$$

- given q, the only possible values for $c(q;a)$ are -1 or $c(q;1)$

Explicit formula for PNT in APs

$$\psi(x;q,a) = \frac{x}{\phi(q)} - \frac{1}{\phi(q)} \sum_{\chi \text{ (mod } q)} \overline{\chi}(a) \sum_{\rho:\ L(\rho,\chi)=0} \frac{x^\rho}{\rho}$$

Differences of two such counting functions:

$$E^\psi(x;q,a,b) = \phi(q)\big(\psi(x;q,a) - \psi(x;q,b)\big)$$
$$= \sum_{\chi \text{ (mod } q)} \big(\overline{\chi}(b) - \overline{\chi}(a)\big) \sum_{\rho:\ L(\rho,\chi)=0} \frac{x^\rho}{\rho}$$

Random variable models

$$X^\psi(q;a,b) = \sum_{\chi \text{ (mod } q)} \big|\chi(b) - \chi(a)\big| \sum_{\rho:\ L(\rho,\chi)=0} \frac{2\Re X_\gamma}{\sqrt{\frac14 + \gamma^2}}$$

- for $X^\pi(q;a,b)$: add $c(q;b) - c(q;a)$ to the right-hand side

Logarithmic densities

$$\delta^\pi(q;a,b) = \lim_{x\to\infty} \int_{\substack{1\le t\le x \\ \pi(x;q,a)>\pi(x;q,b)}} \frac{dt}{t}$$

Rubinstein/Sarnak

Assuming GRH and LI:

- each $\delta^\pi(q;a,b)$ exists and $0 < \delta^\pi(q;a,b) < 1$
- $\delta^\pi(q;a,b) + \delta^\pi(q;b,a) = 1$ ("ties have density 0")
- $\delta^\pi(q;a,b) > \frac{1}{2}$ if and only if a is a nonsquare and b is a square (mod q)
- $X^\pi(q;a,b)$ tends to a standard normal random variable as $q \to \infty$; in particular, $\lim_{q\to\infty} \delta^\pi(q;a,b) = \frac{1}{2}$

Logarithmic densities

$$\delta^\pi(q;a,b) = \lim_{x\to\infty} \int_{\substack{1\le t\le x \\ \pi(x;q,a)>\pi(x;q,b)}} \frac{dt}{t}$$

Fiorilli/M.

Assuming GRH and LI:

- if a is a nonsquare and b is a square (mod q), then
  $\delta^\pi(q;a,b) - \frac{1}{2} \sim \frac{c(q;1)}{2\sqrt{\pi\phi(q)\log q}}$
- calculated all 117 densities greater than 0.9
  - most biased: $\delta^\pi(24;5,1) \approx 0.999988$
  - 117 is up to symmetries such as $\delta^\pi(q;a,b) = \delta^\pi(q;c^2a,c^2b)$
- secondary terms show that when q is large, $\delta^\pi(q;-1,1)$ is the smallest density exceeding $\frac{1}{2}$, followed by $\delta^\pi(q;3,1)$, $\delta^\pi(q;2,1)$, $\delta^\pi(q;5,1)$, …
  - assuming that $-1/3/2/5$ are nonsquares (mod q)

Multi-way races

$\delta^\pi(q; a_1, \dots, a_k)$ is the logarithmic density of the set

$$\{x > 0 \colon \pi(x; q, a_1) > \pi(x; q, a_2) > \cdots > \pi(x; q, a_k)\}$$

- $k!$ possible orderings, so compare $\delta^\pi(q; a_1, \dots, a_k)$ to $\frac{1}{k!}$

Assuming GRH and LI

- Rubinstein/Sarnak: $0 < \delta^\pi(q; a_1, \dots, a_k) < 1$ exists
- Feuerverger/M.: confirmed that $\delta^\pi(q; a, b, c)$ can differ from $\frac{1}{6}$ even when a, b, c are all nonsquares (mod q)
- Lamzouri: asymptotics for $\delta^\pi(q; a_1, \dots, a_k) - \frac{1}{k!}$ for k fixed; the difference can be as large as $\frac{1}{\log q}$
  - Harper/Lamzouri: $\delta^\pi(q; a_1, \dots, a_k) \sim \frac{1}{k!}$ still for $k < (\log q)^{1-\varepsilon}$
- Ford/Harper/Lamzouri: $k!\delta^\pi(q; a_1, \dots, a_k)$ can tend to 0 or to ∞ for $k > (\log q)^{1+\varepsilon}$

Levels of expectations for prime number races

For every permutation $(\sigma_1, \dots, \sigma_k)$ of $(a_1, \dots, a_k)$, the prime number races among the $\pi(x; q, a_j)$ is:

- exhaustive if each $\pi(x; q, \sigma_1) > \cdots > \pi(x; q, \sigma_k)$ has solutions for arbitrarily large x
- weakly inclusive if each $\delta^\pi(q; \sigma_1, \dots, \sigma_k)$ exists
- inclusive if each $\delta^\pi(q; \sigma_1, \dots, \sigma_k)$ is strictly positive
- strongly inclusive if the limiting distribution of $\big(E^\pi(x; q, a_1), \dots, E^\pi(x; q, a_k)\big)$ has full support in $\mathbb{R}^k$

Rubinstein/Sarnak: GRH and LI imply that all prime number races are strongly inclusive. Can we weaken LI?

Definition

if $L(\frac12 + i\gamma_0, \chi) = 0$, then γ_0 is a self-sufficient ordinate if it is not in the $\mathbb{Q}$-span of $\{\gamma > 0,\ \gamma \ne \gamma_0 \colon L(\frac12 + i\gamma, \chi = 0)\}$.

M./Ng

Under GRH, for any prime number races (mod q):

- if each $L(s,\chi)$ (mod q) has 3 self-sufficient ordinates, then weakly inclusive ($\delta^\pi(q;\sigma_1,\dots,\sigma_k)$ exists)
- if $\sum_{\chi \text{ (mod } q)} \sum 1/\gamma$ over self-sufficient zeros diverges, then strongly inclusive (consistent with 100% violations of LI)

Devin

- extended these results to the Selberg class of L-functions
- even without RH, limiting logarithmic distribution exists when normalized by x^Θ (possibly a delta measure at 0)
- with RH: if 1 self-sufficient ordinate exists, this distribution is absolutely continuous (with respect to Lebesgue measure), and the corresponding density exists

ABCPNT

Ideal goal: a comprehensive Annotated Bibliography of all papers (and book chapters, letters, etc.) of Comparative Prime Number Theory, using modern and consistent notation

- it's nontrivial even to define exactly what CPNT is and isn't

Current status

- ABCPNT currently has just over 300 items (missing some from the last 2 years)
  - summaries complete for 75% of them (could use double-checking, especially non-English papers)
  - students' draft summaries exist for the other 25%
- introduction/notational conventions also about 75% written

COVID really derailed my editorial efforts. Help welcome!

Haselgrove's condition

Assuming $L(\sigma,\chi) \ne 0$ for all real $0 < \sigma < 1$ and all χ (mod q):

- Kátai: $\pi(x;q,a) > \pi(x;q,b)$ infinitely often if a and b are both squares or both nonsquares (mod q)
- Knapowski and Turán: $\pi(x;q,a) > \pi(x;q,1)$ and $\pi(x;q,1) > \pi(x;q,a)$ infinitely often
- Almost-periodicity of normalized explicit formula: if $\pi(x;q,a) > \pi(x;q,b)$ once then $\pi(x;q,a) > \pi(x;q,b)$ infinitely often

Sneed used these results and computations to show that every two-way prime number race modulo $q \le 100$ is exhaustive

Can we get other unconditional results?

For example, can we prove unconditionally that $\pi(x;q,a) = \pi(x;q,b)$ occurs only for x in a set of density 0?

Frequency of sign changes

Let $W^\psi(T)$ denote the number of sign changes of $\psi(x) - x$ for $x \in [0, T]$.

Almost state of the art

- Pólya proved that $W^\psi(T) \geq (1 + o(1))\frac{\gamma_1}{\pi}\log T$, where $\gamma_1 \approx 14.135$ is the smallest positive ordinate of a zero of $\zeta(s)$. General method:
  - Since $\psi(x) - x = -\sum_\rho \frac{x^\rho}{\rho}$, averaging both sides yields $\frac{1}{x}\int_0^x (\psi(t) - t)\,dt = -\sum_\rho \frac{x^\rho}{\rho(\rho+1)}$.
  - Repeated averaging yields $-\sum_\rho \frac{x^\rho}{\rho(\rho+1)^K}$.
  - When K is large enough, the sign of the extreme values of the first term dominates the sum of the rest.
  - And sign changes of the iterated average implies sign changes of the original $\psi(x) - x$.
- Indeed, $\psi(x) - x$ has a sign change in any interval of the form $(T, e^{(1+o(1))\gamma_1/\pi}T) \approx (T, 90T)$

- Pólya proved that $W^\psi(T) \ge (1+o(1))\frac{\gamma_1}{\pi}\log T$, where $\gamma_1 \approx 14.135$ has $\zeta(\frac12 + i\gamma_1) = 0$
- Kaczorowski improved this to $W^\psi(T) \ge (1+o(1))(\frac{\gamma_1}{\pi} + 10^{-250})\log T$
- Kaczorowski also proved $W^\pi(T) \gg \log T$, though ineffectively

Sad news

The truth should be closer to $W^\psi(T) \approx \sqrt{T}$ (up to log factors)!

- The large-scale behaviour of $\psi(x) - x$ does somewhat resemble the behaviour of the first term in the explicit formula, being positive/negative on large intervals.
- However, when $\psi(x) - x$ does change sign, it tends to have lots of nearby sign changes. (both emperical observation and analogy with random walks)
- Averaging is completely blind to these local sign changes

Function field analogues

Cha, Fiorilli, Jouve, Lamzouri, Sedrati, …

- Instead of counting prime integers in residue classes modulo a fixed integer, count irreducible polynomials over $\mathbb{F}_q$ in residue classes modulo a fixed polynomial
- For the corresponding zeta function ζ_C, RH is known (Weil)
- Only finitely many zeros, so distribution exists unconditionally. However, linear independence of arguments still relevant for specifics
  - “arguments” because ζ_C is a rational function of q^{-s}, so if $s = \frac{1}{2} + i\gamma$, we really care about γ modulo $\frac{2\pi}{\log q}$
- LI is known to fail sometimes when $q^{-s} = q^{-1/2}$ or $q^{-s} = iq^{-1/2}$, sometimes with two different zeros

Can we describe systematic ways to find violations of LI over function fields?

The Linear Independence hypothesis

What partial progress can we make towards proving LI for $\zeta(s)$?

- Li/Radziwiłł: a positive proportion of points $\frac{1}{2} + i(\alpha k + \beta)$ in a vertical arithmetic progression are not zeros of $\zeta(s)$
- unpublished work of Banks/M./Milinovich/Ng: as $\frac{1}{2} + i\gamma$ runs over zeros of $\zeta(s)$, lots of $\frac{1}{2} + 2i\gamma$ are not zeros of $\zeta(s)$ (and some generalizations)
- "Silberman's problem": Prove that at least one ordinate of a zero of $\zeta(s)$ is irrational!

Related:

- Is there a theoretical way to prove LI for families of $\zeta_C(s)$ (zeta functions of curves over finite fields)?

Quantitative LI: If k_γ are integers, not all 0, with $\sum |k_\gamma| \le K$, then

$$\Bigl|\sum_{0<\gamma\le T} k_\gamma \gamma\Bigr| \gg_{\varepsilon,K} \exp(-T^{1-\varepsilon})$$

We think this conjecture should be better known. It could lead to conditional proofs of some heuristics like:

- Montgomery's conjecture

$$\limsup \frac{\psi(x)-x}{\sqrt{x}(\log\log\log x)^2} = \frac{1}{2\pi}, \quad \liminf = -\frac{1}{2\pi}$$

- Gonek's conjecture: there exists $B > 0$ such that

$$\limsup \frac{M(x)}{\sqrt{x}(\log\log\log x)^{5/4}} = B, \quad \liminf = -B$$

  - compare $\sum_{0<\gamma<T} \frac{1}{|\rho|} \asymp (\log T)^2$ to the conjectured $\sum_{0<\gamma<T} \frac{1}{|\rho\zeta'(\rho)|} \asymp (\log T)^{5/4}$

Three races with the same density

Each of the following sets has (on RH and LI) the same logarithmic density ≈ 0.99999974:

- $\{x > 0 \colon \pi(x) < \mathrm{li}(x)\}$
- $\{x > 0 \colon \theta(x) < x\}$, where $\theta(x) = \sum_{p \le x} \log p$
- "Mertens product race" $\{x > 0 \colon \prod_{p \le x} (1 - \frac{1}{p})^{-1} > e^{C_0} \log x\}$, where C_0 is Euler's constant (Lamzouri)

The first two sets should be identical up to a set of density 0. Can we show that the same is not true of the third set?

Other correlations between similar error terms

Pólya and Turán and between: each function $\sum_{n \le x} \frac{(-1)^{\Omega(n)}}{n^\alpha}$ for $0 \le \alpha \le 1$ has a corresponding set where it exceeds its main term. How are these sets correlated?

Ten-way race modulo 11 (Bays/Hudson)

If we look at how the ordering of $\pi(x;11,1),\dots,\pi(x;11,10)$ evolves as x increases:

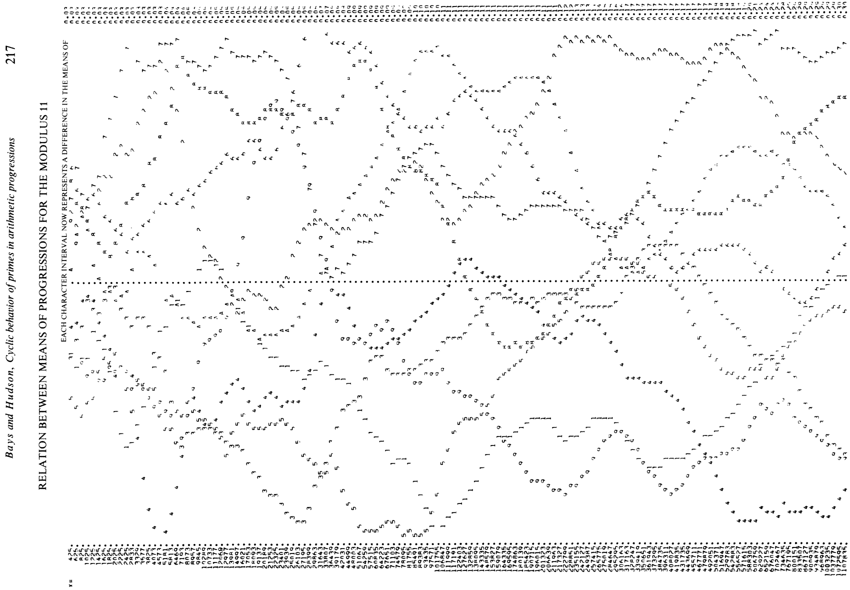
- The smallest function, with minor deviations, cycles in order through $9,4,5,3,1 \equiv 9^1,9^2,9^3,9^4,9^5 \pmod{11}$
- The largest function, with minor deviations, cycles in order through $2,7,6,8,10 \equiv -9^1,-9^2,-9^3,-9^4,-9^5 \pmod{11}$
- When 9^k is in last place, -9^k tends to be in first place

What can we say about the correlations of the various sets implied by these observations?

Public service announcement

Andrey S. Shchebetov has coded a "Chebyshev's Bias Visualizer" that flexibly plots error terms for primes in APs

- you can click on that red link


Bays and Hudson, Cyclic behavior of primes in arithmetic progressions
217
RELATION BETWEEN MEANS OF PROGRESSIONS FOR THE MODULUS 11
EACH CHARACTER INTERVAL NOW REPRESENTS A DIFFERENCE IN THE MEANS OF