Primes in intervals of bounded length

Andrew Granville

Université de Montréal

Joint Math Meeting, Current Events Bulletin Baltimore, Friday, January 17, 2014

1

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

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, ...

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

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

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

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

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

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

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

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 | ...

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

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

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

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

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

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

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

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

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 ...

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

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

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 in-finitely many prime pairsp, p+4

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

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 areinfinitely many prime pairsp, p + 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 areinfinitely many prime pairsp, p + 10

A common generalization?

Generalized twin prime conjecture.(De Polignac, 1849) For any even integerh, there are infinitely many prime pairsp, p + h

Other patterns?

Generalized twin prime conjecture.(De Polignac, 1849) For any even integerh, there are infinitely many prime pairsp, p + h

Other patterns? Last digits

11, 13, 17 and $19 \mid 101, 103, 107$ and 109191, 193, 197 and $199 \mid 821, 823, 827$ and $829, \ldots$

Other patterns? Last digits

11, 13, 17 and $19 \mid 101, 103, 107$ and 109191, 193, 197 and $199 \mid 821, 823, 827$ 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 integerh, there are infinitely many prime pairsp, 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 integerh ,there are infinitely many prime pairsp, 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 | ...;

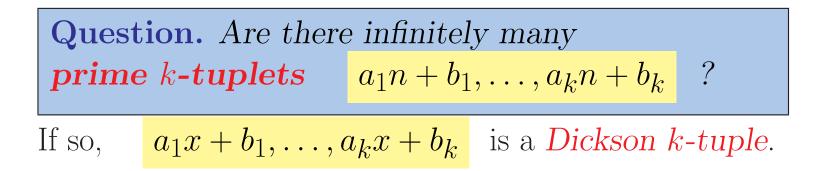
Sophie Germain pairs Conjecture. There are infinitely many prime pairs p, 2p+1

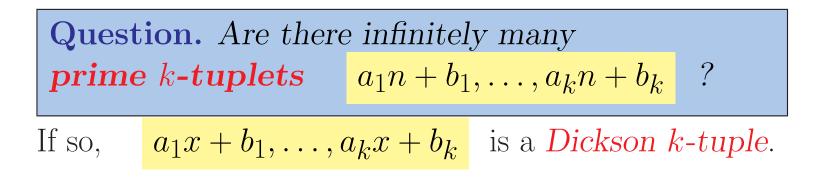
Generalized twin prime conjecture.(De Polignac, 1849) For any even integerh, there are infinitely many prime pairsp, p + h

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

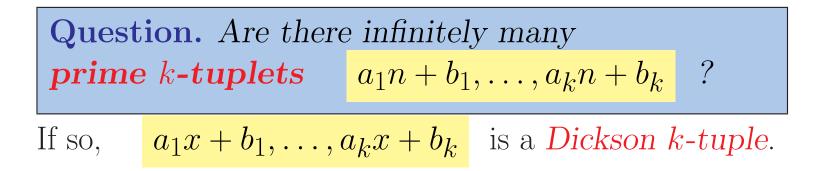
Sophie Germain pairs Conjecture.There areinfinitely many prime pairsp, 2p + 1

A common generalization?





Careful!



Careful!

Prime pairs p, p+1?

Question. Are there infinitely manyprime 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 $\implies h$ even

Question. Are there infinitely manyprime 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 $\implies h$ evenPrime triples?One ofn, 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 $\implies h$ even Prime triples? One of n, n + 2, n + 4 is divisible by 3 Prime p is an obstruction if p always divides $\mathcal{P}(n) = (a_1n + b_1) \dots (a_kn + b_k)$ Question. Are there infinitely manyprime 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.

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

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 <i>Dickson</i> A	k-tuple.

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

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:

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

Recent major breakthrough

Recent major breakthrough

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

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

Recent major breakthrough

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

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

The prime k-tuplets conjecture is almost resolved

The prime k-tuplets conjecture is almost resolved

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

Spectacular new progress.

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 $a_i n + b_i$ 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

 $\begin{array}{l} n+p_1,\ldots,n+p_k\\ \text{prime. This pair of primes differs by}\\ \leq p_k-p_1 \end{array}.$

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

 $p < q \le p + B$.

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

 $p < q \le p + B$.

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

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

 $p < q \le p + B$.

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

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

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

$$p < q \le p + B$$
 with $B := b_k - b_1$

Apr 2013: Zhang

$$k = 3\,500\,000, \quad B \le 70\,000\,000$$

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 $p < q \le p + B$ with $B := b_k - b_1$.

Apr 2013: **Zhang** $k = 3500\,000, B \le 70\,000\,000$

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

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
 $p < q \le p + B$ with $B := b_k - b_1$.Apr 2013: Zhang $k = 3500\,000, B \le 70\,000\,000$ Oct 2013: Polymath 8a $k = 632, B = 4\,680$

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

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 $p < q \leq p + B$ with $B := b_k - b_1$. $k = 3500\,000, B \le 70\,000\,000$ Apr 2013: **Zhang** Oct 2013: Polymath 8a k = 632, $B = 4\,680$ $k = 105, \qquad B = 600$ Nov 2013: Maynard

Jan 2014: Polymath 8b

$$k = 55, \qquad B = 272$$

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, 104110, 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 $m \ge 2$, 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 $m \ge 2$, 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

Consequences of the Maynard/Tao Theorem

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 $B_m \leq cm^3 e^{4m}$).

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 $B_m \leq cm^3 e^{4m}$).

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 $\equiv a \pmod{q}$.

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 $B_m \leq cm^3 e^{4m}$).

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.

Erdős-type consequences of the Maynard/Tao Theorem

Erdős-type consequences of the Maynard/Tao Theorem 1761000<u>1</u>1, 176100<u>1</u>01, 17610<u>1</u>001, 1761<u>1</u>0001 are primes

Erdős-type consequences of the Maynard/Tao Theorem Sets of m primes; each pair differ in two digits

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 *n*th smallest prime.

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

• Infinitely many *n* for which

$$d_n > d_{n+1} > \ldots > d_{n+m}.$$

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 *n*th smallest prime.

• Infinitely many n for which

• Infinitely many n for which

$$d_n < d_{n+1} < \ldots < d_{n+m}.$$

$$d_n > d_{n+1} > \ldots > d_{n+m}.$$

• Infinitely many n for which

$$d_n \mid d_{n+1} \mid \ldots \mid d_{n+m}.$$

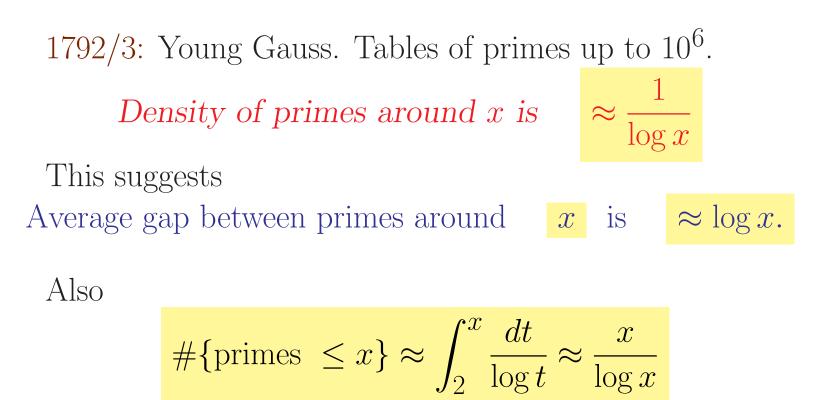
Gaps between primes (History)

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

Gaps between primes (History)

1792/3: Young Gauss. Tables of primes up to 10^6 . Density of primes around x is $\approx \frac{1}{\log x}$ 1792/3: Young Gauss. Tables of primes up to 10^6 . $\frac{1}{\log x}$ Density of primes around x is This suggests

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



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

Question. Fix c > 0. Prove there are infinitely many pairs of primes p < q with q

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

Question. Fix c > 0. Prove there are infinitely many pairs of primes p < q with q

c > 1 by PNT. Any $c \le 1$ is difficult. Conditional 1926 Hardy, Littlewood. Any $c > \frac{2}{3}$ assuming GRH

Question. Fix c > 0. Prove there are infinitely many pairs of primes p < q with q

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 $c \geq \frac{1}{4}$, using combo of techniques

Question. Fix c > 0. Prove there are infinitely many pairs of primes p < q with q

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.

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

Question. Fix c > 0. Prove there are infinitely many pairs of primes p < q with q

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.

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

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

Primes in arithmetic progressions

 $\begin{array}{l} \textit{Riemann Hypothesis} \ (\text{RH}) \\ ``=`` precise estimates for & \#\{ \text{ primes } p \leq x \}. \\ \textit{Generalized Riemann Hypothesis} \ (\text{GRH}) \\ ``=`` precise estimates for \\ & \#\{ \text{ primes } p \leq x, \ p \equiv a \pmod{q} \} . \end{array}$

 $\begin{array}{ll} \textit{Riemann Hypothesis} \ (\text{RH}) \\ ``=`` precise estimates for & \#\{ \text{ primes } p \leq x \}. \\ \textit{Generalized Riemann Hypothesis} \ (\text{GRH}) \\ ``=`` precise estimates for \\ & \#\{ \text{ primes } p \leq x, \ p \equiv a \pmod{q} \} . \\ \text{The large sieve, the Bombieri-Vinogradov Theorem (BV)} \\ & \text{A statistical approximation to GRH} \end{array}$

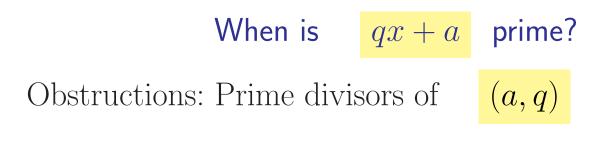
 $\begin{array}{ll} \textit{Riemann Hypothesis} \ (\text{RH}) \\ ``=`` precise estimates for & \#\{ \text{ primes } p \leq x \}. \\ \textit{Generalized Riemann Hypothesis} \ (\text{GRH}) \\ ``=`` precise estimates for \\ & \#\{ \text{ primes } p \leq x, \ p \equiv a \pmod{q} \} . \\ \text{The large sieve, the Bombieri-Vinogradov Theorem (BV)} \\ & \text{A statistical approximation to GRH} \end{array}$

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

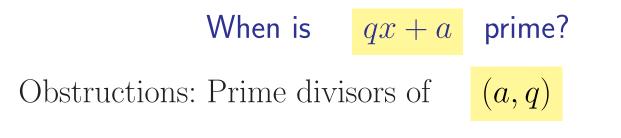
 $\begin{array}{ll} \textit{Riemann Hypothesis} \ (\text{RH}) \\ ``=`` precise estimates for & \#\{ \text{ primes } p \leq x \}. \\ \textit{Generalized Riemann Hypothesis} \ (\text{GRH}) \\ ``=`` precise estimates for \\ & \#\{ \text{ primes } p \leq x, \ p \equiv a \pmod{q} \} . \\ \text{The large sieve, the Bombieri-Vinogradov Theorem (BV)} \\ & \text{A statistical approximation to GRH} \end{array}$

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 isqx + aprime?Obstructions: Prime divisors of(a,q)11, 31, 41, 61, 71, 101, 131, 151, 181,...3, 13, 23, 43, 53, 73, 83, 103, 113, 163, 173, 193...7, 17, 37, 47, 67, 97, 107, 127, 137, 157, 167, 197...19, 29, 59, 79, 89, 109, 139, 149, 179, 199...



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

When isqx + aprime?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: $\begin{aligned}
\# \left\{ \begin{array}{l} \text{primes } p \leq x \\ p \equiv a \pmod{q} \end{array} \right\} \sim \frac{\# \{ \text{primes } p \leq x \}}{\# \{a \pmod{q} : (a,q)=1\}} \\
\text{Prime number theorem for arithmetic progressions} \\
\text{Euler studied } \phi(q) := \# \{a \pmod{q} : (a,q)=1\}
\end{aligned}$ Primes and the Mőbius function

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

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

Equal numbers of -1 and 1? i.e. $\frac{1}{x} \sum_{n \le x} \mu(n) \to 0 \text{ as } n \to \infty ?$

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

Equal numbers of -1 and 1? i.e. $\frac{1}{x} \sum_{n \le x} \mu(n) \to 0 \text{ as } n \to \infty ?$

Equivalent to PNT!

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

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

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

Equivalent to PNT! Recognize primes using

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

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

Recognizing prime k-tuples

Just saw

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

Recognizing prime k-tuples

Just saw

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

Let

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

1956 Golomb's identity: If $n \ge a_1 \dots a_k$ 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 $\begin{array}{ll} \text{GPY: The set up} \\ \text{Given admissible} & a_1 < a_2 < \ldots < a_k. & \text{Select weights} \\ w(n) \geq 0 & \text{for all } n, \text{ such that} \\ \\ & \sum_{x < n \leq 2x} w(n) \# \left\{ \begin{array}{l} i \in \{1, \ldots, k\} \\ n + a_i \text{ is prime} \end{array} \right\} \Big/ \sum_{x < n \leq 2x} w(n) > h, \end{array}$

with h an integer ≥ 1 .

GPY: The set up Given admissible $a_1 < a_2 < \ldots < a_k$. Select weights $w(n) \ge 0$ for all n, such that $\sum_{x < n \le 2x} w(n) \# \left\{ \begin{array}{l} i \in \{1, \dots, k\} \\ n + a_i \text{ is prime} \end{array} \right\} / \sum_{x < n \le 2x} w(n) > h,$ with h an integer ≥ 1 . If so there exists $n \in [x, 2x]$, $\#\left\{\frac{i \in \{1, \dots, k\}}{n + a_i \text{ is prime}}\right\} > h.$

GPY: The set up Given admissible $a_1 < a_2 < \ldots < a_k$. Select weights $w(n) \ge 0$ for all n, such that $\sum_{x < n \le 2x} w(n) \# \left\{ \begin{array}{l} i \in \{1, \dots, k\} \\ n + a_i \text{ is prime} \end{array} \right\} \middle/ \sum_{x < n \le 2x} w(n) > h,$ with h an integer ≥ 1 . If so there exists $n \in [x, 2x]$, $\#\left\{\frac{i \in \{1, \dots, k\}}{n + a_i \text{ is prime}}\right\} > h.$ $\geq m := h + 1$ primes among $n + a_1, \ldots, n + a_k$ That is

To prove m primes in an admissible k-tuple

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

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 $w(n) := \left(\sum_{d \mid \mathcal{P}(n)} \lambda(d)\right)^2$,
sum over d dividing $\mathcal{P}(n) = (n+a_1) \dots (n+a_k)$

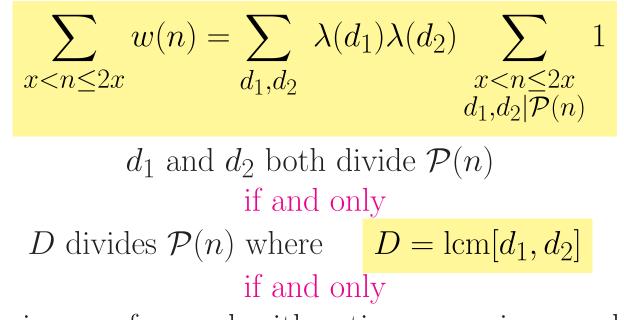
To prove m primes in an admissible k-tuple

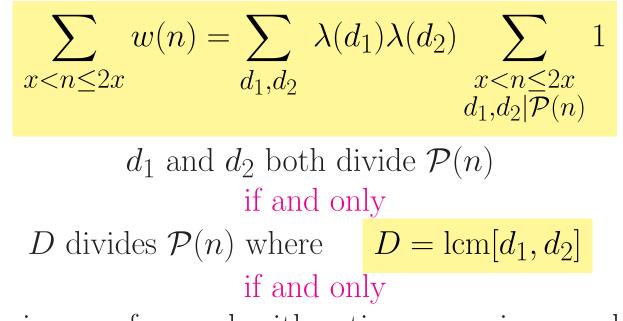
$$\sum_{i=1}^{k} \sum_{\substack{x < n \le 2x \\ n+a_i \text{ is prime}}} w(n) > h \sum_{x < n \le 2x} w(n).$$

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

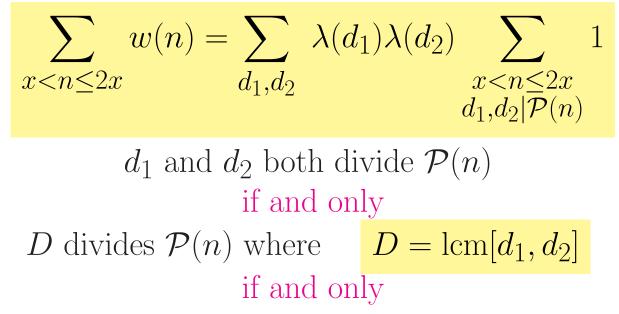
$$\text{sum over } d \text{ dividing} \qquad \mathcal{P}(n) = (n+a_1) \dots (n+a_k).$$

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



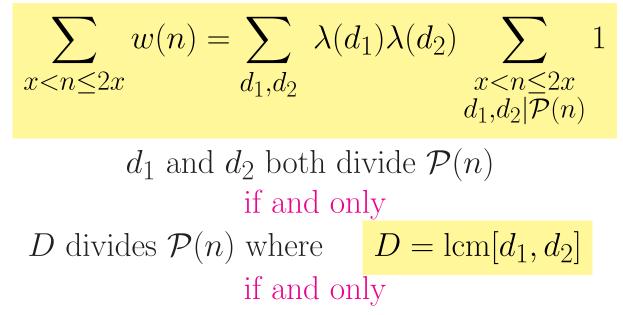


$$\frac{x}{D} - 1 < \#\{x < n \le 2x: \ n \equiv b \pmod{D}\} < \frac{x}{D} + 1$$



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

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

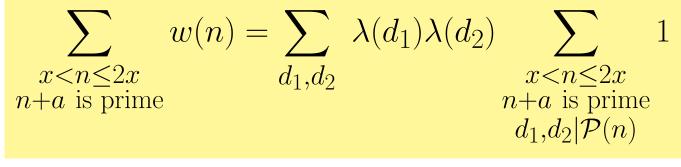


$$\frac{x}{D} - 1 < \#\{x < n \le 2x : n \equiv b \pmod{D}\} < \frac{x}{D} + 1$$

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

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

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



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

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

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

 $\frac{\#\{p \text{ prime}: x$

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

 $\frac{\#\{p \text{ prime}: x$

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

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

We select the weights to be of the form

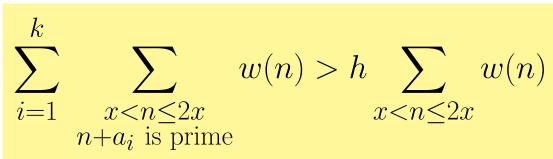
$$\lambda(d) := \mu(d) G\left(\frac{\log d}{\log R}\right),$$

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



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

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

for which

$$\# \left\{ \begin{array}{l} \text{primes } x$$

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 $\# \left\{ \begin{array}{l} \text{primes } x$ How big must x be (in terms of D) for $\begin{aligned}
\# \left\{ \begin{array}{l} \text{primes } x
Calculations: True for <math>x \geq D^{1+\epsilon}$; i.e. $D \leq x^{1-\epsilon}$. How big must x be (in terms of D) for $\begin{aligned}
\# \left\{ \begin{array}{l} \text{primes } x$ How big must x be (in terms of D) for

$$\# \left\{ \begin{array}{l} \text{primes } x$$

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 $D \leq x^{1/2-\epsilon}$. How big must x be (in terms of D) for

$$\# \left\{ \begin{array}{l} \text{primes } x$$

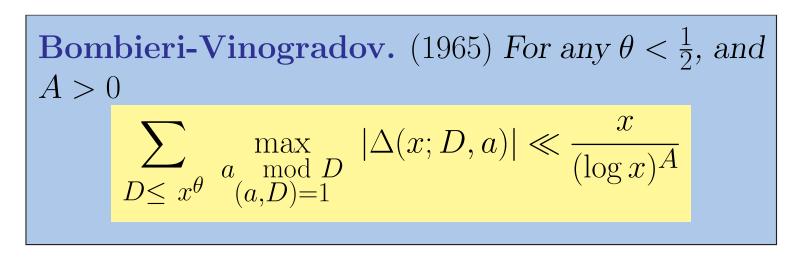
Calculations: True for $x \ge D^{1+\epsilon}$; i.e. $D \le x^{1-\epsilon}$. GRH: True for $D \le x^{\frac{1}{2}-\epsilon}$.

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

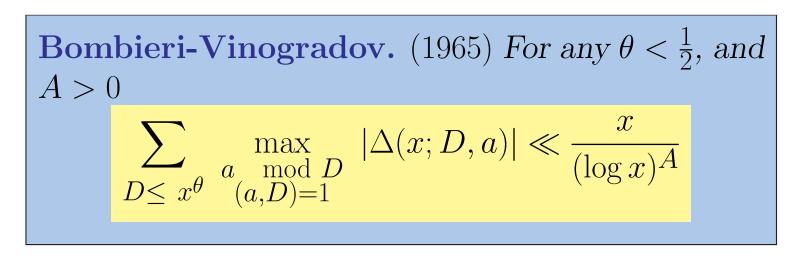
Bombieri-Vinogradov. (1965) For any A > 0 $\sum_{\substack{D \leq x^{\frac{1}{2}} - \epsilon \\ a (a,D) = 1}} \max_{\substack{|\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}}} |\Delta(x; D, a)| \ll \frac{x}{(\log x)^A}$

"Trivial" bound is $\ll x$.

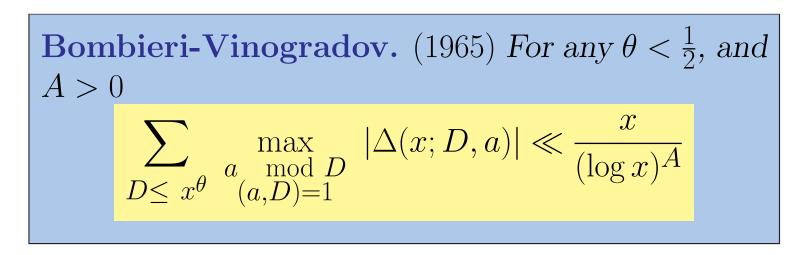
Bombieri-Vinogradov. (1965) For any
$$\theta < \frac{1}{2}$$
, and $A > 0$
$$\sum_{D \leq x^{\theta}} \max_{\substack{a \mod D \\ (a,D)=1}} |\Delta(x;D,a)| \ll \frac{x}{(\log x)^{A}}$$



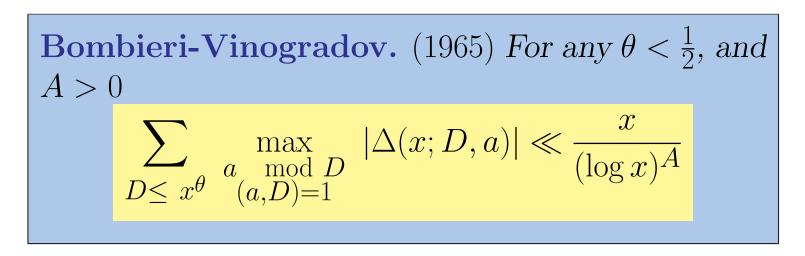
GPY argument works if we can take some $\theta > \frac{1}{2}$.



GPY argument works if we can take some $\theta > \frac{1}{2}$. This is a famous conjecture.



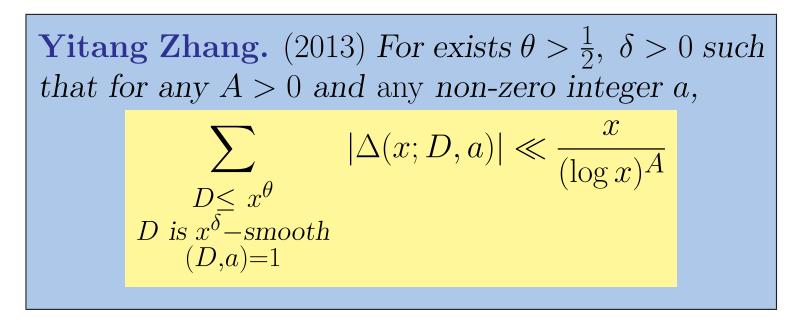
GPY argument works if we can take some $\theta > \frac{1}{2}$. **This is a famous conjecture**. Much important work by **Bombieri, Fouvry, Friedlander and Iwaniec,** in last 25 years: Results with $\theta > \frac{1}{2}$ but with a fixed and bounded, and not large A.



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



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

GPY – Higher dimensional analysis

Changing the weights

The weights above were the square of

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

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

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

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

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

Changing the weights

The weights above were the square of

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

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

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

Maynard/Tao Weights depending on d_1, \ldots, 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

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

where $g(t_1, \ldots, t_k)$ is supported only on $t_1, \ldots, t_k \ge 0$ and $t_1 + \ldots + t_k \le 1$

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

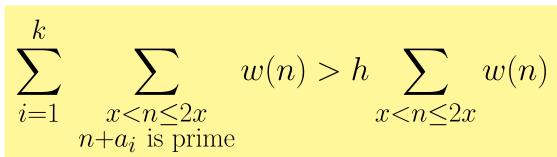
$$\sum_{\substack{d_1|n+a_1\\ \cdots\\ d_k|n+a_k}} \mu(d_1) \cdots \mu(d_k) g\left(\frac{\log d_1}{\log R}, \cdots, \frac{\log d_k}{\log R}\right)$$

where $g(t_1, \ldots, t_k)$ is supported only on $t_1, \ldots, t_k \ge 0$ and $t_1 + \ldots + t_k \le 1$

Same as original GPY construction only if

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

Finding a positive difference



is then equivalent to

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

where

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

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.

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 $\rho(F) = 4.0020697...$ so ok with θ a little less than $\frac{1}{2}$.

Maynard/Tao Theorem

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

where

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

Optimizing choice of A and T we have

$$\max_{k} \rho(F) = \log k + O(1).$$

$Maynard/Tao\ Theorem$

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

where

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

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 $\leq \sqrt{x}$:

$$B \subset \{1, \dots, x\} \quad \text{, and}$$
$$\Delta(B; q, a) := \# \left\{ \begin{array}{c} b \in B \\ b \equiv a \pmod{q} \end{array} \right\} - \left\{ \begin{array}{c} \text{Expected, given} \\ B \pmod{r}, \ r < q \end{array} \right\}$$

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 $\leq \sqrt{x}$:

$$B \subset \{1, \dots, x\} \quad \text{, and}$$
$$\Delta(B; q, a) := \# \left\{ \begin{array}{c} b \in B \\ b \equiv a \pmod{q} \end{array} \right\} - \left\{ \begin{array}{c} \text{Expected, given} \\ B \pmod{r}, \ r < q \end{array} \right\}$$
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 $\leq \sqrt{x}$:

$$B \subset \{1, \dots, x\} \quad \text{, and}$$
$$\Delta(B; q, a) := \# \left\{ \begin{array}{c} b \in B \\ b \equiv a \pmod{q} \end{array} \right\} - \left\{ \begin{array}{c} \text{Expected, given} \\ B \pmod{r}, \ r < q \end{array} \right\}$$
Example:
$$B = \{n \le x : n \text{ even}\}.$$

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.

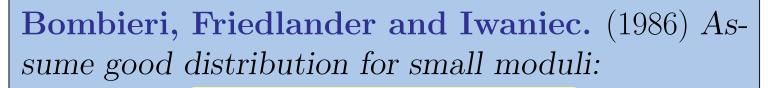
General sequences in arithmetic progression $\sum_{q \le x^{\frac{1}{2}}} q \sum_{a: \ (a,q)=1} |\Delta(B;q,a)|^2 \le 2x \# B$

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".

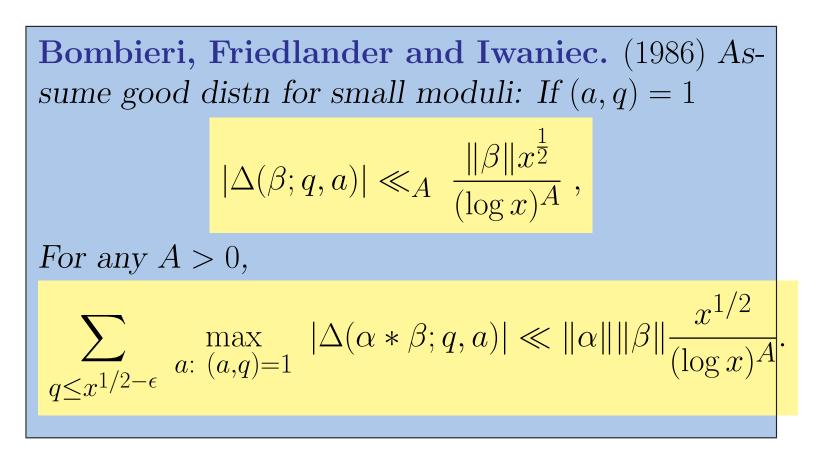


$$|\Delta(\beta; q, a)| \ll_A \frac{\|\beta\|x^{\frac{1}{2}}}{(\log x)^A},$$

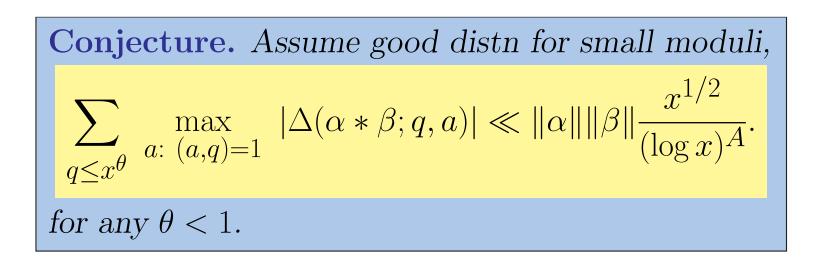
For any A > 0,

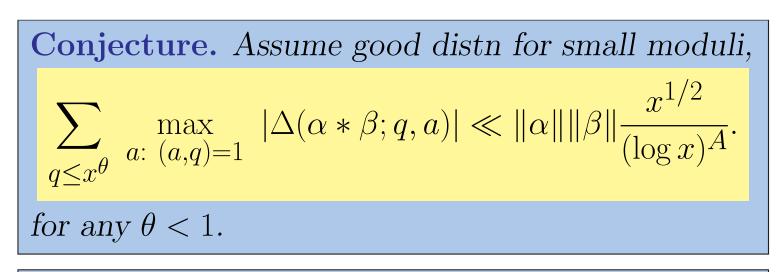
$$\sum_{q \le x^{1/2 - \epsilon}} \max_{a: (a,q) = 1} |\Delta(\alpha * \beta; q, a)| \ll \|\alpha\| \|\beta\| \frac{x^{1/2}}{(\log x)^A}$$

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



Remember: $(\mu * \log)$ recognizes prime powers. **BFI** \implies Bombieri-Vinogradov theorem for primes.





Yitang Zhang / polymath 8a. (2013) Assume α and β are only supported in $[x^{1/3}, x^{2/3}]$, $|\alpha(n)|, |\beta(n)| \leq c(\tau(n) \log n)^B$ $\exists \ \theta > \frac{1}{2}, \ \delta > 0 \text{ s.t. for any } A > 0 \text{ and } a \neq 0,$

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

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

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

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

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

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

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

$$q ext{ is } x^{\delta} ext{-smooth } \Longrightarrow q = dr ext{ where } Q/x^{\delta} < d \le Q.$$

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

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

$$\begin{array}{ll} q \text{ is } & x^{\delta} \text{-smooth} \implies q = dr & \text{where } & Q/x^{\delta} < d \leq Q. \\ & \Delta(\gamma; dr, a) = \Delta(\gamma 1_{a \pmod{r}}; d, a)) + \frac{1}{\phi(d)} \Delta(\gamma 1_{(.,q)=1}; r, a)) \end{array}$$

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

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

q is
$$x^{\delta}$$
-smooth $\implies q = dr$ where $Q/x^{\delta} < d \le Q$.
 $\Delta(\gamma; dr, a) = \Delta(\gamma 1_{a \pmod{r}}; d, a)) + \frac{1}{\phi(d)}\Delta(\gamma 1_{(.,q)=1}; r, a))$
With $\gamma = \alpha * \beta$, second terms follow from **BFI**.

 $\mathbf{BFI}\xspace$ attack 1st term with $\mathbf{Linnik's\ dispersion\ method}$

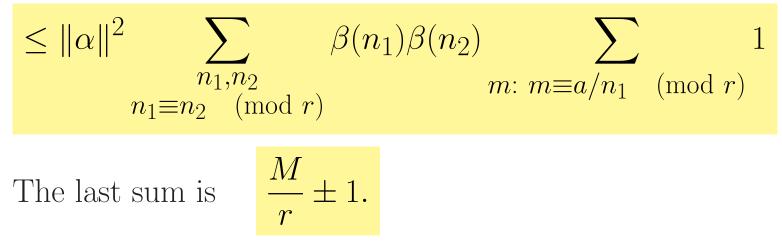
Linnik's dispersion method Can separate sums such as

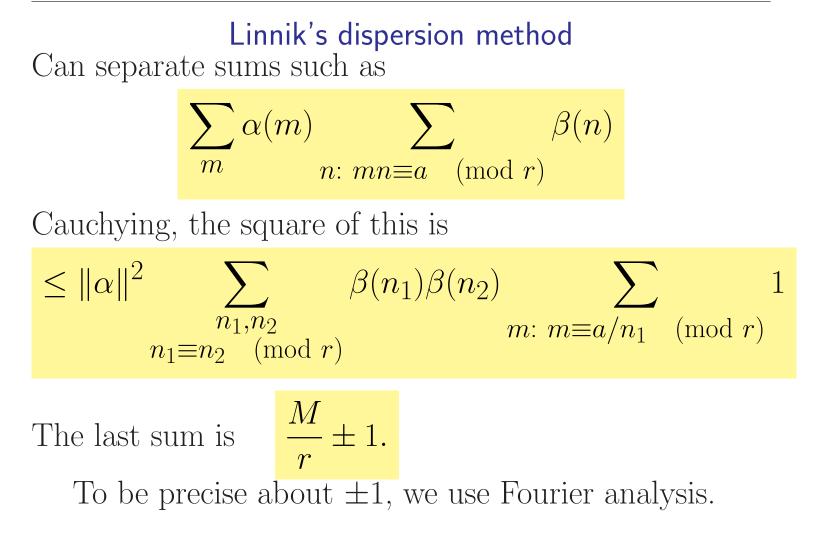
$$\sum_m \alpha(m) \sum_{n: \ mn \equiv a \pmod{r}} \beta(n)$$



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

Cauchying, the square of this is







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

Cauchying, the square of this is

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

The last sum is

$$\frac{M}{r} \pm 1.$$

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

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

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

an incomplete exponential sum.

We have an averages of sums of the form

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

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

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

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

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

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

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

Weil's estimates on each Kloosterman sum gives

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

Taking the Kloostermania out of Kloosterman sums

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

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

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

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 $r_1 |r \max | \le (ry)^{1/3}$, to get: $\ll (ry)^{1/6+\epsilon}N^{1/2}.$ Improvement for $r^{1/3+\epsilon} < N < r^{2/3-\epsilon}$

(polymath 8a)

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

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.