Primes in intervals of bounded length

Andrew Granville

Université de Montréal

Joint Math Meeting, Current Events Bulletin

Baltimore, Friday, January 17, 2014

The primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$$

$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Euclid: Infinitely many primes.

The primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$$

$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Euclid: Infinitely many primes.

You can't help but notice *Patterns in the primes*

Pairs of primes that differ by 2

$$2, \underline{3, 5}, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$$

$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Pairs of primes that differ by 2

$$2, \underline{3, 5}, \underline{7}, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$$

$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Pairs of primes that differ by 2

$2, \underline{3, 5}, \underline{7}, \underline{11, 13}, 17, 19, 23, 29, 31, 37, 41, 43, 47,$

$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$

Pairs of primes that differ by 2

$$2, \underline{3, \underline{5}}, \underline{7}, \underline{11, 13}, \underline{17, 19}, 23, \underline{29, 31}, 37, \underline{41, 43}, 47,$$

$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Pairs of primes that differ by 2

$$2, \underline{3, \underline{5}}, \underline{7}, \underline{11, 13}, \underline{17, 19}, 23, \underline{29, 31}, 37, \underline{41, 43}, 47,$$

$$53, \underline{59, 61}, 67, \underline{71, 73}, 79, 83, 89, 97, \ldots$$

Pairs of primes that differ by 2

$2, \underline{3, 5}, \underline{7}, \underline{11, 13}, \underline{17, 19}, 23, \underline{29, 31}, 37, \underline{41, 43}, 47,$

$53, \underline{59, 61}, 67, \underline{71, 73}, 79, 83, 89, 97, \ldots$

3 and 5 | 5 and 7 | 11 and 13 | 17 and 19 | 29 and 31 | 41 and 43

59 and 61 | 71 and 73 | 101 and 103 | 107 and 109 | . . .

Pairs of primes that differ by 2

$2, \underline{3, 5}, \underline{7}, \underline{11, 13}, \underline{17, 19}, 23, \underline{29, 31}, 37, \underline{41, 43}, 47,$

$53, \underline{59, 61}, 67, \underline{71, 73}, 79, 83, 89, 97, \ldots$

3 and 5 | 5 and 7 | 11 and 13 | 17 and 19 | 29 and 31 | 41 and 43

59 and 61 | 71 and 73 | 101 and 103 | 107 and 109 | ...

The twin prime conjecture. *There are infinitely many prime pairs* $p, \ p+2$

Pairs of primes that differ by 4

$2, \underline{3}, 5, \underline{7}, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$

$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$

Pairs of primes that differ by 4

$$2, \underline{3}, 5, \underline{7, 11}, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$$

$$53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

Pairs of primes that differ by 4

$$2, \underline{3}, 5, \underline{7, 11}, \underline{13, 17}, \underline{19, 23}, 29, 31, \underline{37, 41}, \underline{43, 47},$$

$$53, 59, 61, \underline{67, 71}, 73, \underline{79, 83}, 89, 97, \ldots$$

Pairs of primes that differ by 4

$$2, \underline{3}, 5, \underline{7, 11}, \underline{13, 17}, \underline{19, 23}, 29, 31, \underline{37, 41}, \underline{43, 47},$$

$$53, 59, 61, \underline{67, 71}, 73, \underline{79, 83}, 89, 97, \ldots$$

3 and 7 | 7 and 11 | 13 and 17 | 19 and 23 | 37 and 41 | 43 and 47

67 and 71 | 79 and 83 | 97 and 101 | 103 and 107 ...

Pairs of primes that differ by 4

$2, \underline{3}, 5, \underline{7, 11}, \underline{13, 17}, \underline{19, 23}, 29, 31, \underline{37, 41}, \underline{43, 47},$

$53, 59, 61, \underline{67, 71}, 73, \underline{79, 83}, 89, 97, \ldots$

3 and 7 | 7 and 11 | 13 and 17 | 19 and 23 | 37 and 41 | 43 and 47

67 and 71 | 79 and 83 | 97 and 101 | 103 and 107 . . .

Another twin prime conjecture. *There are infinitely many prime pairs* $p,\ p+4$

Pairs of primes that differ by 6

5 and 11 | 7 and 13 | 11 and 17 | 13 and 19 | 17 and 23

23 and 29 | 31 and 37 | 37 and 43 | 41 and 47 | ...

Yet another twin prime conjecture. *There are infinitely many prime pairs* $p,\ p+6$

Pairs of primes that differ by 10

3 and 13 | 7 and 17 | 13 and 23 | 19 and 29 | 31 and 41

37 and 47 | 43 and 53 | 61 and 71 | 73 and 83 . . . ?

And another twin prime conjecture. *There are infinitely many prime pairs* $p, \; p + 10$

Pairs of primes that differ by 10

3 and 13 | 7 and 17 | 13 and 23 | 19 and 29 | 31 and 41

37 and 47 | 43 and 53 | 61 and 71 | 73 and 83 . . .?

And another twin prime conjecture. *There are infinitely many prime pairs* $p, \ p + 10$

A common generalization?

Generalized twin prime conjecture.
(**De Polignac**, 1849) *For any even integer* h *,
there are infinitely many prime pairs* $p, p + h$ *.*

Generalized twin prime conjecture.
(**De Polignac**, 1849) *For any even integer* h, *there are infinitely many prime pairs* $p, p+h$.

Other patterns?

Generalized twin prime conjecture.
(**De Polignac**, 1849) *For any even integer* h, *there are infinitely many prime pairs* $p, p+h$.

Other patterns? Last digits

$$11, 13, 17 \text{ and } 19 \mid 101, 103, 107 \text{ and } 109$$
$$191, 193, 197 \text{ and } 199 \mid 821, 823, 827 \text{ and } 829, \ldots$$

Generalized twin prime conjecture.
(**De Polignac**, 1849) *For any even integer* h, *there are infinitely many prime pairs* $p, p+h$.

Other patterns? Last digits

$$11, 13, 17 \text{ and } 19 \mid 101, 103, 107 \text{ and } 109$$
$$191, 193, 197 \text{ and } 199 \mid 821, 823, 827 \text{ and } 829, \ldots$$

Prime quadruple Conjecture.
There are infinitely many quadruples of primes
$$10n+1, +3, +7, +9.$$

Generalized twin prime conjecture.
(**De Polignac**, 1849) *For any even integer* h, *there are infinitely many prime pairs* $p, p+h$.

Other patterns? Sophie Germain pairs

Sophie Germain used prime pairs

$$p,\ q := 2p+1$$

Generalized twin prime conjecture. (**De Polignac**, 1849) *For any even integer* h, *there are infinitely many prime pairs* $p, p+h$.

Other patterns? Sophie Germain pairs

Sophie Germain used prime pairs

$$p, \ q := 2p+1$$

2 and 5 | 3 and 7 | 5 and 11 | 11 and 23 | 23 and 47

29 and 59 | 41 and 83 | 53 and 107 | 83 and 167 | . . . ;

Sophie Germain pairs Conjecture. *There are infinitely many prime pairs* $p, 2p+1$

Generalized twin prime conjecture.
(**De Polignac**, 1849) *For any even integer* h , *there are infinitely many prime pairs* $p, p+h$.

Prime quadruple Conjecture.
There are infinitely many quadruples of primes

$$10n+1, +3, +7, +9.$$

Sophie Germain pairs Conjecture. *There are infinitely many prime pairs* $p, 2p+1$

A common generalization?

Question. *Are there infinitely many* ***prime k-tuplets*** $a_1n + b_1, \ldots, a_kn + b_k$?

If so, $a_1x + b_1, \ldots, a_kx + b_k$ is a *Dickson k-tuple*.

Question. *Are there infinitely many* ***prime*** k***-tuplets*** $a_1n + b_1, \ldots, a_kn + b_k$?

If so, $a_1x + b_1, \ldots, a_kx + b_k$ is a *Dickson* k*-tuple*.

Careful!

Question. *Are there infinitely many* ***prime k-tuplets*** $a_1n + b_1, \ldots, a_kn + b_k$ *?*

If so, $a_1x + b_1, \ldots, a_kx + b_k$ is a *Dickson k-tuple*.

Careful!

Prime pairs $p,\ p + 1$?

Question. *Are there infinitely many*
prime k-tuplets $a_1n + b_1, \ldots, a_kn + b_k$?

If so, $a_1x + b_1, \ldots, a_kx + b_k$ is a *Dickson k-tuple*.

Careful!

Prime pairs $p,\ p+1$? Or $p,\ p+h$ with h odd?

$x,\ x+h$ a Dickson 2-tuple $\Longrightarrow$ h even

Question. *Are there infinitely many* ***prime k-tuplets*** $a_1n + b_1, \dots, a_kn + b_k$?

If so, $a_1x + b_1, \dots, a_kx + b_k$ is a *Dickson k-tuple*.

Careful!

Prime pairs $p,\ p + 1$? Or $p,\ p + h$ with h odd?

$x,\ x + h$ a Dickson 2-tuple $\Longrightarrow$ h even

Prime triples?

One of $n, n + 2, n + 4$ is divisible by 3

Question. *Are there infinitely many* ***prime k-tuplets*** $a_1n + b_1, \ldots, a_kn + b_k$ *?*

If so, $a_1x + b_1, \ldots, a_kx + b_k$ is a *Dickson k-tuple*.

Careful!

Prime pairs $p,\ p+1$? Or $p,\ p+h$ with h odd?

$x,\ x+h$ a Dickson 2-tuple $\Longrightarrow$ h even

Prime triples?

One of $n, n+2, n+4$ is divisible by 3

Prime p is an *obstruction* if

p always divides $\mathcal{P}(n) = (a_1n + b_1) \ldots (a_kn + b_k)$

Question. *Are there infinitely many* ***prime k-tuplets*** $a_1n+b_1,\ldots,a_kn+b_k$ *?*

If so, $a_1x+b_1,\ldots,a_kx+b_k$ is a *Dickson k-tuple*.

Prime p is an *obstruction* if
p always divides $\mathcal{P}(n)=(a_1n+b_1)\ldots(a_kn+b_k)$

The set $a_1x+b_1,\ldots,a_kx+b_k$ is *admissible* if there is no obstruction, and all $a_i>0$.

Question. *Are there infinitely many* ***prime k-tuplets*** $a_1n + b_1, \ldots, a_kn + b_k$ *?*

If so, $a_1x + b_1, \ldots, a_kx + b_k$ is a *Dickson k-tuple*.

Prime p is an *obstruction* if
p always divides $\mathcal{P}(n) = (a_1n + b_1) \ldots (a_kn + b_k)$

The set $a_1x + b_1, \ldots, a_kx + b_k$ is *admissible* if there is no obstruction, and all $a_i > 0$.

Dickson's Conjecture. *If* $a_1x + b_1, \ldots, a_kx + b_k$ *is an admissible set then there are infinitely many prime k-tuplets* $a_1n + b_1, \ldots, a_kn + b_k$.

Dickson's Conjecture. *If* $a_1x + b_1, \ldots, a_kx + b_k$ *is an admissible set then there are infinitely many prime* k*-tuplets* $a_1n + b_1, \ldots, a_kn + b_k$.

"An admissible set is a Dickson k-tuple."

Proved by Dirichlet for $k = 1$. Open for $k > 1$.

Dickson's Conjecture. *If* $a_1x + b_1, \ldots, a_kx + b_k$ *is an admissible set then there are infinitely many prime k-tuplets* $a_1n + b_1, \ldots, a_kn + b_k$.

"An admissible set is a Dickson k-tuple."

Proved by Dirichlet for $k = 1$. Open for $k > 1$.

Other patterns?

Dickson's Conjecture. *If* $a_1x + b_1, \ldots, a_kx + b_k$ *is an admissible set then there are infinitely many prime* k*-tuplets* $a_1n + b_1, \ldots, a_kn + b_k$.

"An admissible set is a Dickson k-tuple."

Proved by Dirichlet for $k = 1$. Open for $k > 1$.

Other patterns? Arithmetic progressions

$3, 5, 7 \mid 7, 13, 19 \mid 5, 11, 17, 23, 29 \mid 7, 37, 67, 97, 127, 157$

These are linear forms in two variables:

$$a,\ a + d,\ a + 2d, \ldots, a + (k-1)d$$

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1, \ldots, x_m), \ldots, L_k(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1, \ldots, n_m), \ldots, L_k(n_1, \ldots, n_m).$$

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1, \ldots, x_m), \ldots, L_k(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1, \ldots, n_m), \ldots, L_k(n_1, \ldots, n_m).$$

Recent major breakthrough

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1,\ldots,x_m),\ldots,L_k(x_1,\ldots,x_m)\in\mathbb{Z}[x_1,\ldots,x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1,\ldots,n_m),\ldots,L_k(n_1,\ldots,n_m).$$

Recent major breakthrough

Green & Tao. (2008)
For every k, there are infinitely many k term arithmetic progression of primes

$$a,\ a+d,\ a+2d,\ldots,\ a+(k-1)d$$

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1,\ldots,x_m),\ldots,L_k(x_1,\ldots,x_m)\in\mathbb{Z}[x_1,\ldots,x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1,\ldots,n_m),\ldots,L_k(n_1,\ldots,n_m).$$

Recent major breakthrough

Green & Tao. (2008)
For every k, there are infinitely many k term arithmetic progression of primes

$$a,\ a+d,\ a+2d,\ldots,\ a+(k-1)d$$

The prime k-tuplets conjecture is *almost* resolved

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1, \ldots, x_m), \ldots, L_k(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1, \ldots, n_m), \ldots, L_k(n_1, \ldots, n_m).$$

The prime k-tuplets conjecture is *almost* resolved

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1,\dots,x_m),\dots,L_k(x_1,\dots,x_m)\in\mathbb{Z}[x_1,\dots,x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1,\dots,n_m),\dots,L_k(n_1,\dots,n_m).$$

The prime k-tuplets conjecture is *almost* resolved

Green, Tao & Ziegler. (2012)
Prime k-tuplets conjecture true for any *admissible set of linear forms*, except (perhaps) when *two satisfy a linear equation; e.g. $q-p=2$ and $q-2p=1$.*

The prime k-tuplets conjecture. *For any admissible set of k linear forms in m variables,*

$$L_1(x_1,\ldots,x_m),\ldots,L_k(x_1,\ldots,x_m)\in\mathbb{Z}[x_1,\ldots,x_m],$$

there are infinitely many prime k-tuplets

$$L_1(n_1,\ldots,n_m),\ldots,L_k(n_1,\ldots,n_m).$$

The prime k-tuplets conjecture is *almost* resolved

Green, Tao & Ziegler. (2012)
Prime k-tuplets conjecture true for any *admissible set of linear forms,* except (perhaps) when *two satisfy a linear equation; e.g. $q-p=2$ and $q-2p=1$.*

Only open questions involve two forms in one variable!

Dickson's Conjecture. *If* $a_1x+b_1,\dots,a_kx+b_k$ *is an admissible set then there are infinitely many prime* k*-tuplets* $a_1n+b_1,\dots,a_kn+b_k$.

Spectacular new progress.

Dickson's Conjecture. *If* $a_1x + b_1, \ldots, a_kx + b_k$ *is an admissible set then there are infinitely many prime* k*-tuplets* $a_1n + b_1, \ldots, a_kn + b_k$.

Spectacular new progress.

Yitang Zhang. (2013) *There exists an integer* k *such that: If* $a_1x + b_1, \ldots, a_kx + b_k$ *is an admissible set then* at least two of

$$a_1n + b_1, \ldots, a_kn + b_k$$

are prime, for infinitely many integers n.

Note: Only two of the $a_in + b_i$ are prime, not all.

Yitang Zhang. (2013) *There exists an integer k such that: If $a_1x + b_1, \ldots, a_kx + b_k$ is an admissible set then* at least two of

$$a_1n + b_1, \ldots, a_kn + b_k$$

are prime, for infinitely many integers n.

Let each $a_i = 1$. If $p_1 < \ldots < p_k$ are the k smallest primes $> k$ then $x + p_1, \ldots, x + p_k$ is admissible. By Zhang's Theorem, infinitely many n with two of

$$n + p_1, \ldots, n + p_k$$

prime. This pair of primes differs by

$$\leq p_k - p_1.$$

Yitang Zhang. (2013) *There exists an integer k such that: If $a_1x+b_1,\dots,a_kx+b_k$ is an admissible set then* at least two of $a_1n+b_1,\dots,a_kn+b_k$ *are prime, for infinitely many integers n.*

Corollary. [Bounded gaps between primes]
There exists a bound B such that there are infinitely many pairs of prime numbers

$$p < q \le p+B.$$

Yitang Zhang. (2013) *There exists an integer* k *such that: If* $a_1x+b_1,\ldots,a_kx+b_k$ *is an admissible set then* at least two of $a_1n+b_1,\ldots,a_kn+b_k$ *are prime, for infinitely many integers* n.

Corollary. [Bounded gaps between primes]
There exists a bound B *such that there are infinitely many pairs of prime numbers*

$$p<q\leq p+B.$$

Corollary. [Given gap between primes]
There exists an integer h, $0<h\leq B$ *such that there are infinitely many pairs of primes* $p,p+h$.

Yitang Zhang. (2013) *There exists an integer k such that: If $a_1x+b_1,\dots,a_kx+b_k$ is an admissible set then* at least two of $a_1n+b_1,\dots,a_kn+b_k$ *are prime, for infinitely many integers n.*

Corollary. [Bounded gaps between primes]
There exists a bound B such that there are infinitely many pairs of prime numbers

$$p < q \le p + B.$$

Corollary. [Given gap between primes]
There exists an integer $h, 0 < h \le B$ such that there are infinitely many pairs of primes $p, p+h$.

True for at least $\frac{1}{4}$% of all even integers h.

The records page

Corollary. *There exists an integer k such that if $x+b_1,\dots,x+b_k$ is an admissible set then there are infinitely many prime pairs*

$$p < q \le p + B \quad \text{with} \quad B := b_k - b_1 \; .$$

The records page

Corollary. *There exists an integer k such that if $x+b_1,\ldots,x+b_k$ is an admissible set then there are infinitely many prime pairs*

$$p < q \leq p + B \quad \textit{with} \quad B := b_k - b_1 \ .$$

Apr 2013: **Zhang** $k = 3\,500\,000, \quad B \leq 70\,000\,000$

The records page

Corollary. *There exists an integer k such that if $x+b_1, \ldots, x+b_k$ is an admissible set then there are infinitely many prime pairs*

$$p < q \leq p + B \quad \text{with} \quad B := b_k - b_1 \ .$$

Apr 2013: **Zhang** $k = 3\,500\,000, \quad B \leq 70\,000\,000$

Oct 2013: **Polymath 8a** $k = 632, \quad B = 4\,680$

The records page

Corollary. *There exists an integer k such that if $x+b_1,\dots,x+b_k$ is an admissible set then there are infinitely many prime pairs*

$$p < q \le p+B \quad \text{with} \quad B := b_k - b_1 .$$

Apr 2013: **Zhang** $k = 3\,500\,000, \quad B \le 70\,000\,000$

Oct 2013: **Polymath 8a** $k = 632, \quad B = 4\,680$

Nov 2013: **Maynard** $k = 105, \quad B = 600$

The records page

Corollary. *There exists an integer k such that if $x+b_1,\ldots,x+b_k$ is an admissible set then there are infinitely many prime pairs*

$$p < q \le p + B \quad \text{with} \quad B := b_k - b_1 \,.$$

Apr 2013: **Zhang**	$k = 3\,500\,000, \quad B \le 70\,000\,000$
Oct 2013: **Polymath 8a**	$k = 632, \quad B = 4\,680$
Nov 2013: **Maynard**	$k = 105, \quad B = 600$
Jan 2014: **Polymath 8b**	$k = 55, \quad B = 272$

Corollary. *If* $x + b_1, \ldots, x + b_{55}$ *is an admissible set then there exists* $b_i < b_j$ *such that* $n + b_i,\ n + b_j$ *are a prime pair, infinitely often*

Narrowest admissible 55-*tuple:* Given by $x + \{0, 2, 6, 12, 20, 26, 30, 32, 42, 56, 60, 62, 72, 74, 84, 86, 90, 96, 104, 110, 114, 116, 120, 126, 132, 134, 140, 144, 152, 156, 162, 170, 174, 176, 182, 186, 194, 200, 204, 210, 216, 222, 224, 230, 236, 240, 242, 246, 252, 254, 260, 264, 266, 270, 272\}$

Corollary. *If* $x+b_1,\ldots,x+b_{55}$ *is an admissible set then there exists* $b_i < b_j$ *such that* $n+b_i,\ n+b_j$ *are a prime pair, infinitely often*

Narrowest admissible 55-*tuple:* Given by $x+\{0,2,6,$
$12,20,26,30,32,42,56,60,62,72,74,84,86,90,96,104$
$110,114,116,120,126,132,134,140,144,152,156,162,$
$170,174,176,182,186,194,200,204,210,216,222,224,$
$230,236,240,242,246,252,254,260,264,266,270,272\}$

Most optimistic plan: $k=5$;
Narrowest admissible 5-*tuple:* Given by $x+\{0,2,6,8,12\}$

Infinitely many prime pairs differing by ≤ 12.

Maynard and Tao:
Larger subsets

Yitang Zhang. (2013)
There exists an integer k such that:
If $a_1x + b_1, \ldots, a_kx + b_k$ is an admissible set then at least two *of* $a_1n + b_1, \ldots, a_kn + b_k$ *are prime, for infinitely many integers n.*

Yitang Zhang. (2013)
There exists an integer k such that:
If $a_1x + b_1, \ldots, a_kx + b_k$ is an admissible set then at least two *of* $a_1n + b_1, \ldots, a_kn + b_k$ *are prime, for infinitely many integers n.*

James Maynard / Terry Tao. (2013)
For any $m \geq 2$, there exists $k = k_m$ such that:
If $a_1x + b_1, \ldots, a_kx + b_k$ is an admissible set then at least m of $a_1n + b_1, \ldots, a_kn + b_k$ *are prime, for infinitely many integers n.*

Yitang Zhang. (2013)
There exists an integer k such that:
If $a_1x + b_1, \ldots, a_kx + b_k$ is an admissible set then at least two of $a_1n + b_1, \ldots, a_kn + b_k$ are prime, for infinitely many integers n.

James Maynard / Terry Tao. (2013)
For any $m \geq 2$, there exists $k = k_m$ such that:
If $a_1x + b_1, \ldots, a_kx + b_k$ is an admissible set then at least m of $a_1n + b_1, \ldots, a_kn + b_k$ are prime, for infinitely many integers n.

Can take $k_m \leq ce^{4m}$.

Every admissible k_m-tuple contains a Dickson m-tuple

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Consequences of the Maynard/Tao Theorem

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Consequences of the Maynard/Tao Theorem

Bounded intervals with m primes. *There are infinitely many intervals $[x, x + B_m]$ which contain (exactly) m prime numbers (with $B_m \leq cm^3 e^{4m}$).*

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Consequences of the Maynard/Tao Theorem

Bounded intervals with m primes. *There are infinitely many intervals $[x, x + B_m]$ which contain (exactly) m prime numbers (with $B_m \leq cm^3e^{4m}$).*

In a given $a \pmod q$ with $(a, q) = 1$. *There are infinitely many intervals $[x, x + qB_m]$ which contain exactly m prime numbers, each $\equiv a \pmod q$.*

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Consequences of the Maynard/Tao Theorem

Bounded intervals with m primes. *There are infinitely many intervals $[x, x+B_m]$ which contain (exactly) m prime numbers (with $B_m \leq cm^3e^{4m}$).*

In a given $a \pmod q$ with $(a,q)=1$. *There are infinitely many intervals $[x, x+qB_m]$ which contain exactly m prime numbers, each $\equiv a \pmod q$.*

A positive proportion of admissible m-tuples, are Dickson m-tuples.

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Erdős-type consequences of the Maynard/Tao Theorem

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Erdős-type consequences of the Maynard/Tao Theorem

$17610001\underline{1}1,\ 176100\underline{1}01,\ 17610\underline{1}001,\ 1761\underline{1}0001$ are primes

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Erdős-type consequences of the Maynard/Tao Theorem

Sets of m primes; each pair differ in two digits

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Erdős-type consequences of the Maynard/Tao Theorem

Sets of m primes; each pair differ in two digits

Let $d_n = p_{n+1} - p_n$ with p_n, the nth smallest prime.

- Infinitely many n for which $d_n < d_{n+1} < \ldots < d_{n+m}$.
- Infinitely many n for which $d_n > d_{n+1} > \ldots > d_{n+m}$.

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple*

Erdős-type consequences of the Maynard/Tao Theorem

Sets of m primes; each pair differ in two digits

Let $d_n = p_{n+1} - p_n$ with p_n, the nth smallest prime.

- Infinitely many n for which $d_n < d_{n+1} < \ldots < d_{n+m}$.
- Infinitely many n for which $d_n > d_{n+1} > \ldots > d_{n+m}$.
- Infinitely many n for which $d_n \mid d_{n+1} \mid \ldots \mid d_{n+m}$.

Gaps between primes (History)

1792/3: Young Gauss. Tables of primes up to 10^6.

1792/3: Young Gauss. Tables of primes up to 10^6.

Density of primes around x is $\approx \dfrac{1}{\log x}$

1792/3: Young Gauss. Tables of primes up to 10^6.

Density of primes around x is $\approx \dfrac{1}{\log x}$

This suggests

Average gap between primes around x is $\approx \log x$.

1792/3: Young Gauss. Tables of primes up to 10^6.

Density of primes around x is $\approx \frac{1}{\log x}$

This suggests

Average gap between primes around x is $\approx \log x$.

Also

$$\#\{\text{primes } \leq x\} \approx \int_2^x \frac{dt}{\log t} \approx \frac{x}{\log x}$$

The *Prime Number Theorem* (PNT, 1896).

Average gap between primes $\leq x$ is $\approx \log x$.

Average gap between primes $\leq x$ is $\approx \log x$.

> **Question.** *Fix $c > 0$. Prove there are infinitely many pairs of primes $p < q$ with $q < p + c \log p$*

$c > 1$ by PNT. Any $c \leq 1$ is difficult.

Average gap between primes $\leq x$ is $\approx \log x$.

Question. *Fix $c > 0$. Prove there are infinitely many pairs of primes $p < q$ with $q < p + c \log p$*

$c > 1$ by PNT. Any $c \leq 1$ is difficult.

Conditional

1926 **Hardy, Littlewood**. Any $c > \frac{2}{3}$ *assuming* GRH

Average gap between primes $\leq x$ is $\approx \log x$.

Question. *Fix $c > 0$. Prove there are infinitely many pairs of primes $p < q$ with $q < p + c \log p$*

$c > 1$ by PNT. Any $c \leq 1$ is difficult.

Conditional

1926 **Hardy, Littlewood**. Any $c > \frac{2}{3}$ *assuming* GRH

Unconditional

1940 **Erdős**. Some $c < 1$ using "small sieve"

1966 **Bombieri & Davenport**. Any $c \geq \frac{1}{2}$ using large sieve (for GRH).

1988 **Maier**. Any $c \geq \frac{1}{4}$, using combo of techniques

Average gap between primes $\le x$ is $\approx \log x$.

Question. *Fix $c > 0$. Prove there are infinitely many pairs of primes $p < q$ with $q < p + c \log p$*

$c > 1$ by PNT. Any $c \le 1$ is difficult.

Conditional

1926 **Hardy, Littlewood**. Any $c > \frac{2}{3}$ *assuming* GRH

Unconditional

1940 **Erdős**. Some $c < 1$ using "small sieve"

1966 **Bombieri & Davenport**. Any $c \ge \frac{1}{2}$ using large sieve (for GRH).

1988 **Maier**. Any $c \ge \frac{1}{4}$, using combo of techniques

2005 **Goldston, Pintz, Yıldırım** (GPY) Any $c > 0$.

$$q - p < (\log p)^{1/2+\epsilon}.$$

Average gap between primes $\leq x$ is $\approx \log x$.

Question. *Fix $c > 0$. Prove there are infinitely many pairs of primes $p < q$ with $q < p + c \log p$*

$c > 1$ by PNT. Any $c \leq 1$ is difficult.

Conditional

1926 **Hardy, Littlewood**. Any $c > \frac{2}{3}$ *assuming* GRH

Unconditional

1940 **Erdős**. Some $c < 1$ using “small sieve”

1966 **Bombieri & Davenport**. Any $c \geq \frac{1}{2}$ using large sieve (for GRH).

1988 **Maier**. Any $c \geq \frac{1}{4}$, using combo of techniques

2005 **Goldston, Pintz, Yıldırım** (GPY) Any $c > 0$.

$$q - p < (\log p)^{1/2+\epsilon}.$$

2014 **(ZMT & polymath8)** $q - p \leq 272$

Primes in arithmetic progressions

GRH and the large sieve

Riemann Hypothesis (RH)

"=" precise estimates for $\#\{\text{ primes } p \leq x\}$.

Generalized Riemann Hypothesis (GRH)

"=" precise estimates for

$$\#\{\text{ primes } p \leq x,\ p \equiv a \pmod q\}\ .$$

GRH and the large sieve

Riemann Hypothesis (RH)

"=" precise estimates for $\#\{\text{ primes } p \le x\}$.

Generalized Riemann Hypothesis (GRH)

"=" precise estimates for

$$\#\{\text{ primes } p \le x,\ p \equiv a \pmod q\}\ .$$

The large sieve, the *Bombieri-Vinogradov Theorem* (BV)

A statistical approximation to GRH

GRH and the large sieve

Riemann Hypothesis (RH)

“=” precise estimates for $\#\{\text{ primes } p \leq x\}$.

Generalized Riemann Hypothesis (GRH)

“=” precise estimates for

$$\#\{\text{ primes } p \leq x,\ p \equiv a \pmod q\}\ .$$

The large sieve, the *Bombieri-Vinogradov Theorem* (BV)

A statistical approximation to GRH

How do primes in arithmetic progression tell us about primes in short intervals?

GRH and the large sieve

Riemann Hypothesis (RH)

"=" precise estimates for $\#\{\text{ primes } p \le x\}$.

Generalized Riemann Hypothesis (GRH)

"=" precise estimates for

$$\#\{\text{ primes } p \le x,\ p \equiv a \pmod q\}\ .$$

The large sieve, the *Bombieri-Vinogradov Theorem* (BV)

A statistical approximation to GRH

How do primes in arithmetic progression tell us about primes in short intervals?

Yitang Zhang pushed BV beyond a key barrier.

A great result about primes in arithmetic progressions.

When is $qx + a$ prime?

Obstructions: Prime divisors of (a, q)

When is $qx + a$ prime?

Obstructions: Prime divisors of (a, q)

$11,\ 31,\ 41,\ 61,\ 71,\ 101,\ 131,\ 151,\ 181, \ldots$

$3,\ 13,\ 23,\ 43,\ 53,\ 73,\ 83,\ 103,\ 113,\ 163,\ 173,\ 193 \ldots$

$7,\ 17,\ 37,\ 47,\ 67,\ 97,\ 107,\ 127,\ 137,\ 157,\ 167,\ 197 \ldots$

$19,\ 29,\ 59,\ 79,\ 89,\ 109,\ 139,\ 149,\ 179,\ 199 \ldots$

When is $qx + a$ prime?

Obstructions: Prime divisors of (a, q)

1837 **Dirichlet**. Inf many $p \equiv a \pmod{q}$ if $(a, q) = 1$.

When is $qx + a$ prime?

Obstructions: Prime divisors of (a, q)

1837 **Dirichlet**. Inf many $p \equiv a \pmod q$ if $(a, q) = 1$.

Roughly equal numbers in each such progression:

$$\#\left\{ \begin{matrix} \text{primes } p \le x \\ p \equiv a \pmod q \end{matrix} \right\} \sim \frac{\#\{\text{primes } p \le x\}}{\#\{a \pmod q : \ (a, q) = 1\}}$$

Prime number theorem for arithmetic progressions

Euler studied $\phi(q) := \#\{a \pmod q : \ (a, q) = 1\}$

Primes and the Mőbius function

Recognizing primes

Mőbius fn, essentially $\mu(n) = (-1)^{\#\{\text{prime factors of } n\}}$

Recognizing primes

Mőbius fn, essentially $\mu(n) = (-1)^{\#\{\text{prime factors of } n\}}$

Equal numbers of -1 and 1? i.e.

$$\frac{1}{x}\sum_{n\le x}\mu(n) \to 0 \quad \text{as} \quad n \to \infty \ ?$$

Recognizing primes

Mőbius fn, essentially $\mu(n) = (-1)^{\#\{\text{prime factors of } n\}}$

Equal numbers of -1 and 1? i.e.

$$\frac{1}{x} \sum_{n \leq x} \mu(n) \to 0 \quad \text{as} \quad n \to \infty \ ?$$

Equivalent to PNT!

Recognizing primes

Mőbius fn, essentially $\mu(n) = (-1)^{\#\{\text{prime factors of } n\}}$

Equal numbers of -1 and 1? i.e.

$$\frac{1}{x}\sum_{n\le x}\mu(n) \to 0 \quad \text{as} \quad n \to \infty \ ?$$

Equivalent to PNT! Recognize primes using

$$(\mu * \log)(n) = \begin{cases} \log p & n = p^m, \quad p \text{ prime}, m \ge 1; \\ 0 & \text{otherwise.} \end{cases}$$

where *convolution* $(\alpha * \beta)(n) = \sum_{d|n} \alpha(d)\beta(n/d).$

Recognizing prime k-tuples

Just saw

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

Recognizing prime k-tuples

Just saw

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

Let

$$\mathcal{P}(n) = (n + a_1)(n + a_2) \dots (n + a_k).$$

1956 Golomb's identity: If $n \geq a_1 \dots a_k$ then

$$(\mu * \frac{\log^k}{k!})(\mathcal{P}(n)) = \begin{cases} \prod_{i=1}^k \log p_i & \text{if } \mathcal{P}(n) = \prod_{i=1}^k p_i^{m_i}; \\ 0 & \text{otherwise.} \end{cases}$$

This formula allows us to recognize prime k-tuples

The argument of Goldston, Pintz and Yıldırım

GPY: The set up

Given admissible $a_1 < a_2 < \ldots < a_k$. Select weights $w(n) \geq 0$ for all n, such that

$$\sum_{x<n\leq 2x} w(n) \# \left\{ \begin{matrix} i \in \{1,\ldots,k\} \\ n + a_i \text{ is prime} \end{matrix} \right\} \Big/ \sum_{x<n\leq 2x} w(n) > h,$$

with h an integer ≥ 1.

GPY: The set up

Given admissible $a_1 < a_2 < \ldots < a_k$. Select weights $w(n) \geq 0$ for all n, such that

$$\sum_{x<n\leq 2x} w(n)\#\left\{ \begin{matrix} i \in \{1,\ldots,k\} \\ n+a_i \text{ is prime} \end{matrix} \right\} \Big/ \sum_{x<n\leq 2x} w(n) > h,$$

with h an integer ≥ 1. If so there exists $n \in [x, 2x]$,

$$\#\left\{ \begin{matrix} i \in \{1,\ldots,k\} \\ n+a_i \text{ is prime} \end{matrix} \right\} > h.$$

GPY: The set up

Given admissible $a_1 < a_2 < \ldots < a_k$. Select weights $w(n) \geq 0$ for all n, such that

$$\sum_{x<n\leq 2x} w(n)\# \left\{ \begin{array}{c} i \in \{1,\ldots,k\} \\ n+a_i \text{ is prime} \end{array} \right\} \Big/ \sum_{x<n\leq 2x} w(n) > h,$$

with h an integer ≥ 1. If so there exists $n \in [x, 2x]$,

$$\# \left\{ \begin{array}{c} i \in \{1,\ldots,k\} \\ n+a_i \text{ is prime} \end{array} \right\} > h.$$

That is $\geq m := h+1$ primes among $n+a_1, \ldots, n+a_k$

To prove m primes in an admissible k-tuple

$$\sum_{i=1}^{k} \sum_{\substack{x<n\le 2x \\ n+a_i \text{ is prime}}} w(n) > h \sum_{x<n\le 2x} w(n).$$

To prove m primes in an admissible k-tuple

$$\sum_{i=1}^{k} \sum_{\substack{x<n\le 2x \\ n+a_i \text{ is prime}}} w(n) > h \sum_{x<n\le 2x} w(n).$$

Try $w(n) := \left(\sum_{d|\mathcal{P}(n)} \lambda(d) \right)^2$,

sum over d dividing $\mathcal{P}(n) = (n+a_1)\dots(n+a_k).$

To prove m primes in an admissible k-tuple

$$\sum_{i=1}^{k} \sum_{\substack{x<n\le 2x \\ n+a_i \text{ is prime}}} w(n) > h \sum_{x<n\le 2x} w(n).$$

Try $w(n) := \left(\sum_{d|\mathcal{P}(n)} \lambda(d) \right)^2,$

sum over d dividing $\mathcal{P}(n) = (n+a_1)\dots(n+a_k).$

$$\sum_{x<n\le 2x} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\le 2x \\ d_1,d_2|\mathcal{P}(n)}} 1$$

$$\sum_{x<n\le 2x} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\le 2x \\ d_1,d_2|\mathcal{P}(n)}} 1$$

d_1 and d_2 both divide $\mathcal{P}(n)$

if and only

D divides $\mathcal{P}(n)$ where $D = \mathrm{lcm}[d_1, d_2]$

if and only

n is in one of several arithmetic progressions mod D.

$$\sum_{x<n\leq 2x} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\leq 2x \\ d_1,d_2|\mathcal{P}(n)}} 1$$

d_1 and d_2 both divide $\mathcal{P}(n)$

if and only

D divides $\mathcal{P}(n)$ where $D = \text{lcm}[d_1, d_2]$

if and only

n is in one of several arithmetic progressions mod D.

$$\frac{x}{D} - 1 < \#\{x < n \leq 2x : \ n \equiv b \pmod{D}\} < \frac{x}{D} + 1$$

$$\sum_{x<n\leq 2x} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\leq 2x \\ d_1,d_2|\mathcal{P}(n)}} 1$$

d_1 and d_2 both divide $\mathcal{P}(n)$

if and only

D divides $\mathcal{P}(n)$ where $D = \text{lcm}[d_1, d_2]$

if and only

n is in one of several arithmetic progressions mod D.

$$\frac{x}{D} - 1 < \#\{x < n \leq 2x : \; n \equiv b \pmod{D}\} < \frac{x}{D} + 1$$

Roughly $\dfrac{x}{D}$ in each a.p. if $D < x^{1-\epsilon}$.

$$\sum_{x<n\leq 2x} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\leq 2x \\ d_1,d_2|\mathcal{P}(n)}} 1$$

d_1 and d_2 both divide $\mathcal{P}(n)$

if and only

D divides $\mathcal{P}(n)$ where $D = \mathrm{lcm}[d_1, d_2]$

if and only

n is in one of several arithmetic progressions mod D.

$$\frac{x}{D} - 1 < \#\{x < n \leq 2x : \ n \equiv b \pmod{D}\} < \frac{x}{D} + 1$$

Roughly $\frac{x}{D}$ in each a.p. if $D < x^{1-\epsilon}$.

Often $D := [d_1, d_2] \approx d_1 d_2$, so need all $d < x^{1/2-\epsilon}$.

The sums on the left-hand side are of the form

$$\sum_{\substack{x<n\le 2x \\ n+a \text{ is prime}}} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\le 2x \\ n+a \text{ is prime} \\ d_1,d_2|\mathcal{P}(n)}} 1$$

This last sum is a sum over several values of b of

$$\#\{x < n \le 2x : \ n \equiv b \pmod{D} \text{ and } n \text{ prime}\}$$

for various b with $(b, D) = 1$.

The sums on the left-hand side are of the form

$$\sum_{\substack{x<n\le 2x \\ n+a \text{ is prime}}} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\le 2x \\ n+a \text{ is prime} \\ d_1,d_2|\mathcal{P}(n)}} 1$$

This last sum is a sum over several values of b of

$$\#\{x < n \le 2x : \ n \equiv b \pmod{D} \text{ and } n \text{ prime}\}$$

for various b with $(b, D) = 1$. We expect roughly

$$\frac{\#\{p \text{ prime} : \ x < p \le 2x\}}{\phi(D)}$$

The sums on the left-hand side are of the form

$$\sum_{\substack{x<n\le 2x \\ n+a \text{ is prime}}} w(n) = \sum_{d_1,d_2} \lambda(d_1)\lambda(d_2) \sum_{\substack{x<n\le 2x \\ n+a \text{ is prime} \\ d_1,d_2|\mathcal{P}(n)}} 1$$

This last sum is a sum over several values of b of

$$\#\{x < n \le 2x : \ n \equiv b \pmod{D} \text{ and } n \text{ prime}\}$$

for various b with $(b, D) = 1$. We expect roughly

$$\frac{\#\{p \text{ prime} : \ x < p \le 2x\}}{\phi(D)}$$

Key issue: For what D? Assume for $D < x^{\theta},\ 0 < \theta < 1,$

and so $\lambda(d) \ne 0$ only for $d < R := x^{\theta/2}.$

We select the weights to be of the form

$$\lambda(d) := \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(t)$ is a certain fn of $F(t)$, measurable, bounded, supported only on $[0, 1]$.

We select the weights to be of the form

$$\lambda(d) := \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(t)$ is a certain fn of $F(t)$, measurable, bounded, supported only on $[0, 1]$. The desired inequality

$$\sum_{i=1}^{k} \sum_{\substack{x<n\leq 2x \\ n+a_i \text{ is prime}}} w(n) > h \sum_{x<n\leq 2x} w(n)$$

is then equivalent to

$$\frac{\theta}{2}\,\rho_k(F) > h$$

where

$$\rho_k(F) := \frac{k\int_0^1 \left(\int_t^1 F(u)du\right)^2 \frac{t^{k-2}}{(k-2)!}dt}{\int_0^1 F(t)^2 \frac{t^{k-1}}{(k-1)!}dt}.$$

Two primes in an admissible k-tuple

We need

$$\frac{\theta}{2}\,\rho_k(F) > 1$$

Two primes in an admissible k-tuple

We need

$$\frac{\theta}{2}\,\rho_k(F) > 1$$

It can be shown that

$$4 - \frac{8}{\sqrt{k}} < \max_F \rho_k(F) < 4.$$

Two primes in an admissible k-tuple

We need

$$\frac{\theta}{2}\,\rho_k(F) > 1$$

It can be shown that

$$4 - \frac{8}{\sqrt{k}} < \max_F \rho_k(F) < 4.$$

So to make above inequality work we need that

$$\text{there is some } \theta > \frac{1}{2}$$

for which

$$\#\left\{\begin{matrix}\text{primes } x < p \le 2x \\ p \equiv b \pmod{D}\end{matrix}\right\} \approx \frac{\#\{\text{primes } x < p \le 2x\}}{\phi(D)}?$$

is true for $(b, D) = 1$ for "most" $D < x^{\theta}.$

Uniformity of distribution: Primes in Arithmetic Progressions

How big must x be (in terms of D) for

$$\#\left\{\begin{matrix} \text{primes } x < p \le 2x \\ p \equiv b \pmod{D} \end{matrix}\right\} \approx \frac{\#\{\text{primes } x < p \le 2x\}}{\phi(D)} ?$$

How big must x be (in terms of D) for

$$\#\left\{\begin{matrix} \text{primes } x < p \le 2x \\ p \equiv b \pmod{D} \end{matrix}\right\} \approx \frac{\#\{\text{primes } x < p \le 2x\}}{\phi(D)}?$$

Calculations: True for $x \ge D^{1+\epsilon}$; i.e. $D \le x^{1-\epsilon}$.

How big must x be (in terms of D) for

$$\#\left\{\begin{matrix} \text{primes } x < p \le 2x \\ p \equiv b \pmod{D} \end{matrix}\right\} \approx \frac{\#\{\text{primes } x < p \le 2x\}}{\phi(D)} ?$$

Calculations: True for $x \ge D^{1+\epsilon}$; i.e. $D \le x^{1-\epsilon}$.

GRH: True for $D \le x^{\frac{1}{2}-\epsilon}$.

How big must x be (in terms of D) for

$$\#\left\{\begin{matrix} \text{primes } x < p \le 2x \\ p \equiv b \pmod{D} \end{matrix}\right\} \approx \frac{\#\{\text{primes } x < p \le 2x\}}{\phi(D)}?$$

Calculations: True for $x \ge D^{1+\epsilon}$; i.e. $D \le x^{1-\epsilon}$.
GRH: True for $D \le x^{\frac{1}{2}-\epsilon}$.

The Bombieri-Vinogradov Theorem. True for *almost all* $D \le x^{1/2-\epsilon}$.

How big must x be (in terms of D) for

$$\#\left\{\begin{matrix} \text{primes } x < p \le 2x \\ p \equiv b \pmod{D} \end{matrix}\right\} \approx \frac{\#\{\text{primes } x < p \le 2x\}}{\phi(D)} ?$$

Calculations: True for $x \ge D^{1+\epsilon}$; i.e. $D \le x^{1-\epsilon}$.
GRH: True for $D \le x^{\frac{1}{2}-\epsilon}$.

The Bombieri-Vinogradov Theorem. True for *almost all* $D \le x^{1/2-\epsilon}$.
Let $\Delta(x; D, a)$ be the difference above.

Bombieri-Vinogradov. (1965) *For any* $A > 0$

$$\sum_{D \le x^{\frac{1}{2}-\epsilon}} \max_{\substack{a \mod D \\ (a,D)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

"Trivial" bound is $\ll x$.

Bombieri-Vinogradov. (1965) *For any* $\theta < \frac{1}{2}$, *and* $A > 0$

$$\sum_{D \leq x^\theta} \max_{\substack{a \mod D \\ (a,D)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

Bombieri-Vinogradov. (1965) *For any* $\theta < \frac{1}{2}$, *and* $A > 0$

$$\sum_{D \leq x^\theta} \max_{\substack{a \mod D \\ (a,D)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

GPY argument works if we can take some $\theta > \frac{1}{2}$.

Bombieri-Vinogradov. (1965) *For any* $\theta < \frac{1}{2}$, *and* $A > 0$

$$\sum_{D \leq x^\theta} \max_{\substack{a \mod D \\ (a,D)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

GPY argument works if we can take some $\theta > \frac{1}{2}$.

This is a famous conjecture.

Bombieri-Vinogradov. (1965) *For any* $\theta < \frac{1}{2}$, *and* $A > 0$

$$\sum_{D \leq x^\theta} \max_{\substack{a \mod D \\ (a,D)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

GPY argument works if we can take some $\theta > \frac{1}{2}$.
This is a famous conjecture. Much important work by **Bombieri, Fouvry, Friedlander and Iwaniec,** in last 25 years: Results with $\theta > \frac{1}{2}$ *but* with a fixed and bounded, and not large A.

Bombieri-Vinogradov. (1965) *For any* $\theta < \frac{1}{2}$, *and* $A > 0$

$$\sum_{D \leq x^\theta} \max_{\substack{a \bmod D \\ (a,D)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

GPY argument works if we can take some $\theta > \frac{1}{2}$.
This is a famous conjecture. Much important work by **Bombieri, Fouvry, Friedlander and Iwaniec,** in last 25 years: Results with $\theta > \frac{1}{2}$ *but* with a fixed and bounded, and not large A.

Restricted D-values to those that are "easily factored".

y-smooth: integers whose prime factors are all $\leq y$.
Zhang: Such a result, D restricted to y-smooth integers

Yitang Zhang. (2013) *For exists* $\theta > \frac{1}{2}$, $\delta > 0$ *such that for any* $A > 0$ *and* any *non-zero integer* a,

$$\sum_{\substack{D \le x^\theta \\ D \text{ is } x^\delta\text{-smooth} \\ (D,a)=1}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$$

Can take $$\theta - \frac{1}{2} = \delta = \frac{1}{300}.$$

GPY – Higher dimensional analysis

Changing the weights

The weights above were the square of

$$\sum_{d|\mathcal{P}(n)} \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(.)$ measurable, bounded, supported only on $[0,1]$.
Here we sum over divisors d of $(n+a_1)\dots(n+a_k)$.

Changing the weights

The weights above were the square of

$$\sum_{d|\mathcal{P}(n)} \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(.)$ measurable, bounded, supported only on $[0,1]$.
Here we sum over divisors d of $(n+a_1)\dots(n+a_k)$.
Such a term is a sum, over all factorizations

$$d = d_1 d_2 \dots d_k,$$

where d_j divides $n+a_j$ for each j.

Changing the weights

The weights above were the square of

$$\sum_{d|\mathcal{P}(n)} \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(.)$ measurable, bounded, supported only on $[0,1]$.
Here we sum over divisors d of $(n+a_1)\dots(n+a_k)$.
Such a term is a sum, over all factorizations

$$d = d_1 d_2 \dots d_k,$$

where d_j divides $n+a_j$ for each j.

Maynard/Tao Weights depending on $d_1, \dots, d_k$?

Maynard/Tao: Replace

$$\sum_{d|\mathcal{P}(n)} \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(t)$ is supported only on $[0,1]$, by

$$\sum_{\substack{d_1|n+a_1 \\ \vdots \\ d_k|n+a_k}} \mu(d_1)\ldots\mu(d_k) g\left(\frac{\log d_1}{\log R},\ldots,\frac{\log d_k}{\log R}\right)$$

where $g(t_1,\ldots,t_k)$ is supported only on

$$t_1,\ldots,t_k \geq 0 \text{ and } \ t_1+\ldots+t_k \leq 1$$

Maynard/Tao: Replace

$$\sum_{d|\mathcal{P}(n)} \mu(d) G\left(\frac{\log d}{\log R}\right),$$

where $G(t)$ is supported only on $[0,1]$, by

$$\sum_{\substack{d_1|n+a_1\\ \dots \\ d_k|n+a_k}} \mu(d_1)\dots\mu(d_k) g\left(\frac{\log d_1}{\log R}, \dots, \frac{\log d_k}{\log R}\right)$$

where $g(t_1,\dots,t_k)$ is supported only on

$$t_1,\dots,t_k \geq 0 \text{ and } \; t_1+\dots+t_k \leq 1$$

Same as original GPY construction only if

$$g(t_1,\dots,t_k) = G(t_1+\dots+t_k)$$

Finding a positive difference

The inequality

$$\sum_{i=1}^{k} \sum_{\substack{x<n\leq 2x \\ n+a_i \text{ is prime}}} w(n) > h \sum_{x<n\leq 2x} w(n)$$

is then equivalent to

$$\frac{\theta}{2}\,\rho(F) > h$$

where

$$\rho(F) := \frac{\sum_{j=1}^{k} \int^{*\ j}_{t_1,\ldots,t_k\geq 0} \left(\int_{t_j\geq 0} F(t_1,\ldots,t_k)dt_j\right)^2 \, dt_k \ldots dt_1}{\int_{t_1,\ldots,t_k\geq 0} F(t_1,\ldots,t_k)^2 \, dt_k \ldots dt_1}$$

Choosing F (Maynard)

$$F(t_1, \ldots, t_5) = 70P_1P_2 - 49P_1^2 - 75P_2 + 83P_1 - 34.$$

where $P_m := t_1^m + \ldots + t_k^m$. A calculation yields that

$$\rho(F) = \frac{1417255}{708216} > 2.$$

Therefore, if θ is close to 1 then we can take $k = 5$.

Choosing F (Maynard)

$$F(t_1, \dots, t_5) = 70P_1P_2 - 49P_1^2 - 75P_2 + 83P_1 - 34.$$

where $P_m := t_1^m + \dots + t_k^m$. A calculation yields that

$$\rho(F) = \frac{1417255}{708216} > 2.$$

Therefore, if θ is close to 1 then we can take $k = 5$.

Unconditionally, there is an F of the form

$$\sum_{\substack{a,b \geq 0 \\ a+2b \leq 11}} c_{a,b}(1 - P_1)^a P_2^b$$

with $k = 105$, for which $\rho(F) = 4.0020697\dots$ so ok with θ a little less than $\frac{1}{2}$.

Maynard/Tao Theorem

$$F(t_1, \ldots t_k) = \begin{cases} g(kt_1)\ldots g(kt_k) & \text{if } t_1 + \ldots + t_k \leq 1, \\ 0 & \text{otherwise,} \end{cases}$$

where

$$g(t) = \frac{1}{1 + At} \quad \text{for} \quad 0 \leq t \leq T.$$

Optimizing choice of A and T we have

$$\max_k \rho(F) = \log k + O(1).$$

Maynard/Tao Theorem

$$F(t_1, \ldots t_k) = \begin{cases} g(kt_1) \ldots g(kt_k) & \text{if } t_1 + \ldots + t_k \leq 1, \\ 0 & \text{otherwise,} \end{cases}$$

where

$$g(t) = \frac{1}{1 + At} \quad \text{for} \quad 0 \leq t \leq T.$$

Optimizing choice of A and T we have

$$\max_k \rho(F) = \log k + O(1).$$

Hence $\rho(F) > 4m$ provided $k < ce^{4m}$.

Maynard/Tao. (2013) *Every admissible k_m-tuple contains a Dickson m-tuple, for some $k_m < ce^{4m}$*

Breaking the $\sqrt{x}$-barrier
The work of Yitang Zhang

General sequences in arithmetic progression

The large sieve shows that all (non-sparse) subsets of $\{1,\ldots,x\}$ are well-distributed in "most" arithmetic progressions with modulus $\le \sqrt{x}$:

$B \subset \{1,\ldots,x\}$, and

$$\Delta(B;q,a) := \#\left\{\begin{matrix} b\in B \\ b\equiv a \pmod q\end{matrix}\right\} - \left\{\begin{matrix}\text{Expected, given} \\ B \pmod r,\ r<q\end{matrix}\right\}$$

General sequences in arithmetic progression

The large sieve shows that all (non-sparse) subsets of $\{1,\ldots,x\}$ are well-distributed in "most" arithmetic progressions with modulus $\le \sqrt{x}$:

$B \subset \{1,\ldots,x\}$, and

$$\Delta(B;q,a) := \#\left\{ \begin{array}{c} b \in B \\ b \equiv a \pmod q \end{array} \right\} - \left\{ \begin{array}{c} \text{Expected, given} \\ B \pmod r,\ r < q \end{array} \right\}$$

Example: $B = \{n \le x : \ n \text{ even}\}.$

General sequences in arithmetic progression

The large sieve shows that all (non-sparse) subsets of $\{1, \ldots, x\}$ are well-distributed in "most" arithmetic progressions with modulus $\leq \sqrt{x}$:

$B \subset \{1, \ldots, x\}$, and

$$\Delta(B; q, a) := \#\left\{ \begin{array}{c} b \in B \\ b \equiv a \pmod q \end{array} \right\} - \left\{ \begin{array}{c} \text{Expected, given} \\ B \pmod r,\ r < q \end{array} \right\}$$

Example: $B = \{n \leq x : \ n \text{ even}\}.$

Then **the large sieve** implies the strong bound

$$\sum_{q \leq x^{\frac{1}{2}}} q \sum_{a:\ (a,q)=1} |\Delta(B; q, a)|^2 \leq 2x\#B$$

Example gives upper bound, up to the constant.

General sequences in arithmetic progression

$$\sum_{q \le x^{\frac{1}{2}}} q \sum_{a:\ (a,q)=1} |\Delta(B; q, a)|^2 \le 2x\#B$$

Need for given $a \pmod q$, or worst case, not “average”.

General sequences in arithmetic progression

$$\sum_{q \le x^{\frac{1}{2}}} q \sum_{a:\ (a,q)=1} |\Delta(B; q, a)|^2 \le 2x\#B$$

Need for given $a \pmod q$, or worst case, not "average".

Bombieri, Friedlander and Iwaniec. (1986) *Assume good distribution for small moduli:*

$$|\Delta(\beta; q, a)| \ll_A \frac{\|\beta\| x^{\frac{1}{2}}}{(\log x)^A},$$

For any $A > 0$,

$$\sum_{q \le x^{1/2-\epsilon}} \max_{a:\ (a,q)=1} |\Delta(\alpha * \beta; q, a)| \ll \|\alpha\| \|\beta\| \frac{x^{1/2}}{(\log x)^A}$$

where

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(d)\beta(n/d).$$

Bombieri, Friedlander and Iwaniec. (1986) *Assume good distn for small moduli: If* $(a,q)=1$

$$|\Delta(\beta;q,a)| \ll_A \frac{\|\beta\| x^{\frac{1}{2}}}{(\log x)^A},$$

For any $A>0$,

$$\sum_{q\le x^{1/2-\epsilon}} \max_{a:\ (a,q)=1} |\Delta(\alpha*\beta;q,a)| \ll \|\alpha\|\|\beta\| \frac{x^{1/2}}{(\log x)^A}.$$

Remember: $(\mu * \log)$ recognizes prime powers.

BFI $\Longrightarrow$ Bombieri-Vinogradov theorem for primes.

Conjecture. *Assume good distn for small moduli,*

$$\sum_{q \le x^\theta} \max_{a:\ (a,q)=1} |\Delta(\alpha * \beta; q, a)| \ll \|\alpha\| \|\beta\| \frac{x^{1/2}}{(\log x)^A}.$$

for any $\theta < 1$.

Conjecture. *Assume good distn for small moduli,*

$$\sum_{q \le x^\theta} \max_{a:\ (a,q)=1} |\Delta(\alpha * \beta; q, a)| \ll \|\alpha\| \|\beta\| \frac{x^{1/2}}{(\log x)^A}.$$

for any $\theta < 1$.

Yitang Zhang / polymath 8a. (2013) *Assume*

α *and* β *are only supported in* $[x^{1/3}, x^{2/3}]$,

$|\alpha(n)|, |\beta(n)| \le c(\tau(n)\log n)^B$

$\exists\ \theta > \frac{1}{2},\ \delta > 0$ *s.t. for any* $A > 0$ *and* $a \ne 0$,

$$\sum_{\substack{q \le x^\theta \\ q \text{ is } x^\delta\text{-smooth} \\ (q,a)=1}} |\Delta(\alpha * \beta; q, a)| \ll \frac{x}{(\log x)^A}$$

How does one prove

$$\sum_{\substack{q \leq x^\theta \\ q \text{ is } x^\delta\text{-smooth} \\ (q,a)=1}} |\Delta(\alpha * \beta; q, a)| \ll \frac{x}{(\log x)^A} \quad ?$$

And how do techniques work for arbitrary seqs α and β?

How does one prove

$$\sum_{\substack{q \leq x^\theta \\ q \text{ is } x^\delta\text{−smooth} \\ (q,a)=1}} |\Delta(\alpha * \beta; q, a)| \ll \frac{x}{(\log x)^A} \quad ?$$

And how do techniques work for arbitrary seqs α and β?
May assume $q > x^{1/2-\epsilon}$ by **BFI**.

How does one prove

$$\sum_{\substack{q \le x^\theta \\ q \text{ is } x^\delta-\text{smooth} \\ (q,a)=1}} |\Delta(\alpha * \beta; q, a)| \ll \frac{x}{(\log x)^A} \quad ?$$

And how do techniques work for arbitrary seqs α and β?

May assume $q > x^{1/2-\epsilon}$ by **BFI**.

q is x^δ-smooth $\implies q = dr$ where $Q/x^\delta < d \le Q.$

How does one prove

$$\sum_{\substack{q \leq x^\theta \\ q \text{ is } x^\delta-\text{smooth} \\ (q,a)=1}} |\Delta(\alpha * \beta; q, a)| \ll \frac{x}{(\log x)^A} \quad ?$$

And how do techniques work for arbitrary seqs α and β?
May assume $q > x^{1/2-\epsilon}$ by **BFI**.

q is x^δ-smooth $\implies q = dr$ where $Q/x^\delta < d \leq Q$.

Th

$$\Delta(\gamma; dr, a) = \Delta(\gamma 1_{a \pmod r}; d, a)) + \frac{1}{\phi(d)} \Delta(\gamma 1_{(.,q)=1}; r, a))$$

How does one prove

$$\sum_{\substack{q \leq x^{\theta} \\ q \text{ is } x^{\delta}-\text{smooth} \\ (q,a)=1}} |\Delta(\alpha * \beta; q, a)| \ll \frac{x}{(\log x)^A} \quad ?$$

And how do techniques work for arbitrary seqs α and β?
May assume $q > x^{1/2-\epsilon}$ by **BFI**.

q is x^{δ}-smooth $\implies q = dr$ where $Q/x^{\delta} < d \leq Q$.

Th

$$\Delta(\gamma; dr, a) = \Delta(\gamma 1_{a \pmod r}; d, a)) + \frac{1}{\phi(d)} \Delta(\gamma 1_{(.,q)=1}; r, a))$$

With $\gamma = \alpha * \beta$, second terms follow from **BFI**.

BFI attack 1st term with **Linnik's dispersion method**

Linnik's dispersion method

Can separate sums such as

$$\sum_m \alpha(m) \sum_{n:\ mn \equiv a \pmod r} \beta(n)$$

Linnik's dispersion method

Can separate sums such as

$$\sum_m \alpha(m) \sum_{n:\ mn \equiv a \pmod r} \beta(n)$$

Cauchying, the square of this is

$$\leq \|\alpha\|^2 \sum_{\substack{n_1,n_2 \\ n_1 \equiv n_2 \pmod r}} \beta(n_1)\beta(n_2) \sum_{m:\ m \equiv a/n_1 \pmod r} 1$$

The last sum is $\dfrac{M}{r} \pm 1.$

Linnik's dispersion method

Can separate sums such as

$$\sum_{m} \alpha(m) \sum_{n:\ mn \equiv a \pmod r} \beta(n)$$

Cauchying, the square of this is

$$\le \|\alpha\|^2 \sum_{\substack{n_1, n_2 \\ n_1 \equiv n_2 \pmod r}} \beta(n_1)\beta(n_2) \sum_{m:\ m \equiv a/n_1 \pmod r} 1$$

The last sum is $\dfrac{M}{r} \pm 1.$

To be precise about ± 1, we use Fourier analysis.

Linnik's dispersion method

Can separate sums such as

$$\sum_m \alpha(m) \sum_{n:\ mn\equiv a \pmod r} \beta(n)$$

Cauchying, the square of this is

$$\leq \|\alpha\|^2 \sum_{\substack{n_1,n_2 \\ n_1\equiv n_2 \pmod r}} \beta(n_1)\beta(n_2) \sum_{m:\ m\equiv a/n_1 \pmod r} 1$$

The last sum is $\dfrac{M}{r} \pm 1.$

To be precise about ± 1, we use Fourier analysis.

Cauchy again to obtain $\|\beta\|_2^2$ times terms

$$\left|\sum_{n\leq N} e^{\frac{2i\pi f(n)}{r}}\right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x),$$

an **incomplete exponential sum**.

We have an averages of sums of the form

$$\left|\sum_{n\leq N} e^{\frac{2i\pi f(n)}{r}}\right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x).$$

By Fourier analysis, write as a sum of Kloosterman sums.
Weil's estimates on each Kloosterman sum gives

$$\ll r^{1/2+\epsilon}.$$

This is not quite good enough.

We have an averages of sums of the form

$$\left|\sum_{n\le N} e^{\frac{2i\pi f(n)}{r}}\right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x).$$

By Fourier analysis, write as a sum of Kloosterman sums.
Weil's estimates on each Kloosterman sum gives

$$\ll r^{1/2+\epsilon}.$$

This is not quite good enough.

BFI - Better bounds from averages of Kloosterman sums:
Kloostermania: Exploits links between these averages and the spectral theory of certain automorphic forms.

We have an averages of sums of the form

$$\left|\sum_{n\le N} e^{\frac{2i\pi f(n)}{r}}\right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x).$$

By Fourier analysis, write as a sum of Kloosterman sums.
Weil's estimates on each Kloosterman sum gives

$$\ll r^{1/2+\epsilon}.$$

This is not quite good enough.

BFI - Better bounds from averages of Kloosterman sums:
Kloostermania: Exploits links between these averages and the spectral theory of certain automorphic forms.

Zhang: Took Kloostermania out of Kloosterman sums
Went back to basics. With a twist ...

Taking the Kloostermania out of Kloosterman sums

$$\left|\sum_{n\le N} e^{\frac{2i\pi f(n)}{r}}\right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x).$$

Weil's estimates on each Kloosterman sum gives

$$\ll r^{1/2+\epsilon}.$$

Taking the Kloostermania out of Kloosterman sums

$$\left| \sum_{n \le N} e^{\frac{2i\pi f(n)}{r}} \right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x).$$

Weil's estimates on each Kloosterman sum gives

$$\ll r^{1/2+\epsilon}.$$

New idea: If $r = r_1 r_2$ we have instead

$$\ll (r_1^{1/2+\epsilon} + r_2^{1/4+\epsilon}) N^{1/2}$$

Taking the Kloostermania out of Kloosterman sums

$$\left|\sum_{n\leq N} e^{\frac{2i\pi f(n)}{r}}\right| \quad \text{where } f = P/Q \in \mathbb{Z}/r\mathbb{Z}(x).$$

Weil's estimates on each Kloosterman sum gives

$$\ll r^{1/2+\epsilon}.$$

New idea: If $r = r_1 r_2$ we have instead

$$\ll (r_1^{1/2+\epsilon} + r_2^{1/4+\epsilon})N^{1/2}$$

If r is y-smooth, pick $r_1|r$ maxl $\leq (ry)^{1/3}$, to get:

$$\ll (ry)^{1/6+\epsilon}N^{1/2}.$$

Improvement for $r^{1/3+\epsilon} < N < r^{2/3-\epsilon}$

(polymath 8a)

Zhang: Modified BFI to also work with sums $\alpha * 1 * 1 * 1.$

Zhang: Modified BFI to also work with sums $\alpha * 1 * 1 * 1.$

Gets Kloosterman sums studied by **Friedlander and Iwaniec** in their work on the distribution of $1 * 1 * 1.$

Zhang: Modified BFI to also work with sums $\alpha * 1 * 1 * 1.$

Gets Kloosterman sums studied by **Friedlander and Iwaniec** in their work on the distribution of $1 * 1 * 1.$

Their estimate is also not quite good enough.

Zhang: Modified BFI to also work with sums $\alpha * 1 * 1 * 1.$

Gets Kloosterman sums studied by **Friedlander and Iwaniec** in their work on the distribution of $1 * 1 * 1.$

Their estimate is also not quite good enough.

Zhang observes that if the moduli d are factorable then one can get a slight (but sufficient) improvement through a similar (though more difficult) trick to that on the last slide.