Prime gaps

Lola Thompson

Oberlin College & Max Planck Institute for Mathematics

December 12, 2016

Bounded gaps between primes: a brief history

Conjecture (de Polignac, 1849)

For even integers h, there are infinitely many pairs of primes $p, p+h$.

We refer to such values of h as *de Polignac numbers*.

Natural questions about de Polignac numbers

Some natural questions arise:

Natural questions about de Polignac numbers

Some natural questions arise:

- What proportion of even integers are de Polignac numbers?

Natural questions about de Polignac numbers

Some natural questions arise:

- What proportion of even integers are de Polignac numbers?
- Are there infinitely many de Polignac numbers?

Natural questions about de Polignac numbers

Some natural questions arise:

- What proportion of even integers are de Polignac numbers?
- Are there infinitely many de Polignac numbers?
- What is the smallest de Polignac number?

Natural questions about de Polignac numbers

Some natural questions arise:

- What proportion of even integers are de Polignac numbers?
- Are there infinitely many de Polignac numbers?
- What is the smallest de Polignac number?
- Do de Polignac numbers even exist???

Natural questions about de Polignac numbers

Some natural questions arise:

- What proportion of even integers are de Polignac numbers?
- Are there infinitely many de Polignac numbers?
- What is the smallest de Polignac number?
- Do de Polignac numbers even exist???

Natural questions about de Polignac numbers

Some natural questions arise:

- What proportion of even integers are de Polignac numbers?
- Are there infinitely many de Polignac numbers?
- What is the smallest de Polignac number?
- Do de Polignac numbers even exist???

It is widely conjectured that $h = 2$ is the smallest de Polignac number, i.e., that there are infinitely many pairs of **twin primes**.

A (crude) heuristic approach

A heuristic lemma

Theorem (Chebyshev, 1852)

Approximately $\frac{1}{\log x}$ *of the integers in* $[1, x]$ *are prime.*

A crude heuristic approach

For the integers in $[1, x]$:

A crude heuristic approach

For the integers in $[1, x]$:

- $P(p \text{ is prime}) = \frac{1}{\log x}$

A crude heuristic approach

For the integers in $[1, x]$:

- $P(p \text{ is prime}) = \frac{1}{\log x}$
- $P(p+2 \text{ is prime}) = \frac{1}{\log x}$

A crude heuristic approach

For the integers in $[1, x]$:

- $P(p \text{ is prime}) = \frac{1}{\log x}$
- $P(p+2 \text{ is prime}) = \frac{1}{\log x}$

If these two events are **independent**, then

$$\begin{aligned} P(p \text{ and } p+2 \text{ prime}) &= P(p \text{ prime}) \cdot P(p+2 \text{ prime}) \\ &= \frac{1}{\log x} \cdot \frac{1}{\log x} \\ &= \left(\frac{1}{\log x}\right)^2. \end{aligned}$$

A crude heuristic approach

Thus, we'd expect

$$\#\{p \leq x : p \text{ and } p+2 \text{ prime}\} \approx \frac{x}{(\log x)^2}.$$

Since $\lim_{x\to\infty} \frac{x}{(\log x)^2} = \infty$, this gives us reason to believe that there are infinitely many pairs of twin primes!

A problem with our crude heuristic

Problem: The events "p prime" and "$p+2$ prime" aren't independent!

A problem with our crude heuristic

Problem: The events "p prime" and "$p+2$ prime" aren't independent!

One could show (using an analogous argument) that

$$\#\{p \le x : p \text{ and } p+1 \text{ prime}\} \approx \frac{x}{(\log x)^2},$$

which is clearly false!

Refining our heuristic...

An improved heuristic

To correct for non-independence, let p and p' be independently chosen random integers. Look at:

$$\frac{P(p, p+2 \text{ not both divisible by } q)}{P(p, p' \text{ not both divisible by } q)},$$

for each small prime q.

An improved heuristic

To correct for non-independence, let p and p' be independently chosen random integers. Look at:

$$\frac{P(p, p+2 \text{ not both divisible by } q)}{P(p, p' \text{ not both divisible by } q)},$$

for each small prime q.

Since

$$P(q \mid p) = \frac{1}{q},$$

then

$$P(q \nmid p) = 1 - \frac{1}{q}.$$

An improved heuristic

To correct for non-independence, let p and p' be independently chosen random integers. Look at:

$$\frac{P(p, p+2 \text{ not both divisible by } q)}{P(p, p' \text{ not both divisible by } q)},$$

for each small prime q.

Since

$$P(q \mid p) = \frac{1}{q},$$

then

$$P(q \nmid p) = 1 - \frac{1}{q}.$$

Thus, we have

$$P(q \nmid p \text{ and } q \nmid p') = \left(1 - \frac{1}{q}\right)^2.$$

An improved heuristic

$$P(q \nmid p \text{ and } q \nmid (p+2)) = P(p \not\equiv 0 \text{ or } -2 \pmod{q})$$

An improved heuristic

$$P(q \nmid p \text{ and } q \nmid (p+2)) = P(p \not\equiv 0 \text{ or } -2 \pmod q)$$

Observe that

$$P(p \not\equiv 0 \text{ or } -2 \pmod q) = \begin{cases} 1 - 2/q & \text{if } q > 2 \\ 1 - 1/2 & \text{if } q = 2 \end{cases}$$

An improved heuristic

$$P(q \nmid p \text{ and } q \nmid (p+2)) = P(p \not\equiv 0 \text{ or } -2 \pmod q)$$

Observe that

$$P(p \not\equiv 0 \text{ or } -2 \pmod q) = \begin{cases} 1 - 2/q & \text{if } q > 2 \\ 1 - 1/2 & \text{if } q = 2 \end{cases}$$

Hence, if $q > 2$ then the correction factor for divisibility by q is

$$\frac{(1 - \frac{2}{q})}{(1 - \frac{1}{q})^2}.$$

An improved heuristic

$$P(q \nmid p \text{ and } q \nmid (p+2)) = P(p \not\equiv 0 \text{ or } -2 \pmod{q})$$

Observe that

$$P(p \not\equiv 0 \text{ or } -2 \pmod{q}) = \begin{cases} 1 - 2/q & \text{if } q > 2 \\ 1 - 1/2 & \text{if } q = 2 \end{cases}$$

Hence, if $q > 2$ then the correction factor for divisibility by q is

$$\frac{(1 - \frac{2}{q})}{(1 - \frac{1}{q})^2}.$$

If $q = 2$ then the correction factor is

$$\frac{1 - \frac{1}{2}}{(1 - \frac{1}{2})^2} = 2.$$

The heuristic with correction factor

Thus, we define

$$C := 2 \prod_{\substack{q \text{ prime} \\ q \geq 3}} \frac{(1 - 2/q)}{(1 - 1/q)^2} \approx 1.3203236\ldots.$$

This suggests that

$$\#\{p \leq x : p \text{ and } p + 2 \text{ prime}\} \approx C \frac{x}{(\log x)^2}.$$

Where the heuristics fail

The heuristic argument relies heavily on the assumption that the primes p are *uniformly distributed* among the residue classes $\pmod q$.

Let $\pi(x; q, a) := \#\{p \leq x : p \equiv a \pmod q\}$.

If the primes **were** uniformly distributed (mod q), we'd expect:

$$\pi(x; q, a) \approx \frac{x}{\varphi(q) \log x},$$

when $\gcd(a, q) = 1$.

Equidistribution for "small" q

Theorem (Bombieri-Vinogradov)

For any constant $A > 0$, *there exists* $B = B(A)$ *such that*

$$\sum_{q \le Q} \max_{\substack{a \pmod{q} \\ (a,q)=1}} \left| \pi(x; q, a) - \frac{x}{\varphi(q) \log x} \right| \ll_A \frac{x}{(\log x)^A},$$

where $Q = \frac{x^{1/2}}{(\log x)^B}$.

Equidistribution for all q?

Conjecture (Elliott-Halberstam)

The Bombieri-Vinogradov theorem still holds if we take $Q = x^\theta$, for any $\theta < 1$.

We call θ the *level of distribution* of the set of primes.

Recent results on bounded gaps between primes

Admissible k-tuples

Definition

We say that a k-tuple $(h_1, ..., h_k)$ of nonnegative integers is *admissible* if it doesn't cover all of the possible remainders (mod p) for any prime p.

Example: $(0, 2, 6, 8, 12)$ is an admissible 5-tuple.

Residue classes not covered:

$1 \pmod 2$

$1 \pmod 3$

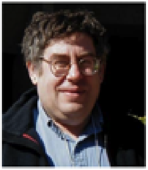
$4 \pmod 5$

$3 \pmod 7$

$3 \pmod{11}$

A conditional proof of the Bounded Gaps Theorem

G P Y



Theorem (Goldston, Pintz and Yıldırım, 2009)

If $(h_1, ..., h_k)$ is admissible and the Elliot-Halberstam Conjecture holds with $Q = x^{1/2+\eta}$, then there are infinitely many n such that at least 2 of $n + h_1, ..., n + h_k$ are prime.

Zhang's "relaxation" of Bombieri-Vinogradov

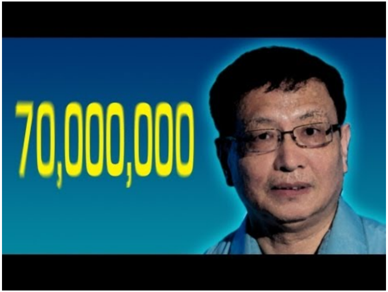
Theorem (Zhang, 2013)

There exist $\eta, \delta > 0$ *such that for any given* a,

$$\sum_{\substack{q \le Q \\ (q,a)=1 \\ q \text{ squarefree } \& \ y\text{-smooth}}} \left| \pi(x;q,a) - \frac{x}{\varphi(q)\log x} \right| \ll_A \frac{x}{(\log x)^A},$$

where $Q = x^{1/2+\eta}$ *and* $y = x^{\delta}$.

Bounded gaps between primes (at last!)



Corollary (Zhang, 2013)

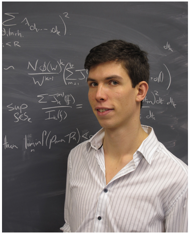
There are infinitely many pairs of primes that differ by at most $70,000,000$.

A stronger conjecture: prime k-tuples

Conjecture (Hardy-Littlewood prime k-tuples)

Let $\mathcal{H} = (h_1, \ldots, h_k)$ be admissible. Then there are infinitely many integers n such that all of $n + h_1, \ldots, n + h_k$ are prime.

Maynard and Tao's independent work



Theorem (Maynard-Tao, November 2013)

Let $m \geq 2$. There for any admissible k-tuple $\mathcal{H} = (h_1, \ldots, h_k)$ with "large enough" k (relative to m), there are infinitely many n such that at least m of $n + h_1, \ldots, n + h_k$ are prime.

The state of the art

Theorem (D. H. J. Polymath, 2014)

There are infinitely many pairs of primes that are at most 246 apart.

The state of the art

Theorem (D. H. J. Polymath, 2014)

There are infinitely many pairs of primes that are at most 246 *apart.*

By assuming the Generalized Elliot–Halberstam Conjecture, this number can be reduced to 6!!!

The Maynard-Tao method

A sketch of the Maynard-Tao method

Goal: Find values of n for which the tuple $n + h_1, ..., n + h_k$ contains several primes.

Setup: For large N, look for n in the dyadic interval $[N, 2N)$.

Let $W := \prod_{p \le \log_3 N} p$. Since $\mathcal{H}$ is admissible, we can choose an integer ν so that $\gcd(\nu + h_i, W) = 1$ for all $1 \le i \le k$.

The W-trick: Pre-sieve the set to just those n satisfying $n \equiv \nu \pmod{W}$.

Thus, our sample space becomes

$$\Omega := \{N \le n < 2N : n \equiv \nu \pmod{W}\}.$$

A sketch of the Maynard-Tao method

Let $w(n)$ denote nonnegative weights and let $\chi_{\mathcal{P}}$ denote the characteristic function of the set $\mathcal{P}$ of primes. Consider

$$S_1 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod{W}}} w(n)$$

$$S_2 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathcal{P}}(n + h_i) \right) w(n).$$

The fraction S_2/S_1 is a weighted average of the number of primes among $n + h_1, \ldots, n + h_k$ over Ω.

A sketch of the Maynard-Tao method

Key idea: If $S_2/S_1 > (m-1)$ for some $m \in \mathbb{Z}^+$ then at least m of $n+h_1, ..., n+h_k$ are prime, for some $n \in \Omega$.

For this method to work, one needs to select the weights $w(n)$ so that:

1. S_2 and S_1 can be estimated using tools of asymptotic analysis

A sketch of the Maynard-Tao method

Key idea: If $S_2/S_1 > (m-1)$ for some $m \in \mathbb{Z}^+$ then at least m of $n+h_1, ..., n+h_k$ are prime, for some $n \in \Omega$.

For this method to work, one needs to select the weights $w(n)$ so that:

1. S_2 and S_1 can be estimated using tools of asymptotic analysis
2. S_2/S_1 is large.

Variants of the Maynard-Tao theorem

Maynard-Tao for number fields

Theorem (Castillo, Hall, Lemke Oliver, Pollack, T., 2014)

Let $m \geq 2$. Given a number field K, there exists an integer $k_0 := k_0(m, K)$ such that for any admissible k-tuple $(h_1, ..., h_k)$ in $\mathcal{O}_K$ with $k \geq k_0$, there are infinitely many $\alpha \in \mathcal{O}_K$ such that at least m of $\alpha + h_1, ..., \alpha + h_k$ are prime.

Maynard-Tao for Chebotarev sets

A set of primes $q_1, q_2, \ldots$ has the *bounded gaps property* if $\liminf_{n\to\infty} q_{n+m} - q_n < \infty$ for every m.

Theorem (Thorner, 2014)

Chebotarev sets have the bounded gaps property.

Maynard-Tao for Chebotarev sets

Some examples of Chebotarev sets:

Maynard-Tao for Chebotarev sets

Some examples of Chebotarev sets:

- The set of primes $p \equiv 1 \pmod 3$ for which 2 is a cube $\pmod p$.

Maynard-Tao for Chebotarev sets

Some examples of Chebotarev sets:

- The set of primes $p \equiv 1 \pmod 3$ for which 2 is a cube $\pmod p$.
- Fix $n \in \mathbb{Z}^+$. The set of primes expressible in the form $x^2 + ny^2$.

Maynard-Tao for Chebotarev sets

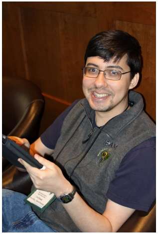
Some examples of Chebotarev sets:

- The set of primes $p \equiv 1 \pmod{3}$ for which 2 is a cube $\pmod{p}$.
- Fix $n \in \mathbb{Z}^+$. The set of primes expressible in the form $x^2 + ny^2$.
- Let τ be the Ramanujan tau function. The set of primes p for which $\tau(p) \equiv 0 \pmod{d}$ for any positive integer d.

Maynard-Tao for Chebotarev sets

Some examples of Chebotarev sets:

- The set of primes $p \equiv 1 \pmod{3}$ for which 2 is a cube $\pmod{p}$.
- Fix $n \in \mathbb{Z}^+$. The set of primes expressible in the form $x^2 + ny^2$.
- Let τ be the Ramanujan tau function. The set of primes p for which $\tau(p) \equiv 0 \pmod{d}$ for any positive integer d.
- The set of primes p for which $\#E(\mathbb{F}_p) \equiv p + 1 \pmod{d}$ for any positive integer d.



Theorem (Hall, Ph.D. 2006; Pollack, Ph.D. 2008)

If $q \geq 3$, then any $a \in \mathbb{F}_q$ (excluding $a = 0$) occurs infinitely often as a gap between irreducible polynomials.

($q > 3$ due to Hall; $q = 3$ due to Pollack)

An improvement on Hall and Pollack's work

Theorem (Castillo, Hall, Lemke Oliver, Pollack, T., 2014)

Let $m \geq 2$. There is an integer $k_0 := k_0(m)$ such that for any admissible k-tuple $(h_1, \ldots, h_k)$ of polynomials in $\mathbb{F}_q[x]$ with $k \geq k_0$, there are infinitely many $f \in \mathbb{F}_q[x]$ such that at least m of $f + h_1, \ldots, f + h_k$ are irreducible.

Applications to runs of consecutive primes

Consecutive primes in arithmetic progressions

Theorem (Shiu, 2000)

Each set of remainders $a \pmod q$ with $\gcd(a, q) = 1$ contains arbitrarily long runs of consecutive primes.

A paradigm shift

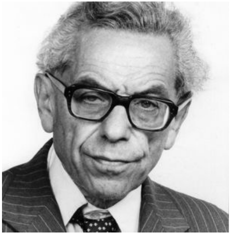
In a paper in 2013, Banks, Freiberg and Turnage-Butterbaugh used the Maynard-Tao method to give a strikingly simple re-proof of Shiu's result.

A paradigm shift

In a paper in 2013, Banks, Freiberg and Turnage-Butterbaugh used the Maynard-Tao method to give a strikingly simple re-proof of Shiu's result.

This begs the question: can the Maynard-Tao method be used to handle other "consecutive primes" problems?

A Conjecture of Erdős and Turan



For each k, let $d_k = p_{k+1} - p_k$.

Conjecture (Erdős, Turan 1948)

The sequence $\{d_k\}$ contains arbitrarily long (strictly) increasing runs and arbitrarily long (strictly) decreasing runs.

Increasing/decreasing runs of prime gaps

Theorem (Banks, Freiberg, Turnage-Butterbaugh, 2013)

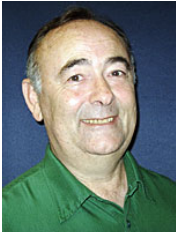
The sequence $\{d_k\}$ contains arbitrarily long (strictly) increasing runs and arbitrarily long (strictly) decreasing runs.

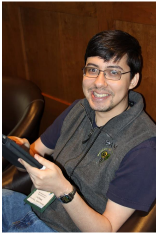
Consecutive primes with a given primitive root

Theorem (Pollack, 2014)

Under GRH, there exist arbitrarily long runs of consecutive primes possessing a given primitive root, g (where $g \neq -1$ and not a square).

Runs of primes with cyclic $E(\mathbb{F}_p)$





Theorem (Baker and Pollack, 2016)

Assume GRH. Fix an elliptic curve $E/\mathbb{Q}$. There are arbitrarily long runs of primes p for which $E(\mathbb{F}_p)$ is cyclic.

Arithmetic functions at consecutive shifted primes

Theorem (Pollack, T., 2015)

Let $f = \varphi, \sigma, \omega, \Omega, \tau$. There are arbitrarily long runs of consecutive primes p on which $f(p-1)$ is decreasing. The same holds for $f(p-1)$ increasing.

Proof sketch for decreasing runs of $\varphi(p-1)$'s

Same basic setup as in Maynard-Tao:

For large N, let $W := \prod_{p \le \log_3 N} p$ and define

$$S_1 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod{W}}} w(n)$$

$$S_2 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathcal{P}}(n + h_i) \right) w(n).$$

We want $\frac{S_2}{S_1} > m - 1$ so that at least m of $n + h_1, \ldots, n + h_k$ are prime for $n \in \Omega$.

Proof sketch for decreasing runs of $\varphi(p-1)$'s

Key innovation: **Modify the W-trick**

Fix $\mathcal{H} = \{h_1, ..., h_k\}$ where $h_i = (i-1)(2k)!$. With this $\mathcal{H}$, we want to choose $\nu \pmod W$ such that:

1. (Consecutive Primes) For $n \in \Omega$, any prime $[n+h_1, n+h_k]$ is in $n+\mathcal{H}$.

2. (Decreasing φ values) With probability $1+o(1)$,

$$\frac{n+h_i-1}{\varphi(n+h_i-1)} \in (2^{4i}, 2^{4i+3}]$$

for $1 \le i \le k$.

Variations

Theorem (Pollack, T., 2015)

Let $f = \varphi, \sigma, \omega, \Omega, \tau$. There are arbitrarily long runs of consecutive primes p on which $f(p-1)$ is decreasing. The same holds for $f(p-1)$ increasing.

Variation	Modification
Increasing φ's	Replace $\mathcal{H}$ with $-\mathcal{H}$
Increasing σ's	Replace $\frac{n+h_i-1}{\varphi(n+h_i-1)}$ with $\frac{\sigma(n+h_i-1)}{n+h_i-1}$.
Decreasing σ's	Like increasing σ's but replace $\mathcal{H}$ with $-\mathcal{H}$.

**Need additional modifications to handle ω, Ω, τ.

Digit sums of consecutive primes

Definition

Let $s_g(n)$ denote the sum of the base-g digits of n.

Example: $s_{10}(523) = 5 + 2 + 3 = 10$

$$s_{10}(541) = 5 + 4 + 1 = 10$$

Question (Sierpinski, 1961): Are there arbitrarily long runs of consecutive primes p on which $s_g(p)$ is constant? increasing? decreasing?

Digit sums of consecutive primes

A brief history:

Digit sums of consecutive primes

A brief history:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.

Digit sums of consecutive primes

A brief history:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.
- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitely often.

Digit sums of consecutive primes

A brief history:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.
- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitely often.
- Sierpinski (1968): **Assuming Dickson's prime k-tuples conjecture**, $s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2})$ infinitely often.

Digit sums of consecutive primes

A brief history:

- Sierpinski (1961): $s_{10}(p_n) < s_{10}(p_{n+1})$ infinitely often.
- Erdős (1962): $s_{10}(p_n) > s_{10}(p_{n+1})$ infinitely often.
- Sierpinski (1968): **Assuming Dickson's prime k-tuples conjecture**, $s_{10}(p_n) > s_{10}(p_{n+1}) > s_{10}(p_{n+2})$ infinitely often.
- Schinzel (unpublished claim): **Assuming Hypothesis H**, there are arbitrarily long runs of consecutive p on which $s_{10}(p)$ is increasing (decreasing).

Digit sums of consecutive primes

Theorem (Pollack, T., 2015)

For any base g, there are arbitrarily long runs of consecutive primes p on which $s_g(p)$ is constant/increasing/decreasing.

Thank you!