Isaac Newton Institute for Mathematical Sciences
RMAw02 - Recent Perspectives in Random Matrix Theory and Number Theory

Prime number theory & the Riemann zeta-function I

R. Heath-Brown (Oxford)

29 March 2004

Isaac Newton Institute for Mathematical Sciences
20 Clarkson Road, Cambridge CB3 0EH, UK

Tel: +44 1223 335999 Fax: +44 1223 330508
E-mail: webseminars@newton.cam.ac.uk
http://www.newton.cam.ac.uk/webseminars

Prime Number Theory and the Riemann Zeta-Function

Roger Heath-Brown

Oxford

Lecture 1

- The lecture notes

  lots of misprints
  (> 1 per page on average)
  Report errors etc to me

  2nd part yet to come

- The lectures

  Interupt – PLEASE

Primes

$p \in \mathbb{N}$ is "prime" iff $p \neq 1$ and $\nexists\, n \in \mathbb{N}$, $n | p$, $1 < n < p$.

Multiplicative building blocks

The Fundamental Theorem of Arithmetic

Every $n \in \mathbb{N}$ can be written $\sim$ exactly one

4

way as

$$n \quad p \quad p_2^{e_2} \quad p_k^{e_k}$$

with $k \geq 0$, $e_1, e_2, \ , e_k \geq 1$

and $p_1 < p_2 < \ < p_k$ prime.

Proof Hardy & Wright

Contrast

$$\{ m + n\sqrt{-5} \quad m, n \in \mathbb{Z} \}$$

$$6 = 2 \times 3 = (1 - \sqrt{-5}) \times (1 + \sqrt{-5})$$

all "primes"

Theorem (Euclid)

There are infinitely many primes

Proof: Suppose $p_1, \dots, p_n$ were all the primes

$$N = p_1 \cdots p_2 + 1$$

$N \geq 2 \quad \therefore \quad \exists\, p \mid N$

$p = p_j$ say $\therefore\ p \mid N-1$

$\therefore\ p \mid 1 = N - (N-1)$

19th Tables by hand to 10^8 Very erratic distribution, some large gaps, some small

$\pi(x)$ $\#\{p \leq x \;\; p \text{ prime}\}$

Gauss

$$\pi(x) \sim L(x) \;?$$

$$L(x) - \int_2^x \frac{dt}{\log t}$$

$$\frac{\pi(x)}{L_i(x)} \to 1 \text{ as } x \to \infty$$

$$\pi(10^8) = 5,776,455$$

$$\pi(10^{12}) = 37,607,92,018$$

$$\pi(10^{16}) = 279,238,341,033,925$$

$$\frac{\pi(x)}{Li(x)} = 0.999869147\ldots,$$

$$= 0.999989825\ldots,$$

$$= 0.99999989$$

$Li(x) \sim \frac{x}{\log x}$, but $Li(x)$

is better.

The Prime Number Theorem

(Hadamard, de la Vallée Poussin, independently, 1896)

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as } x \to \infty$$

Interpretation

1) for $n \approx x$, the "probability" that n is prime, is $\sim 1/\log x$

2) Prob(n prime) $\sim 1/\log n$

Deterministic

$$\text{Prob}(n \text{ prime}) = \begin{cases} 1, & n \text{ prime}, \\ 0, & \text{not}. \end{cases}$$

Useful none the less!

Prob($n+1, n+2, \ldots, n+k$ all composite) ?

k events, each probability $\left(1 - \frac{1}{\log n}\right)$. Independent?

<u>No</u>. But if they were...

$$\left(1 - \frac{1}{\log n}\right)^k.$$

$$k = \mu (\log n)^2$$

$$\left(1-\frac{1}{\log n}\right)^{\log n} \doteq e^{-1}$$

$\therefore$ Prob(all composite) $\approx n^{-\mu}$.

$E_n :=$ $n+1, n+2, \ldots, n+k$ all composite

Independent? No!

But if they were...

Borel-Cantelli lemma

Predict E_n occurs finitely often iff $\sum_{n=1}^{\infty} n^{-\mu} < \infty$

Expect E_m and E_n to be independent if $|m-n|>k$. !!

Conjecture: If p' is the prime after p, then

$$\limsup_{p\to\infty} \frac{p'-p}{(\log p)^2} = 1$$

—

P.N.T. Average size of $p'-p$ is $\sim \log p$

—

Prob (n, $n+1$ both prime)

$$\sim \frac{1}{(\log n)^2} \quad ??$$

One of $n, n+1$ is even composte

Conjecture

If $c \quad 2 \prod_{p>2} \left(1 \quad \frac{1}{(p \quad)^2}\right)$

1.3202

Then

$\# \{ n < x \quad n, n+2$ both prime $\}$

$$= c \int_2^x \frac{dt}{(\log t)^2}$$

Cramérs Model

$H \leq N$

$$\#\{p : N < p \leq N+H\}$$

$$= \pi(N+H) - \pi(N).$$

$$\doteqdot \int_N^{N+H} \frac{dt}{\log t} \sim \frac{H}{\log N}.$$

Beware!

$$\pi(x) = \int_2^x \frac{dt}{\log t} + f(x),$$

$$\frac{f(x)}{/\log x} \rightarrow 0$$

$$\pi(N+H) - \pi(N) = \int_N^{N+H} \frac{dt}{\log t}$$

$$+ f(N+H) - f(N)$$

$$? \quad \frac{f(N+H) - f(N)}{H / \log N} \to 0 \; ?$$

Only OK if $cN \leq H \leq N$

$c > 0$ constant.

However (Hoheisel, ..., H-B)

$$\pi(N+H) - \pi(N) \sim \frac{H}{\log N}$$

for $N^{7/12} \leq H \leq N$.

Smaller H?

What does Cramér suggest?

"Conjecture 3" Let $k > 2$ be constant Then f $H = (\log N)^k$ we should have

$$\pi(N+H) \;\; \pi(N) \sim \frac{H}{\log N}$$

as $N \to \infty$

Theorem (Selberg, 1943)
Assume the Riemann Hypothesis. Let $f(n) \nearrow \infty$ as $n \to \infty$. Then $\exists\ \mathcal{E} \subset \mathbb{N}$ s.t. $\#\{n \in \mathcal{E} : n \leq N\} = o(N)$ as $N \to \infty$, such that

$$\pi(n+h) - \pi(n) \sim \frac{h}{\log n}$$

with $h = f(n)\log^2 n$, $\forall\ n \notin \mathcal{E}$.

"Conjecture 3". Can take $\mathcal{E} = \emptyset$ if $f(n) = (\log n)^\delta$

Cramér $\Rightarrow$ "Conjecture 3"

Selberg's theorem supports "Conjecture 3"

But Maier (1985) disproved "Conjecture 3"!

Theorem (Maier, 1985)

For any $\kappa > 0$, $\exists\ \delta_\kappa > 0$ s.t.

$$\limsup_{n \to \infty} \frac{\pi(n + (\log n)^\kappa) - \pi(n)}{(\log n)^{\kappa - 1}} \geqslant 1 + \delta_\kappa$$

and

$$\liminf_{n\to\infty} \frac{\pi(n+(\log n)^{k}) - \pi(n)}{(\log n)^{k-1}} \leq 1-\delta_k$$

A shock! It isn't just that the limiting value "$\ldots > 2$" predicted by Cramér is wrong. <u>No</u> value of k works!

The exceptional n are very rare

Cramér's Model breaks down: arithmetic effects are more important than previously expected

—

A good alternative to Cramér's Model?