Big doings with small g a p s

Paul Pollack

Southeastern AMS Sectional Meeting

March 27, 2015

The University of Georgia

PART I: (MOSTLY) PREHISTORY

PART I: (MOSTLY) PREHISTORY

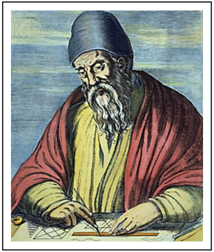
(More than two years ago)

300 BCE

Let p_n denote the nth prime number, so $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$.

Theorem (Euclid)

There are infinitely many primes. In other words, if $\pi(x) := \#\{p \le x : p \text{ prime}\}$, then $\pi(x) \to \infty$ as $x \to \infty$.



There are at this point seemingly infinitely many proofs of this theorem. Euclid's theorem suggests there might be something to be gained by studying the sequence of gaps

$$d_n := p_{n+1} - p_n.$$

Twin primes

The sequence $\{d_n\}$ begins
$1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, \ldots$
(`OEIS A001223`)

It was noticed many moons ago that $d_n = 2$ appears to appear infinitely often.

Twin primes

The sequence $\{d_n\}$ begins
$1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, \ldots$
(`OEIS A001223`)

It was noticed many moons ago that $d_n = 2$ appears to appear infinitely often.

A pair of prime numbers $\{p, p+2\}$ is called a *twin prime pair*.

Twin prime pairs: $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$, $\{41, 43\}$, $\{59, 61\}$, $\{71, 73\}$, ...

Twin prime conjecture: There are infinitely many twin prime pairs.


WORLD PREMIERE!
A TAUT, GRIPPING PSYCHOLOGICAL SPINE-TINGLER
TWIN PRIMES
BY ALEX LEWIN

A desperate professor, a brilliant student and a 2000-year-old math problem collide in this thriller about ambition, ego and the nature of genius.

What counts as progress towards the twin primes conjecture?

Think statistically: What is the average gap between primes $p \in (x, 2x]$?

What counts as progress towards the twin primes conjecture?

Think statistically: What is the average gap between primes $p \in (x, 2x]$?

Prime number theorem (1899): As $x \to \infty$, the count of primes in $(x, 2x]$ is $\sim x/\log x$. In other words,

$$\lim_{x\to\infty} \frac{\#\{p : x < p \leq 2x\}}{x/\log x} = 1.$$

Thus, the average gap between primes $p \in (x, 2x]$ is $\sim \log x$.
Notice: $\log x \sim \log p$ for $p \in (x, 2x]$.

In particular, one gets that

$$\liminf_{n\to\infty} \frac{d_n}{\log p_n} \leq 1.$$

We'll call this the trivial result. A nontrivial result is any improvement on this upper bound.

In particular, one gets that

$$\liminf_{n\to\infty} \frac{d_n}{\log p_n} \leq 1.$$

We'll call this the trivial result. A nontrivial result is any improvement on this upper bound.

Theorem (Erdős, 1940)

$\liminf \dfrac{d_n}{\log p_n} < 1.$

One does not win by very much. Using Erdős's argument, Ricci showed in 1954 that $\liminf \frac{d_n}{\log p_n} \leq \frac{15}{16}$.

Landmark results

Theorem (Bombieri and Davenport, 1966)

$$\liminf \frac{d_n}{\log p_n} \leq 0.46650\ldots.$$

Theorem (Maier, 1988)

$$\liminf \frac{d_n}{\log p_n} \leq 0.2486\ldots.$$

A new hope

(YPG)

Theorem (Goldston, Pintz, and Yıldırım, 2005)

$$\liminf \frac{d_n}{\log p_n} = 0.$$

BUT WAIT, THERE'S MORE!

A new hope

(YPG)

Theorem (Goldston, Pintz, and Yıldırım, 2005)

$$\liminf \frac{d_n}{\log p_n} = 0.$$

BUT WAIT, THERE'S MORE!

Any improvement in the level of distribution of the primes would imply that $\liminf d_n < \infty$ — i.e., infinitely many pairs of primes that lie in a bounded length interval.

An aside: Primes in arithmetic progressions

Let $q \in \mathbb{N}$. There are q residue classes: 1, 2, 3, ..., q mod q.

If a and q share a common factor, then this factor is shared by every element of the residue class. So there is at most one prime in the class a mod q.

Here is an illustration for $q = 6$:

1	7	13	19	25	31	37	43	49	55	61	67	73
2	8	14	20	26	32	38	44	50	56	62	68	74
3	9	15	21	27	33	39	45	51	57	63	69	75
4	10	16	22	28	34	40	46	52	58	64	70	76
5	11	17	23	29	35	41	47	53	59	65	71	77
6	12	18	24	30	36	42	48	54	60	66	72	78

Let $\phi(q)$ denote the number of residue classes a mod q where $\gcd(a, q) = 1$. For example, $\phi(6) = 2$, corresponding to the two classes 1 mod 6 and 5 mod 6.

Theorem (Dirichlet, 1837)

Each of the $\phi(q)$ coprime residue classes contains infinitely many primes.

Example

Take $q = 10000$ and $a = 9999$. There are infinitely many primes that end with the digits 9999.

Things even out

Once you realize that things even out, its like a light being turned on in your head, then being turned off, then being turned to "dim." – Jack Handey

In fact, each coprime residue class eventually gets its fair share of primes. The number of primes $p \leq x$ landing in each of the $\phi(q)$ residue classes is

$$\sim \frac{\pi(x)}{\phi(q)}$$

(the **prime number theorem for progressions**, 1899).

Thus, the distribution of primes **eventually** "evens out" over all the coprime residue classes modulo q.

The notion of level of distribution is about how large x has to be in terms of q to see this “even”-ing out.

The notion of level of distribution is about how large x has to be in terms of q to see this "even"-ing out.

We expect that if $q \leq x^{1-\epsilon}$ for some fixed $\epsilon > 0$, then the distribution of $p \leq x$ among coprime residue classes modulo q is asymptotically uniform.

The notion of level of distribution is about how large x has to be in terms of q to see this “even”-ing out.

We expect that if $q \leq x^{1-\epsilon}$ for some fixed $\epsilon > 0$, then the distribution of $p \leq x$ among coprime residue classes modulo q is asymptotically uniform.

The *Extended Riemann Hypothesis* would imply this for $q \leq x^{1/2-\epsilon}$. (Still weaker than the expected truth!)

The notion of level of distribution is about how large x has to be in terms of q to see this “even”-ing out.

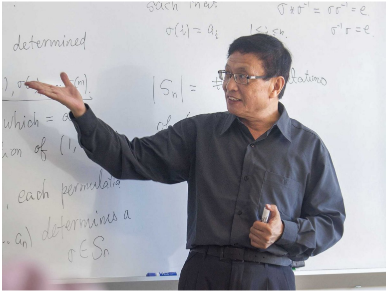
We expect that if $q \leq x^{1-\epsilon}$ for some fixed $\epsilon > 0$, then the distribution of $p \leq x$ among coprime residue classes modulo q is asymptotically uniform.

The *Extended Riemann Hypothesis* would imply this for $q \leq x^{1/2-\epsilon}$. (Still weaker than the expected truth!)

The *Bombieri–A.I. Vinogradov theorem* says that we see this even-ing out *on average* over $q \leq x^{1/2-\epsilon}$.

GPY wanted to replace $\frac{1}{2} - \epsilon$ with $\frac{1}{2} + \delta$, for some $\delta > 0$.

PART II: Zhang, Maynard, and Tao (OH MY!)



Theorem (Y. Zhang, April 2013)

One can prove a certain technically restricted version of the GPY Hypothesis, still sufficient to give bounded gaps between primes.

Corollary

$\liminf_{n\to\infty} d_n < 70 \cdot 10^6$.

Theorem (Maynard)

We have $\liminf d_n \leq 600$*.*

BUT WAIT, THERE'S MORE!

For each k*, define the* k*th order gap* $d_n^{(k)} := p_{n+k} - p_n$*. We always have*

$$\liminf_{n\to\infty} d_n^{(k)} < \infty.$$

Similar results were discovered concurrently by Terry Tao.

Polymath 8b: $\liminf_{n\to\infty} d_n \leq 246$.

The story behind the story

GPY, Zhang, and Maynard do not study d_n directly.
Rather, they study a variant of the twin prime conjecture due to Hardy and Littlewood, called the *k-tuples conjecture.*

Problem

Let $\mathcal{H}$ be a set of k integers, say $a_1, \ldots, a_k$. Under what conditions on $\mathcal{H}$ do we expect that $n + a_1, \ldots, n + a_k$ are simultaneously prime infinitely often?

The story behind the story

GPY, Zhang, and Maynard do not study d_n directly.
Rather, they study a variant of the twin prime conjecture due to Hardy and Littlewood, called the *k-tuples conjecture.*

Problem

Let $\mathcal{H}$ be a set of k integers, say $a_1, \ldots, a_k$. Under what conditions on $\mathcal{H}$ do we expect that $n + a_1, \ldots, n + a_k$ are simultaneously prime infinitely often?

We need to rule out examples like $n, n+1$, one of which is always even, or $n, n+2, n+4$, one of which is always a multiple of 3.

Definition

We say $\mathcal{H}$ is admissible if $\#\mathcal{H} \bmod p < p$ for all primes p.

Conjecture (k-tuples conjecture)

If $\mathcal{H}$ is admissible, then there are infinitely many n with all $n + h_i$ simultaneously prime.

Conjecture (k-tuples conjecture)

If $\mathcal{H}$ is admissible, then there are infinitely many n with all $n + h_i$ simultaneously prime.

The theorems of GPY, Maynard, and Zhang about prime gaps are really corollaries of their results towards the k-tuples conjecture.

Theorem (Zhang)

*There is a constant k_0 so that if $k \geq k_0$, and $\mathcal{H}$ is an admissible k-tuple, then infinitely often **at least two** of $n + h_1, \ldots, n + h_k$ are prime.*

Theorem (Maynard)

*Fix $m \geq 2$. There is a constant $k_0(m)$ so that if $k \geq k_0(m)$, and $\mathcal{H}$ is an admissible k-tuple, then infinitely often **at least** m of $n + h_1, \ldots, n + h_k$ are prime.*

Maynard showed that one could take $k_0(2) = 105$.

Hence, if we fix an admissible 105-tuple, say $h_1 < \cdots < h_{105}$, then infinitely often at least two of $n + h_1, \ldots, n + h_{105}$ are prime. So infinitely often

$$p_{j+1} - p_j \leq h_{105} - h_1.$$

Maynard showed that one could take $k_0(2) = 105$.

Hence, if we fix an admissible 105-tuple, say $h_1 < \cdots < h_{105}$, then infinitely often at least two of $n + h_1, \ldots, n + h_{105}$ are prime. So infinitely often

$$p_{j+1} - p_j \leq h_{105} - h_1.$$

There is an example of such an $\mathcal{H}$ with $h_{105} - h_1 = 600$;

$$\mathcal{H} = \{0, 10, 12, 24, 28, \ldots, 598, 600\}.$$

Hence,

$$\liminf_{n\to\infty} d_n \leq 600.$$

Polymath8b: Can take $k_0(2) = 50$.
Choosing a "narrow" admissible 50-tuple gives $\liminf d_n \leq 246$.

PART III: THE REST OF THE STORY

The k-tuples conjecture (and a variant due to Dickson allowing leading coefficients) has traditionally been a “working hypothesis” in a number of investigations in elementary number theory. Many theorems have been proved conditionally on the truth of this conjecture.

The work of Maynard–Tao opens the door towards the **unconditional** resolution of some of these problems.

Erdős, Turán, and the local behavior of prime gaps

Question

Are there infinitely many n with $d_n < d_{n+1}$?

Yes, trivially, because otherwise $\{d_n\}$ would be bounded.

Erdős, Turán, and the local behavior of prime gaps

Question

Are there infinitely many n with $d_n < d_{n+1}$?

Yes, trivially, because otherwise $\{d_n\}$ would be bounded.

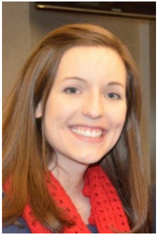
Question

Are there infinitely many n with $d_n > d_{n+1}$?

Yes (E&T, 1948), but no longer so trivial.

Question (Erdős and Turán, 1948)

Are there infinitely many n with $d_n > d_{n+1} > d_{n+2}$? What about $d_n < d_{n+1} < d_{n+2}$?

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

For every k, one can find infinitely many n with $d_n < d_{n+1} < \cdots < d_{n+k}$, and infinitely many n with $d_n > d_{n+1} > \cdots > d_{n+k}$.

Shiu strings 

Theorem (D. K. L. Shiu, 2000)

Each of the $\phi(q)$ coprime arithmetic progressions modulo q contains arbitrarily long runs of consecutive primes.

Example

There are 10^{10} consecutive primes all ending in the decimal digits 9999.

Banks, Freiberg, and Turnage-Butterbaugh have shown that the Maynard–Tao methods give a much simpler proof of Shiu's theorem.

In fact, the approach through Maynard–Tao is the “right” one, because it gives much improved quantitative results.

Theorem (Maynard, 2014)

For a positive proportion of primes p, the run of 10000 *primes starting with p all end in the digit* 9999*.*

Such a result was previously unknown even for runs of two consecutive primes!

Some questions of Sierpiński

Let $s(n)$ denote the sum of the decimal digits of n. For example, $s(2014) = 2 + 1 + 4 = 7$. We can observe that

$$s(1442173) = s(1442191) = s(1442209) = s(1442227).$$

Questions (Sierpiński, 1961)

Given m, are there infinitely many m-tuples of consecutive primes $p_n, \ldots, p_{n+m-1}$ with

$$s(p_n) = s(p_{n+1}) = \cdots = s(p_{n+m-1})?$$

Answer (Thompson and P.): Yes.

Another question of Erdős

Let $\sigma(\cdot)$ be the usual sum-of-divisors function, so $\sigma(n) = \sum_{d|n} d$.

Questions

If $\sigma(a) = \sigma(b)$, what can be said about the ratio a/b?

Example

$\sigma^{-1}(8960) = \{3348, 5116, 5187, 6021, 7189, 7657\}$.

Another question of Erdős

Let $\sigma(\cdot)$ be the usual sum-of-divisors function, so $\sigma(n) = \sum_{d|n} d$.

Questions

If $\sigma(a) = \sigma(b)$, what can be said about the ratio a/b?

Example

$\sigma^{-1}(8960) = \{3348, 5116, 5187, 6021, 7189, 7657\}$.

Conjecture (Erdős, 1959)

Nothing. More precisely, the set of ratios $\{a/b : \sigma(a) = \sigma(b)\}$ *is dense in* $\mathbb{R}_{>0}$.

Theorem (P., 2014)

Erdős's conjecture is true.

Back to normalized prime gaps

Recall that the nth normalized prime gap was defined by $\frac{p_{n+1}-p_n}{\log p_n}$. GPY says 0 is a limit point. Westzynthius (1931) proved that ∞ is also a limit point. Let $\mathbf{L}$ denote the set of limit points.

Back to normalized prime gaps

Recall that the nth normalized prime gap was defined by $\frac{p_{n+1}-p_n}{\log p_n}$. GPY says 0 is a limit point. Westzynthius (1931) proved that ∞ is also a limit point. Let **L** denote the set of limit points.

Erdős and Ricci (mid 50s): $\mu(\mathbf{L}) > 0$.
Hildebrand and Maier (1988): $\mu(\mathbf{L} \cap [0, T]) > cT$ for large T.
Pintz (2013): $\mathbf{L} \supset [0, c]$ for some $c > 0$.

Back to normalized prime gaps

Recall that the nth normalized prime gap was defined by $\frac{p_{n+1}-p_n}{\log p_n}$. GPY says 0 is a limit point. Westzynthius (1931) proved that ∞ is also a limit point. Let **L** denote the set of limit points.

Erdős and Ricci (mid 50s): $\mu(\mathbf{L}) > 0$.
Hildebrand and Maier (1988): $\mu(\mathbf{L} \cap [0, T]) > cT$ for large T.
Pintz (2013): $\mathbf{L} \supset [0, c]$ for some $c > 0$.

Theorem (Banks–Freiberg–Maynard, 2014)

Given any 9 distinct real numbers $\beta_1 < \cdots < \beta_9$, some $\beta_j - \beta_i$ belongs to **L**.

Corollary

At least 12.5% of the nonnegative reals belong to **L**.

Maynard–Tao in other number systems

The Maynard–Tao work on gaps between primes can be ported over to other settings, as long as those settings share enough properties in common with the usual setting of positive integers.

Example

Define a B**-number** as a finite nonempty sequence of 0s and 1s, with no leading 0s unless the string consists only of 0. Listing strings by length, the first few examples are thus 0, 1, 10, 11, 101, $\ldots$. We define **non-carry addition** $(+)$ and **non-carry multiplication** $(\times)$ of B-numbers by the usual grade-school algorithms for addition and multiplication but systematically ignoring carries. For example, $1 + 1 = 0$ with our definition.

And...

$$\begin{array}{r} 10101 \\ +\ \ 1101 \\ \hline 11000 \end{array} \qquad \text{while} \qquad \begin{array}{rr} & 10101 \\ \times & 1101 \\ \hline & 10101 \\ & 00000 \\ & 10101 \\ & 10101 \\ \hline & 11101001 \end{array}$$

A **prime** *B*-number is one with more than one digit which cannot be written as a non-carry product except as $1 \times$ itself or itself $\times$ 1. For example, 10 and 11 are prime, but 11101001 is not.

Not-so-secret dictionary: The *B*-numbers are the polynomials over $\mathbb{F}_2$, with the prime *B*-numbers corresponding to irreducibles.

Questions

Is there a bounded gaps theorem for prime B-numbers?

Yes!

Theorem

There are infinitely many pairs of prime B-numbers which differ only in their last 9 digits.

This is worked out by Castillo, Hall, Lemke Oliver, Thompson and P. (2014).

Questions

Is there a bounded gaps theorem for prime B-numbers?

Yes!

Theorem

There are infinitely many pairs of prime B-numbers which differ only in their last 9 digits.

This is worked out by Castillo, Hall, Lemke Oliver, Thompson and P. (2014).

More generally, we prove bounded gaps results for irreducible polynomials over arbitrary finite fields.

Thank you very much!