A talk given at Xiamen Univ. (March 21, 2014)
and Tsinghua Univ. (April 18, 2014)
and Zhejiang Normal Univ. (June 28, 2014)
and the NCTS Conference *Impact of Computation on Number Theory*
(Hsinchu, July 29 – August 3, 2014)

Problems on Combinatorial Properties of Primes

Zhi-Wei Sun

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

August 3, 2014

Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate. To convince oneself, one has only to glance at the tables of primes which some people took the trouble to computer beyond a hundred thousand, and one perceives that there is no order and no rule.

— L. Euler

Abstract

For $x \geqslant 0$ let $\pi(x)$ be the number of primes not exceeding x. The asymptotic behaviors of the prime-counting function $\pi(x)$ and the n-th prime p_n have been studied intensively in analytic number theory. Surprisingly, we find that $\pi(x)$ and p_n have many combinatorial properties which should not be ignored. In this talk we will introduce many new open problems on combinatorial properties of primes as well as some connections between primes and partition functions. We will also mention our computational evidence to support the related conjectures.

Part I. Introduction to $\pi(x)$, p_n, $p(n)$ and $q(n)$

The prime-counting function $\pi(x)$ and the n-th prime p_n

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

The prime-counting function:

$$\pi(x) = |\{p \leqslant x : \ p \text{ is prime}\}|,$$

i.e., $\pi(x)$ is the number of primes not exceeding x.

For example,

$$\pi(10) = 4, \ \pi(20) = 8, \ \pi(30) = 10, \ \pi(40) = 12, \ \pi(50) = 15.$$

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

For example,

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

Primes are generally *irregular*. No closed formula for $\pi(x)$ or p_n has been found.

Asymptotic behaviors of $\pi(x)$ and p_n

The primes have tantalized mathematicians since the Greeks, because they appear to be somewhat randomly distributed but not completely so.

— W. T. Gowers (2002)

The Prime Number Theorem. We have

$$\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \quad \text{as } x \to +\infty.$$

This has the following equivalent form:

$$p_n \sim n \log n \quad \text{as } n \to +\infty.$$

If Riemann's Hypothesis is true, then

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x} \log x)$$

and

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

The partition function $p(n)$

A *partition* of a positive integer n is a way to write n as a sum of positive integers with the order of addends ignored. The partition function $p(n)$ denotes the total number of partitions of n.

Example. $p(5) = 7$ since

$$\begin{aligned} 5 =& 1+4 = 2+3 = 1+1+3 = 1+2+2 \\ =& 1+1+1+2 = 1+1+1+1+1. \end{aligned}$$

Hardy-Ramanujan Formula:

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4\sqrt{3}n} \quad \text{as } n \to +\infty,$$

and hence

$$\log p(n) \sim c\sqrt{n} \ \text{ with } c = \pi\sqrt{\frac{2}{3}}.$$

Note that $p(n)$ grows eventually faster than any polynomial in n but slightly slower than 2^n.

The strict partition function $q(n)$

A *strict partition* of a positive integer n is a way to write n as a sum of *distinct* positive integers with the order of addends ignored.

The **strict partition function** $q(n)$ denotes the total number of strict partitions of n.

Example. $q(5) = 3$ since

$$5 = 1 + 4 = 2 + 3.$$

Asymptotic Formula:

$$q(n) \sim \frac{e^{\pi\sqrt{n/3}}}{4(3n^3)^{1/4}} \quad \text{as } n \to +\infty,$$

and hence

$$\log q(n) \sim \frac{\pi}{\sqrt{3}}\sqrt{n}.$$

Note that $q(n)$ also grows eventually faster than any polynomial in n but slightly slower than 2^n.

Euler's observation and the function $\bar{q}(n)$

Euler: $q(n)$ is also the number of unordered ways to write n as a sum of positive odd numbers.

For example, $q(5) = 3$ and $5 = 1+1+3 = 1+1+1+1+1$.

We define $\bar{q}(n) = p(n) - q(n)$, which is the number of partitions of n with some part repeated (or even).

For example,

$$\bar{q}(5) = p(5) - q(5) = 7 - 3 = 4,$$

$$5 = 1+1+3 = 1+2+2 = 1+1+1+2 = 1+1+1+1+1$$

and

$$5 = 1+4 = 2+3 = 1+2+2 = 1+1+1+2.$$

Part II. Combinatorial properties of $\pi(x)$

On $\pi(n), \pi(2n), \ldots, \pi(n^2)$

Bertrand's Postulate (proved by Chebyshev in 1850).
$\pi(2n) > \pi(n)$ for any positive integer n.

Legendre's Conjecture. For any positive integer n, there is a prime between n^2 and $(n+1)^2$.

Oppermann's Refinement of Legendre's Conjecture. For any integer $n > 1$, we have

$$\pi((n-1)n) < \pi(n^2) < \pi(n(n+1)).$$

Our computation suggests that for any integer $n > 1$ we have

$$\pi(n) < \pi(2n) < \ldots < \pi((n-1)n) < \pi(n^2).$$

Conjectures on divisibilities of $\pi(kn)$

Conjecture 1 (Sun, 2014-02-09). For any integer $n > 1$, $\pi(kn)$ is prime for some $k = 1, \ldots, n$. Moreover, for every $n = 1, 2, 3, \ldots$, there is a positive integer $k < 3\sqrt{n} + 3$ with $\pi(kn)$ prime. We also have $|\{1 \leqslant k \leqslant n : \ \pi(kn) \text{ is prime}\}| \sim \pi(n)/2$.

Example. $\pi(6 \times 10) = 17$ is prime.

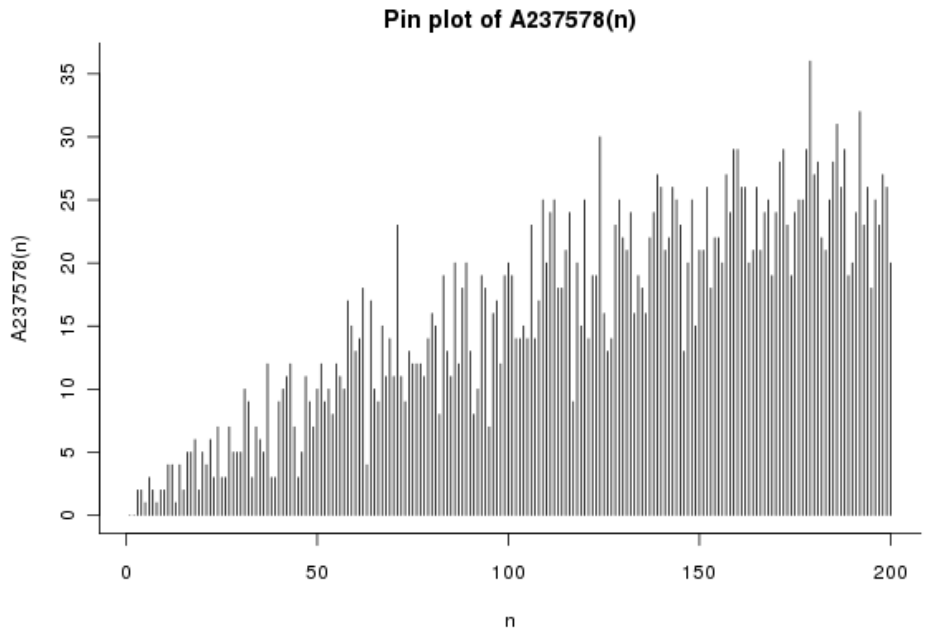
Remark. We have verified the conjecture for n up to 10^7.

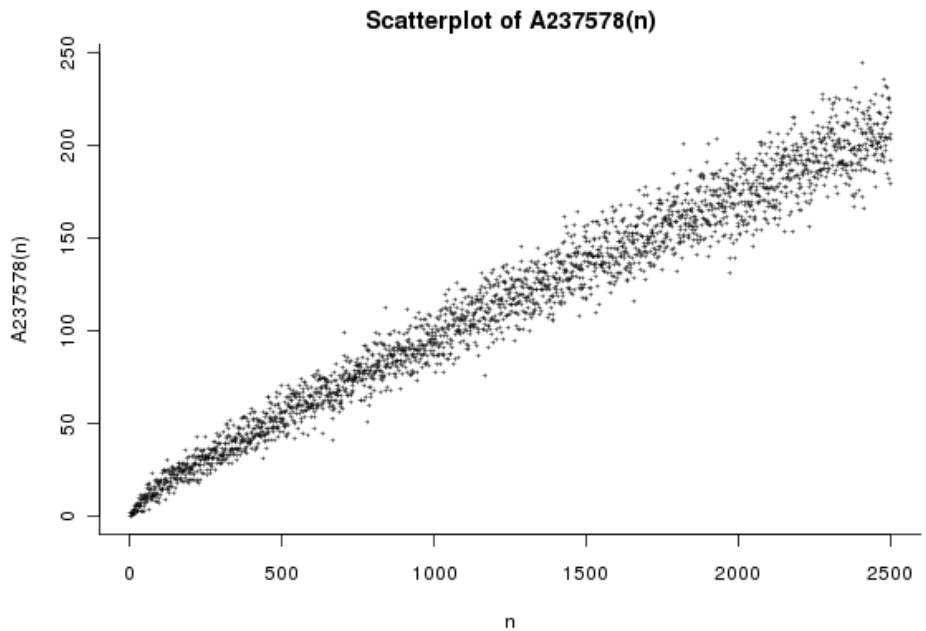
The conjecture is somewhat incredible and mysterious, nevertheless our numerical data and graphs provide strong evidences for its truth.

Conjecture 2 (Sun, 2014-02-10). For any positive integer n, $\pi(kn)$ is divisibly by n for some $k = 1, \ldots, p_n - 1$.

Conjecture 3 (Sun, 2014-02-20). Let $n > 1$ be an integer. Then $\pi(jn) \mid \pi(kn)$ for some $1 \leqslant j < k \leqslant n$ with $k \equiv 1 \pmod{j}$.

Graph for $a(n) = |\{0 < k < n : \ \pi(kn) \text{ is prime}\}|$





$\pi(kn)$, $\pi_2(kn)$ and squares

Conjecture 1 (Sun, 2014-02-10) For any positive integer n, there is a positive integer $k < p_n$ such that $\pi(kn)$ is a square.

Conjecture 2 (Sun, 2014-02-14). Let n be any positive integer. Then $\pi_2(kn)$ is a square for some $k = 1, \ldots, n$, where

$$\pi_2(x) := |\{p \leqslant x : \ p \text{ and } p-2 \text{ are both prime}\}|$$

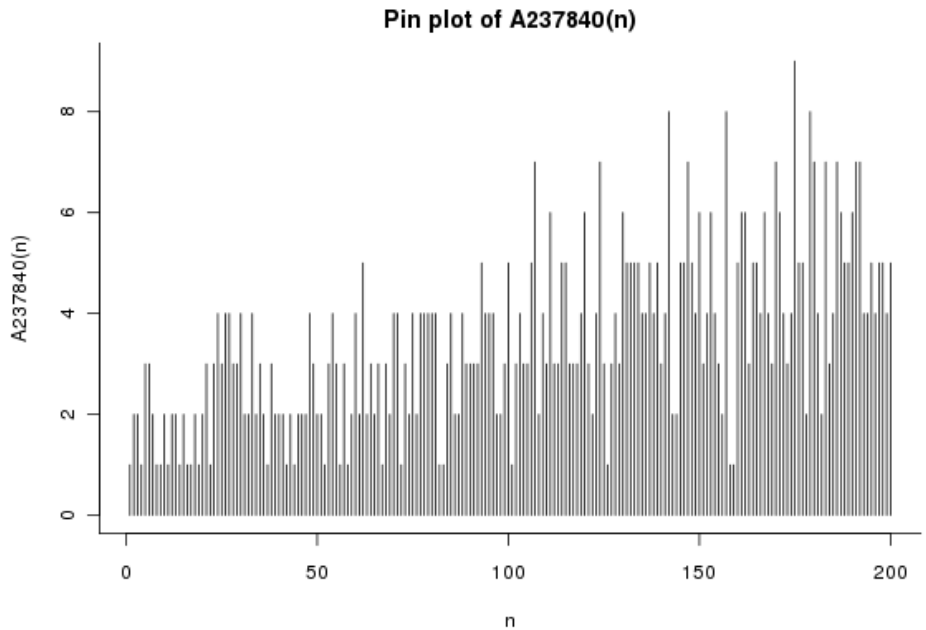
is the number of twin prime pairs not exceeding x.

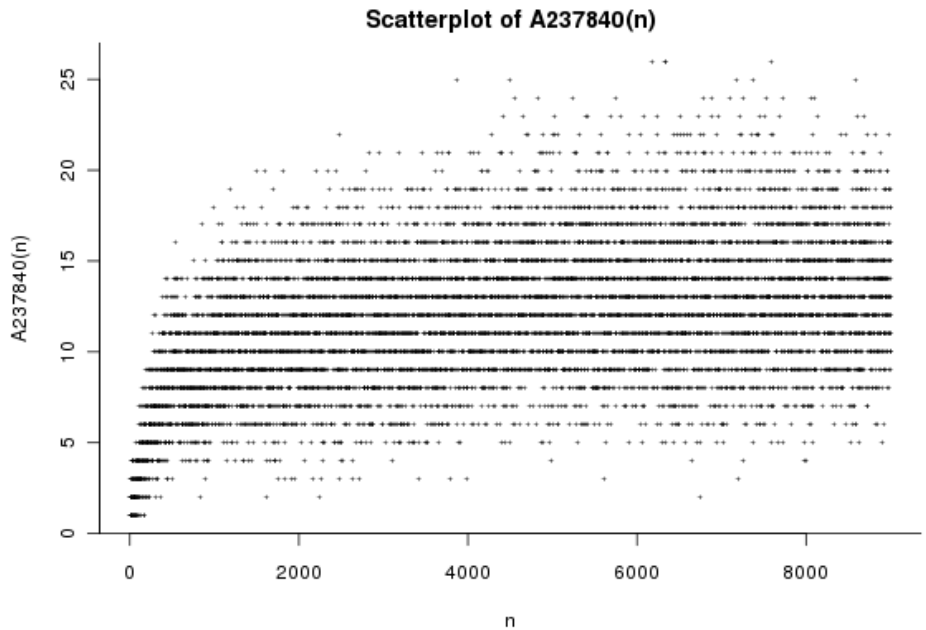
Remark. We have verified this for all $n = 1, \ldots, 22000$.

Example. For $n = 19939$ we may take $k = 12660$ since

$$\pi_2(12660 \times 19939) = \pi_2(252427740) = 1000^2 = 10^6.$$

Graph for $a(n) = |\{0 < k \leqslant n : \ \pi_2(kn) \text{ is a square}\}|$





Conjectures on $\pi(\pi(x))$

Conjecture (Sun, 2014-03-07) (i) For any integer $n > 2$, there is a prime $p \leqslant n$ with $\pi(\pi((p-1)n))$ prime.

(ii) For any positive integer n, $\pi(\pi(kn))$ is a square for some $k = 1, \ldots, n$.

(iii) For any positive integer n, $\pi(\pi(kn))$ is a triangular number for some positive integer $k \leqslant (n+1)/2$.

Remark. We have verified parts (ii) and (iii) for n up to 2×10^5 and 10^5 respectively.

Examples for part (ii):

$$\pi(\pi(8514 \times 9143)) = \pi(4550901) = 565^2,$$
$$\pi(\pi(37308 \times 98213)) = \pi(174740922) = 3123^2,$$
$$\pi(\pi(83187 \times 192969)) = \pi(715034817) = 6082^2.$$

Conjectures on $\pi(\pi(x))$

Conjecture (Sun, 2014-03-07) (i) For any integer $n > 2$, there is a prime $p \leqslant n$ with $\pi(\pi((p-1)n))$ prime.

(ii) For any positive integer n, $\pi(\pi(kn))$ is a square for some $k = 1, \ldots, n$.

(iii) For any positive integer n, $\pi(\pi(kn))$ is a triangular number for some positive integer $k \leqslant (n+1)/2$.

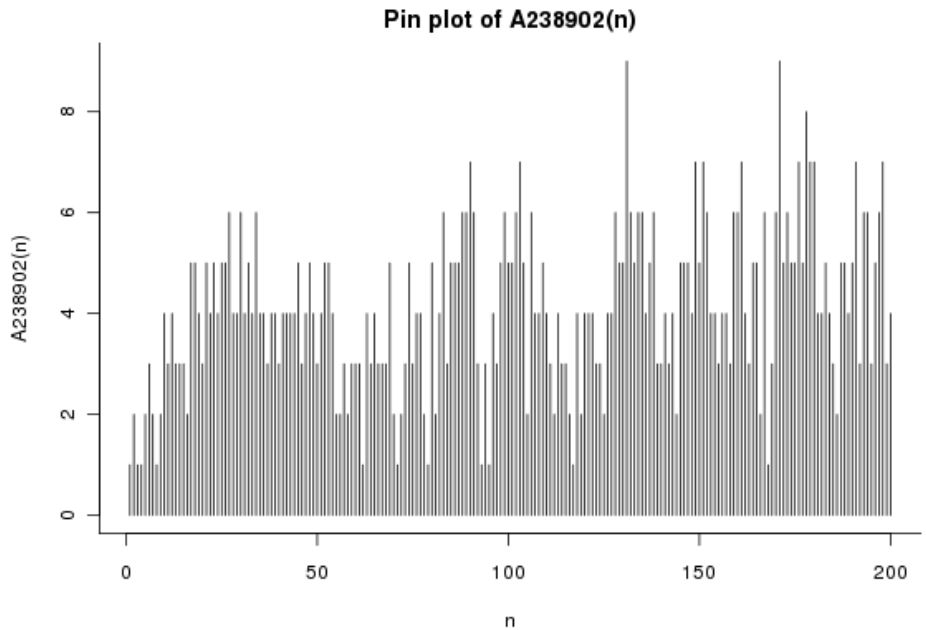
Remark. We have verified parts (ii) and (iii) for n up to 2×10^5 and 10^5 respectively.

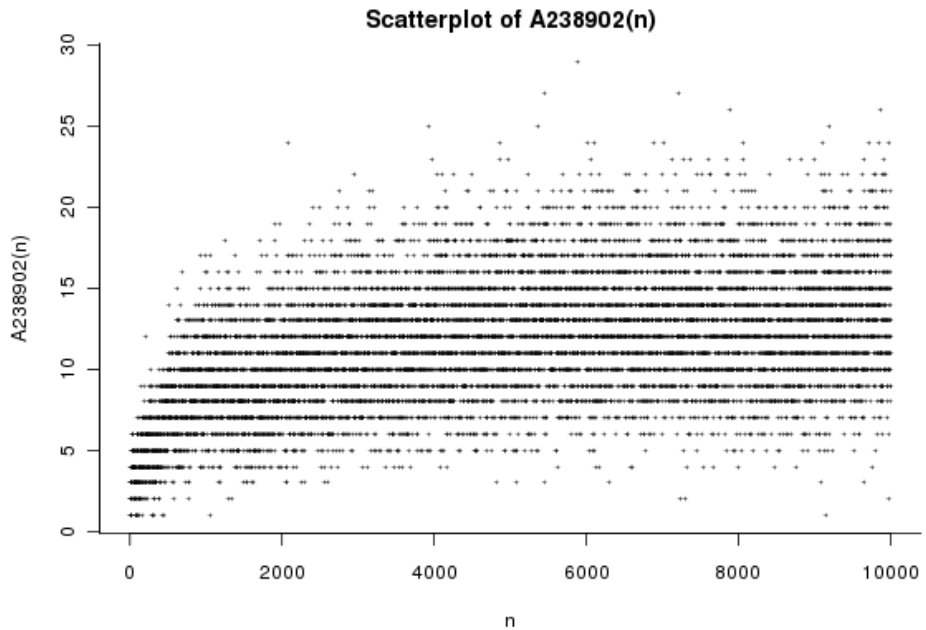
Examples for part (ii):

$$\pi(\pi(8514 \times 9143)) = \pi(4550901) = 565^2,$$
$$\pi(\pi(37308 \times 98213)) = \pi(174740922) = 3123^2,$$
$$\pi(\pi(83187 \times 192969)) = \pi(715034817) = 6082^2.$$

Part (ii) of the conjecture might never be solved by human beings!

Graph for $a(n) = |\{0 < k \leqslant n : \ \pi(\pi(kn)) \text{ is a square}\}|$





Conjectures on $\pi((k+1)n)-\pi(kn)$

Conjecture 1 (Sun, 2014-02-22) For any integer $n>1$, there is a positive integer $k<n$ such that the intervals $(kn,(k+1)n)$ and $((k+1)n,(k+2)n)$ contain the same number of primes, i.e.,

$$\pi(kn),\ \pi((k+1)n),\ \pi((k+2)n)$$

form a three-term arithmetic progression.

Remark. The famous Green-Tao theorem asserts that for each $k\geqslant 3$ there is a nontrivial k-term arithmetic progression of k primes.

Conjecture 2 (Sun, 2014-02-23) For any positive integer n, we have

$$|\{\pi((k+1)n)-\pi(kn):\ k=0,\ldots,n-1\}|\geqslant\sqrt{n-1},$$

and equality holds only when n is 2 or 26.

Conjectures involving $\pi(p)$

Conjecture 1 (Sun, 2013-02-08) For any integer $n > 4$, there is a prime $p < n$ with $pn + \pi(p)$ prime. Moreover, for every positive integer n, there is a prime $p < \sqrt{2n}\log(5n)$ with $pn + \pi(p)$ prime.

Conjecture 2 (Sun, 2013-03-02) For any integer $n > 2$, there is a prime $p \leqslant n$ with $2\pi(p) - (-1)^n$ and $pn + ((-1)^n - 3)/2$ both prime.

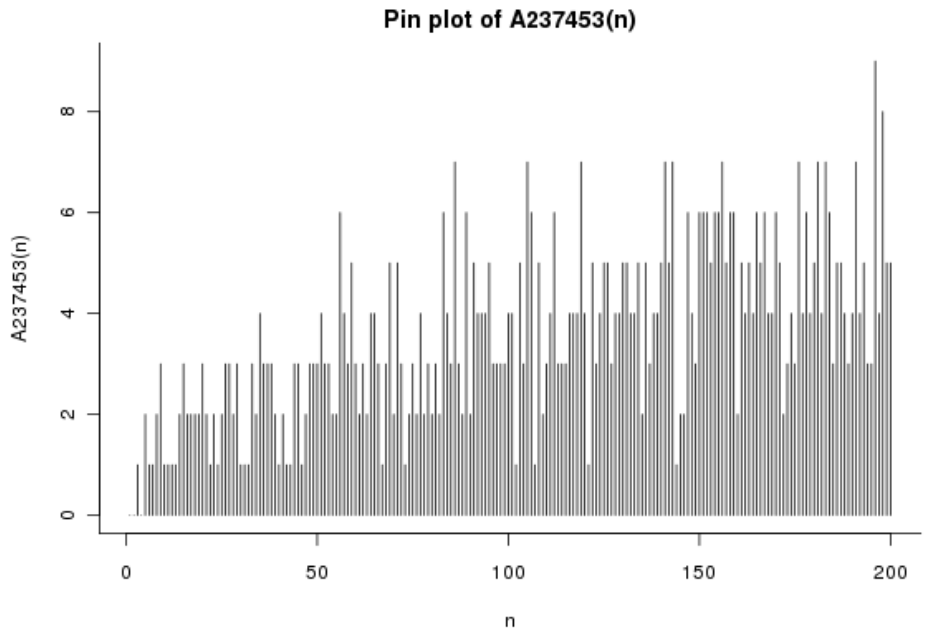
Remark. We have verified the two conjectures for n up to 10^8.

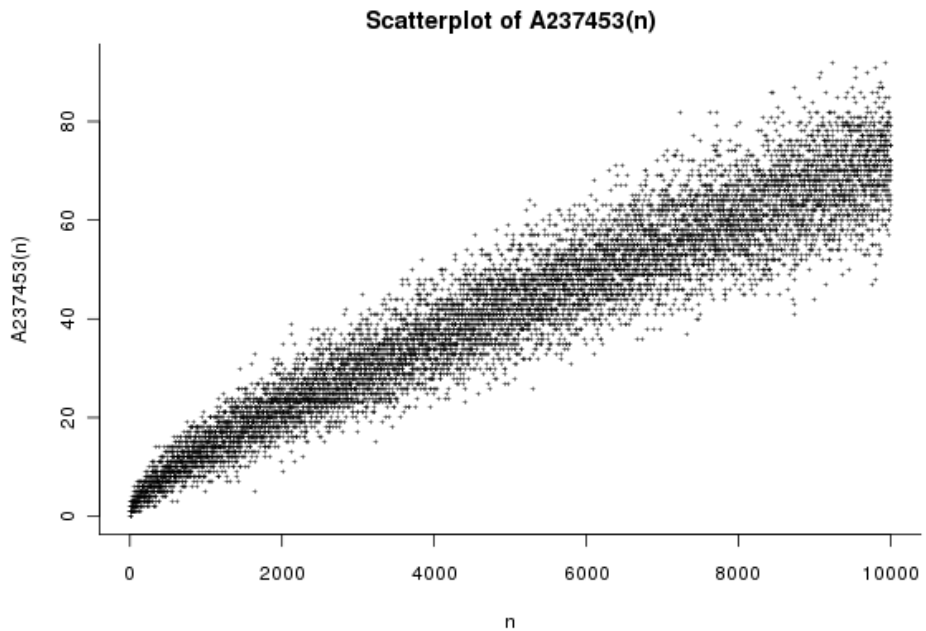
A prime p is called a **Chen prime** if $p + 2$ is a product of at most two primes.

Jing-run Chen proved in 1973 that there are infinitely many Chen primes.

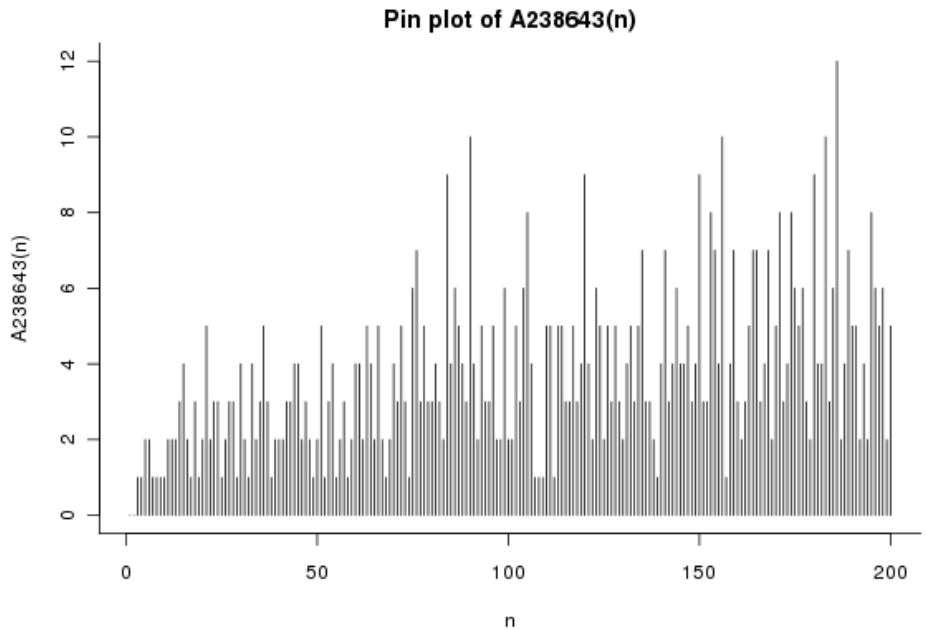
Conjecture 2 implies that for any odd prime p there is a prime $q \leqslant p$ with $pq - 2$ a Chen prime.

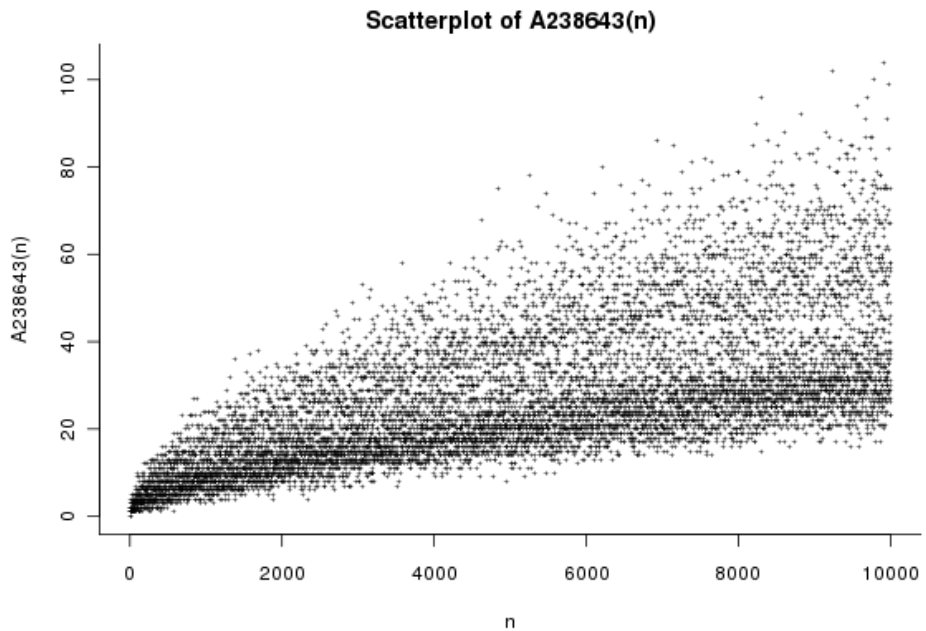
Graph for $a(n) = |\{p < n : \ pn + \pi(p) \text{ is prime}\}|$





Graph for $a(n) = |\{p \leqslant n : \ 2\pi(p) - (-1)^n \ \&\ pn + ((-1)^n - 3)/2 \text{ are both prime}\}|$





Goldbach-type conjectures involving $\pi(p)$

Goldbach's Conjecture. For any integer $n \geqslant 2$, there is a prime $p < 2n$ with $2n - p$ prime.
Goldbach's Weak Conjecture (finally proved by Helfgott in 2013). For any integer $n > 3$, $2n - 1$ can be written as a sum of three primes.

Conjecture 1 (Sun, 2014-02-06). (i) For any integer $n > 2$, there is a prime $p < 2n$ with $\pi(p)$ and $2n - p$ both prime.
(ii) For any integer $n > 36$, we can write $2n - 1$ as a sum of three elements of the set $\{p : \ p \text{ and } \pi(p) \text{ are both prime}\}$.

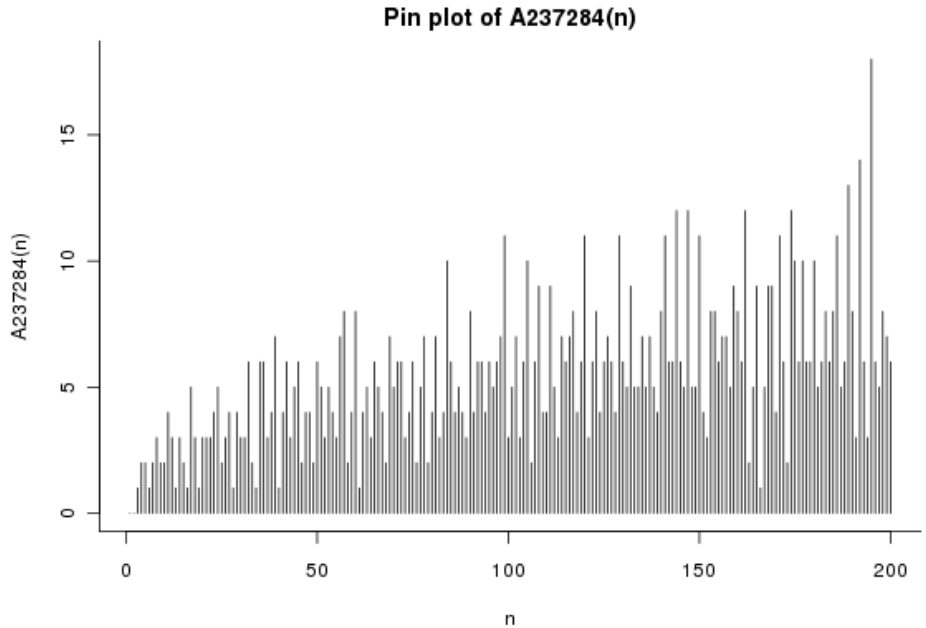
Conjecture 2 (Sun, 2013-11-24). (i) Every $n = 4, 5, \ldots$ can be written as $p + q - \pi(q)$, where p and q are odd primes not exceeding n.

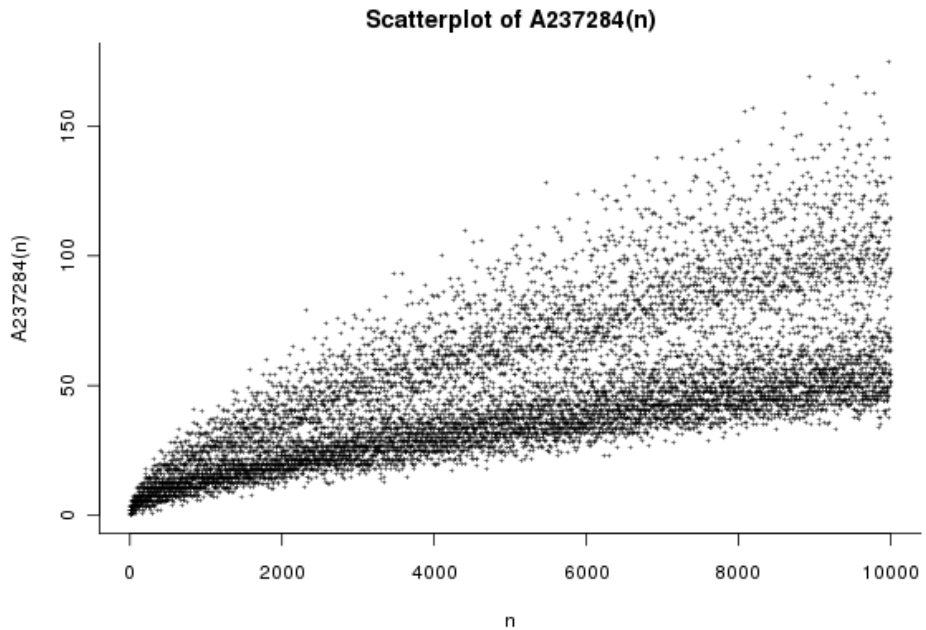
(ii) For any integer $n > 7$, there is a prime $p < n$ such that $n + p - \pi(p)$ is prime.

Remark. We have verified Conj. 2(i) for n up to 10^8.

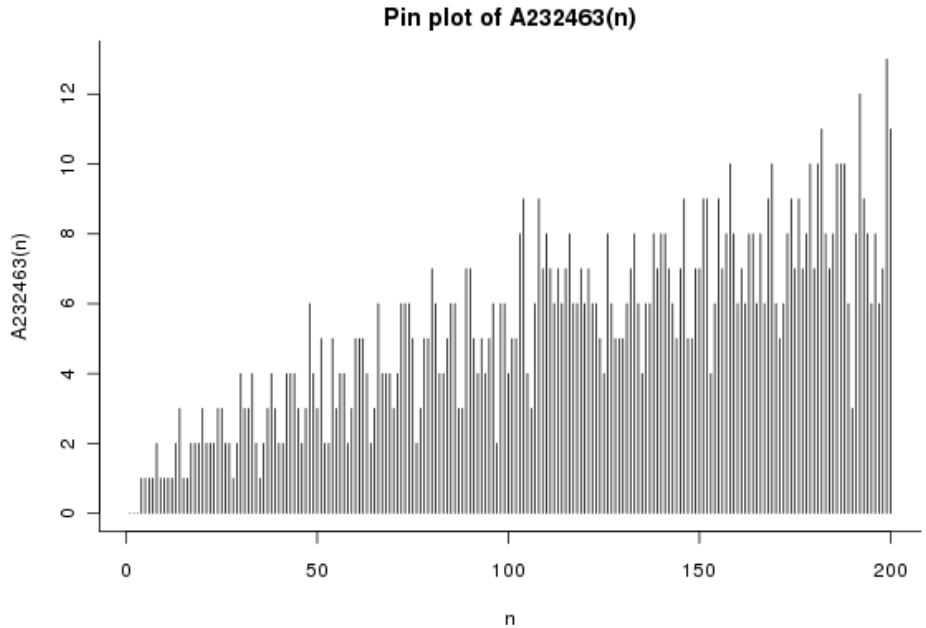
Example of Conj. 2(i). $9 = 7 + 5 - \pi(5)$ with 7 and 5 prime.

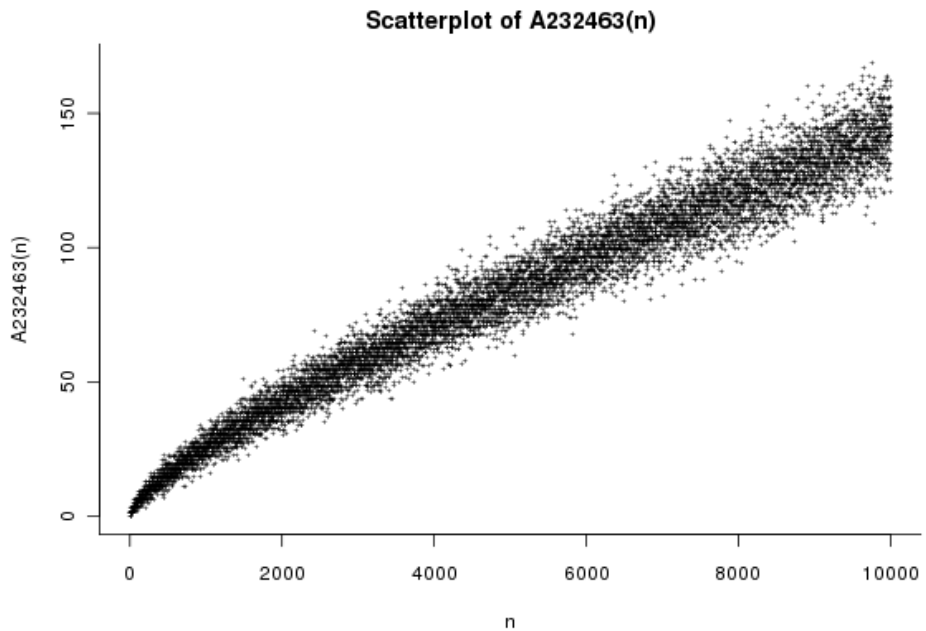
Graphs for $a(n) = |\{p < 2n : \ p,\ \pi(p) \text{ and } 2n - p \text{ are all prime}\}|$





Number of ways to write $n = p + q - \pi(q)$ with p and q primes not exceeding n





Conjectures on $\pi(n-p)$

A prime p with $2p+1$ also prime is called a Sophie Germain prime.

Conjecture 1 (Sun, 2014-02-13). For any integer $n > 4$, there is a prime $p < n$ such that $\pi(n-p)$ is a Sophie Germain prime. Also, for any integer $n > 8$ there is a prime $p < n$ such that $\pi(n-p)-1$ and $\pi(n-p)+1$ are twin prime.

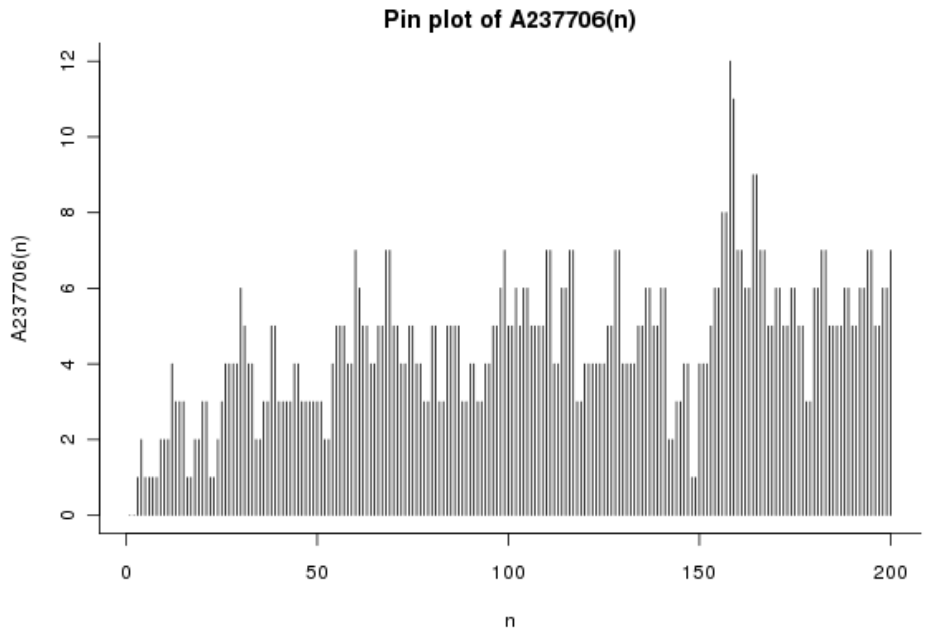
Conjecture 2 (Sun, 2014-02-12). For any integer $n > 2$, there is a prime $p < n$ such that $\pi(n-p)$ is a square (or a triangular number).

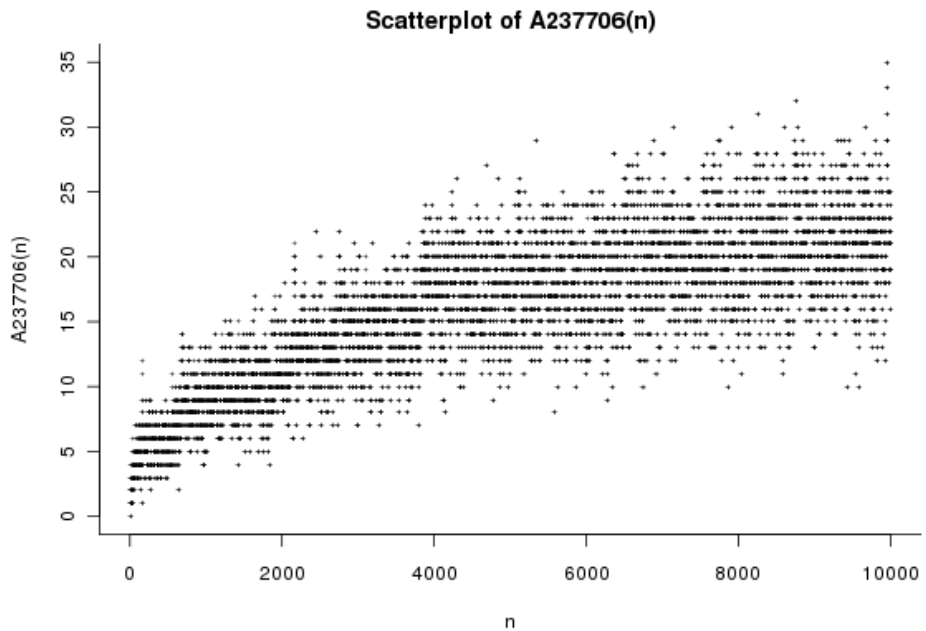
Remark. We have verified this for n up to 5×10^8.

Conjecture 3 (Sun, 2014-03-04). For any integers $m > 2$ and $n > 2$, there is a prime $p < n$ such that $\lfloor (n-p)/m \rfloor$ is a square.

Remark. $\lfloor (n-p)/m \rfloor$ is the number of multiples of m among $1, \ldots, n-p$.

Graph for $a(n) = |\{p < n : \ \pi(n-p) \text{ is a square}\}|$





Part III. Combinatorial properties involving p_n

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.

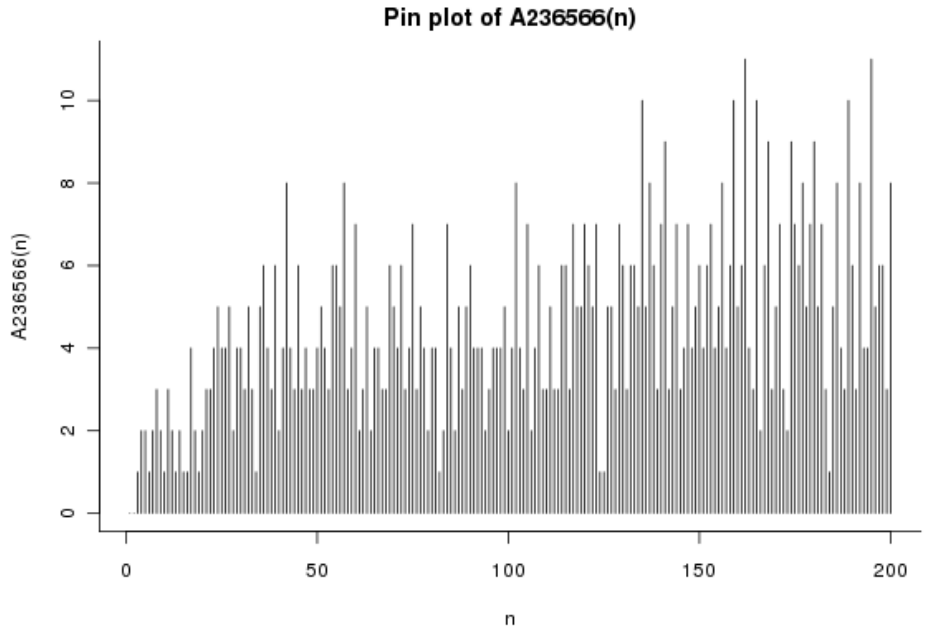
We have verified the conjecture for n up to 2×10^8. Clearly, it is stronger than Goldbach's conjecture. Now we explain why it implies the twin prime conjecture.

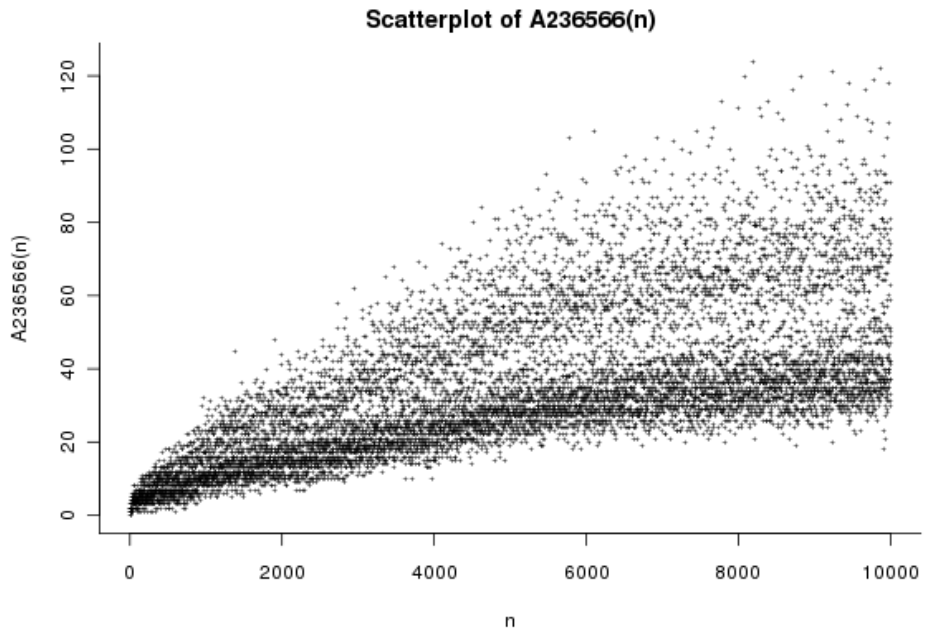
In fact, if all primes q with $p_{q+2} + 2$ prime are smaller than an even number $N > 2$, then for any such a prime q the number $N! - q$ is composite since

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

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.

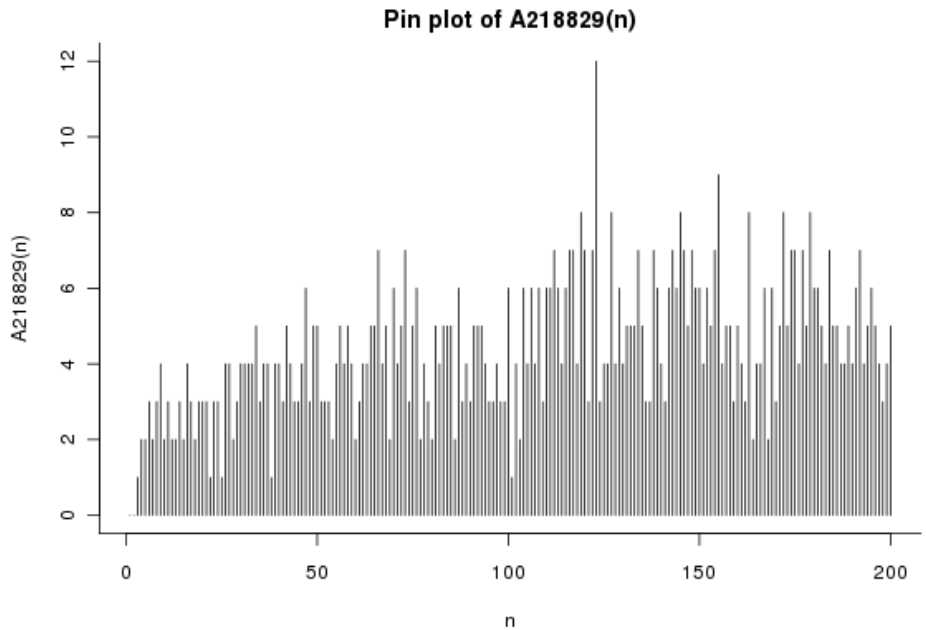
Example. $22 = 20 + 2$ with $p_{20} + 2 = 71 + 2 = 73$ and $p_{p_2} + 2 = p_3 + 2 = 5 + 2 = 7$ both prime.

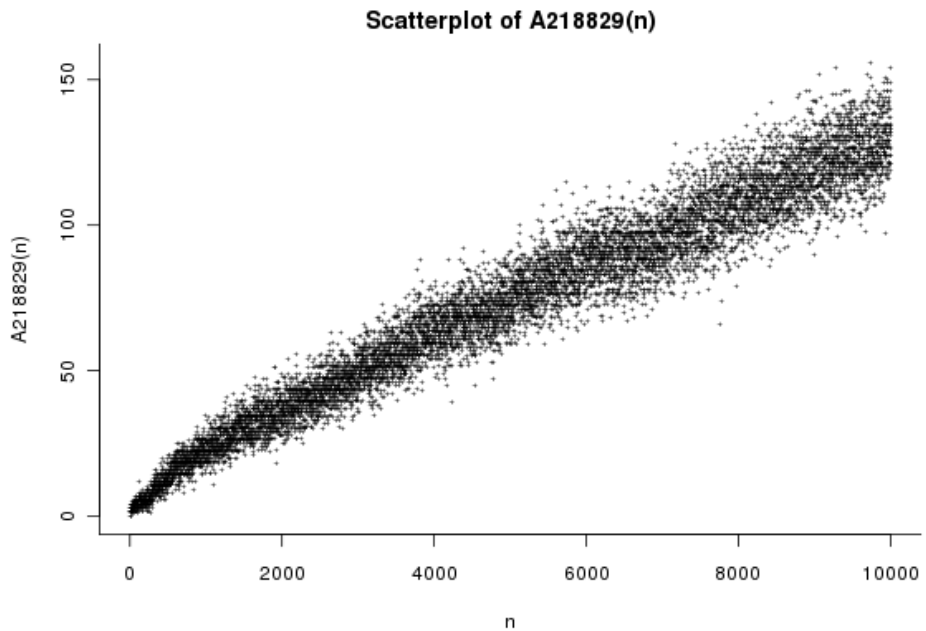
Remark. If all those positive integer m with $p_{p_m} + 2$ prime are smaller than an integer $N > 2$, then by the conjecture, for each $j = 1, 2, 3, \ldots$, there are positive integers $k(j)$ and $m(j)$ with $k(j) + m(j) = jN$ such that $p_{k(j)} + 2$ and $p_{p_{m(j)}} + 2$ are both prime, and hence $k(j) \in ((j-1)N, jN)$ 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 $a(n) = |\{0 < k < n : \ p_k + 2 \text{ and } p_{p_{n-k}} + 2 \text{ are both prime}\}|$





A conjecture on primes of the form $p^2 - 2$

Conjecture (Sun, 2014-02-07). Any integer $n > 1$ can be written as $k + m$ with k and m positive integers such that $p_k^2 - 2$, $p_m^2 - 2$ and $p_{p_m}^2 - 2$ are all prime.

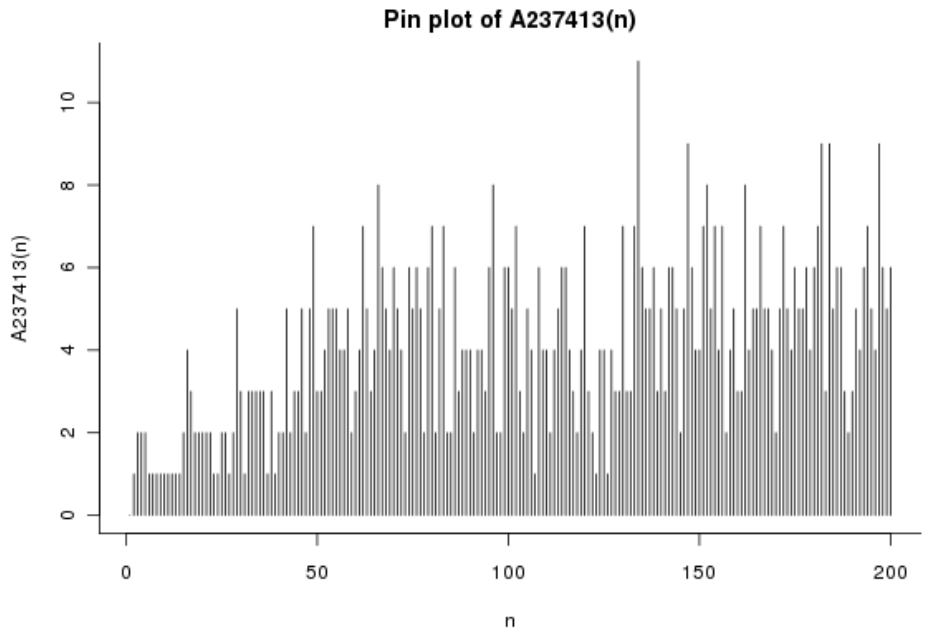
Remark. We have verified this for n up to 10^8. It is not yet proven that there are infinitely many primes of the form $x^2 - 2$ with $x \in \mathbb{Z}$.

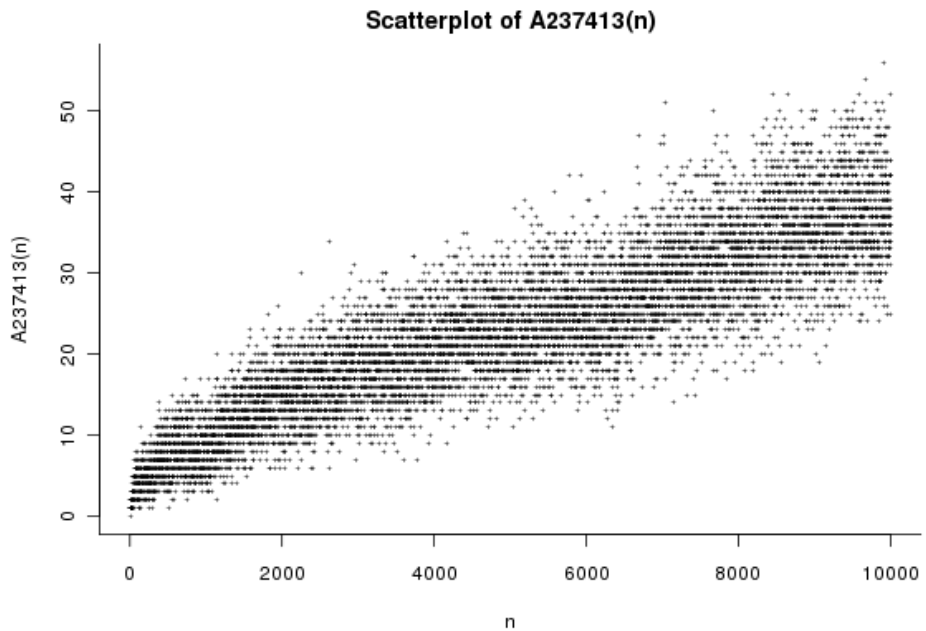
Example. $7 = 6 + 1$ with

$$\begin{aligned} p_6^2 - 2 &= 13^2 - 2 = 167, \\ p_1^2 - 2 &= 2^2 - 2 = 2, \\ p_{p_1}^2 - 2 &= p_2^2 - 2 = 3^2 - 2 = 7 \end{aligned}$$

all prime.

Graph for $a(n) = |\{0 < k < n : \ p_k^2 - 2, \ p_{n-k}^2 - 2, \ p_{p_{n-k}}^2 - 2 \text{ are all prime}\}|$





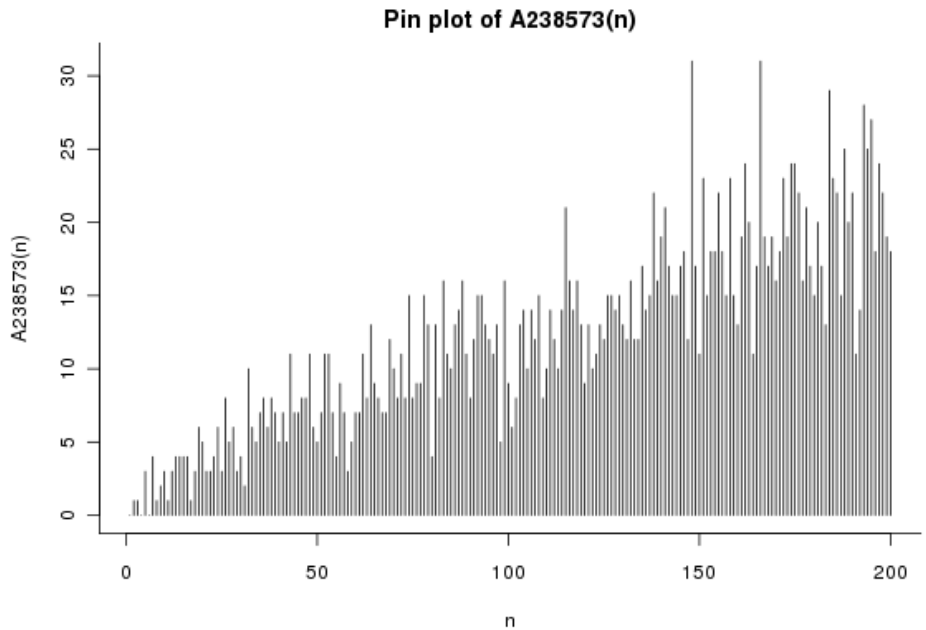
A finite version of the twin prime conjecture

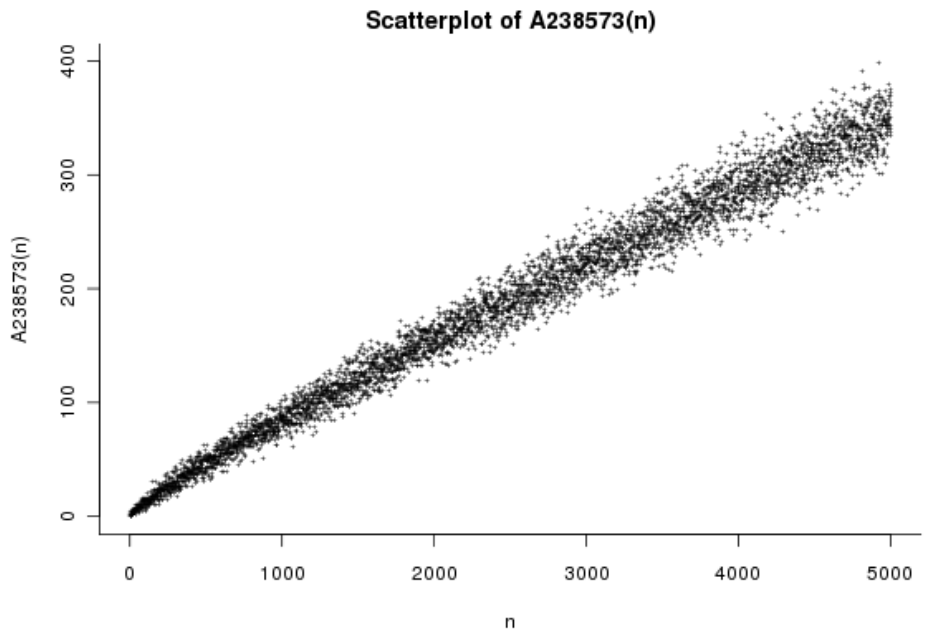
Conjecture (Sun, 2014-03-01). For any integer $n > 6$, there is a number $k \in \{1, \ldots, n\}$ with $p_{kn} + 2$ prime. Moreover, for every $n = 1, 2, 3, \ldots$ there is a positive integer $k < 3\sqrt{n} + 6$ with $p_{kn} + 2$ prime.

Example. $p_{3\times 11} + 2 = 137 + 2 = 139$ is prime.

Remark. Clearly the conjecture is stronger than the Twin Prime Conjecture.

Graph for $a(n) = |\{0 < k \leqslant n : \ p_{kn} + 2 \text{ is prime}\}|$





Infinitely many primes of special forms

Conjecture 1 (2013-12-01). There are infinitely many positive integers n such that

$$n \pm 1,\ p_n \pm n,\ np_n \pm 1$$

are all prime.

Remark. The first such a number n is 22110. I have listed the first 2000 such numbers n.

Conjecture 2 (2014-01-20). There are infinitely many primes q with $p_q^2 + 4q^2$ and $q^2 + 4p_q^2$ both prime.

Remark. I have listed the first 10000 such primes q:

$$3,\ 139,\ 179,\ 233,\ 491,\ 929,\ 1217,\ 1429,\ 1597,\ 1613,\ \ldots$$

I even don't know how to prove that there are infinitely positive integers x and y such that $x^2 + 4y^2$ and $y^2 + 4x^2$ are both prime.

Conjectures involving central binomial coefficients

Conjecture 1 (Sun, 2013-12-05). Any integer $n > 2$ can be written as $k + m$ with k and m positive integers such that $\binom{2k}{k} + p_m$ is prime.

Remark. I have verified this for n up to 10^8. For example, $9 = 2 + 7$ with $\binom{2\cdot 2}{2} + p_7 = 6 + 17 = 23$ prime.

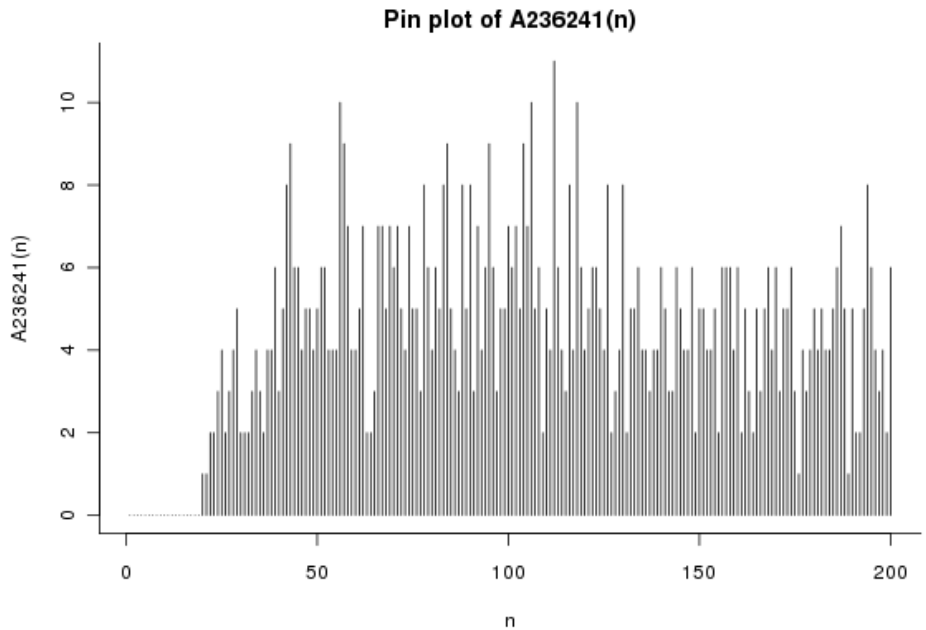
Conjecture 2 (Sun, 2014-01-21). For any integer $n \geqslant 20$, there is a positive integer $k < n$ such that $m = \varphi(k) + \varphi(n-k)/8$ is an integer with $\binom{2m}{m} + p_m$ prime.

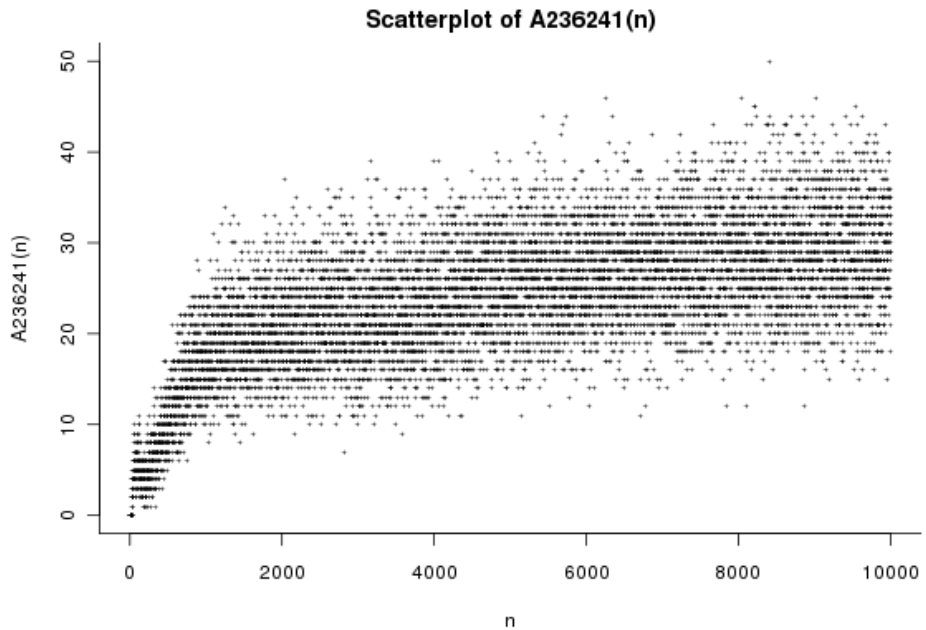
Remark. This implies that there are infinitely many positive integers m with $\binom{2m}{m} + p_m$ prime. (Note that $\binom{2m}{m} \sim 4^m/\sqrt{m\pi}$.) I have found 52 values of m with $\binom{2m}{m} + p_m$ prime. For example, when $m = 30734$ the number $\binom{2m}{m} + p_m$ is a prime with 18502 decimal digits.

Conjecture 3 (Sun, 2014-03-19). For any integer $n > 4$, $p_n + \binom{p_k - 1}{(p_k-1)/2}$ is prime for some $1 < k < \sqrt{n}\log n$.

Remark. I have verified Conjecture 3 for all $n = 5, 6, \ldots, 10^7$.

Graph for $a(n) = |\{0 < k < n : \ m = \varphi(k) + \frac{\varphi(n-k)}{8} \in \mathbb{Z}, \ \binom{2m}{m} + p_m \text{ is prime}\}|$





Conjectures on primes of the form $p_q - q + 1$ with q prime

Conjecture 1 (Sun, 2014-01-17). For any integer $n \geqslant 38$, there is a positive integer $k < n$ such that

$$\begin{aligned} q =& \varphi(k) + \frac{\varphi(n-k)}{3} + 1, \\ r =& p_q - q + 1, \\ s =& p_r - r + 1 \end{aligned}$$

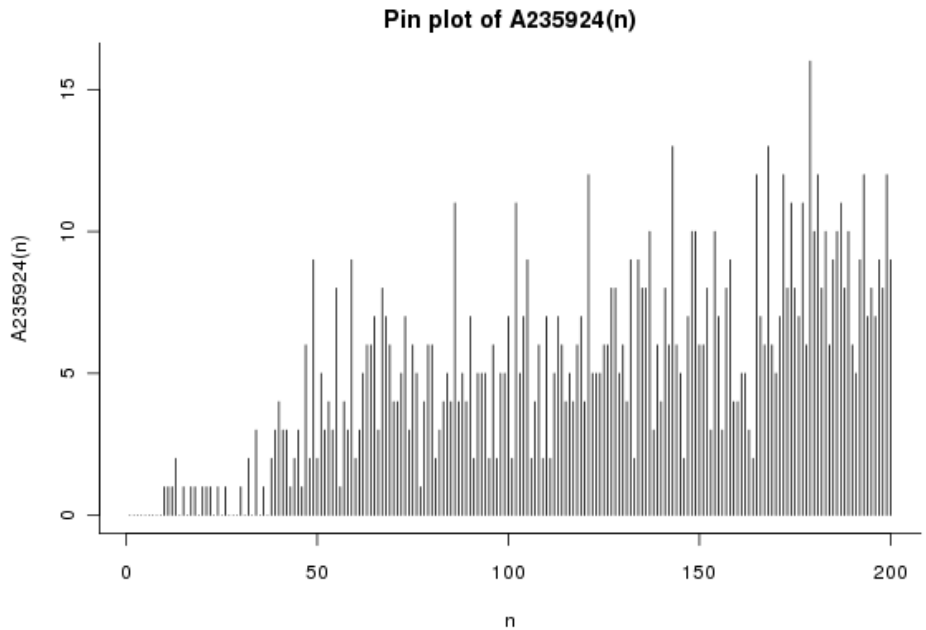
are all prime.

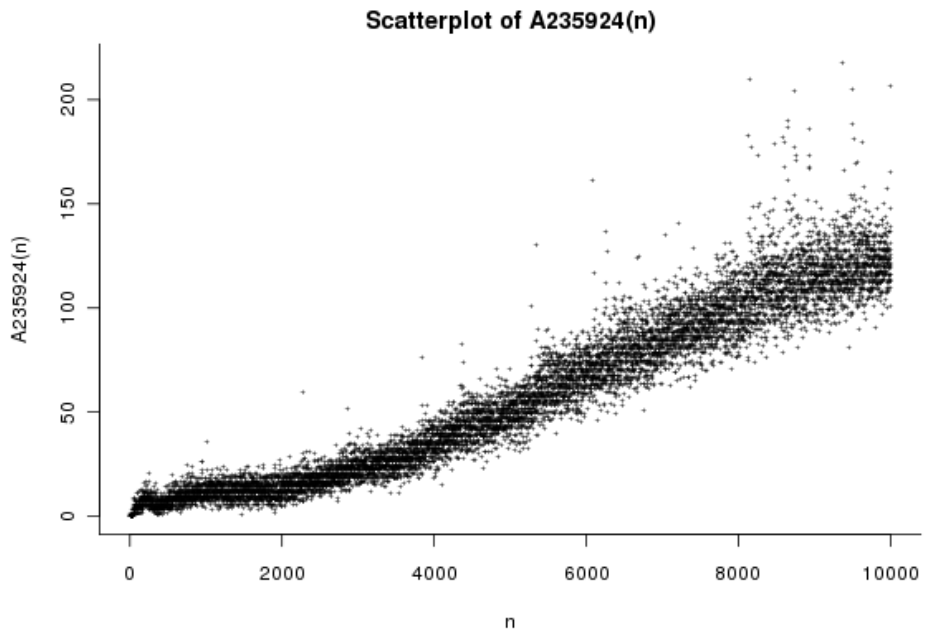
Remark. This implies that there are infinitely primes q with $r = p_q - q + 1$ and $s = p_r - r + 1$ both prime.

Conjecture 2 (Sun, 2014-01-17). For each $m = 2, 3, \ldots$, there is a prime chain $q_1 < \ldots < q_m$ of length m such that $q_{k+1} = p_{q_k} - q_k + 1$ for all $0 < k < m$.

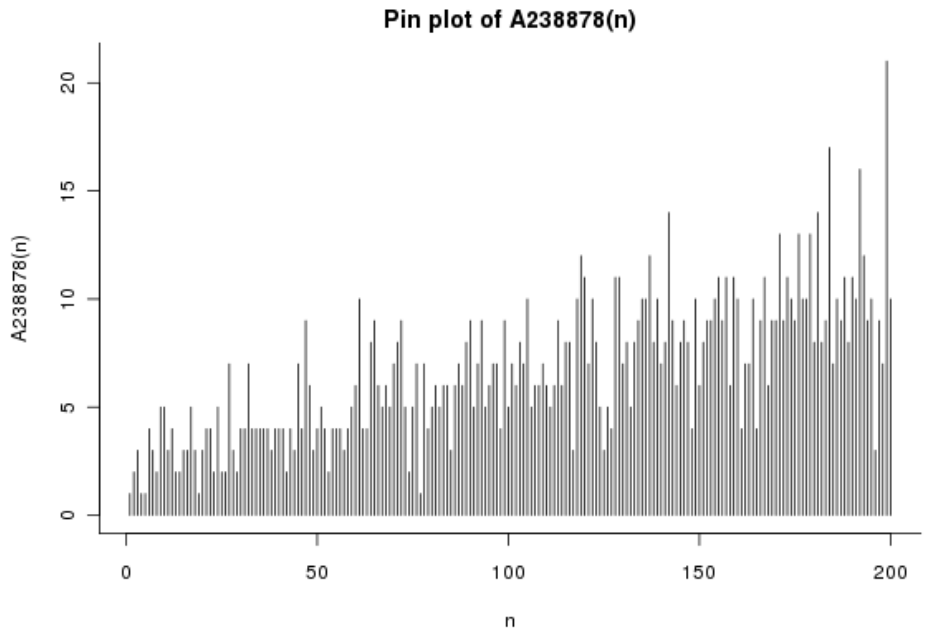
Conjecture 3 (Sun, 2014-03-06). For any positive integer n, there is a number $k \in \{1, \ldots, n\}$ such that $p_{p_k} - p_k + 1$ and $p_{p_{kn}} - p_{kn} + 1$ are both prime.

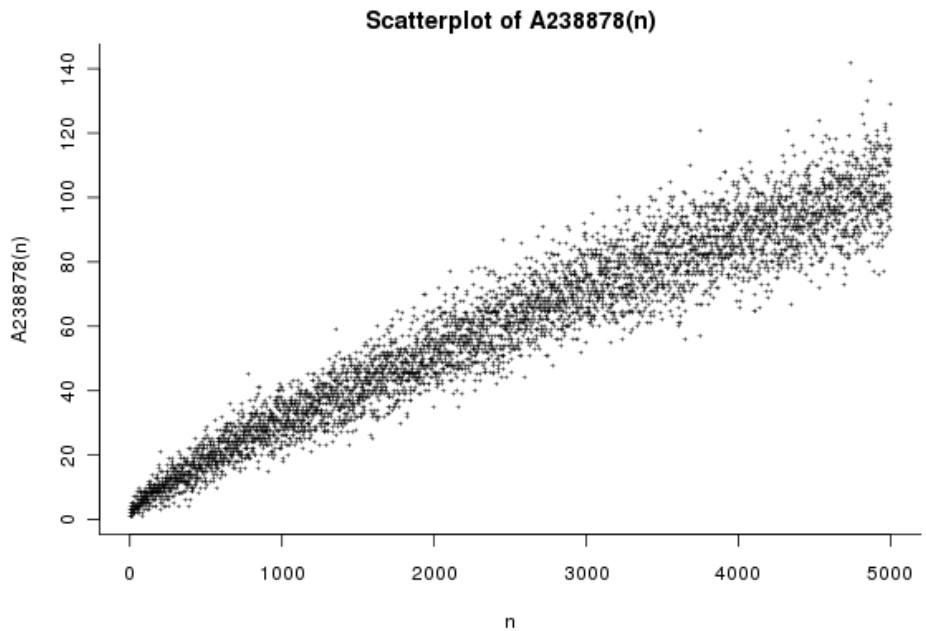
$$|\{0 < k < n : \ q = q(k) + \tfrac{q(n-k)}{3} + 1, \ r = p_q - q + 1, \ s = p_r - r + 1 \text{ are all prime}\}|$$





Graphs for $a(n) = |\{0 < k \leqslant n : \ p_{p_k} - p_k + 1 \text{ and } p_{p_{kn}} - p_{kn} + 1 \text{ are both prime}\}|$





On the inverse of n modulo p_n

For a positive integer n, the inverse of n modulo p_n refers to the unique $x \in \{1, \ldots, p_n - 1\}$ with $nx \equiv 1 \pmod{p_n}$.

Conjecture (Sun, 2014-05-22) Any integer $n > 3$ can be written as a sum of two elements of the set

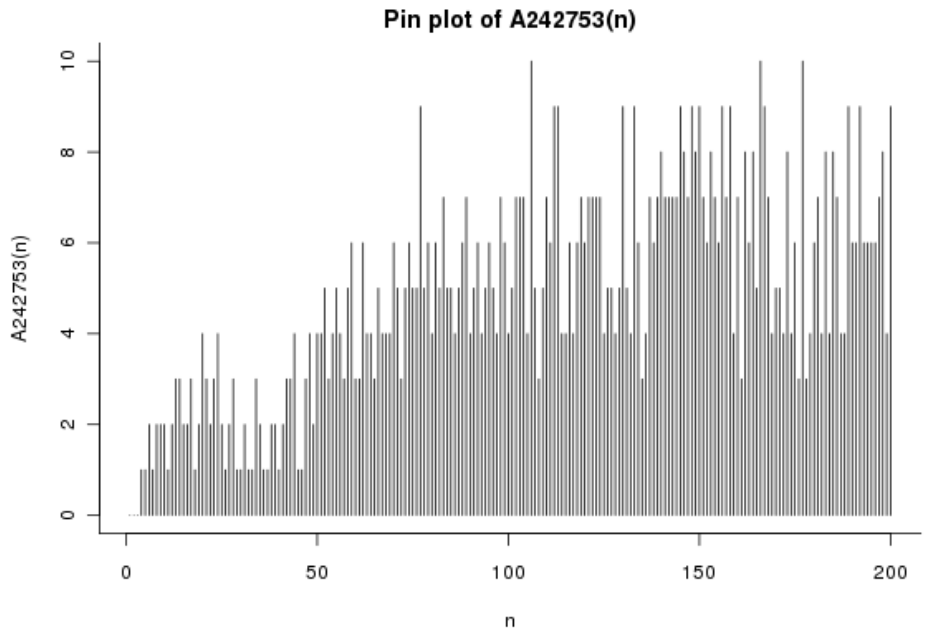
$$S = \{k > 0 : \text{ the inverse of } k \text{ modulo } p_k \text{ is prime}\}.$$

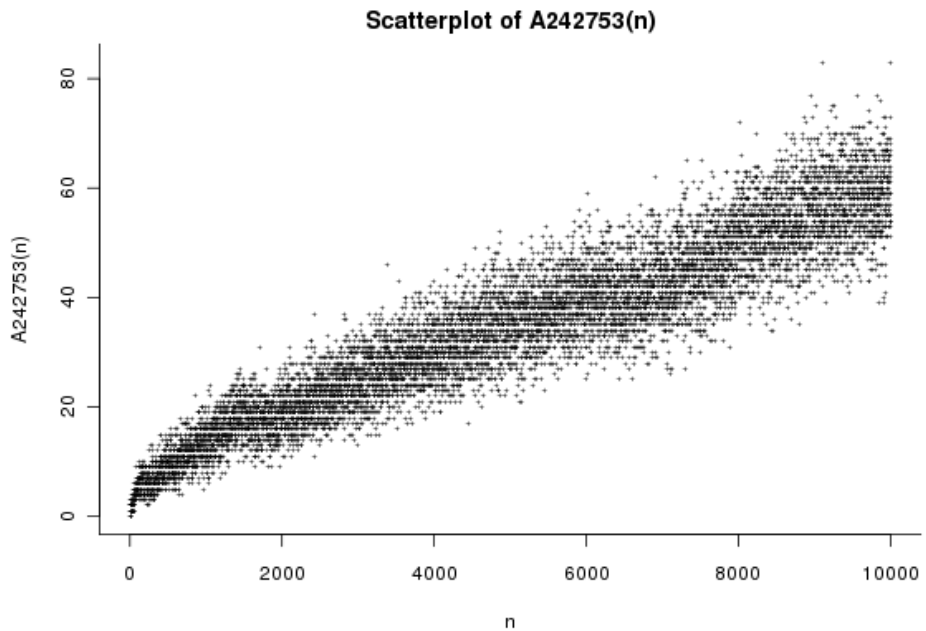
This is somewhat similar to Goldbach's Conjecture.

Example. $11 = 4 + 7$, the inverse of 4 mod $p_4 = 7$ is the prime 2, and the inverse of 7 mod $p_7 = 17$ is the prime 5.

Another Conjecture (Sun, 2014-05-14). For any prime $p > 5$, there is a square $k^2 < p$ such that the inverse of k^2 mod p is prime. Moreover, for any integer $n > 1848$, there is a square $k^2 < n$ such that the inverse of k^2 mod n is prime.

Number of ways to write $n = k + m$ with $0 < k \leqslant m$ and $k, m \in S$





Part IV. On primes related to partition functions

On primes related to $p(n)$

Conjecture 1 (Sun, 2014-02-27). Let n be any positive integer. Then one of the n numbers

$$p(n)+1,\ p(n)+2,\ \ldots,\ p(n)+n$$

is prime.

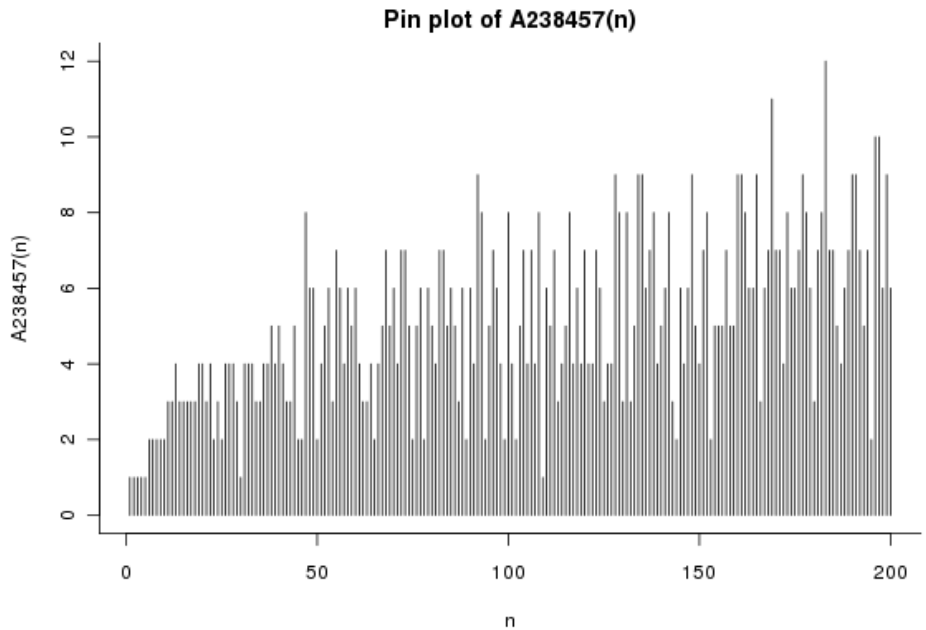
Conjecture 2 (Sun, 2014-02-28). Let $n>1$ be an integer. Then $p(n)+p(k)-1$ is prime for some $0<k<n$.

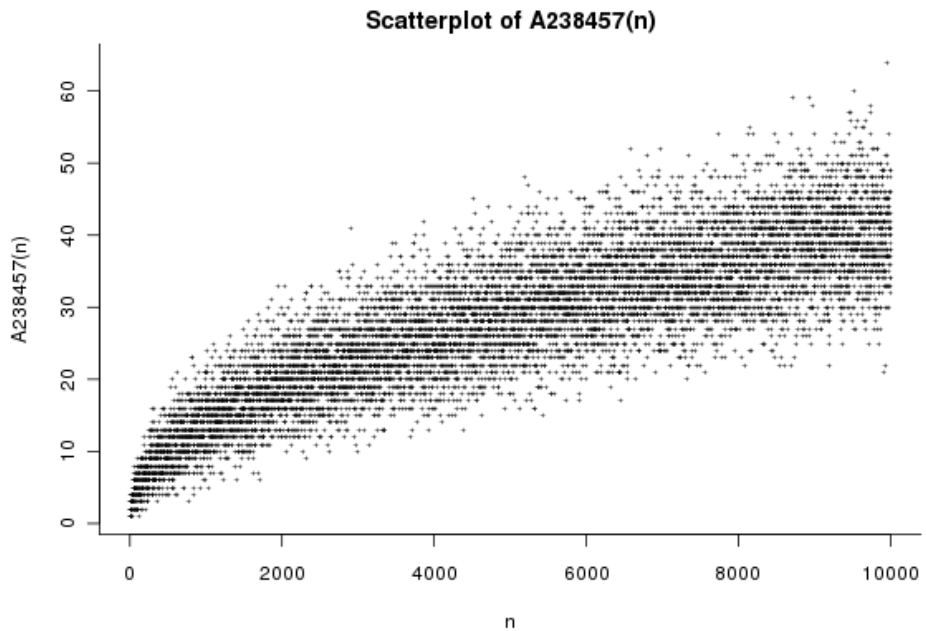
Conjecture 3 (Sun, 2014-03-13). Let $n>3$ be an integer. Then $p(n+k)+1$ is prime for some $k=1,\ldots,n$.

Conjecture 4 (Sun, 2014-03-12). Let $n>1$ be an integer. Then there exists a number $k\in\{1,\ldots,n-1\}$ such that $kp(n)(p(n)-1)+1$ is prime. Also, we may replace $kp(n)(p(n)-1)+1$ by $p(k)p(n)(p(n)-1)+1$ or $p(k)p(n)(p(n)+1)-1$.

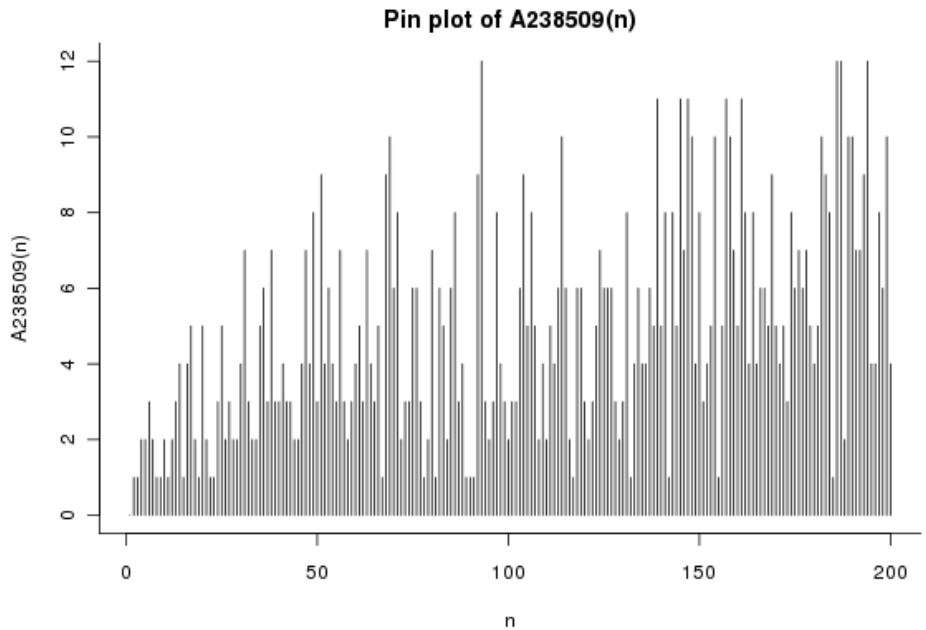
These conjectures might be helpful in finding large primes.

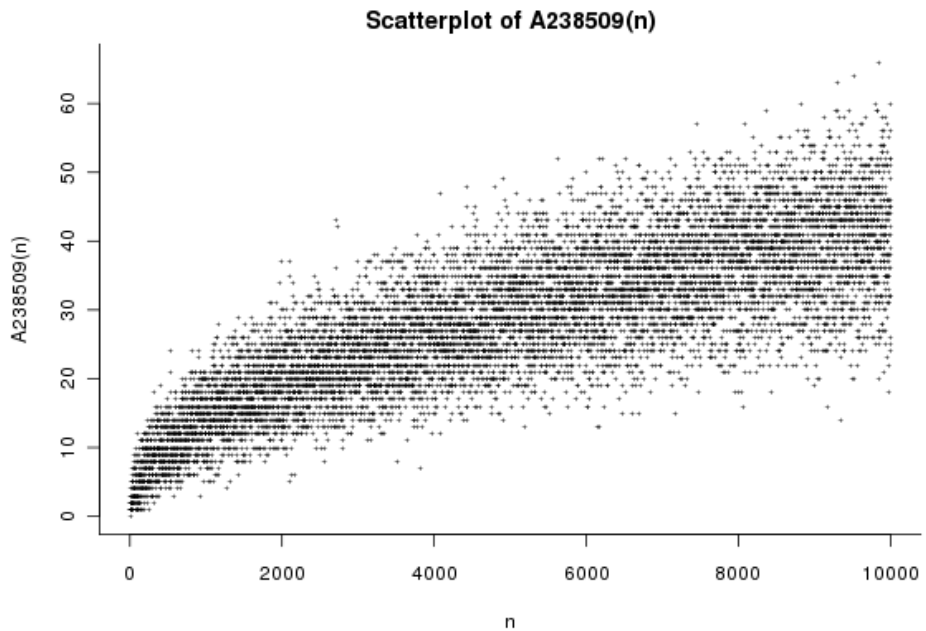
Graph for $a(n) = |\{0 < k \leqslant n : \ p(n) + k \text{ is prime}\}|$



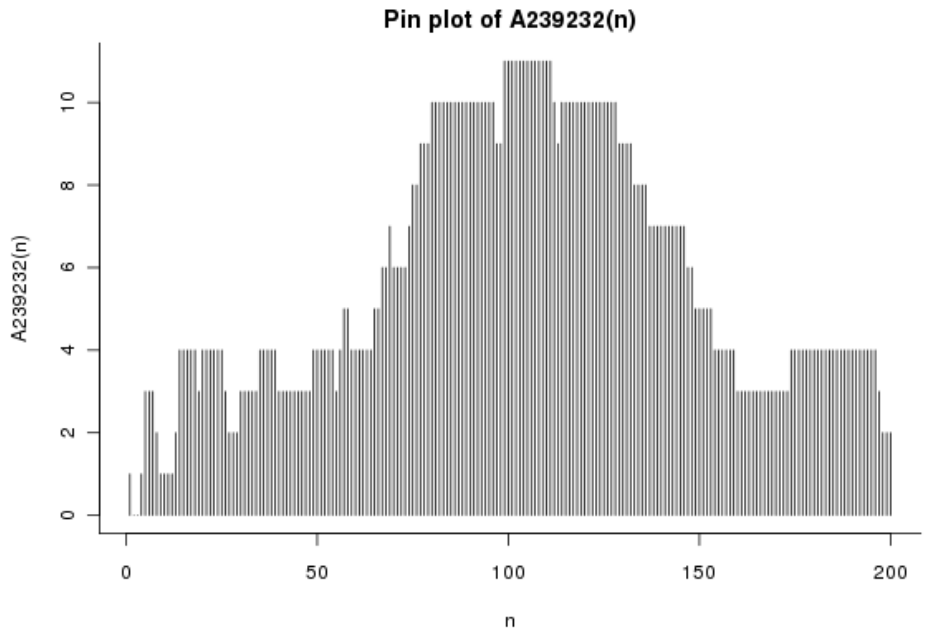


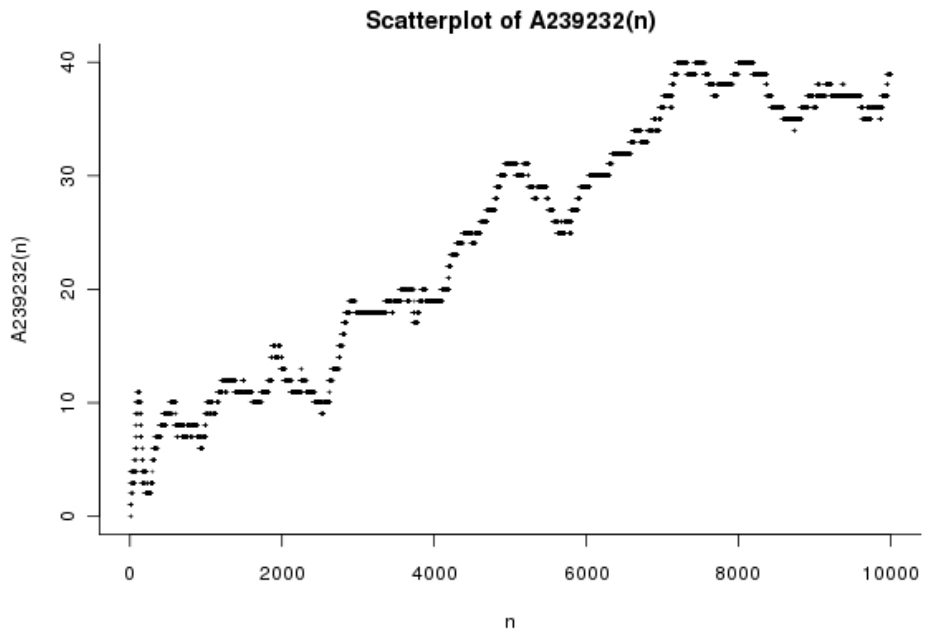
Graph for $a(n) = |\{0 < k < n : \ p(n) + p(k) - 1 \text{ is prime}\}|$



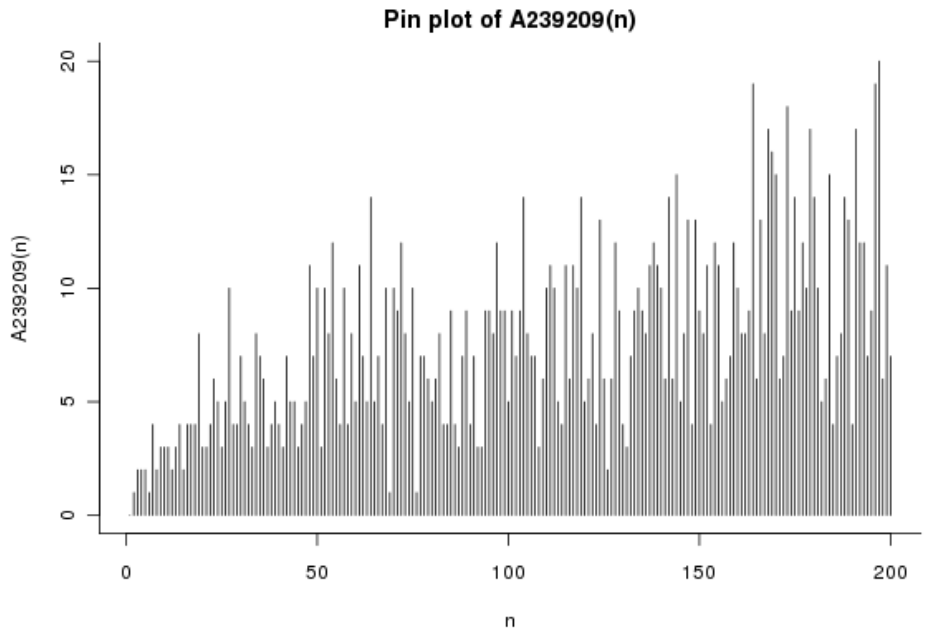


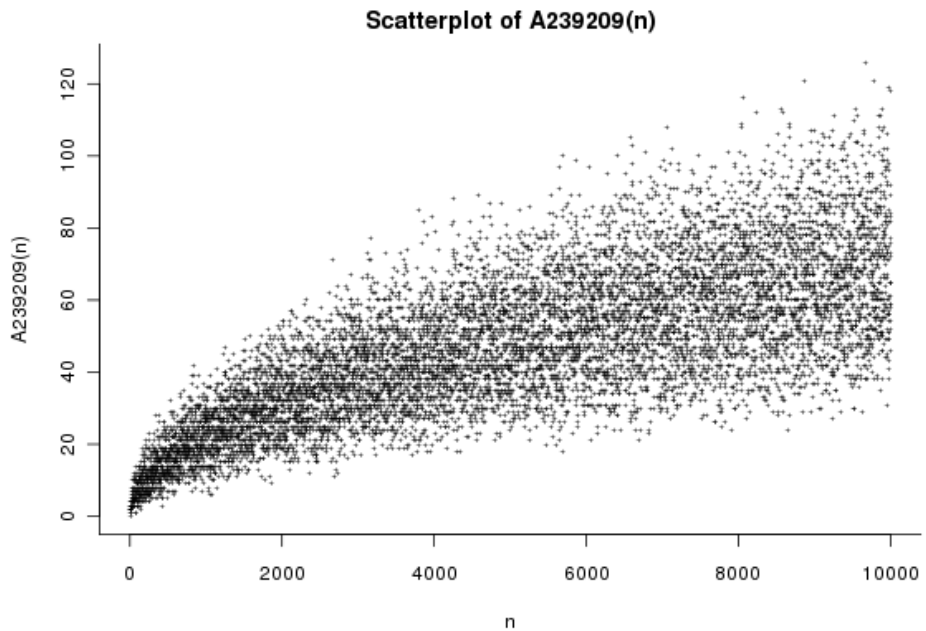
Graph for $a(n) = |\{1 \leqslant k \leqslant n : \ p(n+k)+1 \text{ is prime}\}|$





Graph for $a(n) = |\{0 < k < n : \ kp(n)(p(n) - 1) + 1 \text{ is prime}\}|$





On primes related to $q(n)$ and $\bar{q}(n)$

Conjecture 1 (Sun, 2014-01-07). For any integer $n \geqslant 60$, there is a positive integer $k < n$ such that $m \pm 1$ and $q(m) + 1$ are all prime, where $m = \varphi(k) + \varphi(n-k)/4$.

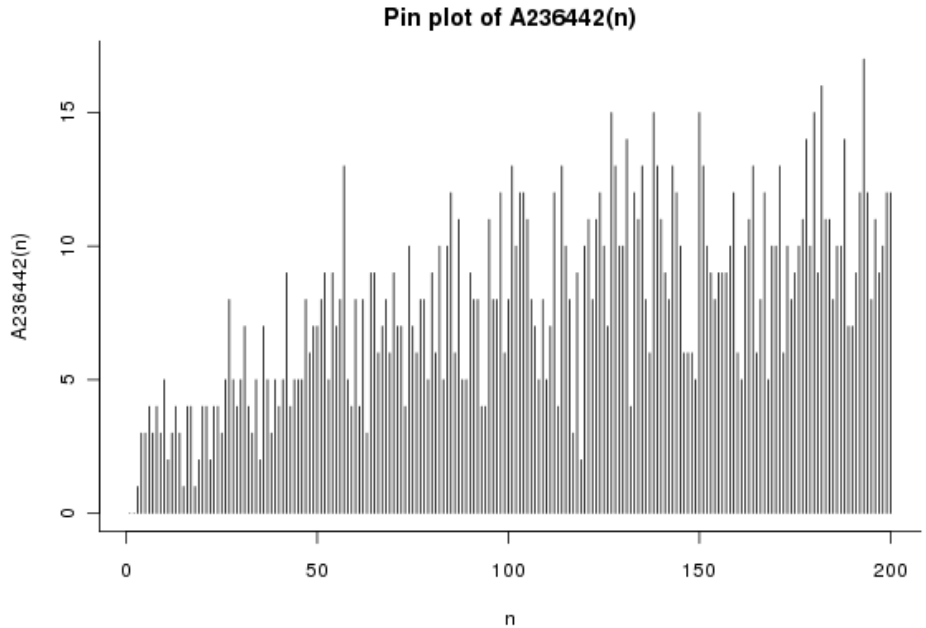
Conjecture 2 (Sun, 2014-01-25). (i) For any integer $n \geqslant 128$, there is a positive integer $k < n$ such that $r = \varphi(k) + \varphi(n-k)/6 + 1$ and $p(r) + q(r)$ are both prime.

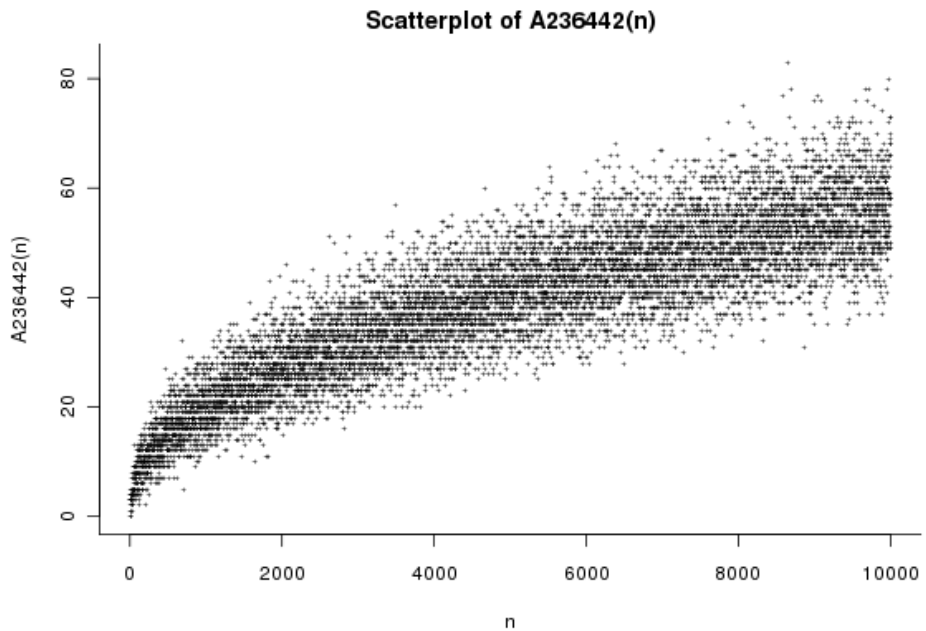
(ii) For every $n = 18, 19, \ldots$, there is a positive integer $k < n$ such that $m = \varphi(k)/2 + \varphi(n-k)/8$ is an integer with $p(m)^2 + q(m)^2$ prime.

Conjecture 3 (Sun, 2014-01-26). Any integer $n > 2$ can be written as $k + m$ with k and m positive integers such that $q(k) + \bar{q}(m)$ is prime.

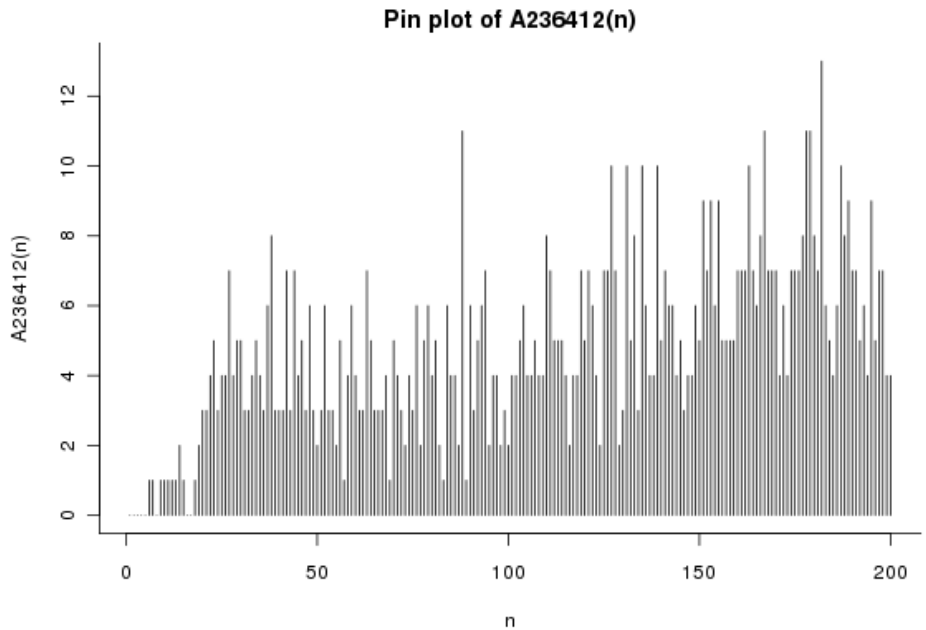
Conjecture 4 (Sun, 2014-03-12). Let $n > 1$ be an integer. Then $kp(n)q(n)\bar{q}(n) - 1$ is prime for some $k = 1, \ldots, n$. Also, $2p(k)p(n)q(n)\bar{q}(n) + 1$ is prime for some $k = 1, \ldots, n-1$.

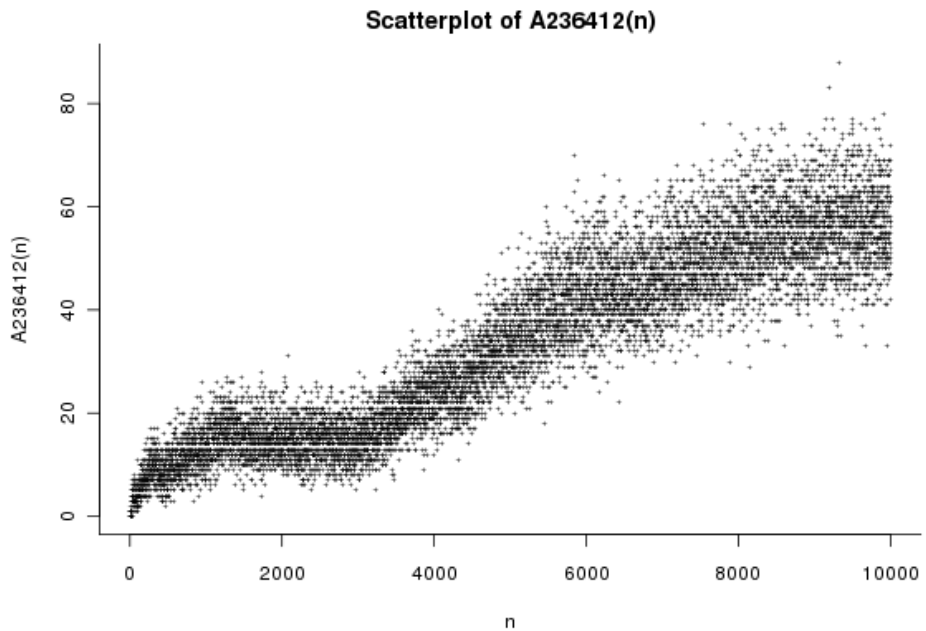
Graph for $a(n) = |\{0 < k < n : \ q(k) \text{ and } \bar{q}(n-k) \text{ are both prime}\}|$





Graph for $|\{0 < k < n :\ m = \varphi(k)/2 + \varphi(n-k)/8 \in \mathbb{Z},\ p(m)^2 + q(m)^2 \text{ is prime}\}|$





Part V. On quadratic nonresidues and primitive roots modulo primes

How to solve $x^2 \equiv a \pmod{p}$?

Let p be an odd prime and a be any quadratic residue modulo p. How to solve the congruence $x^2 \equiv a \pmod{p}$ quickly?

Tonelli-Shanks Algorithm. Knowing a *quadratic nonresidue* $d \in \mathbb{Z} \bmod p$, one can solve $x^2 \equiv a \pmod{p}$ in **polynomial time**:

Write $p - 1 = 2^s t$ with $s, t \in \mathbb{Z}^+$ and $2 \nmid t$, and find even integers $m_1, \ldots, m_s$ with $(ad^{m_i})^{2^{s-i}t} \equiv 1 \pmod{p}$ for all $i = 1, \ldots, s$ in the following way: $m_1 := 0$, and after those $m_1, \ldots, m_i$ (with $1 \leqslant i < s$) have been chosen we select $m_{i+1} \in \{m_i, m_i + 2^i\}$ such that $(ad^{m_{i+1}})^{2^{s-i-1}t} \equiv 1 \pmod{p}$. Note that $((ad^{m_i})^{2^{s-i-1}t})^2 \equiv 1 \pmod{p}$ and hence $(ad^{m_i})^{2^{s-i-1}t} \equiv \pm 1 \pmod{p}$. If $(ad^{m_i})^{2^{s-i-1}t} \equiv -1 \pmod{p}$, then

$$(ad^{m_i+2^i})^{2^{s-1-i}t} \equiv -d^{2^{s-1}t} = -d^{(p-1)/2} \equiv 1 \pmod{p}.$$

As $(ad^{m_s})^t \equiv 1 \pmod{p}$, we have $x^2 \equiv a \pmod{p}$ with $x = \pm a^{(t+1)/2}(d^t)^{m_s/2}$.

Remark. In 1985 R. Schoof gave a polynomial (depending on a) algorithm to solve the congruence $x^2 \equiv a \pmod{p}$ with a given.

Fibonacci quadratic nonresidues

The Fibonacci numbers are given by

$$F_0 = 0,\ F_1 = 1,\ \text{and } F_{n+1} = F_n + F_{n-1}\ (n = 1, 2, 3, \ldots).$$

Carmichael's Theorem. For any integer $n > 12$, the n-th Fibonacci number F_n has a prime divisor p which does not divide any previous Fibonacci number F_k with $0 < k < n$.

Conjecture (Sun, 2014-04-26). (i) For any integer $n > 4$, there is a Fibonacci number $f < n/2$ with $x^2 \not\equiv f \pmod{n}$ for all $x \in \mathbb{Z}$.

(ii) For any odd prime p, let $f(p)$ be the least Fibonacci number with $(\frac{f(p)}{p}) = -1$. Then $f(p) = o(p^{0.7})$ as $p \to \infty$. Moreover, we have $f(p) = O(p^c)$ for any $c > c_0 = \log_2 \frac{1+\sqrt{5}}{2} \approx 0.694$.

Remark. Part (i) can be reduced to the case with $n = p$ prime. We have verified that for any prime $3 < p < 3 \times 10^9$ there is a Fibonacci number $F_k < p/2$ with $(\frac{F_k}{p}) = -1$.

Heuristic arguments for part (ii) of the conjecture

In light of Carmichael's theorem on primitive prime divisors of Fibonacci numbers, we may think that a positive Fibonacci number not exceeding p^c is a quadratic residue modulo p with '*probability*' $1/2$. Roughly speaking, there are about

$$\frac{\log_2 p^c}{\log_2 \frac{1+\sqrt{5}}{2}} = \frac{c}{c_0} \log_2 p$$

positive Fibonacci numbers not exceeding p^c. So we might expect that all positive Fibonacci numbers not exceeding p^c are quadratic residues modulo p with probability

$$\left(\frac{1}{2}\right)^{(\log_2 p)c/c_0} = \frac{1}{p^{c/c_0}}.$$

As $\sum_p p^{-c/c_0}$ converges, it seems reasonable to think that there are finitely many primes p for which all positive Fibonacci numbers not exceeding p^c are quadratic residues modulo p. So the guess $f(p) = O(p^c)$ probably holds.

On primitive roots modulo primes (I)

Conjecture 1 (Sun, 2014-04-23). Any prime p has a primitive root $g < p$ with $g - 1$ a square.

Remark. Verified for $p < 10^7$. $8^2 + 1$ is a primitive root mod 71.

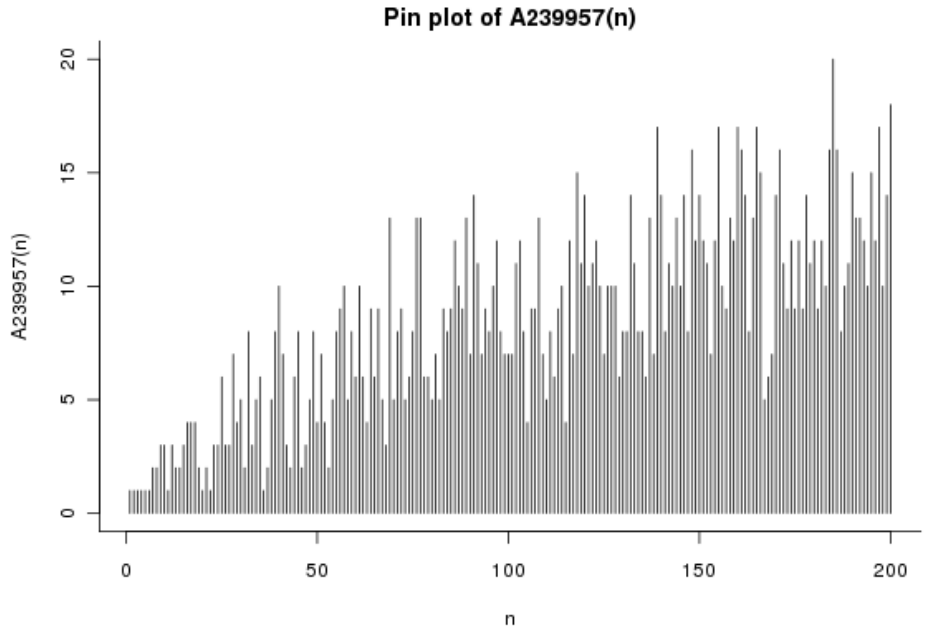
Conjecture 2 (Sun, 2014-05-09). For any prime $p > 3$, there is a number $g \in \{1, \ldots, p-1\}$ such that all the three integers g, $2^g - 1$ and $(g-1)!$ are primitive roots modulo p.

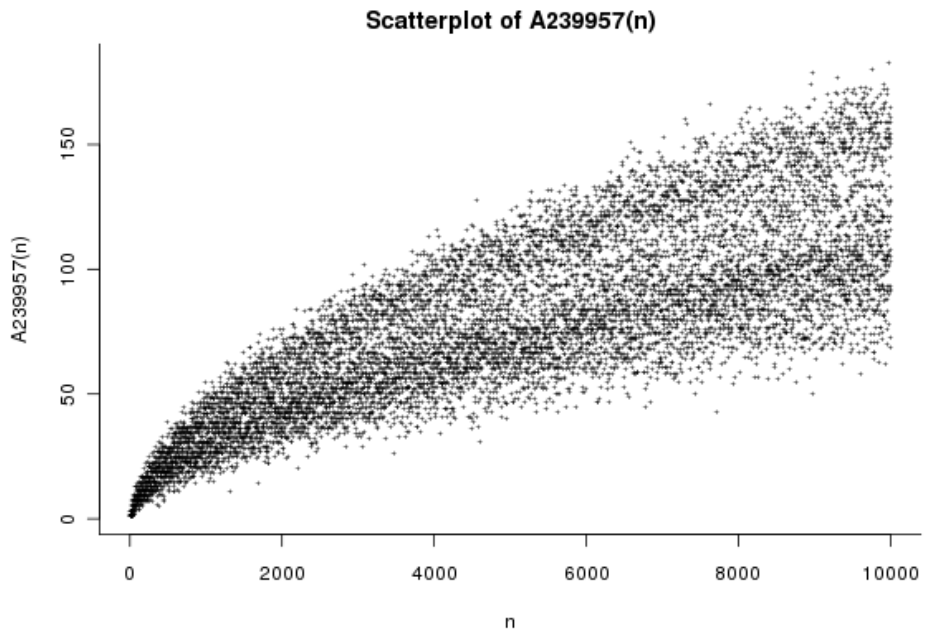
Remark. We even don't know how to prove that any prime $p > 3$ has a quadratic nonresidue of the form $2^n - 1$. We have verified Conjecture 2 for any prime $3 < p < 10^6$. For example, 8, $2^8 - 1 = 255$, $(8-1)! = 5040$ are all primitive roots mod 11.

Conjecture 3 (Sun, 2014-05-11). For any odd prime p, there is a prime $q < p$ such that q and $2^q - q$ are both primitive roots modulo p.

Example. $q = 19$ and $2^q - q = 524269$ are primitive roots mod 23.
Remark. P. Erdős ever asked whether sufficiently large prime p has a prime primitive root $q < p$.

Graph for $a(n) = |\{g < p_n : \ g \text{ is a primitive root mod } p_n \text{ of the form } k^2 + 1\}|$





On primitive roots modulo primes (II)

Conjecture 1 (Sun, 2014-04-24) For any prime q, there is a partition number $p(n) < q$ which is a primitive root modulo q.

Remark. I have verified this for all primes $p < 2 \times 10^7$. For example, $p(35) = 14883$ is a primitive root modulo the prime $q = 16921$.

On primitive roots modulo primes (II)

Conjecture 1 (Sun, 2014-04-24) For any prime q, there is a partition number $p(n) < q$ which is a primitive root modulo q.

Remark. I have verified this for all primes $p < 2 \times 10^7$. For example, $p(35) = 14883$ is a primitive root modulo the prime $q = 16921$.

Conjecture 2 (Sun, 2014-05-07). For any prime $p > 3$, there is a prime $q < p$ such that the Bernoulli number B_{q-1} is a primitive root modulo p.

Remark. I have verified this for all prime $3 < p < 6 \times 10^6$.

On primitive roots modulo primes (II)

Conjecture 1 (Sun, 2014-04-24) For any prime q, there is a partition number $p(n) < q$ which is a primitive root modulo q.

Remark. I have verified this for all primes $p < 2 \times 10^7$. For example, $p(35) = 14883$ is a primitive root modulo the prime $q = 16921$.

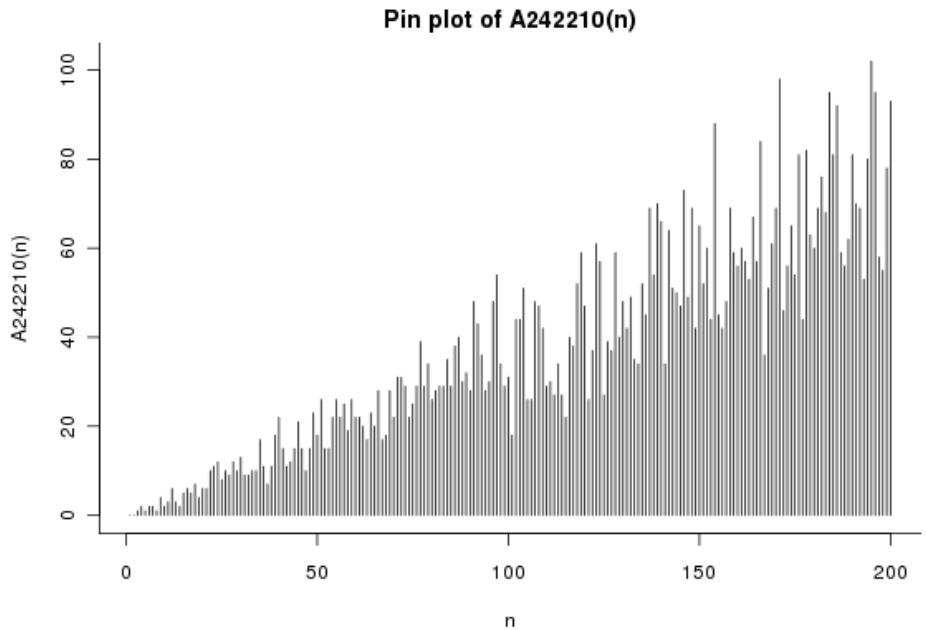
Conjecture 2 (Sun, 2014-05-07). For any prime $p > 3$, there is a prime $q < p$ such that the Bernoulli number B_{q-1} is a primitive root modulo p.

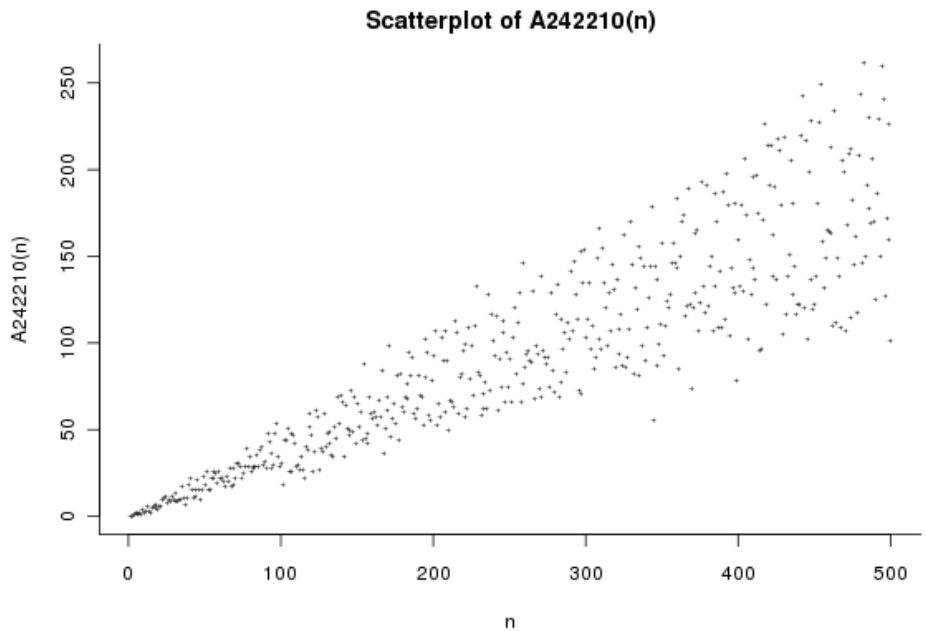
Remark. I have verified this for all prime $3 < p < 6 \times 10^6$.

Conjecture 3 (Sun, 2014-06-01). For any integer $n > 6$, there is a prime $p < n$ such that pn is a primitive root modulo the n-th prime p_n.

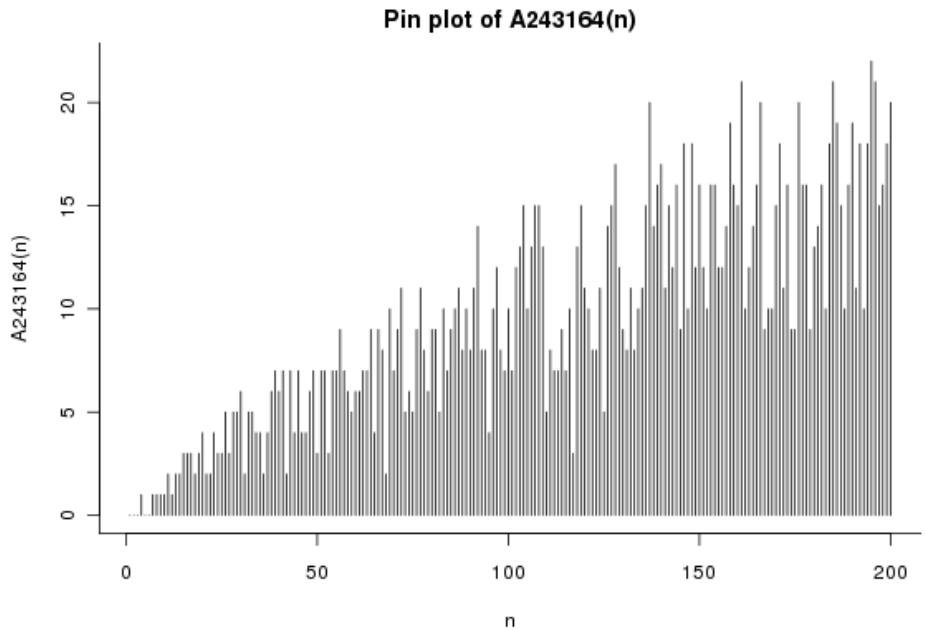
Remark. I have verified this for all $n = 7, \ldots, 200000$.

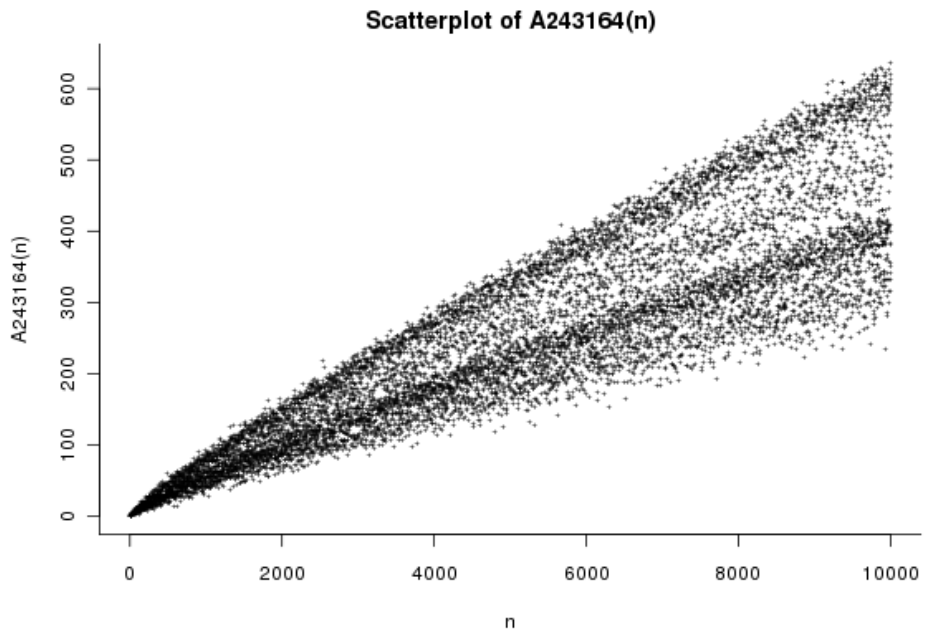
Graph for $a(n) = |\{0 < k < n : \ B_{p_k - 1} \text{ is a primitive root mod } p_n\}|$





Graph for $a(n) = |\{p < n : \ pn \text{ is a primitive root mod } p_n\}|$





Concluding remarks

For sources of my above conjectures, you may loot at my preprints

Zhi-Wei Sun, *Problems on combinatorial properties of primes*, `arXiv:1402.6641`, `http://arxiv.org/abs/1402.6641`

and

Zhi-Wei Sun, *New observations on primitive roots modulo primes*, `arXiv:1405.0290`, `http://arxiv.org/abs/1405.0290`.

The first preprint contains 60 selected conjectures, and it seems none of them could be proved by human beings.

After proving that $[0,1]\times[0,1]\approx[0,1]$, Cantor felt very surprising. He wrote: "*I see it, but I don't believe it*."

After discovering those conjectures on combinatorial properties of primes, I'd like to say "**I believe them, but I don't see them**."

Thank you!