A talk given at the NCTS (Hsinchu, Taiwan, August 6, 2014)
and Northwest Univ. (Xi'an, October 26, 2014)
and Center for Combinatorics, Nankai Univ. (Tianjin, Nov. 3, 2014)

Towards the Twin Prime Conjecture

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

Nov. 3, 2014

Abstract

Prime numbers are the most basic objects in mathematics. They also are among the most mysterious, for after centuries of study, the structure of the set of prime numbers is still not well understood. Describing the distribution of primes is at the heart of much mathematics ... — Andrew Granville (1997)

If p and $p+2$ are both prime, then $\{p, p+2\}$ is called a twin prime pair. The famous Twin Prime Conjecture asserts that there are infinitely many twin prime pairs. In this talk we will give a survey of the developments towards the solution of the Twin Prime Conjecture. We will introduce Brun's theorem on twin primes, Chen's theorem on Chen primes, the recent breakthrough of Yitang Zhang and the Maynard-Tao theorem on m consecutive primes. We will also mention the Super Twin Prime Conjecture posed by the speaker and the recent work of Pan and Sun on consecutive primes and Legendre symbols.

Twin Primes

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

Euclid (around 300 BC): There are infinitely many primes.

For $n = 1, 2, 3, \dots$ let p_n denote *the n-th prime*.

For example,

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ p_6 = 13.$$

If p and $p + 2$ are both prime, then we call $\{p, p + 2\}$ (of the form $\{p_n, p_{n+1}\}$ with $p_{n+1} - p_n = 2$) a *twin prime pair*. For example,

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

are all the twin prime pairs below 100.

Twin Prime Conjecture and Cramér's Conjecture

The Twin Prime Conjecture. There are infinitely many twin prime pairs. In other words,

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = 2.$$

de Polignac's Conjecture (1849). For each $d = 2, 4, 6, \ldots$, there are infinitely many positive integers n with $p_{n+1} - p_n = d$.

Cramér's Conjecture (1936). We have

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = 1.$$

Cramér showed that Riemann's Hypothesis implies that

$$p_{n+1} - p_n = O(\sqrt{p_n}\log p_n).$$

k-Tuple Prime Conjecture and Admissible Sets

Let $h_1, \ldots, h_k$ be integers. If there are infinitely many integers n such that $n + h_1, \ldots, n + h_k$ are all prime, then there is no prime p such that

$$p \;\Big|\; \prod_{i=1}^{k} (n + h_i) \quad \text{for all } n \in \mathbb{Z},$$

i.e., $\bigcup_{i=1}^{k} h_i \pmod{p} \neq \mathbb{Z}$ for any prime p, where $a \pmod{p}$ refers to $a + p\mathbb{Z}$.

Definition. Let $h_1, \ldots, h_k$ be distinct integers. If $\bigcup_{i=1}^{k} h_i \pmod{p} \neq \mathbb{Z}$ for any prime p, then we call $\mathcal{H} = \{h_1, \ldots, h_k\}$ an *admissible set* or an *admissible k-tuple*.

***k*-Tuple Prime Conjecture (Hardy and Littlewood, 1923)**: If $\mathcal{H} = \{h_1, \ldots, h_k\}$ is an admissible k-tuple, then there are infinitely many positive integers n such that

$$n + h_1,\ n + h_2,\ \ldots,\ n + h_k$$

are all prime.

Special Cases of the k-Tuple Prime Conjecture

If $\mathcal{H} = \{h_1, h_2, \ldots, h_k\}$ is an admissible k-tuple, then so is

$$a + \mathcal{H} = \{a + h_i : \ i = 1, \ldots, k\},$$

where a is an arbitrary integer. So we need only consider admissible set of the form $\mathcal{H} = \{h_1 = 0 < h_2 < \ldots < h_k\}$.

As $\{0, 2\}$ is an admissible set, the k-Tuple Prime Conjecture implies the Twin Prime Conjecture.

Note that $\{0, 2, 4\}$ is not admissible since $0(\mathrm{mod}\ 3) \cup 2(\mathrm{mod}\ 3) \cup 4(\mathrm{mod}\ 3) = \mathbb{Z}$. But $\{0, 2, 6\}$ and $\{0, 4, 6\}$ are both admissible sets, so the k-Tuple Conjecture implies the following conjecture.

Prime Triplet Conjecture: There are infinitely many primes p with $p + 2$ and $p + 6$ both prime. Also, there are infinitely many primes p with $p + 4$ and $p + 6$ both prime.

Examples. $\{11, 13, 17\}$ and $\{7, 11, 13\}$ are both prime triplets.

Dikson's Conjecture

Dickson's Conjecture: Let $a_i > 1$ and b_i be integers for all $i = 1, \ldots, k$. If there is no prime p dividing $\prod_{i=1}^{k}(a_i n + b_i)$ for all $n \in \mathbb{Z}$, then there are infinitely many integers n such that $a_1 n + b_1, a_2 n + b_2, \ldots, a_k n + b_k$ are all prime.

Note that if a prime p divides $an + b$ for all $n \in \mathbb{Z}$, then both a and b are multiples of p. So Dirichlet's theorem on primes in arithmetic progressions is just Dickson's Conjecture in the case $k = 1$.

Example. Any prime p does not divide $n(2n+1)$ with $n = p - 1$, so Dickson's Conjecture implies that there are infinitely many primes p with $2p + 1$ also prime. Such primes p are called *Sophie Germain primes*.

Schinzel's Hypothesis H and Bateman-Horn Conjecture

Schinzel's Hypothesis H (1958). If $f_1(x), \ldots, f_k(x)$ are irreducible polynomials with integer coefficients and positive leading coefficients such that there is no prime dividing the product $f_1(q)f_2(q)...f_k(q)$ for all $q \in \mathbb{Z}$, then there are infinitely many $n \in \mathbb{Z}^+$ such that $f_1(n), f_2(n), \ldots, f_k(n)$ are all primes.

Remark. The hypothesis with $k = 1$ was a conjecture posed by Bunyakovsky in 1857.

Bateman-Horn Conjecture (1962). Let $f_1(x), \ldots, f_k(x)$ be distinct irreducible polynomials with integer coefficients and positive leading coefficients such that there is no prime dividing $f(q)$ for all $q \in \mathbb{Z}$, where $f = f_1 \cdots f_k$. Then

$$|\{1 \leqslant n \leqslant x : \ f_1(n), \ldots, f_k(n) \text{ are all prime}\}|$$
$$\sim \frac{1}{\prod_{i=1}^k \deg(f_i)} \left(\prod_p \frac{1 - N_f(p)/p}{(1 - 1/p)^k} \right) \int_2^x \frac{dt}{(\log t)^k},$$

where $N_f(p) = |\{0 \leqslant x \leqslant p - 1 : \ f(x) \equiv 0 \pmod p\}| < p$.

Hardy-Littlewood Conjecture on $\pi_2(x)$

Prime Number Theorem. For $x > 0$ let $\pi(x)$ denote the number of primes not exceeding x. Then

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

For $x > 0$, let

$$\pi_2(x) := |\{p \leqslant x : \ p + 2 \text{ is prime}\}|.$$

The Bateman-Horn Conjecture with $f_1(x) = x$ and $f_2(x) = x + 2$ yields the following conjecture on $\pi_2(x)$.

Hardy-Littlewood Conjecture. We have

$$\pi_2(x) \sim 2C_2 \frac{x}{\log^2 x} \quad \text{as } x \to \infty,$$

where

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66.$$

The sieve method

Let $A = (a_1, a_2, \ldots)$ be a finite integer sequence and let P be a set of some primes. The *sift function*

$$S(A, P, z) := \sum_{\substack{a \in A \\ (a, P_z)=1}} 1, \qquad \text{where } P_z = \prod_{\substack{p \in P \\ p \leqslant z}} p.$$

Note that $S(A, P, z)$ is the number of remaining terms of A after we *sieve* out those terms of A divisible by some primes $p \in P$ with $p \leqslant z$.

Eratosthenes' Sieve. Let $z \geqslant 2$ and $A = \{n > z : \ n \leqslant z^2\}$, and let P be the set of all primes. Then

$$\begin{aligned} S(A, P, z) =& |\{z < n \leqslant z^2 : \ n \text{ is divisible by no prime } p \leqslant z\}| \\ =& \text{the number of primes in } (z, z^2] = \pi(z^2) - \pi(z). \end{aligned}$$

Remark. If $S(A, P, z) > 0$ for sufficiently large z, then we deduce that there are infinitely many primes.

Brun's sieve

Inclusion-Exclusion Principle. Let S be a finite set, and let

$$S_k = \{a \in S : \ a \text{ has the property } P_k\} \ \text{ for } k = 1, \ldots, n.$$

Then

$$|\{a \in S : \ a \text{ has the property } P_k \text{ for no } k = 1, \ldots, n\}|$$

$$= |S| - \sum_{k=1}^{n} |S_k| + \sum_{1 \leqslant i < j \leqslant n} |S_i \cap S_j| - \ldots + (-1)^n |S_1 \cap \cdots \cap S_n|.$$

Brun's Observation. If $m \in \{1, \ldots, n\}$ is *even*, then

$$\left| S \setminus \bigcup_{k=1}^{n} S_k \right| \leqslant |S| - \sum_{i=1}^{n} |S_i| + \sum_{1 \leqslant i < j \leqslant n} |S_i \cap S_j| - \ldots$$

$$+ \sum_{1 \leqslant i_1 < \ldots < i_m \leqslant n} (-1)^m |S_{i_1} \cap \ldots \cap S_{i_m}|.$$

Remark. This is similar to the fact that

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots \leqslant 1 - \frac{1}{3} + \frac{1}{5}.$$

Brun's theorem

Brun's Theorem (1920) There is a constant $C > 0$ such that

$$\pi_2(x) := |\{p \leqslant x : \ p+2 \text{ is prime}\}| \leqslant C\frac{x(\log\log x)^2}{(\log x)^2}$$

for all $x \geqslant 2$.

Idea of the Proof. Let $5 \leqslant y < x$, and let $q_1, q_2, \ldots, q_r$ be all the distinct odd primes not exceeding y. If $\{n, n+2\}$ is a twin prime pair with $y < n \leqslant x$, then $n > q_i$ and $q_i \nmid n(n+2)$ for all $i = 1, \ldots, r$. Thus

$$\pi_2(x) \leqslant y + |\{p \in (y, x] : \ p+2 \text{ is prime}\}| \leqslant y + N(y, x),$$

where

$$N(y, x) = |\{n \leqslant x : \ n(n+2) \not\equiv 0 \pmod{q_i} \text{ for all } i = 1, \ldots, r\}|.$$

If we take $y = x^{1/(c\log\log x)}$ for suitable $c > 0$, then we obtain via Brun's sieve

$$\pi_2(x) \leqslant y + N(y, x) \leqslant C\frac{x(\log\log x)^2}{(\log x)^2} \text{ for some } C > 0.$$

Brun's constant

Choose a constant $C' > 0$ such that

$$\pi_2(x) \leqslant C\frac{x(\log\log x)^2}{(\log x)^2} \leqslant C'\frac{x}{(\log x)^{1.5}} \quad \text{for all } x \geqslant 2.$$

Let $\{t_n, t_n + 2\}$ be the n-th twin prime pair. Then

$$n = \pi_2(t_n) \leqslant C'\frac{t_n}{(\log t_n)^{1.5}} \text{ and hence } \frac{1}{t_n} \leqslant \frac{C'}{(\log n)^{1.5}}.$$

It follows that

$$\sum_{n=1}^{\infty}\frac{1}{t_n} \leqslant C'\sum_{n=1}^{\infty}\frac{1}{n(\log n)^{1.5}} < \infty.$$

Brun's constant:

$$\sum_{n=1}^{\infty}\left(\frac{1}{t_n} + \frac{1}{t_n+2}\right) \approx 1.9021604.$$

Chen primes

Via a very sophisticated weighted linear sieve, the Chinese mathematician Jing-run Chen established the following famous result.

Chen's Theorem (Jing-run Chen, 1973) (i) Large even numbers can be written as $p+q$, where p is a prime, and q is either a prime or a product of two primes.

(ii) There are infinitely many primes p such that $p+2$ is either a prime or a product of two primes.

Remark. Part (i) is the best record on Goldbach's conjecture, while part (ii) is close to the Twin Prime Conjecture.

Chen prime: A prime p is called a *Chen prime* if $p+2$ is a product of at most two primes.

Example. 13 is a Chen prime since $13+2=3\times 5$.

Bombieri-Vinorgradov Theorem

Prime Number Theorem for Arithmetic Progressions. Let $1 \leqslant a \leqslant q$ with $(a, q) = 1$, then

$$\pi(x; a, q) := \sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} 1 \sim \frac{\pi(x)}{\varphi(q)} \sim \frac{\mathrm{Li}(x)}{\varphi(q)},$$

where

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

Bombieri-Vinorgradov Theorem (1965). For any $A > 0$, there is a constant $B > 0$ depending on A such that

$$\sum_{q \leqslant \sqrt{x}/(\log x)^B} E(q, x) = O\left(\frac{x}{(\log x)^A}\right),$$

where

$$E(q, x) := \max_{\substack{1 \leqslant a \leqslant q \\ (a,q)=1}} \left|\pi(x; a, q) - \frac{\mathrm{Li}(x)}{\varphi(q)}\right|.$$

Elliott-Hlberstam Conjecture

The Bombieri-Vinorgradov Theorem plays a very important role in analytic number theory. It led Bombieri and Vinorgradov to obtain "$1+3$" on Goldbach's conjecture. Jing-run Chen also needed the Bombieri-Vinorgradov Theorem in his proof of Chen's theorem ("$1+2$").

Elliott-Halberstam Conjecture (1973). For any $0 < \theta < 1$, we have the following property (called EH(θ)): *For any $A > 0$, there is a constant $C_A > 0$ such that*

$$\sum_{q \leqslant x^\theta} E(x,q) \leqslant C_A \frac{x}{(\log x)^A}.$$

The Bombieri-Vinorgradov Theorem indicates that EH(θ) holds for any $0 < \theta < \frac{1}{2}$. Up to now, nobody succeeds to prove EH(θ) for some $\theta > \frac{1}{2}$.

Selberg's upper bound sieve

Selberg's Sieve. Let $A = (a_1, a_2, \ldots)$ be a finite sequence and let $|A|$ be its length. Let P be a set of some primes, and let

$$P(z) = \prod_{\substack{p \leqslant z \\ p \in P}} p \quad \text{for } z \geqslant 2.$$

For a squarefree positive integer d, let A_d denote the subsequence of A consisting of terms divisible by d. Let g be a multiplicative arithmetic function with $0 < g(p) < 1$ for all $p \in P$. And let g_1 be a completely multiplicative function with $g_1(p) = g(p)$ for all $p \in P$. Then

$$S(A, P, z) \leqslant \frac{|A|}{G(z)} + \sum_{\substack{d \leqslant z^2 \\ d | P_z}} 3^{\omega(d)} |r(d)|,$$

where $\omega(d)$ is the number of distinct prime divisors of d,

$$G(z) = \sum_{\substack{m \leqslant z \\ p | m \Rightarrow p \in P}} g_1(m) \quad \text{and} \quad r(d) = |A_d| - g(d)|A|.$$

Starting point of the proof

Let $z \geqslant 2$, and let λ be a real arithmetic function with $\lambda(1) = 1$ and $\lambda(z) = 0$ for $z > D$. Observe that

$$\begin{aligned} S(A,P,z) &= \sum_{\substack{a \in A \\ (a,P_z)=1}} 1 \\ &\leqslant \sum_{a \in A} \Big(\sum_{d|(a,P_z)} \lambda(d) \Big)^2 = \sum_{a \in A} \sum_{d_1|(a,P_z)} \lambda(d_1) \sum_{d_2|(a,P_z)} \lambda(d_2) \\ &= \sum_{d_1,d_2|P_z} \lambda(d_1)\lambda(d_2) \sum_{\substack{a \in A \\ [d_1,d_2]|a}} 1 = \sum_{d_1,d_2|P_z} \lambda(d_1)\lambda(d_2)|A_{[d_1,d_2]}| \\ &= \cdots \end{aligned}$$

$w(n) = \Big(\sum_{d|n} \lambda(d) \Big)^2$ is called a weight of n.

To get an ideal upper bound for $S(A,P,z)$, we should manage to optimize the choice of the auxiliary function $\lambda(d)$.

Applying the Cauchy-Schwarz inequality

Cauchy-Schwarz Inequality. Let $a_i, b_i \in \mathbb{R}$ for $i = 1, \ldots, n$. Then

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leqslant \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right).$$

If $a_j \neq 0$ for some $j \in \{1, \ldots, n\}$, then the equality holds if and only for some $t \in \mathbb{R}$ we have $b_i = ta_i$ for all $i = 1, \ldots, n$.

Sketch of the Proof.

$$0 \leqslant \sum_{1 \leqslant i < j \leqslant n} (a_i b_j - a_j b_i)^2 = \sum_{i=1}^{n} a_i^2 \sum_{j=1}^{n} b_j^2 - \left(\sum_{i=1}^{n} a_i b_i\right)^2.$$

The Cauchy-Schwarz Inequality implies the following lemma needed for Selberg's sieve.

Lemma. Let $a_1, \ldots, a_n$ be positive reals and let $b_1, \ldots, b_n \in \mathbb{R}$. Under the restriction $b_1 y_1 + \cdots + b_n y_n = 1$,

$$Q(y_1, \ldots, y_n) = a_1 y_1^2 + \ldots + a_n y_n^2$$

has the minimum $m = (\sum_{i=1}^{n} b_i^2 / a_i)^{-1}$. And the minimum is attained if and only if $y_i = m b_i / a_i$ for all $i = 1, \ldots, n$.

The work of Goldston-Pintz-Yildirim

Let P be the set of all primes, and let $\chi_P(n)$ take 1 or 0 according as n is prime or not.

D.A. Goldston, J. Pintz, C.Y. Yildirim (posted to arXiv in 2005): Let $\mathcal{H} = \{h_1, \ldots, h_k\}$ be an admissible k-tuple. Choose $\lambda(d) = \mu(d)P(\log \frac{D}{d})$ with $d \leqslant D$ for suitable polynomial P with $P(1) = 1$, and set $W(n) = (\sum_{d \mid \prod_{j=1}^k (n+h_j)} \lambda(d))^2$. If EH($\theta$) holds for some $\theta > 1/2$, then for large N we have

$$\sum_{N \leqslant n < 2N} \chi_P(n + h_j) W(n) > \frac{1}{k} \sum_{N \leqslant n < 2N} W(n) \quad \text{for all } j = 1, \ldots, k,$$

hence

$$\sum_{N \leqslant n < 2N} \sum_{j=1}^{k} \chi_p(n + h_j) W(n) > \sum_{N \leqslant n < 2N} W(n)$$

and thus there are $1 \leqslant i < j \leqslant k$ such that $p = n + h_i$ and $q = n + h_j$ are both prime. Note that $|p - q|$ does not exceed $d(\mathcal{H}) = \max \mathcal{H} - \min \mathcal{H}$ (the *diameter* of $\mathcal{H}$).

Main Results of Goldston-Pintz-Yildirim

D.A. Goldston, J. Pintz, C.Y. Yildirim [Annals of Math. 170(2009)]: We have

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

Under the Elliott-Halberstam conjecture,

$$\liminf_{n\to\infty} (p_{n+1}-p_n) \leqslant 16.$$

D.A. Goldston, J. Pintz, C.Y. Yildirim [Acta Math. 204(2010)]:

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\sqrt{\log p_n}(\log\log p_n)^2} < \infty.$$

Discrepancy

Let f be an arithmetic function with $\text{supp}(f) = \{n : f(n) \neq 0\}$ finite. For a primitive residue class $a(q) = a + q\mathbb{Z}$ (with $(a, q) = 1$), define the *discrepancy*

$$\Delta(f; a(q)) := \sum_{n \equiv a \pmod q} f(n) - \frac{1}{\varphi(q)} \sum_{(n,q)=1} f(n).$$

Below we let $\mathbf{1}_I(n)$ take 1 or 0 according as $n \in I$ or not.

Fouvry and Iwaniec [Mathematica 27(1980)]: Let $A > 0$ and let x be large. Let $f(n) = 1$ if no prime divisor of n is smaller than $x^{1/883}$, and $f(n) = 0$ otherwise. Then

$$\sum_{q \leqslant x^{1/2+1/42}} \max_{\substack{1 \leqslant a \leqslant q \\ (a,q)=1}} |\Delta(f \mathbf{1}_{[1,x]}, a(q))| = O\left(\frac{x}{(\log x)^A}\right).$$

Friedlander and Iwaniec [Annals of Math. 34(1985)]: Let $A > 0$, and let $q \leqslant x^{1/2+1/230}$ and $(a, q) = 1$. Then

$$\Delta(\tau_3 \mathbf{1}_{[1,x]}, a(q)) = O\left(\frac{x}{q(\log x)^A}\right), \quad \text{where } \tau_3(n) = \Sigma_{abc=n} 1.$$

The work of Motohashi and Pintz

In 2008, Y. Motohashi and J. Pintz published a paper with the title "*A smoothed GPY sieve*" in Bull. Lond. Math. Soc. 40(2008), 298-310. This paper was posted to arXiv in 2006.

Motohashi-Pintz (2006): Let $f(n) = \log n$ if n is a prime, and let $f(n) = 0$ otherwise. If there is a $\theta > 1/2$ and an admissible $\mathcal{H} = \{h_1, \ldots, h_k\}$ such that for any $A > 0$ and large x we have

$$\sum_{\substack{q \leqslant x^{\theta} \\ q \mid \prod_{p \leqslant x^{\theta/2-1/4}} p}} \sum_{\substack{1 \leqslant a \leqslant q,\, (a,q)=1 \\ q \mid \prod_{j=1}^{k} (a+h_j)}} |\Delta(f\mathbf{1}_{[x,2x]}, a(q))| = O\left(\frac{x}{(\log x)^A}\right),$$

then there are infinitely many n such that $\{n+h_1, \ldots, n+h_k\}$ contains at least two primes, and hence

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leqslant d(\mathcal{H}) < \infty.$$

Yitang Zhang's breakthrough

In 2013, Yitang Zhang rediscovered the approach of Motohashi and Pintz. Moreover, he proved that the condition holds for

$$\theta = \frac{1}{2} + \frac{1}{584} \quad \text{and} \quad k = 3.5 \times 10^6.$$

To deduce this, he needed to bound incomplete exponential sums in the form

$$\sum_{N \leqslant n \leqslant 2N} e^{2\pi i \frac{c_1 \bar{n} + c_2 \overline{n+l}}{q}},$$

where $\bar{n}$ denotes the inverse of n modulo q. In this step, Zhang employed some deep results like Deligne's theorem which extends the Weil bound on Kloosterman sums.

Zhang noted that $\mathcal{H} = \{p_{\pi(k)+j} : \ j = 1, \ldots, k\}$ is an admissible k-tuple. In fact, for any prime $p \leqslant k$, we have $p_{\pi(k)+j} \not\equiv 0 \pmod{p}$ for all $j = 1, \ldots, k$; for any prime $p > k$ obviously $\bigcup_{j=1}^{k} p_{\pi(k)+j} (\mathrm{mod}\ p) \neq \mathbb{Z}$. For $k = 3.5 \times 10^6$, $p_{\pi(k)+k} < 7 \times 10^7$.

Zhang's Theorem (2013). $\liminf_{n\to\infty}(p_{n+1} - p_n) < 7 \times 10^7$.

Some comments on Zhang's work

The main results are of the first rank. The author had proved a landmark theorem in the distribution of prime numbers.

— One of the referees

Basically no one knows him. Now suddenly he has proved one of the great result in the history of number theory.

— Andrew Granville

Maynard's approach

In Oct. 2013, the young number theorist James Maynard announced a new approach to bounded gaps between primes. On Nov. 19, 2013 he posted a preprint "*Small gaps between primes*" on `arXiv`.

Maynard did not follow Zhang's approach. Instead, he modified Goldston-Yildirim's original unsuccessful approach. Instead of using weights of the form

$$W(n) = \Big(\sum_{d \mid \prod_{i=1}^{k}(n+h_i)} \lambda(d) \Big)^2$$

(where $\mathcal{H} = \{h_1, \ldots, h_k\}$ is an admissible k-tuple), Maynard employed the weights of the new form

$$w(n) = \Big(\sum_{d_i \mid n+h_i \ (i=1,\ldots,k)} \lambda_{d_1,\ldots,d_k} \Big)^2.$$

Maynard's approach

Let N be large and set $W = \prod_{p \leqslant \log\log\log N} p$. As $\mathcal{H} = \{h_1, \ldots, h_k\}$ is admissible, for any prime $p \mid W$, there is an integer $r_p \notin \bigcup_{i=1}^k h_i \pmod p)$. By the Chinese Remainder Theorem, there is an integer ν such that $\nu \equiv -r_p \pmod p$ for all $p \mid W$ and hence W is coprime to $\prod_{i=1}^k (\nu + h_i)$. Maynard restricted his attention only to those $n \equiv \nu \pmod W$. Let

$$S_1 = \sum_{\substack{N \leqslant n < 2N \\ n \equiv \nu \pmod W}} w(n), \quad S_2 = \sum_{\substack{N \leqslant n < 2N \\ n \equiv \nu \pmod W}} \left(\sum_{i=1}^k \chi_P(n + h_i) \right) w(n).$$

If $S_2 > mS_1$, then at least $m+1$ of the numbers $n + h_1, \ldots, n + h_k$ are primes.

Maynard's approach

Let F be a piecewise differentiable function with $F(x_1, \ldots, x_k) \neq 0$ for all $x_1, \ldots, x_k \geqslant 0$ with $x_1 + \cdots + x_k \leqslant 1$. Let $\theta > 0$ and $R = N^{\theta/2-\delta}$ for some small fixed $\delta > 0$. For integers $d_1, \ldots, d_k > 0$, if $(\prod_{i=1}^k d_i, W) = 1$ then put

$$\lambda_{d_1,\ldots,d_k} := \left(\prod_{i=1}^{k} \mu(d_i) d_i \right) \times \sum_{\substack{r_i \equiv 0 \pmod{d_i} \ (0<i\leqslant k) \\ (\prod_{i=1}^k r_i, W)=1}} \frac{\mu(\prod_{i=1}^k r_i)^2}{\prod_{i=1}^k \varphi(r_i)} F\left(\frac{\log r_1}{\log R}, \ldots, \frac{\log r_k}{\log R} \right),$$

and let $\lambda_{d_1,\ldots,d_k} = 0$ otherwise. Set

$$w(n) := \left(\Sigma_{d_i | n+h_i \ (i=1,\ldots,k)} \lambda_{d_1,\ldots,d_k} \right)^2,$$

$$I_k(F) := \int_0^1 \cdots \int_0^1 F(t_1, \ldots, t_k)^2 dt_1 dt_2 \cdots dt_k,$$

$$J_k^{(s)}(F) := \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \ldots, t_k) dt_s \right)^2 dt_1 \cdots dt_{s-1} dt_{s+1} \cdots dt_k.$$

Maynard's approach

Suppose that $\mathrm{EH}(\theta)$ holds. Provided $I_k(F)\prod_{s=1}^k K_k^{(s)}(F) \neq 0$,

$$S_1 \sim \frac{\varphi(W)^k}{W^{k+1}} N(\log R)^k I_k(F),\ S_2 \sim \frac{\varphi(W)^k}{W^{k+1}} \cdot \frac{N}{\log N} (\log R)^{k+1} \sum_{s=1}^{k} J_k^{(s)}(F),$$

and thus

$$\frac{S_2}{S_1} \to \left(\frac{\theta}{2} - \delta\right) \frac{\sum_{s=1}^k J_k^{(s)}(F)}{I_k(F)} \quad \text{as } N \to \infty.$$

Define

$$M_k = \sum_F \frac{\sum_{s=1}^k J_k^{(s)}(F)}{I_k(F)}.$$

Then there are infinitely many $n \equiv \nu \pmod{W}$ such that $\{n + h_i : \ i = 1, \ldots, k\}$ contains at least $m = \lceil \theta M_k / 2 \rceil$ primes, in particular

$$\liminf_{n\to\infty} (p_{n+m-1} - p_n) \leqslant d(\mathcal{H}) < \infty.$$

Maynard-Tao Theorem

Theorem (Maynard, 2013, `arXiv:1311.4600`).
(i) $M_5 > 2$, thus the EH conjecture implies that $\liminf_{n\to\infty}(p_{n+1} - p_n) \leqslant 12$ since $\{0, 2, 6, 8, 12\}$ is admissible.

(ii) $M_{105} > 4$ and thus $\liminf_{n\to\infty}(p_{n+1} - p_n) \leqslant 600$ (since EH(θ) holds fore all $0 < \theta < \frac{1}{2}$ and there is an admissible 105-tuple with diameter 600).

(iii) For large values of k, we have $M_k > \log k - 2\log\log k - 2$.

Maynard-Tao Theorem (2013). There is an absolute constant $C > 0$ such that

$$\liminf_{n\to\infty}(p_{n+m} - p_n) \leqslant Cm^3e^{4m}$$

for all $m = 1, 2, 3, \ldots$.

Polymath. $\liminf_{n\to\infty}(p_{n+1} - p_n) \leqslant 246$ (P. Nielsen), and $M_k > \log k + O(1)$.

Consecutive primes and Legendre symbols

Theorem (H. Pan & Z.-W. Sun, `arXiv:1405.0290`) Let m be any positive integer and let $\delta_1, \delta_2 \in \{1, -1\}$. Then, for some constant $C_m > 0$ there are infinitely many integers $n > 1$ with $p_{n+m} - p_n \leqslant C_m$ such that

$$\left(\frac{p_{n+i}}{p_{n+j}}\right) = \delta_1 \quad \text{and} \quad \left(\frac{p_{n+j}}{p_{n+i}}\right) = \delta_2$$

for all $0 \leqslant i < j \leqslant m$, where p_k denotes the k-th prime, and $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol for any odd prime p.

Conjecture. Let $m \in \mathbb{Z}^+$, $\delta \in \{1, -1\}$, and $\delta_{ij} \in \{\pm 1\}$ for all $0 \leqslant i < j \leqslant m$. Then, there are infinitely many integers $n > 1$ such that

$$\left(\frac{p_{n+i}}{p_{n+j}}\right) = \delta_{ij} = \delta \left(\frac{p_{n+j}}{p_{n+i}}\right) \quad \text{for all } 0 \leqslant i < j \leqslant m.$$

Examples

Example 1. The smallest integer $n > 1$ with

$$\left(\frac{p_{n+i}}{p_{n+j}}\right) = 1 \quad \text{for all } i, j = 0, \ldots, 6 \text{ with } i \neq j$$

is 176833. The 7 consecutive primes p_{176833}, p_{176834}, $\ldots$, p_{178639} have concrete values:

2434589, 2434609, 2434613, 2434657, 2434669, 2434673, 2434681.

Example 2. The smallest integer $n > 1$ with

$$\left(\frac{p_{n+i}}{p_{n+j}}\right) = -1 \quad \text{for all } i, j = 0, \ldots, 5 \text{ with } i \neq j$$

is 2066981, and the 6 consecutive primes $p_{2066981}$, $p_{2066982}$, $\ldots$, $p_{2066986}$ have concrete values:

33611561, 33611573, 33611603, 33611621, 33611629, 33611653.

Examples (continued)

Example 3. The smallest integer $n > 1$ with

$$-\left(\frac{p_{n+i}}{p_{n+j}}\right) = 1 = \left(\frac{p_{n+j}}{p_{n+i}}\right) \quad \text{for all } 0 \leqslant i < j \leqslant 6$$

is 7455790, and the 7 consecutive primes $p_{7455790}$, $p_{7455791}$, $\ldots$, $p_{7455796}$ have concrete values:

$$131449631,\ 131449639,\ 131449679,\ 131449691,$$
$$131449727,\ 131449739,\ 131449751.$$

Example 4. The smallest integer $n > 1$ with

$$\left(\frac{p_{n+i}}{p_{n+j}}\right) = 1 = -\left(\frac{p_{n+j}}{p_{n+i}}\right) \quad \text{for all } 0 \leqslant i < j \leqslant 5$$

is 59753753, and the 6 consecutive primes $p_{59753753}$, $p_{59753754}$, $\ldots$, $p_{59753758}$ have concrete values:

$$1185350899,\ 1185350939,\ 1185350983,$$
$$1185351031,\ 1185351059,\ 1185351091.$$

Two Lemmas

Lemma 1 (Maynard-Tao) Let m be any positive integer. Then there is an integer $k > m$ depending only on m such that if $\mathcal{H} = \{h_i : \ i = 1, \ldots, k\}$ is an admissible set of cardinality k and $W = q_0 \prod_{p \leqslant w} p$ (with $q_0 \in \mathbb{Z}^+$) is relatively prime to $\prod_{i=1}^{k} h_i$ with $w = \log\log\log x$ large enough, then for some integer $n \in [x, 2x]$ with $W \mid n$ there are more than m primes among $n + h_1, n + h_2, \ldots, n + h_k$.

Lemma 2 (Pan-Sun) Let $k > 1$ be an integer. Then there is an admissible set $\mathcal{H} = \{h_1, \ldots, h_k\}$ with $h_1 = 0 < h_2 < \ldots < h_k$ which has the following properties:

(i) All those $h_1, h_2, \ldots, h_k$ are multiples of $K = 4 \prod_{p<2k} p$.

(ii) Each $h_i - h_j$ with $1 \leqslant i < j \leqslant k$ has a prime divisor $p > 2k$ with $h_i \not\equiv h_j \pmod{p^2}$.

(iii) If $1 \leqslant i < j \leqslant k$, $1 \leqslant s < t \leqslant k$ and $\{i, j\} \neq \{s, t\}$, then no prime $p > 2k$ divides both $h_i - h_j$ and $h_s - h_t$.

Proof of the Theorem

By Lemma 1, there is an integer $k = k_m > m$ depending on m such that for any admissible set $\mathcal{H} = \{h_1, \ldots, h_k\}$ of cardinality k if x is sufficiently large and $\prod_{i=1}^{k} h_i$ is relatively prime to $W = 4\prod_{p \leqslant w} p$ then for some integer $n \in [x/W, 2x/W]$ there are more than m primes among $Wn + h_1, Wn + h_2, \ldots, Wn + h_k$, where $w = \log\log\log x$.

Let $\mathcal{H} = \{h_1, \ldots, h_k\}$ with $h_1 = 0 < h_2 < \ldots < h_k$ be an admissible set satisfying the conditions (i)-(iii) in Lemma 2. Clearly $K = 4\prod_{p \leqslant 2k} p \equiv 0 \pmod 8$. Let x be sufficiently large with the interval $(h_k, w]$ containing more than $h_k - k$ primes. Note that $8 \mid W$ since $w \geqslant 2$.

Let $\delta := \delta_1\delta_2$. For any integer $b \equiv \delta \pmod K$ and each prime $p < 2k$, clearly $b + h_i \equiv \delta + 0 \pmod p$ and hence $\gcd(b + h_i, p) = 1$ for all $i = 1, \ldots, k$.

Proof of the Theorem (continued)

For any $1 \leqslant i < j \leqslant k$, the number $h_i - h_j$ has a prime divisor $p_{ij} > 2k$ with $h_i \not\equiv h_j \pmod{p_{ij}^2}$. Suppose that $p > 2k$ is a prime dividing $\prod_{1 \leqslant i < j \leqslant k}(h_i - h_j)$, then there is a unique pair $\{i, j\}$ with $1 \leqslant i < j \leqslant k$ such that $h_i \equiv h_j \pmod{p}$. Note that $p \leqslant h_k$. All the $k - 2 < (p-3)/2$ numbers $h_i - h_s$ with $1 \leqslant s \leqslant k$ and $s \neq i, j$ are relatively prime to p, so there is an integer $r_p \not\equiv h_i - h_s \pmod{p}$ for all $s = 1, \ldots, k$ such that

$$\left(\frac{r_p\,\delta}{p}\right) = \begin{cases} \delta_2 & \text{if } p = p_{ij}, \\ 1 & \text{otherwise.} \end{cases}$$

So, for any integer $b \equiv r_p - h_i \pmod{p}$, we have $b + h_s \not\equiv 0 \pmod{p}$ for all $s = 1, \ldots, k$.

Assume that $S = \{h_1, h_1 + 1, \ldots, h_k\} \setminus \mathcal{H}$ is a set $\{a_i : \ i = 1, \ldots, t\}$ of cardinality $t > 0$. Clearly $t \leqslant h_k - k + 1$ and hence we may choose t distinct primes $q_1, \ldots, q_t \in (h_k, w]$. If $b \equiv -a_i \pmod{q_i}$, then $b + h_s \equiv h_s - a_i \not\equiv 0 \pmod{q_i}$ for all $s = 1, \ldots, k$ since $0 < |h_s - a_i| < h_k < q_i$.

Proof of the Theorem (continued)

Let

$$Q = \left\{ p \in (2k, w] : \ p \nmid \prod_{1 \leqslant i < j \leqslant k} (h_i - h_j) \right\} \setminus \{q_i : \ i = 1, \ldots, t\}.$$

For any prime $q \in Q$, there is an integer $r_q \not\equiv -h_i \pmod{q}$ for all $i = 1, \ldots, k$ since $\mathcal{H}$ is admissible.

By the Chinese Remainder Theorem, there is an integer b satisfying the following (1)-(4).

(1) $b \equiv \delta = \delta_1 \delta_2 \pmod{K}$.
(2) $b \equiv r_p - h_i \equiv r_p - h_j \pmod{p}$ if $p > 2k$ is a prime dividing $h_i - h_j$ with $1 \leqslant i < j \leqslant k$.
(3) $b \equiv -a_i \pmod{q_i}$ for all $i = 1, \ldots, t$.
(4) $b \equiv r_q \pmod{q}$ for all $q \in Q$.

By the above analysis, $\prod_{s=1}^{k} (b + h_s)$ is relatively prime to W.

Proof of the Theorem (continued)

As $\mathcal{H}' = \{b + h_s : \ s = 1, \ldots, k\}$ is also an admissible set of cardinality k, for large x there is an integer $n \in [x/W, 2x/W]$ such that there are more than m primes among $Wn + b + h_s$ $(s = 1, \ldots, k)$. For $a_i \in S$, we have

$$Wn + b + a_i \equiv 0 - a_i + a_i = 0 \pmod{q_i}$$

and hence $Wn + b + a_i$ is composite since $W > q_i$. Therefore, there are consecutive primes $p_N, p_{N+1}, \ldots, p_{N+m}$ with $p_{N+i} = Wn + b + h_{s(i)}$ for all $i = 0, \ldots, m$, where $1 \leqslant s(0) < s(1) < \ldots < s(m) \leqslant k$. Note that

$$p_{N+m} - p_N = (Wn + b + h_{s(m)}) - (Wn + b + h_{s(0)}) = h_{s(m)} - h_{s(0)} \leqslant h_k.$$

For each $s = 1, \ldots, k$, clearly $Wn + b + h_s \equiv 0 + \delta + 0 = \delta \pmod 8$ and hence

$$\left(\frac{-1}{Wn + b + h_s}\right) = \delta \ \text{ and } \ \left(\frac{2}{Wn + b + h_s}\right) = 1.$$

Proof of the Theorem (continued)

As $p_{N+i} = Wn + b + h_{s(i)} \equiv \delta \pmod 8$ for all $i = 0, \ldots, m$, by the Quadratic Reciprocal Law we have

$$\left(\frac{p_{n+j}}{p_{N+i}}\right) = \delta \left(\frac{p_{n+i}}{p_{N+j}}\right) \quad \text{for all } 0 \leqslant i < j \leqslant m.$$

Let $0 \leqslant i < j \leqslant m$. Then

$$\left(\frac{p_{N+i}}{p_{N+j}}\right) = \left(\frac{h_{s(i)} - h_{s(j)}}{Wn + b + h_{s(j)}}\right) = \delta \left(\frac{h_{ij}}{Wn + b + h_{s(j)}}\right),$$

where h_{ij} is the odd part of $h_{s(j)} - h_{s(i)}$. For any prime divisor p of h_{ij}, clearly $p \leqslant h_k \leqslant w$ and

$$\left(\frac{p}{Wn + b + h_{s(j)}}\right) = \delta^{(p-1)/2} \left(\frac{Wn + b + h_{s(j)}}{p}\right) = \delta^{(p-1)/2} \left(\frac{b + h_{s(j)}}{p}\right)$$

If $p < 2k$, then $p \mid K$, hence $b + h_{s(j)} \equiv \delta + 0 \pmod p$ and thus

$$\left(\frac{p}{Wn + b + h_{s(j)}}\right) = \delta^{(p-1)/2} \left(\frac{b + h_{s(j)}}{p}\right) = \delta^{(p-1)/2} \left(\frac{\delta}{p}\right) = 1.$$

Proof of the Theorem (continued)

If $p > 2k$, then by the choice of b we have

$$\left(\frac{p}{Wn+b+h_{s(j)}}\right) = \delta^{(p-1)/2}\left(\frac{b+h_{s(j)}}{p}\right) = \delta^{(p-1)/2}\left(\frac{r_p}{p}\right)$$
$$= \left(\frac{r_p\,\delta}{p}\right) = \begin{cases} \delta_2 & \text{if } p = p_{s(i),s(j)}, \\ 1 & \text{otherwise.} \end{cases}$$

Recall that $p_{s(i),s(j)} \| h_{ij}$. Therefore,

$$\left(\frac{p_{N+i}}{p_{N+j}}\right) = \delta\left(\frac{h_{ij}}{Wn+b+h_{s(j)}}\right) = \delta\delta_2 = \delta_1$$

and

$$\left(\frac{p_{N+j}}{p_{N+i}}\right) = \delta\left(\frac{p_{N+i}}{p_{N+j}}\right) = \delta_2.$$

This concludes the proof.

Artin's Primitive Root Conjecture

Artin's Primitive Root Conjecture (1927). Let $g \neq -1$ be an integer which is not a square. Then there are infinitely many primes p for which g is a primitive root modulo p.

C. Hooley (1967): Artin's conjecture holds under the Extended Riemann Hypothesis for Dedekind zeta functions.

By combining Hooley's work with the Manard-Tao method, P. Pollack obtained the following result.

P. Pollack (arXiv:1404.4007). Let $g \neq -1$ be an integer which is not a square. Let $q_1 < q_2 < \ldots$ denote the sequence of primes having g as a primitive root. For any positive integer m, there is a constant $C_m > 0$ not depending on g such that

$$\liminf_{n \to +\infty} (q_{n+m} - q_n) \leqslant C_m.$$

Consecutive primes and primitive roots

Conjecture (Z.-W. Sun, 2014). For any positive integer m, there are infinitely many positive integers n such that p_{n+i} is a primitive root modulo p_{n+j} for any distinct i and j among $0, 1, \ldots, m$.

Example. The least $n \in \mathbb{Z}^+$ with p_{n+i} a primitive root modulo p_{n+j} for any distinct i and j among $0, 1, 2, 3$ is 8560. Note that

$$p_{8560} = 88259,\ p_{8561} = 88261 \text{ and } \ p_{8562} = 88289.$$

Theorem (H. Pan & Z.-W. Sun, `arXiv:1405.0290`). The conjecture holds under the Extended Riemann Hypothesis.

A Firoozbakht-type conjecture for twin primes

Firoozbakht's Conjecture (1982). The sequence $(\sqrt[n]{p_n})_{n\geqslant 1}$ is strictly decreasing.

Conjecture (Z.-W. Sun, 2012) (i) If $\{t_1, t_1+2\}, \ldots, \{t_n, t_n+2\}$ are the first n pairs of twin primes, then the first prime t_{n+1} in the next pair of twin primes is smaller than $t_n^{1+1/n}$, i.e., $\sqrt[n]{t_n} > \sqrt[n+1]{t_{n+1}}$.
(ii) The sequence $(\sqrt[n+1]{T(n+1)}/\sqrt[n]{T(n)})_{n\geqslant 9}$ is strictly increasing with limit 1, where $T(n) = \sum_{k=1}^{n} t_k$.

Remark. Via `Mathematica` I verified that $\sqrt[n]{t_n} > \sqrt[n+1]{t_{n+1}}$ for all $n = 1, \ldots, 500000$, and

$$\sqrt[n+1]{T(n+1)}/\sqrt[n]{T(n)} < \sqrt[n+2]{T(n+2)}/\sqrt[n+1]{T(n+1)}$$

for all $n = 9, 10, \ldots, 500000$. Note that $t_{500000} = 115438667$.

After I made the conjecture public, Marek Wolf verified the inequality $\sqrt[n]{t_n} > \sqrt[n+1]{t_{n+1}}$ for all the 44849427 pairs of twin primes below $2^{34} \approx 1.718 \times 10^{10}$.

Unification of Goldbach's conjecture and the twin prime conjecture

Unification of Goldbach's Conjecture and the Twin Prime Conjecture (Sun, 2014-01-29). For any integer $n > 2$, there is a prime q with $2n - q$ and $p_{q+2} + 2$ both prime.

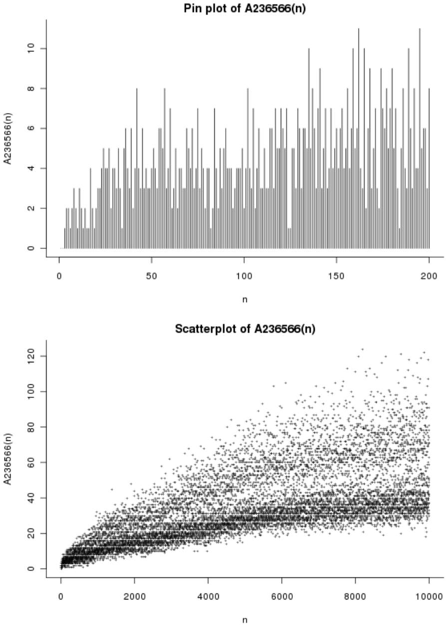
We have verified the conjecture for n up to 2×10^8. Clearly, it is stronger than Goldbach's conjecture. Now we explain why it implies the twin prime conjecture.

In fact, if all primes q with $p_{q+2} + 2$ prime are smaller than an even number $N > 2$, then for any such a prime q the number $N! - q$ is composite since

$$N! - q \equiv 0 \pmod{q} \text{ and } N! - q \geqslant q(q+1) - q > q.$$

Example. $20 = 3 + 17$ with 3, 17 and $p_{3+2} + 2 = 11 + 2 = 13$ all prime.

Graph for $a(n) = |\{q < 2n : \ q, 2n-q, \ p_{q+2}+2 \text{ are all prime}\}|$



Super Twin Prime Conjecture

If $p, p+2$ and $\pi(p)$ are all prime, then we call $\{p, p+2\}$ a *super twin prime pair*.

Super Twin Prime Conjecture (Sun, 2014-02-05). Any integer $n > 2$ can be written as $k + m$ with k and m positive integers such that $p_k + 2$ and $p_{p_m} + 2$ are both prime.

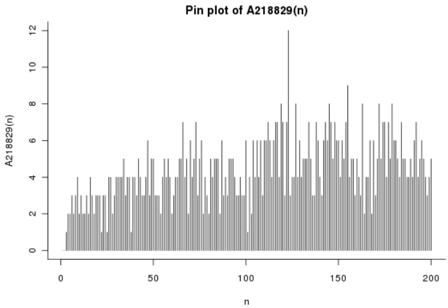
Example. $22 = 20 + 2$ with $p_{20} + 2 = 71 + 2 = 73$ and $p_{p_2} + 2 = p_3 + 2 = 5 + 2 = 7$ both prime.

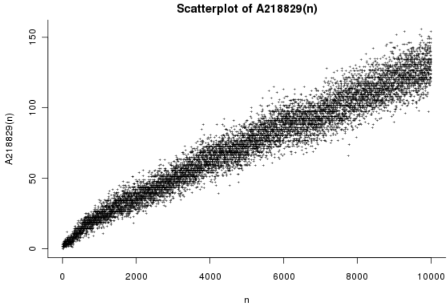
Remark. If all those positive integer m with $p_{p_m} + 2$ prime are smaller than an integer $N > 2$, then by the conjecture, for each $j = 1, 2, 3, \ldots$, there are positive integers $k(j)$ and $m(j)$ with $k(j) + m(j) = jN$ such that $p_{k(j)} + 2$ and $p_{p_{m(j)}} + 2$ are both prime, and hence $k(j) \in ((j-1)N, jN)$ since $m(j) < N$; thus

$$\sum_{j=1}^{\infty} \frac{1}{p_{k(j)}} \geqslant \sum_{j=1}^{\infty} \frac{1}{p_{jN}},$$

which is impossible since the series on the right-hand side diverges while the series on the left-hand side converges by Brun's theorem.

Graph for $a(n) = |\{0 < k < n: \ p_k + 2 \text{ and } p_{p_{n-k}} + 2 \text{ are both prime}\}|$





Concluding remarks

The current methods of Yitang Zhang or Mynard-Tao could not be modified to prove the Twin Prime Conjecture, To solve the Twin Prime Conjecture, number theorists must invent new tools and build a new powerful theory! There is a long way to go!

I have verified the Super Twin Prime Conjecture for all $n = 3, \ldots, 10^9$. In my opinion, **the solution of the Super Twin Prime Conjecture might be beyond the intelligence of human beings!**

Thank you!