Lecture 1: Small Prime Gaps: From the Riemann Zeta-Function and Pair Correlation to the Circle Method

Daniel Goldston

$\pi(x)$: The number of primes $\le x$.

The prime number theorem:

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

The average distance between two consecutive primes in $[0, x]$:

$$\text{Average gap} \sim \frac{\text{length of } [0, x]}{\frac{x}{\log x}} \sim \log x.$$

Our goal in these talks: Study the distribution of primes around this average, especially small gaps.

What is the smallest gap that occurs infinitely often?

The Twin Prime Conjecture:

$$p_{n+1} - p_n = 2 \quad \text{infinitely often},$$

We now can prove this (small) step towards TPC:

Theorem 1 *(Goldston, Pintz, Yildirim 2005) We have*

$$\liminf_{n\to\infty} \left(\frac{p_{n+1} - p_n}{\log p_n} \right) = 0.$$

How do we answer questions about primes, and gaps between primes?

We often use Multiplicative Number Theory. (Rule 1 of MNT: $s = \sigma + it$)

The Riemann zeta-function $\zeta(s)$ is defined, for $\sigma > 1$, by the Dirichlet series or Euler product

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right)$$
$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

To extract the primes, use the power series for $-\log(1-z)$, to obtain, for $\sigma > 1$,

$$\begin{aligned}\frac{\zeta'}{\zeta}(s) := \frac{\zeta'(s)}{\zeta(s)} &= \frac{d}{ds} \log \zeta(s) \\ &= \frac{d}{ds}\Big(\sum_{m=1}^{\infty} \sum_p \frac{1}{mp^{ms}}\Big) \\ &= -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},\end{aligned}$$

where the von Mangoldt function $\Lambda(n)$ is

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^m,\ p \text{ prime},\ m \geq 1, \\ 0, & \text{otherwise.} \end{cases}$$

The Prime Number Theorem (PNT):

$$\psi(x) := \sum_{n \leq x} \Lambda(n), \quad \psi(x) \sim x, \quad \text{as } x \to \infty$$

The PNT with the error term obtained by de la Vallée Poussin(1899): for c a small constant,

$$\psi(x) = x + O\left(xe^{-c\sqrt{\log x}}\right),$$

which on returning to $\pi(x)$ gives (c may differ)

$$\pi(x) = \mathrm{li}(x) + O\left(xe^{-c\sqrt{\log x}}\right),$$

where

$$\mathrm{li}(x) = \int_2^x \frac{du}{\log u}.$$

Often we use: for any constant $A > 0$

$$e^{-c\sqrt{\log x}} \ll \frac{1}{(\log x)^A}.$$

Proof of PNT with error:

1. Truncate the Dirichlet series for $\frac{\zeta'}{\zeta}(s)$ using

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{s}\,ds = \begin{cases} 0, & \text{if } 0 < x < 1, \\ \frac{1}{2}, & \text{if } x = 1, \\ 1, & \text{if } x > 1. \end{cases}$$

Thus

$$\begin{aligned} \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \left(-\frac{\zeta'}{\zeta}(s)\right)\frac{x^s}{s}\,ds &= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\right) \frac{x^s}{s}\,ds \\ &= \sum_{n=1}^{\infty} \Lambda(n) \left(\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{(x/n)^s}{s}\,ds\right) \\ &= {\sum_{n\le x}}' \Lambda(n) = \psi_0(x) \end{aligned}$$

where $\psi_0(x)$ differs from $\psi(x)$ only by the term $n = x$ being weighted by $1/2$.

Hence

$$\psi_0(x) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \left(-\frac{\zeta'}{\zeta}(s)\right) \frac{x^s}{s}\,ds.$$

2. Use the analytic facts that $\zeta(s)$ has:

i) a simple pole with residue 1 at $s = 1$, and is analytic elsewhere

ii) no zeros to right of $\mathcal{L}$ given by

$$\sigma = 1 - \frac{c}{\log(|t| + 2)}$$

iii) $\frac{\zeta'}{\zeta}(s) \ll (\log|t|)^2$ in this region if $|t| \geq 2$.

3. Move the contour to the left to $\mathcal{L}$.

This procedure is the same that we apply in our recent work on gaps.

Riemann von Mangoldt Explicit Formula

As well as at $s = 1$, $\frac{\zeta'}{\zeta}(s)$ has poles at the zeros of $\zeta(s)$.

These occur at:

i) $s = -2n$, $n = 1, 2, 3, \ldots$, (the trivial zeros)

ii) $\rho = \beta + i\gamma$, $0 < \beta < 1$, (the complex zeros)

(ρ, $\bar{\rho}$, $1 - \rho$, and $1 - \bar{\rho}$ are all zeros)

The Riemann Hypothesis (RH): $\beta = \frac{1}{2}$
(The \$1,000,000 Question)

We count complex zeros up to height T with

$$N(T) = \sum_{0<\gamma\le T}{}' 1,$$

where zeros with $\gamma = T$ have weight 1/2.

Riemann von Mangoldt formula for $N(T)$:

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + R(T) + S(T),$$

where $R(T) \ll 1/T$, and $S(T) \ll \log T$.

Thus

$$N(T+1) - N(T) = \sum_{T<\gamma\le T+1} 1 \ll \log T.$$

In the formula for $\psi_0(x)$, move the contour to the left all the way to $-\infty$, and obtain for $x > 1$,

$$\psi_0(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \log 2\pi - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right),$$

(The terms are added with ρ and $\bar{\rho}$ grouped together.) For applications we often use:

$$\psi(x) = x - \sum_{|\gamma| \le T} \frac{x^\rho}{\rho} + O\left(\frac{x}{T}(\log xT)^2\right) + O(\log x).$$

Assuming RH:

$$\frac{x^\rho}{\rho} \ll \frac{x^{\frac{1}{2}}}{|\gamma|},$$

Thus in above take $T = x$ to obtain (von Koch 1901)

$$\psi(x) = x + O\left(x^{\frac{1}{2}}(\log x)^2\right).$$

This also implies RH, and therefore is equivalent to the RH.

Actually even $\pi(x) = \mathrm{li}(x) + O\left(x^{\frac{1}{2}+\epsilon}\right)$ for any $\epsilon > 0$ is equivalent to RH.

Now consider gaps between primes on RH. Removing prime powers,

$$\psi(x) = \sum_{p \le x} \log p + O\left(x^{\frac{1}{2}}\right).$$

Differencing:

$$\sum_{x < p \le x+h} \log p = h + O\left(x^{\frac{1}{2}} (\log x)^2\right).$$

Taking $h = Cx^{\frac{1}{2}}(\log x)^2$, with large constant C, the sum is positive:

$(x, x+h]$ contains $\gg \frac{h}{\log x}$ primes and

$$p_{n+1} - p_n < h \ll p_n^{\frac{1}{2}} (\log p_n)^2.$$

Selberg improving Cramér a little, proved on RH

$$\frac{1}{X}\int_X^{2X} (\psi(x+h)-\psi(x)-h)^2\, dx \ll h(\log X)^2$$

To go further, we need: **Pair Correlation Conjecture** For any fixed $\beta > 0$,

$$\frac{1}{N(T)} \sum_{\substack{0<\gamma,\gamma'\le T \\ 0<\gamma'-\gamma\le \frac{2\pi\beta}{\log T}}} 1 \sim \int_0^\beta 1 - \left(\frac{\sin \pi u}{\pi u}\right)^2\, du.$$

Actually we need a stronger version of this (or Montgomery's $F(\alpha)$ conjecture) By work of Gallagher and Mueller(1976), Heath-Brown(1982), Goldston-Montgomery(1986):

On RH, (Strong)PC is equivalent to

$$\frac{1}{X}\int_X^{2X}(\psi(x+h)-\psi(x)-h)^2\, dx \sim h \log \frac{X}{h}$$

for $1 \le h \le X^{1-\epsilon}$

In particular, with $h = \lambda \log x$, we have

$$\frac{1}{X}\int_X^{2X} (\pi(x+\lambda\log x) - \pi(x))^2 \, dx \sim (\lambda+\lambda^2)X$$

This is the second moment for a Poisson distribution!

Theorem 2 *Assuming RH and Strong PC We have*

$$\liminf_{n\to\infty} \left(\frac{p_{n+1}-p_n}{\log p_n}\right) = 0.$$

Proof If not, for small enough λ, $(x, x+\lambda\log x]$ contains only zero or one prime. Thus

$$(\pi(x+\lambda\log x)-\pi(x))^2 = (\pi(x+\lambda\log x)-\pi(x))^1$$

Thus variance = expected value $\sim \lambda$, contradicting above.

Next step: Prove RH and PC.

Basic Problem: Deeper properties of $\zeta(s)$ are proved using number theory, often prime number theory.

Alternative: Additive Number Theory

Theorem 3 *(Bombieri-Davenport 1965) We have*

$$\liminf_{n\to\infty}\left(\frac{p_{n+1}-p_n}{\log p_n}\right)\leq\frac{1}{2}.$$

In fact, their method proves

$$\frac{1}{X}\int_X^{2X}(\pi(x+\lambda\log x)-\pi(x))^2\,dx>((\frac{1}{2}-\epsilon)\lambda+\lambda^2)X$$

This uses the circle method.

Question Where does the circle method gather its information about primes?

The Circle Method - a Wooley Intro

The twin prime conjecture: Solve

$$x_1 - x_2 = 2, \quad x_1, x_2 \in P = \{\text{primes}\}$$

Circle Method: For k an integer,

$$e(u) := e^{2\pi i u}, \quad \int_0^1 e(k\alpha)\, d\alpha = \begin{cases} 1, & \text{if } k = 0, \\ 0, & k \neq 0. \end{cases}$$

Thus the number of twin primes in $[1, N]$ is

$$\int_0^1 \sum_{x_1, x_2 \in P \cap [1,N]} e((x_1 - x_2 - 2)\alpha))\, d\alpha$$
$$= \int_0^1 \left| \sum_{\substack{1 \le x \le N \\ x \in P}} e(x\alpha) \right|^2 e(-2\alpha)\, d\alpha$$

Now analyze the generating function, major, minor arcs, . . .

Let

$$S(\alpha) = \sum_{n \le N} \Lambda(n)\, e(n\alpha), \qquad e(u) = e^{2\pi i u}.$$

Now

$$\begin{aligned} |S(\alpha)| \le S(0) &= \sum_{n \le N} \Lambda(n) \\ &= \psi(N) \sim N. \end{aligned}$$

Next, if α is small, by partial summation,

$$\begin{aligned} S(\alpha) &= \int_1^N e(\alpha u) d\psi(u) \\ &= \int_1^N e(\alpha u) du + \int_1^N e(\alpha u) dR(u) \\ &= \sum_{n \le N} e(\alpha n) + \text{error} := I(\alpha) + \text{error}, \end{aligned}$$

where $R(u) = \psi(u) - u$. Thus $S(\alpha)$ has a spike shaped like $I(\alpha)$ for small α.

Hardy-Littlewood: At fraction $\frac{a}{q}$, $(a,q)=1$,

$$S(\frac{a}{q}+\beta) = \sum_{n\leq N} \Lambda(n)e(n\frac{a}{q})e(n\beta)$$
$$= \sum_{1\leq m\leq q} e(\frac{ma}{q}) \sum_{\substack{1\leq n\leq N\\ n\equiv m (\mathrm{mod}\, q)}} \Lambda(n)e(n\beta).$$

If $\beta=0$, inner sum is

$$\psi(N;q,m) = \sum_{\substack{1\leq n\leq N\\ n\equiv m (\mathrm{mod}\, q)}} \Lambda(n).$$

de la Vallée Poisson also proved in 1899, if $(m,q)=1$, (fixed q)

$$\psi(N;q,m) \sim \frac{N}{\phi(q)}.$$

Hence by partial summation we find

$$S(\frac{a}{q}+\beta) = \left(\sum_{\substack{1\le m\le q\\(m,q)=1}} e(\frac{ma}{q})\right)\frac{1}{\phi(q)}I(\beta) + \text{error}$$
$$= \frac{c_q(m)}{\phi(q)}I(\beta) + \text{error}$$
$$= \frac{\mu(q)}{\phi(q)}I(\beta) + \text{error},$$

where $c_q(m)$ is the Ramanujan sum, and

$$c_q(m) = \mu(q) \quad \text{if} \quad (m,q) = 1.$$

Two questions:

1. Can we prove this approximation is good?

2. How can we stitch these local approximations together?

Answers: 1. Not really. 2. I don't know.

Let

$$R(\beta; q, a) = S(\frac{a}{q} + \beta) - \frac{\mu(q)}{\phi(q)} I(\beta).$$

On GRH:

$$R(\beta; q, a) \ll q^{1/2} \left(N^{1/2} + \beta^{1/2} N \right) \log^2(qN)$$

Unconditionally Vinogradov, Vaughan:

For $|\beta| \le \frac{1}{q^2}$,

$$R(\beta; q, a) \ll q^{1/2} \left(N^{1/2} + \frac{N}{q} \right) \log^4(qN) + N^{4/5} \log^4(qN)$$

For binary problems these are killers, but for ternary problems they are useful.

However, Hardy-Littlewood still had a trick up their sleeves (next lecture).

How do we stitch these local approximations together?

Hardy-Littlewood: Introduce the Farey decomposition:

1. Pick a parameter Q and consider the Farey fractions of order Q:

$$\left\{\frac{a}{q} : 1 \leq q \leq Q, \quad 0 \leq a \leq q, \text{ where } (a,q) = 1\right\}.$$

Define Farey arcs around each fractions (except 0/1 which we exclude) For consecutive fractions:

$$\frac{a'}{q'} < \frac{a}{q} < \frac{a''}{q''}$$

the Farey arc around a/q is

$$\mathcal{M}_Q(q,a) = \left(\frac{a+a'}{q+q'}, \frac{a+a''}{q+q''}\right], \qquad \text{for } \frac{a}{q} \neq \frac{1}{1}, a \neq 0,$$

and

$$\mathcal{M}_Q(1,1) = \left(1 - \frac{1}{Q+1}, 1 + \frac{1}{Q+1}\right] \ .$$

These intervals are disjoint and their union covers the interval $(\frac{1}{Q+1}, 1 + \frac{1}{Q+1}]$. For fractions with denominator q these arcs vary in length a bit: "Littlewood's fuzzy ends"

(This is the origin of Kloosterman sums)

Denote a Farey arc shifted to the origin by $\theta_Q(q,a)$. Then

$$\left(\frac{-1}{2qQ}, \frac{1}{2qQ}\right) \subseteq \theta_Q(q,a) \subseteq \left(\frac{-1}{qQ}, \frac{1}{qQ}\right).$$

Thus Hardy-Littlewood use the (major arc) approximation for $S(\alpha)$

$$J_Q(\alpha) = \sum_{q \le Q} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \frac{\mu(q)}{\phi(q)} I(\alpha - \frac{a}{q}) \chi_Q(\alpha, \frac{a}{q})$$

where $\chi_Q(\alpha, \frac{a}{q})$ is the characteristic function of the Farey arc, or sometimes some subinterval of this.

Returning to the twin prime problem (now $p - p' = k$)

$$Z(N;k) := \sum_{\substack{n \\ 1\le n, n+k \le N}} \Lambda(n)\Lambda(n+k)$$
$$= \int_0^1 |S(\alpha)|^2 e(-k\alpha)\, d\alpha.$$

Usual procedure: breaking this into Farey intervals and approximate S.

This is equivalent to replacing S by J_Q. Because each spike has its own support, the spikes are orthogonal to each other, and trivially

$$|J_Q(\alpha)|^2 = \sum_{q\le q} \sum_{\substack{1\le a\le q \\ (a,q)=1}} \frac{\mu(q)^2}{\phi(q)^2} |I(\alpha - \frac{a}{q})|^2 \chi_Q(\alpha, \frac{a}{q})$$

Thus our approximation of $Z(N,k)$ is

$$\int_0^1 |J_Q(\alpha)|^2 e(-k\alpha)\,d\alpha$$
$$= \sum_{q\le Q} \sum_{\substack{1\le a\le q\\(a,q)=1}} \frac{\mu(q)^2}{\phi(q)^2} e(-\frac{ka}{q}) \int_{\theta_Q(\frac{a}{q})} |I(\beta)|^2 e(-k\beta)\,d\beta.$$

Using $|I(\beta)| \ll \min(N, \frac{1}{|\beta|})$,

$$\begin{aligned}\int_{\theta_Q(\frac{a}{q})} |I(\beta)|^2 e(-k\beta)\,d\beta &= \int_0^1 \cdots + O(qQ)\\ &= \sum_{\substack{n\\1\le n, n+k\le N}} 1 + O(qQ)\\ &= (N-|k|) + O(qQ).\end{aligned}$$

Substituting we get

$$(\mathfrak{S}(k) + o(1))(N-|k|) + O(Q^2).$$

where for k odd $\mathfrak{S}(k) = 0$, and for even $k \neq 0$

$$\mathfrak{S}(k) = 2C \prod_{\substack{p|k\\p>2}} \Big(\frac{p-1}{p-2}\Big), \;\; C = \prod_{p>2} \Big(1 - \frac{1}{(p-2)^2}\Big).$$

This provides the conjectured formula for $Z(N,k)$.

Evidence for the Twin Prime Conjecture?

We can check one case: $k=0$.
By Parseval and PNT

$$\int_0^1 |S(\alpha)|^2\,d\alpha = \sum_{n\le N} \Lambda(n)^2 \sim N\log N.$$

Above gives

$$\int_0^1 |J_Q(\alpha)|^2\,d\alpha = N(1+o(1))\log Q + O(Q^2).$$

Thus for $Q \le N^{1/2}$ we get wrong answer.

Actually for larger Q we still get the wrong answer:

Using trivial estimate

$$\int_{\theta_Q(\frac{a}{q})} |I(\beta)|^2 \ll \frac{N^2}{qQ}$$

we get a contribution above of only $O(N)$ from terms $q > N/Q$. Thus for $1 \le Q \le N$

$$\int_0^1 |J_Q(\alpha)|^2 \, d\alpha \sim N \log\left(\min(Q, \frac{N}{Q})\right).$$

Thus the best we can do is when $Q = N^{1/2}$ and this is only half of what we should get.

Solution of this problem (1990): **DROP** $\chi_Q(\alpha, \frac{a}{q})$.

$$\begin{aligned} V_Q(\alpha) &= \sum_{q \le Q} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} \frac{\mu(q)}{\phi(q)} I(\alpha - \frac{a}{q}) \\ &= \sum_{n \le N} \left(\sum_{q \le Q} \frac{\mu(q)}{\phi(q)} c_q(-n) \right) e(n\alpha) \\ &= \sum_{n \le N} \lambda_Q(n) e(n\alpha) \end{aligned}$$

This is supposed to be an approximation of

$$S(\alpha) = \sum_{n \le N} \Lambda(n) e(n\alpha).$$

This suggests that the content of the circle method is to approximate $\Lambda(n)$ by $\lambda_Q(n)$. Now

$$\lambda_Q(n) = \sum_{q \le Q} \frac{\mu(q)^2}{\phi(q)} \sum_{\substack{d|q \\ d|n}} d\mu(d).$$

Changing the order of summation:

$$\lambda_Q(n) = \sum_{\substack{d|n \\ d \le Q}} \frac{d\mu(d)}{\phi(d)} \sum_{\substack{q \le Q/d \\ (q,d)=1}} \frac{\mu(q)^2}{\phi(q)}$$

Thus $\lambda_Q(n)$ is a divisor sum of n with divisors less than Q. Now

$$\sum_{\substack{q \le Q \\ (q,d)=1}} \frac{\mu(q)^2}{\phi(q)}$$

$$= \frac{\phi(d)}{d} \left\{ \log Q + A_0 + A_1 \sum_{p|d} \frac{\log p}{p-1} + O(\frac{d^{\epsilon}}{Q^{1/4}}) \right\}.$$

Thus a simple approximation of $\lambda_Q(n)$ is just

$$\Lambda_Q(n) = \sum_{\substack{d|n \\ d \le Q}} \mu(d) \log(Q/d),$$

but from elementary number theory

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(1/d).$$

Thus the content of the circle method for primes is reduced to a short smoothed truncation of this elementary formula.