A talk given at the Workshop on Analytic Number Theory and Cryptology (Beijing, June 14, 2014)

On Some Arithmetic Functions

Zhi-Wei Sun

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

June 14, 2014

Abstract

We mainly introduce the speaker's recent results and problems on arithmetic functions. We will talk about analytic tools in the speaker's work on functions taking only prime values and primes in arithmetic progressions, and his work on a pair of zeta functions involving $\Omega(n)$ and $\omega(n)$. We will also mention few conjectures of the speaker involving the Möbius function $\mu(n)$, Euler's totient function $\varphi(n)$ and the partition function $p(n)$.

Part I. On functions taking only prime values

Mills' Theorem

Theorem (Mills, 1947). There is a real number A such that $M(n) = \lfloor A^{3^n} \rfloor$ takes only prime values.

Sketch of the Proof. Since $p_{n+1} - p_n = O(p_n^{5/8})$ (A. E. Ingham, 1937), one can construct infinitely many primes $P_0, P_1, P_2, \ldots$ with

$$P_n^3 < P_{n+1} < (P_n + 1)^3 - 1.$$

Then the sequence $u_n = P_n^{3^{-n}}$ is increasing while the sequence $v_n = (P_n + 1)^{3^{-n}}$ is decreasing. As $u_n < v_n$, we see that $A = \lim_{n\to\infty} u_n \leqslant B = \lim_{n\to\infty} v_n$, hence

$$P_n = u_n^{3^n} < A^{3^n} < P_n + 1 = v_n^{3^n}.$$

So $\lfloor A^{3^n} \rfloor = P_n$ is a prime for all $n = 1, 2, 3, \ldots$.

Discriminator problems

Theorem 1 (L. K. Arnold, S. J. Benkoski and B. J. McCabe, 1985). For $n > 4$ the least positive integer m (denoted by $D(n)$) such that $1^2, 2^2, \ldots, n^2$ are distinct modulo m, is

$$\min\{m \geqslant 2n : \ m = p \text{ or } m = 2p \ \text{ with } p \text{ an odd prime}\}.$$

Remark. The range of $D(n)$ does not contain those primes $p = 2q + 1$ with q an odd prime.

Theorem 2 (P. S. Bremser, P. D. Schumer and L. C. Washington, 1990). Let $k > 2$ and $n > 0$ be integers, and let $D(k, n)$ denote the the least positive integer m such that $1^k, 2^k, \ldots, n^k$ are distinct modulo m.

(i) If k is odd and n is sufficiently large, then

$$D(k, n) = \min\{m \geqslant n : \ m \text{ is squarefree, and } (k, \varphi(m)) = 1\}.$$

(ii) If k is even and n is sufficiently large, then

$$D(k, n) = \min\{m \geqslant 2n : m = p \text{ or } 2p \text{ with } p \text{ a prime, and } (k, \varphi(m)) = 2\}.$$

Generate all primes in a combinatorial manner

Theorem 1 (Sun [J. Number Theory 133(2013)]) For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1)$ mod m for $k = 1, \ldots, n$ are pairwise distinct. Then $S(n)$ is the least prime greater than $2n - 2$.

Remark.

(a) **The range of $S(n)$ is exactly the set of all primes!**

(b) I also proved that the least positive integer m such that those $\binom{k}{2} = k(k-1)/2$ ($k = 1, \ldots, n$) are pairwise distinct modulo m, is just the least power of two not smaller than n.

On primes $p \equiv r \pmod 3$ with $r \in \{\pm 1\}$

Theorem 2 (Sun [J. Number Theory 133(2013)])
(i) Let $n \in \{4, 5, \ldots\}$. Then the least positive integer m such that $18k(3k-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is just the least prime $p > 3n$ with $p \equiv 1 \pmod 3$.

(ii) For $n > 5$ the least $m \in \mathbb{Z}^+$ such that those $18k(3k+1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is just the first prime $p \equiv -1 \pmod 3$ after $3n$.

On primes $p \equiv -1 \pmod d$ with $d \in \{4, 6, 12\}$, and primes $p \equiv 1 \pmod q$ with q prime

Theorem (Sun [J. Number Theory 133(2013)]). (i) For $d, n \in \mathbb{Z}^+$ let $\lambda_d(n)$ be the smallest integer $m > 1$ such that those $(2k-1)^d$ ($k = 1, \ldots, n$) are pairwise incongruent modulo m. Then $\lambda_d(n)$ with $d \in \{4, 6, 12\}$ and $n > 2$ is the least prime $p \geqslant 2n - 1$ with $p \equiv -1 \pmod d$.

(ii) Let q be an odd prime. Then the smallest integer $m > 1$ such that those $k^q(k-1)^q$ with $k = 1, \ldots, n$ are pairwise incongruent mod m, is just the least prime $p \geqslant 2n - 1$ with $p \not\equiv 1 \pmod q$.

Auxiliary results used in the proofs

A Result of P. Dusart [Math. Comp. 68(1999)]. For $x \geq 3275$, the interval $[x, x + x/(2\log^2 x)]$ contains at least one prime.

Lemma 1. Let $d \in \{4, 6, 12\}$ and $n \in \mathbb{Z}^+$. Then $[2n-1, 2.4n]$ contains at least a prime $p \equiv -1 \pmod d$ except for $n \in E(d)$, where

$$E(4) = \{1, 7, 17\}, \quad E(6) = \{1, 2, 4, 7, 16, 17\},$$

$$E(12) = \{1, 2, 3, 4, 7, 8, 9, 13, 14, 15, 16, 17, 18, 19, 43, 44, 67, 68, 69\}.$$

Lemma 2. For any odd prime q and positive integer n, the interval $[2n-1, 2.4n]$ contains at least a prime $p \not\equiv 1 \pmod q$ unless $n \leq 17$ and $q < 2.4n$.

To prove Lemma 2 we need

Brun-Titchmarsh Theorem. If $a, q \in \mathbb{Z}^+$ and $\gcd(a, q) = 1$, then

$$|\{p \leqslant x : \ p \equiv a \pmod q\}| \leqslant \frac{2x}{\varphi(q)\log(x/q)} \text{ for all } x > q.$$

Alternating sums of primes

Let p_n be the nth prime and define

$$s_n = p_n - p_{n-1} + \cdots + (-1)^{n-1} p_1.$$

Note that

$$s_{2n} = \sum_{k=1}^{n} (p_{2k} - p_{2k-1}) > 0, \quad s_{2n+1} = \sum_{k=1}^{n} (p_{2k+1} - p_{2k}) + p_1 > 0.$$

Here are values of $s_1, \ldots, s_{16}$:

$$2,\ 1,\ 4,\ 3,\ 8,\ 5,\ 12,\ 7,\ 16,\ 13,\ 18,\ 19,\ 22,\ 21,\ 26,\ 27.$$

The sequence $0, s_1, s_2, \ldots$ were first introduced by N.J.A. Sloane and J.H. Conway (see A008347 at OEIS).

It is not difficult to show that those s_n $(n = 1, 2, 3, \ldots)$ are pairwise distinct.

An amazing recurrence for primes

The following surprising conjecture on recurrence for primes allows us to compute p_{n+1} in terms of $p_1, \ldots, p_n$.

Conjecture (Sun [J. Number Theory 133(2013)]). For any positive integer $n \neq 1, 2, 4, 9$, the $(n+1)$-th prime p_{n+1} is the least positive integer m such that

$$2s_1^2, \ldots, 2s_n^2$$

are pairwise distinct modulo m.

Remark. I have verified the conjecture for $n \leqslant 10^5$, and proved that $2s_1^2, \ldots, 2s_n^2$ **are indeed pairwise distinct modulo** p_{n+1}.

A Related Conjecture (Sun, March 21, 2012). The least integer $m > 1$ such that $2S_k^2$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m is a prime smaller than n^2 unless $n \mid 6$, where $S_k = \sum_{j=1}^{k} p_j$.

Conjecture on alternating sums of consecutive primes

Conjecture (Sun [J. Number Theory 133(2013)]). For any positive integer m, there are consecutive primes $p_k, \ldots, p_n$ $(k \leqslant n)$ not exceeding $2m + 2.2\sqrt{m}$ (or $m + 4.6\sqrt{m}$ if $2 \nmid m$) such that

$$m = p_n - p_{n-1} + \cdots + (-1)^{n-k} p_k.$$

Examples.

$$10 = 17 - 13 + 11 - 7 + 5 - 3;$$

$$20 = 41 - 37 + 31 - 29 + 23 - 19 + 17 - 13 + 11 - 7 + 5 - 3;$$

$$303 = p_{76} - p_{75} + \cdots + p_{52},$$

$$p_{76} = 383 = \lfloor 303 + 4.6\sqrt{303} \rfloor, \ p_{52} = 239;$$

$$2382 = p_{652} - p_{651} + \cdots + p_{44} - p_{43},$$

$$p_{652} = 4871 = \lfloor 2 \cdot 2382 + 2.2\sqrt{2382} \rfloor, \ p_{43} = 191.$$

The conjecture has been verified for m up to 10^7. We also conjecture that the upper bound $2m + 2.2\sqrt{m}$ can be replaced by $m + 4.6\sqrt{m}$ if m is odd.

Prize. I would like to offer 1000 US dollars for the first proof.

On primes in arithmetic progressions

Theorem (Sun, `arXiv:1304.5988`). Let $d \geqslant 4$ and $c \in (-d, d)$ be relatively prime integers, and let $r(d)$ be the radical of d (i.e., the product of all the distinct prime divisors of d).

(i) For any sufficiently large integer n, the least positive integer m with $2r(d)k(dk-c)$ $(k=1,\ldots,n)$ pairwise distinct modulo m is just the first prime $p \equiv c \pmod{d}$ with $p \geqslant (2dn-c)/(d-1)$.

(ii) When $4 \leqslant d \leqslant 36$ and $n > M_d$, the required result in the first part holds, where

$$M_4 = 8,\ M_5 = 14,\ M_6 = 10,\ M_7 = 100,\ M_8 = 21,\ M_9 = 315,$$
$$M_{10} = 53,\ M_{11} = 1067,\ M_{12} = 27,\ M_{13} = 1074,\ M_{14} = 122,$$
$$M_{15} = 809,\ M_{16} = 329,\ M_{17} = 5115,\ M_{18} = 95,\ M_{19} = 5390,$$
$$M_{20} = 755,\ M_{21} = 3672,\ M_{22} = 640, M_{23} = 11193,\ M_{24} = 220,$$
$$M_{25} = 12810,\ M_{26} = 1207,\ M_{27} = 7087,\ M_{28} = 2036,$$
$$M_{29} = 13250,\ M_{30} = 177,\ M_{31} = 24310,\ M_{32} = 3678,$$
$$M_{33} = 12794,\ M_{34} = 5303,\ M_{35} = 15628,\ M_{36} = 551.$$

A corollary

Corollary (Sun, `arXiv:1304.5988`). (i) For each integer $n \geqslant 6$, the least positive integer m such that $4k(4k-1)$ (or $4k(4k+1)$) for $k = 1, \ldots, n$ are pairwise distinct modulo m, is just the least prime $p \equiv 1 \pmod 4$ with $p \geqslant (8n-1)/3$ (resp., $p \equiv -1 \pmod 4$ with $p \geqslant (8n+1)/3$).

(ii) Let $C_1 = 8,\ C_2 = 10,\ C_3 = 15$ and $C_{-2} = 5$. For any $r \in \{\pm 1, \pm 2\}$ and integer $n \geqslant C_r$, the least positive integer m such that $10k(5k-r)$ for $k = 1, \ldots, n$ are pairwise distinct modulo m, is just the least prime $p \equiv r \pmod 5$ with $p \geqslant (10n-r)/4$.

A corollary

Corollary (Sun, `arXiv:1304.5988`). (i) For each integer $n \geqslant 6$, the least positive integer m such that $4k(4k-1)$ (or $4k(4k+1)$) for $k = 1, \ldots, n$ are pairwise distinct modulo m, is just the least prime $p \equiv 1 \pmod 4$ with $p \geqslant (8n-1)/3$ (resp., $p \equiv -1 \pmod 4$ with $p \geqslant (8n+1)/3$).

(ii) Let $C_1 = 8,\ C_2 = 10,\ C_3 = 15$ and $C_{-2} = 5$. For any $r \in \{\pm 1, \pm 2\}$ and integer $n \geqslant C_r$, the least positive integer m such that $10k(5k-r)$ for $k = 1, \ldots, n$ are pairwise distinct modulo m, is just the least prime $p \equiv r \pmod 5$ with $p \geqslant (10n-r)/4$.

Auxiliary results

Prime Number Theorem for Arithmetic Progressions. If c and $d > 0$ are relatively prime integers, then

$$\pi(x; c, d) := |\{p \leqslant x : \ p \text{ is prime with } p \equiv c \pmod{d}\}| \sim \frac{x}{\varphi(d) \log x}$$

as $x \to +\infty$, where φ is Euler's totient function.

O. Ramaré and R. Rumely [Math. Comp. 65(1996)]. Let $4 \leqslant d \leqslant 36$ and $n > M_d$. Then

$$(1 - \varepsilon_d)\frac{x}{\varphi(d)} \leqslant \theta(x; c, d) \leqslant (1 + \varepsilon_d)\frac{x}{\varphi(d)} \text{ for all } x \geqslant 10^{10},$$

where $\theta(x; c, d) := \sum_{p \leqslant x, \ p \equiv c \pmod{d}} \log p$ with p prime, and

$$\varepsilon_4 = 0.002238, \ \varepsilon_5 = 0.002785, \ \varepsilon_6 = 0.002238, \ \varepsilon_7 = 0.003248,$$
$$\varepsilon_8 = 0.002811, \ \varepsilon_9 = 0.003228, \ \varepsilon_{10} = 0.002785, \ \varepsilon_{11} = 0.004125,$$
$$\cdots\cdots$$
$$\varepsilon_{33} = 0.011685, \ \varepsilon_{34} = 0.010746, \ \varepsilon_{35} = 0.012809, \ \varepsilon_{36} = 0.009544.$$

Two conjectures

Conjecture 1. For any integer $n > 4$ the least positive integer m such that

$$\begin{aligned} &|\{k(k-1)/2 \bmod m : \ k = 1, \ldots, n\}| \\ =&|\{k(k-1)/2 \bmod m+2 : \ k = 1, \ldots, n\}| = n \end{aligned}$$

is just the least prime $p \geqslant 2n-1$ with $p+2$ also prime.

Remark 1. Clearly this implies the twin prime conjecture.

Conjecture 2. For any integer $n > 2$, the smallest positive integer m such that those $6p_k(p_k-1)$ $(k = 1, \ldots, n)$ are pairwise incongruent modulo m is just the first prime $p \geqslant p_n$ dividing none of those $p_i + p_j - 1$ $(1 \leqslant i < j \leqslant n)$, where p_k denotes the k-th prime.

Remark 2. For any prime $p \geqslant p_n$ dividing none of those $p_i + p_j - 1$ $(1 \leqslant i < j \leqslant n)$, if $1 \leqslant i < j \leqslant n$ then $p_j(p_j-1) - p_i(p_i-1) = (p_j - p_i)(p_i + p_j - 1) \not\equiv 0 \pmod p$.

Part II. On some special arithmetic functions

On monotonicity related to $S_n = \sum_{k=1}^n p_k$

Theorem (Sun [Bull. Austral. Math. Soc. 88(2013)]). (i) Both $(\sqrt[n]{S_n})_{n\geqslant 2}$ and $(\sqrt[n]{S_n/n})_{n\geqslant 1}$ are strictly decreasing. Moreover,

$$\left(\frac{\sqrt[n+1]{S_{n+1}}}{\sqrt[n]{S_n}}\right)_{n\geqslant 5} \quad \text{and} \quad \left(\frac{\sqrt[n+1]{S_{n+1}/(n+1)}}{\sqrt[n]{S_n/n}}\right)_{n\geqslant 10}$$

are strictly increasing.
(ii) Let $S_n^{(m)} = \sum_{k=1}^n p_k^m$. Then the sequences

$$\left(\sqrt[n+1]{S_{n+1}^{(2)}}\Big/\sqrt[n]{S_n^{(2)}}\right)_{n\geqslant 10},$$

$$\left(\sqrt[n+1]{S_{n+1}^{(3)}}\Big/\sqrt[n]{S_n^{(3)}}\right)_{n\geqslant 10},$$

$$\left(\sqrt[n+1]{S_{n+1}^{(4)}}\Big/\sqrt[n]{S_n^{(4)}}\right)_{n\geqslant 17}$$

are all strictly increasing.

A conjecture related to $S_n = \sum_{k=1}^n p_k$

D.K.L. Shiu's Theorem [J. London Math. Soc. 61(2000)]. If a and $q > 0$ are relatively prime integers, then for any $k \in \mathbb{Z}^+$ there is a positive integer n such that

$$p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv p_{n+k} \equiv a \pmod{q}.$$

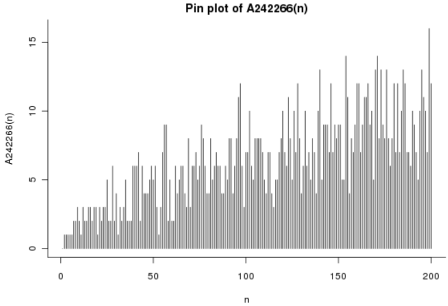
This implies that $\{S_n = \sum_{k=1}^n p_k : \ n = 1, 2, 3, \ldots\}$ contains a complete system of residues modulo any positive integer m.

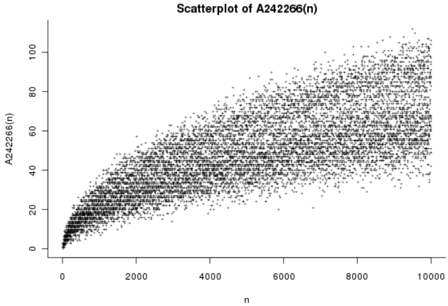
Conjecture (Sun, `arXiv:1405.0290`). For any odd prime p, there is a primitive root $0 < g < p$ modulo p in the form $S_n = \sum_{k=1}^n p_k$.

Example. $S_2 = 2 + 3 = 5$ is a primitive root modulo 7.

We have verified the conjecture for all odd primes below 10^7. I also conjecture that any prime p has a primitive root $g < p$ with $g - 1$ a square, and each prime $p > 3$ has a primitive root $0 < g < p$ with $2^g - 1$ and $(g - 1)!$ also primitive roots mod p.

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





On $\omega(n)$ and $\Omega(n)$

For $n \in \mathbb{Z}^+$, $\omega(n)$ denotes the number of distinct prime divisors of n, and $\Omega(n)$ denotes the total number of prime divisors of n (with multiplicity counted).

Theorem (Sun, arXiv:1204.6689). For any integer $m > 4$,

$$\zeta_m(1) := \sum_{n=1}^{\infty} \frac{(-e^{2\pi i/m})^{\omega(n)}}{n} = 0,$$

$$\zeta_m^*(1) := \sum_{n=1}^{\infty} \frac{(-e^{2\pi i/m})^{\Omega(n)}}{n} = 0.$$

Moreover,

$$(\log x)^{e^{2\pi i/m}} \sum_{n \leqslant x} \frac{(-e^{2\pi i/m})^{\omega(n)}}{n} = c_m + O\left(\frac{1}{\log x}\right),$$

$$(\log x)^{e^{2\pi i/m}} \sum_{n \leqslant x} \frac{(-e^{2\pi i/m})^{\Omega(n)}}{n} = C_m + O\left(\frac{1}{\log x}\right),$$

where c_m and C_m are constants depending on m.

A hypothesis implying Riemann's Hypothesis

Pólya's Conjecture (1919). $L(x)=\sum_{n\leqslant x}(-1)^{\Omega(n)}<0$ for $x\geqslant 1$.
This is false. The smallest x with $L(x)>0$ is $x=906150257$.

Turán's Conjecture (1948). $\sum_{n\leqslant x}\lambda(n)/n>0$ for all $x\geqslant 1$.

This also fails. Now it is known that the smallest x with $\sum_{n\leqslant x}\lambda(n)/n<0$ is $x=72185376951205$.

New Hypothesis (Sun, arXiv:1204.6689). We have

$$S(x):=\sum_{n\leqslant x}(-1)^{n-\Omega(n)}>0 \quad \text{for all } x\geqslant 5,$$

$$T(x):=\sum_{n\leqslant x}\frac{(-1)^{n-\Omega(n)}}{n}<0 \quad \text{for all } x\geqslant 1,$$

$$1<\frac{S(x)}{\sqrt{x}}<2.3 \quad \text{for all } x\geqslant 325,$$

$$-2.3<T(x)\sqrt{x}<-1 \quad \text{for all } x\geqslant 3.$$

Remark. RH follows if $S(x)>0$ for $x\geqslant 5$ or $T(x)<0$ for $x\geqslant 1$.

A conjecture involving the Möbius function

Conjecture (Sun, August 2013). For any positive integer n, we have

$$|\mu(i+j-1)|_{1\leqslant i,j\leqslant n} \neq 0 \quad \text{and} \quad |\mu^2(i+j)|_{1\leqslant i,j\leqslant n} \neq 0.$$

Conjecture (Sun, August 2013). Let $f(p)$ take 1 or 0 according as p is prime or not. Then, for any integer $n > 15$ we have

$$|f(i+j)|_{1\leqslant i,j\leqslant n} \neq 0.$$

On generalized Möbius functions

For any positive integers m and n, define

$$\mu_m(n) = \begin{cases} (-e^{2\pi i/m})^{\omega(n)} & \text{if } n \text{ is squarefree,} \\ 0 & \text{otherwise.} \end{cases}$$

Note that μ_2 is the classical Móbius function μ.

Theorem (Sun, arXiv:1204.6689). We have

$$\sum_{n=1}^{\infty} \frac{\mu_5(n)}{n} = \sum_{n=1}^{\infty} \frac{\mu_6(n)}{n} = \cdots = 0.$$

Moreover, for any positive integer $m \neq 2$ we have

$$(\log x)^{e^{2\pi i/m}} \sum_{n \leqslant x} \frac{\mu_m(n)}{n} = c_m + O\left(\frac{1}{\log x}\right) \quad (x \geqslant 2),$$

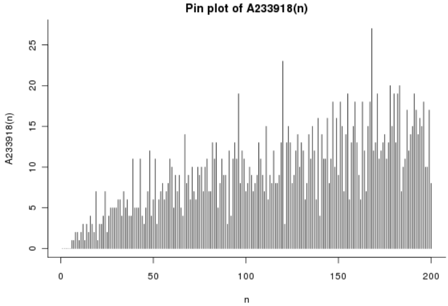
where c_m is a constant depending on m which can be written explicitly.

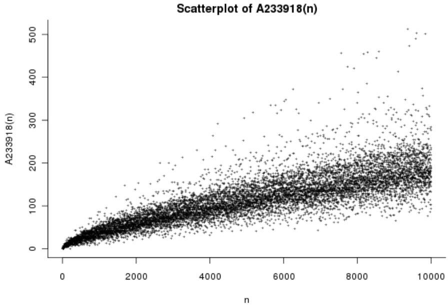
On Euler's totient function

Conjecture (Sun) (i) (2013-12) Any integer $n > 5$ can be written as a sum of two positive integers k and m such that $(\varphi(k) + \varphi(m))/2$ is prime.

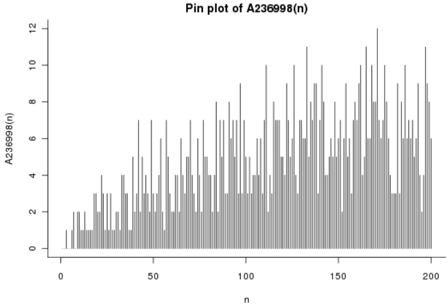
(ii) (2014-02) Any integer $n > 8$ can be written as a sum of two distinct positive integers k and m such that $\varphi(k)\varphi(m)$ is a square. Also, any integer $n > 7$ can be written as a sum of two distinct positive integers k and m such that $\varphi(km) + 1$ is a square.

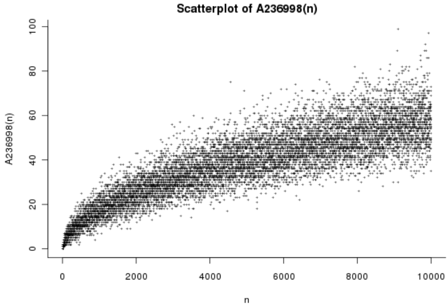
Graph for $a(n) = |\{0 < k \leqslant n/2 : \ (\varphi(k) + \varphi(n-k))/2 \text{ is prime}\}|$





Graph for $a(n) = |\{0 < k < n/2 : \varphi(k)\varphi(n-k) \text{ is a square}\}|$





On the function $\sigma(n)$

By Goldbach's conjecture, any even number $2n > 2$ can be written as $p + q$ with p and q both prime, and thus

$$2n + 1 = p + (q + 1) = p + \sigma(q).$$

Conjecture (Sun, 2013-12) For any integer $n > 1$, we can write $2n$ as $p + \sigma(k)$, where p is an odd prime and k is a positive integer.

Conjecture (Sun, 2013-12) Any integer $n > 1$ can be written as $k^2 + m$ with $0 < k^2 \leqslant m$ such that $\sigma(k^2) + \varphi(m)$ is 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) Any integer $n > 3$ can be written as a sum of two elements of the set

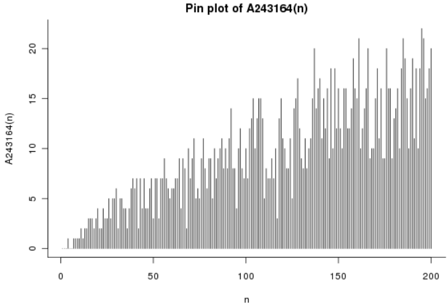
$$S = \{k > 0 : \text{ the inverse of } k \text{ modulo } p_k \text{ is prime}\}.$$

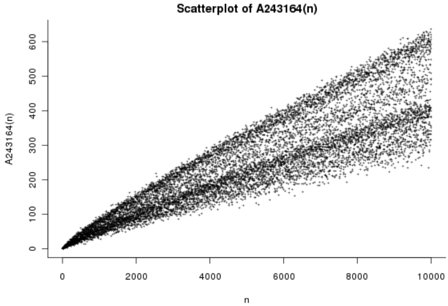
This is somewhat similar to Goldbach's Conjecture.

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). 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 $k, m \in S$





On the prime-counting function $\pi(x)$

Conjecture (Sun, 2014-03) For any positive integer n, $\pi(\pi(kn))$ is a square for some $k = 1, \ldots, n$.

Remark. I have verified this for n up to 2×10^5.

Examples for part (ii):

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

On the prime-counting function $\pi(x)$

Conjecture (Sun, 2014-03) For any positive integer n, $\pi(\pi(kn))$ is a square for some $k = 1, \ldots, n$.

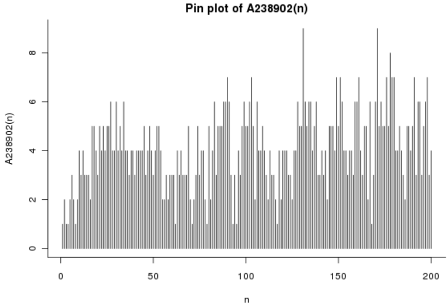
Remark. I have verified this for n up to 2×10^5.

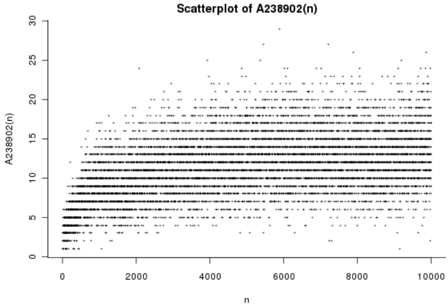
Examples for part (ii):

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

The conjecture might never be solved by human beings!

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





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.

A mysterious conjecture on the partition function

Conjecture (Sun, 2014-04) 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 $q = 16921$.

Below are two more challenging conjectures involving primitive roots.

A mysterious conjecture on the partition function

Conjecture (Sun, 2014-04) 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 $q = 16921$.

Below are two more challenging conjectures involving primitive roots.

Conjecture (Sun, 2014-05). 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.

A mysterious conjecture on the partition function

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

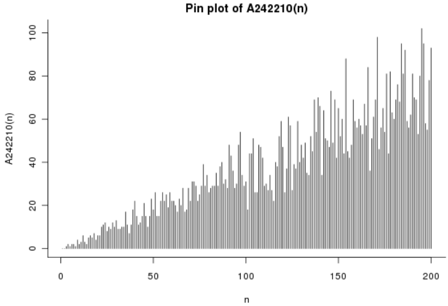
Remark. I have verified this for all primes $p < 2 \times 10^7$. For example, $p(35) = 14883$ is a primitive root modulo the prime $q = 16921$.

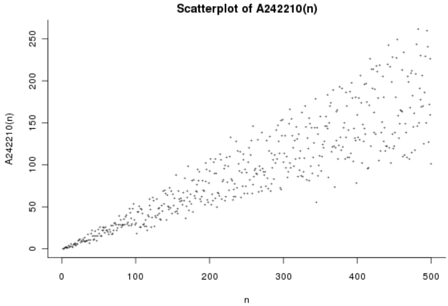
Below are two more challenging conjectures involving primitive roots.

Conjecture (Sun, 2014-05). 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.

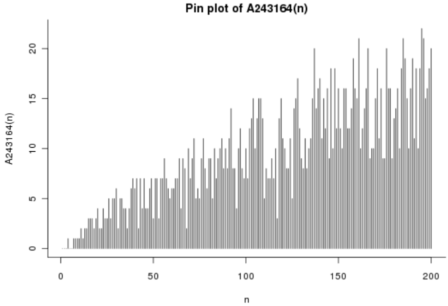
Conjecture (Sun, 2014-06). For any integer $n > 6$, there is a prime $p < n$ such that pn is a primitive root modulo the n-th prime p_n.

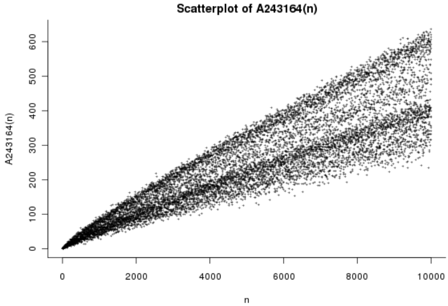
Graph for $a(n) = |\{0 < k < n : \ B_{p_k - 1} \text{ is a primitive root mod } p_n\}|$





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





For sources of my conjectures, you may visit my homepage
`http://math.nju.edu.cn/~zwsun`

You are welcome to solve my conjectures!

Thank you!