A talk given at the Workshop on Analytic Number Theory
(Shanghai, Nov. 28-29, 2015)

On primes in arithmetic progressions

Zhi-Wei Sun

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

Nov. 29, 2015

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

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

— W. T. Gowers (2002)

Part I. On functions taking only prime values

Mills' theorem

To find nontrivial arithmetical functions taking only prime values is a fascinating topic in number theory.

Theorem (Mills, 1947). There is a constant $A > 0$ 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 $n = 1, 2, 3, \ldots$.

Remark. Mills' constant A *cannot be effectively found*.

Discriminant 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

Unaware of the previous results on discriminants, in 2012 I was led to consider arithmetical functions whose discriminants are always prime. This resulted in my following paper:

Z.-W. Sun, *On functions taking only prime values*, J. Number Theory, 133(2013), no.8, 2794-2812.

Theorem 1 (Sun, Feb. 29, 2012) For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m. Then $S(n)$ is the least prime $p \geqslant 2n-1$.

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

$$\binom{k}{2} = \frac{k(k-1)}{2} \quad (k = 1, \ldots, n)$$

are pairwise distinct modulo m, is just the least power of two not smaller than n.

Another theorem

Theorem 2 (Sun, March 2012) (i) Let $d \in \{2, 3\}$ and $n \in \mathbb{Z}^+$. Then the smallest positive integer m such that those $k(dk-1)$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m, is the least power of d not smaller than n.

(ii) 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 $p \equiv 1 \pmod 3$.

Remark. We are also able to prove some other similar results including the following one:

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 $3n$.

One more theorem

Theorem (Sun, March 2012). (i) For $d, n \in \mathbb{Z}^+$ let $\lambda_d(n)$ be the smallest integer $m > 1$ such that those

$$(2k-1)^d \quad (k = 1, \ldots, n)$$

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

$$k^q(k-1)^q \quad (k = 1, \ldots, n)$$

are pairwise incongruent mod m, is just the least prime $p \geqslant 2n-1$ with $p \not\equiv 1 \pmod{q}$.

Remark. In the proof I used the Brun-Titchmarsh theorem which asserts that if $a, q \in \mathbb{Z}^+$, $\gcd(a, q) = 1$ and $x > q$ then

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

Alternating sums of primes

Let p_n be the n-th 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, March 28, 2012). 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, April 2-3, 2012). For any positive integer m, there are consecutive primes $p_k, \ldots, p_n$ $(k < n)$ 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. Most known results on primes are about local properties of primes, not about relations of primes.

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

Part II. On primes in arithmetic progressions

My result on primes in arithmetic progressions

For $d = 1, 2, 3, \ldots$ the *radical of* d (denoted by $r(d)$) is the product of all the distinct prime divisors of d. ($r(1)$ is regarded as 1).

In 2013, I found the following result based on my numerical computations via a computer.

Main Theorem (Sun [J. Number Theory, 160(2016)]). Let $d \geqslant 4$ and $c \in (-d, d)$ be relatively prime integers. For $n \in \mathbb{Z}^+$ define $m_{d,c}(n)$ as the least positive integer m for which the integers

$$f_{d,c}(k) = 2r(d)k(dk - c) \quad (k = 1, \ldots, n)$$

are pairwise distinct modulo m.

(i) If $n \in \mathbb{Z}^+$ is sufficiently large, then $m_{d,c}(n)$ is the least prime $p \equiv c \pmod{d}$ with $p \geqslant (2dn - c)/(d - 1)$.

My result on primes in AP (continued)

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

$$M_4 = 8,\ M_5 = 14,\ M_6 = 9,\ M_7 = 100,\ M_8 = 21,\ M_9 = 315,$$
$$M_{10} = 53,\ M_{11} = 1067,\ M_{12} = 27,\ M_{13} = 1074,\ M_{14} = 122,$$
$$M_{15} = 809,\ M_{16} = 329, M_{17} = 5115,\ M_{18} = 95,\ M_{19} = 5390,$$
$$M_{20} = 755,\ M_{21} = 3672,\ M_{22} = 640,\ M_{23} = 11193,$$
$$M_{24} = 220,\ M_{25} = 12810,\ M_{26} = 1207,\ M_{27} = 7087,$$
$$M_{28} = 2036,\ M_{29} = 13250,\ M_{30} = 177,\ M_{31} = 24310,$$
$$M_{32} = 3678,\ M_{33} = 12794,\ M_{34} = 5303,\ M_{35} = 15628,\ M_{36} = 551.$$

A corollary

The theorem with $d = 4, 5$ yields the following concrete consequence.

Corollary. (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 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

$$C_1 = 8,\ C_2 = 10,\ C_{-1} = 15,\ C_{-2} = 5.$$

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 the least prime $p \equiv r \pmod 5$ with $p \geqslant (10n-r)/4$.

A supplement to the Main Theorem

As a supplement to the theorem with $d \geqslant 4$, we are able to prove the following result for the cases $d = 2, 3$.

Theorem (Sun, JNT 160(2016)). For $d \in \{2, 3\}$ and integer $c \in (-d, d)$, let $S_{d,c}$ be the set of all primes $p \equiv c \pmod{d}$ and powers of d. Then

$$\begin{aligned}
m_{2,1}(n) &= \min\{a \geqslant 4n-1 : \ a \in S_{2,1}\} \ \text{ for } n \geqslant 5,\\
m_{2,-1}(n) &= \min\{a \geqslant 4n : \ a \in S_{2,-1}\} \ \text{ for } n \geqslant 7,\\
m_{3,1}(n) &= \min\{a \geqslant 3n : \ a \in S_{3,1}\} \ \text{ for } n \geqslant 4,\\
m_{3,-1}(n) &= \min\{a \geqslant 3n : \ a \in S_{3,-1}\} \ \text{ for } n \geqslant 5,\\
m_{3,2}(n) &= \min\{a \geqslant 3n-1 : \ a \in S_{3,2}\} \ \text{ for } n \geqslant 3,\\
m_{3,-2}(n) &= \min\{a \geqslant 3n : \ a \in S_{3,-2}\} \ \text{ for } n \geqslant 8.
\end{aligned}$$

The first lemma

Lemma 1. Let c and $d > 1$ be relatively prime integers. For any $\varepsilon > 0$, if $n \in \mathbb{Z}^+$ is large enough, then there is a prime $p \equiv c \pmod{d}$ with

$$\frac{d(2n-1)-c}{d-1} < p \leqslant \frac{d((2+\varepsilon)n-1)-c}{d-1}.$$

This lemma is an easy consequence of the Prime Number Theorem for arithmetic progressions which states that

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

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

Two key lemmas

Lemma 2. Let $d > 2$ and $c \in (-d, d)$ be relatively prime integers. Suppose that p is a prime not exceeding

$$(d((2+\varepsilon)n - 1) - c)/(d-1),$$

where $n \geqslant 3d$ and $0 < \varepsilon \leqslant 2/(d-2)$. Then

$$\begin{aligned} & f_{d,c}(k)\ (k = 1, \ldots, n) \text{ are pairwise distinct modulo } p \\ \iff & p \equiv c \pmod{d} \text{ and } p > (d(2n-1) - c)/(d-1). \end{aligned}$$

Lemma 3. Let $d > 2$ and $c \in (-d, d)$ be relatively prime integers, and let $n \geqslant 6d$ be an integer. Suppose that

$$m \in [n, (d((2+\varepsilon)n - 1) - c)/(d-1)]$$

is a power of two or twice an odd prime, where $0 < \varepsilon \leqslant 2/3$. Then, there are $1 \leqslant k < l \leqslant n$ such that $f_{d,c}(k) \equiv f_{d,c}(l) \pmod{m}$.

Proof of the Main Theorem

Let $\varepsilon = 2/(\max\{11, d\} - 2)$. By Lemma 1, if $n \in \mathbb{Z}^+$ is large enough then there is at least a prime $p \equiv c \pmod{d}$ with

$$\frac{d(2n-1)-c}{d-1} < p \leqslant \frac{d((2+\varepsilon)n-1)-c}{d-1}. \qquad (*)$$

(i) Choose an integer $N \geqslant \max\{6d, 243\}$ such that for any integer $n \geqslant N$ there is a prime $p \equiv c \pmod{d}$ satisfying $(*)$. Fix an integer $n \geqslant N$ and let $m = m_{d,c}(n)$. Clearly $m \geqslant n$. By Lemma 2, $m \leqslant m'$ where m' denotes the least prime $p \equiv c \pmod{d}$ satisfying $(*)$.

Assume that $m \neq m'$. We want to reach a contradiction. Clearly m is not a prime by Lemma 2. Note that $\varepsilon \leqslant 2/9$. In view of Lemma 3, m is neither a power of two nor twice an odd prime. So we have $m = pq$ for some odd prime p and integer $q > 2$.

Proof of part (i) of the Main Theorem

Observe that

$$\frac{m}{3} \leqslant \frac{d((2+\varepsilon)n-1)-c}{3(d-1)} < \frac{d(2+2/9)}{3(d-1)}n = \frac{20d}{27(d-1)}n \leqslant \frac{80}{81}n$$

and hence

$$\frac{m}{3} + 3 < \frac{80}{81}n + \frac{n}{81} = n.$$

If $p \mid d$, then for $k := 1$ and $l := q+1 = m/p+1 < m/3+3 < n$, we have $pq \mid r(d)(l-k)$ and hence $f_{d,c}(k) \equiv f_{d,c}(l) \pmod{m}$.

Now suppose that $p \nmid d$. Then $2dk \equiv c - dq \pmod{p}$ for some $1 \leqslant k \leqslant p$. Clearly, $l := k+q \leqslant p+q = m/q + m/p$. Note that

$$(l-k)(d(l+k)-c) = q(d(2k+q)-c) \equiv 0 \pmod{pq}$$

and hence $f_{d,c}(k) \equiv f_{d,c}(l) \pmod{m}$.

Proof of part (i) of the Main Theorem

If $\min\{p, q\} \leqslant 4$, then

$$l \leqslant p + q = \frac{m}{\min\{p, q\}} + \min\{p, q\} \leqslant \frac{m}{3} + 4 < n + 1.$$

If $\min\{p, q\} \geqslant 5$, then

$$l \leqslant \frac{m}{q} + \frac{m}{p} \leqslant \max\left\{\frac{m}{6} + \frac{m}{7},\ \frac{m}{5} + \frac{m}{8}\right\} < \frac{m}{3} < n$$

since $pq = m \geqslant n \geqslant 243 \geqslant 40$. So we get a contradiction as desired.

Proof of part (ii) of the Main Theorem

Now assume that $4 \leqslant d \leqslant 36$. By O. Ramaré and R. Rumely [Math. Comp 1996], we have

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

where

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

$$\begin{aligned}
\varepsilon_4 &= 0.002238,\ \varepsilon_5 = 0.002785,\ \varepsilon_6 = 0.002238,\ \varepsilon_7 = 0.003248,\\
\varepsilon_8 &= 0.002811,\ \varepsilon_9 = 0.003228,\ \varepsilon_{10} = 0.002785,\ \varepsilon_{11} = 0.004125,\\
\varepsilon_{12} &= 0.002781,\ \varepsilon_{13} = 0.004560,\ \varepsilon_{14} = 0.003248,\ \varepsilon_{15} = 0.008634,\\
\varepsilon_{16} &= 0.008994,\ \varepsilon_{17} = 0.010746,\ \varepsilon_{18} = 0.003228,\ \varepsilon_{19} = 0.011892,\\
\varepsilon_{20} &= 0.008501,\ \cdots\cdots,\ \varepsilon_{31} = 0.014535,\ \varepsilon_{32} = 0.011103,\\
\varepsilon_{33} &= 0.011685,\ \varepsilon_{34} = 0.010746,\ \varepsilon_{35} = 0.012809,\ \varepsilon_{36} = 0.009544.
\end{aligned}$$

Proof of part (ii) of the Main Theorem

As $\varepsilon = 2/(\max\{11, d\} - 2)$, we can easily verify that

$$\frac{\varepsilon}{2} - \frac{2}{10^{10}} > \frac{2\varepsilon_d}{1-\varepsilon_d} = \frac{1+\varepsilon_d}{1-\varepsilon_d} - 1.$$

If $n \geqslant 10^{10}/2$, then

$$((2+\varepsilon)n - 2)\frac{d}{d-1} \geqslant 2n\frac{d}{d-1} > 10^{10},$$

$$\frac{\varepsilon}{2} - \frac{1}{n} + 1 \geqslant \frac{\varepsilon}{2} - \frac{2}{10^{10}} + 1 > \frac{1+\varepsilon_d}{1-\varepsilon_d},$$

hence we have

$$\frac{\theta(((2+\varepsilon)n-2)d/(d-1); c, d)}{\theta(2nd/(d-1); c, d)}$$

$$\geqslant \frac{(1-\varepsilon_d)((2+\varepsilon)n-2)d/(d-1)}{(1+\varepsilon_d)2nd/(d-1)} = \frac{1-\varepsilon_d}{1+\varepsilon_d}\left(1 + \frac{\varepsilon}{2} - \frac{1}{n}\right) > 1$$

and thus there is a prime $p \equiv c \pmod{d}$ for which

$$\frac{2dn}{d-1} < p \leqslant \frac{((2+\varepsilon)n-2)d}{d-1}.$$

Proof of part (ii) of the Main Theorem

Let N_d be the least positive integer such that for any $n = N_d, \ldots, 10^{10}/2$ and any $a \in \mathbb{Z}$ relatively prime to d, the interval $(2dn/(d-1), ((2+\varepsilon)n - 2)d/(d-1))$ contains a prime congruent to a modulo d. Via a computer we find that

$$N_4 = 79,\ N_5 = 206,\ N_6 = 103,\ N_7 = 471,\ N_8 = 301,\ N_9 = 356,$$
$$N_{10} = 232,\ N_{11} = 1079,\ N_{12} = 346,\ N_{13} = 1166,\ N_{14} = 806,$$
$$N_{15} = 1310,\ N_{16} = 2183,\ N_{17} = 5153,\ N_{18} = 1135,\ N_{19} = 5402,$$
$$N_{20} = 2388,\ N_{21} = 4059,\ N_{22} = 2934,\ N_{23} = 11246,\ N_{24} = 2480,$$
$$N_{25} = 13144,\ N_{26} = 4775,\ N_{27} = 11646,\ N_{28} = 5314,$$
$$N_{29} = 13478,\ N_{30} = 5215,\ N_{31} = 24334,\ N_{32} = 8964,$$
$$N_{33} = 15044,\ N_{34} = 14748,\ N_{35} = 16896,\ N_{36} = 9847.$$

For any integer $n \geqslant N_d$, there is a prime $p \equiv c \pmod{d}$ satisfying $(*)$. Note that $6d \leqslant 6 \times 36 < 243$. For $n \geqslant N = \max\{N_d, 243\}$ we may apply part (i) to get the desired result.
If $M_d < n \leqslant \max\{N_d, 243\}$, then we can easily verify the desired result via a computer. This ends the proof.

Part III. Some new conjectures of mine on primes

A conjecture related to the Twin Prime Conjecture

Conjecture (Sun, JNT 160(2016)). For any $d \in \mathbb{Z}^+$ there is a positive integer n_d such that for any integer $n \geqslant n_d$ the least positive integer m satisfying

$$\begin{aligned}&\left|\left\{\binom{k}{2} \bmod m:\ k=1,\ldots,n\right\}\right|\\ =&\left|\left\{\binom{k}{2} \bmod m+2d:\ k=1,\ldots,n\right\}\right|=n\end{aligned}$$

is the smallest prime $p \geqslant 2n-1$ with $p+2d$ also prime. Moreover, we may take

$$n_1=5,\ n_2=n_3=6,\ n_4=10,\ n_5=9,$$
$$n_6=8,\ n_7=9,\ n_8=18,\ n_9=11,\ n_{10}=9.$$

Remark. A well-known conjecture of de Polignac asserts that for any positive integer d there are infinitely many prime pairs $\{p,q\}$ with $p-q=2d$.

Two more conjectures

Conjecture (Sun, JNT 160(2016)). Let n be any positive integer and consider the least positive integer m such that

$$\left|\left\{\binom{k}{2} \bmod m:\ k=1,\ldots,n\right\}\right|$$
$$=\left|\left\{\binom{k}{2} \bmod m+1:\ k=1,\ldots,n\right\}\right|=n.$$

Then, each of m and $m+1$ is either a power of two (including $2^0=1$) or a prime times a power of two.

Conjecture (Sun, JNT 160(2016)). Let n be any positive integer. Then the least positive integer m of the form x^2+x+1 (or $4x^2+1$) with $x\in\mathbb{Z}$ such that the numbers

$$\binom{k}{2}\ \ (k=1,\ldots,n)$$

are pairwise distinct modulo m, is the the smallest prime $p\geqslant 2n-1$ of the form x^2+x+1 (resp., $4x^2+1$) with $x\in\mathbb{Z}$.

One more conjecture on discriminants

Let p_n denote the n-th prime.

Conjecture (Sun, JNT 160(2016)). For any integer $n > 2$, the smallest positive integer m such that the integers

$$6p_k(p_k-1)\ \ (k=1,\ldots,n)$$

are pairwise incongruent modulo m is precisely the least prime $p \geqslant p_n$ dividing none of the numbers p_i+p_j-1 $(1 \leqslant i < j \leqslant n)$.

Remark. For any prime $p \geqslant p_n$ dividing none of the numbers p_i+p_j-1 $(1 \leqslant i < j \leqslant n)$, clearly

$$p_j(p_j-1)-p_i(p_i-1)=(p_j-p_i)(p_i+p_j-1)\not\equiv 0 \pmod{p}$$

for all $1 \leqslant i < j \leqslant n$.

Example. The least positive integer m such that $6p_k(p_k-1)$ $(k=1,\ldots,10)$ are pairwise distinct mod m is 37 which is greater than $p_{10}=29$ and divides none of p_i+p_j-1 $(1 \leqslant i < j \leqslant 10)$.

Green-Tao Theorem for sparse primes

Green-Tao Theorem (2004). For any integer $k \geqslant 3$, the set P of primes contains a k-AP (arithmetic progression with k terms).

Define

$$P_1 = P, \quad \text{and} \quad P_{m+1} = \{p_n : \ n \in P_m\} \ (m = 1, 2, 3, \ldots).$$

Thus

$$P_1 = \{p_n : \ n = 1, 2, 3, \ldots\}, \ P_2 = \{p_{p_n} : \ n = 1, 2, 3, \ldots\},$$
$$P_3 = \{p_{p_{p_n}} : \ n = 1, 2, 3, \ldots\}, \quad \ldots\ldots$$

Clearly, the n term in P_m has the main term $n \log^m n$ as $n \to +\infty$.

Conjecture (Sun, 2015-08-20). For any integer $m \geqslant 1$ and $k \geqslant 3$, the set P_m contains a k-AP.

A conjecture on $\pi(n^k)/n^k$

As $\pi(x) \sim x/\log x$, we see that

$$\lim_{n\to\infty} \frac{\pi(n^k)}{n^k} = 0 \quad \text{for all } k = 1, 2, 3, \ldots.$$

Conjecture (Sun, 2015-10-14).

(i) All the numbers $\pi(n^2)/n^2$ $(n = 1, 2, 3, \ldots)$ are pairwise distinct. Moreover, we have

$$\frac{\pi(n^2)}{n^2} > \frac{\pi((n+1)^2)}{(n+1)^2} \quad \text{for all } n > 15646.$$

(ii) For any integer $k > 2$ the sequence $\pi(n^k)/n^k$ $(n = 2, 3, \ldots)$ is strictly decreasing.

A symmetric conjecture

Goldbach's Conjecture. Any even number $n > 3$ can be written as $p + q$ with p and q both prime.

Lemoine's Conjecture. Any odd number $n > 6$ can be written as $2p + q$ with p and q both prime.

A Symmetric Conjecture (Sun, August 28, 2015). Let $n > 6$ be any integer, and let n' be 1 or 2 according as n is odd or even. Then there is a prime $p < n/n'$ such that $n \pm (n'p - 1)$ are both prime.

I have verified the symmetric conjecture for $6 < n \leqslant 10^8$.

Examples. For $n = 11$, the three numbers 7, $11 - (7 - 1) = 5$ and $11 + (7 - 1) = 17$ are all prime. For $n = 46$, the three numbers 17, $46 - (2 \times 17 - 1) = 13$ and $46 + (2 \times 17 - 1) = 79$ are all prime.

In view of Chen's theorem, is it practical to prove the following weaker version of the symmetric conjecture? *For any sufficiently large integer n, there is a prime $p < n/n'$ such that $n \pm (n'p - 1)$ are both P_2 (a product of at most two primes).*

On representations of positive rational numbers

Conjecture (Z.-W. Sun, 2015-07-03) The set

$$\left\{\frac{m}{n}:\ m,n\in\mathbb{Z}^+ \text{ and } p_m+p_n \text{ is a square}\right\}$$

contains any positive rational number r.

Remark. We have verified this for all those rational numbers $r=a/b$ with $a,b\in\{1,\ldots,200\}$. For example, $2=20/10$ with $p_{20}+p_{10}=71+29=10^2$ a square.

Conjecture (Z.-W. Sun, 2015-07-03) Any positive rational number r can be written as m/n with $m,n\in\mathbb{Z}^+$ such that $\pi(m)\pi(n)$ is a positive square.

Remark. We have verified this for $r=a/b$ with $a,b\in\{1,\ldots,60\}$. For example, $49/58=1076068567/1273713814$ with

$$\pi(1076068567)\pi(1273713814)=54511776\times 63975626=59054424^2.$$

A conjecture related to additive chains

A (finite or infinite) strictly increasing sequence with the initial term 1 is called an **addition chain** if each term after the initial one can be written as the sum of two earlier (not necessarily distinct) terms. For example,

$$a(1) = 1,\ a(2) = 1 + 1 = 2,\ a(3) = 2 + 2 = 4,$$
$$a(4) = 4 + 2 = 6,\ a(5) = 4 + 4 = 8,\ a(6) = 8 + 6 = 14$$

is an addition chain for 14.

Conjecture (Sun, 2015-09-23). The sequence

$$s(n) = \pi\left(\frac{n(n+1)}{2} + 1\right) \quad (n = 1, 2, 3, \ldots)$$

is an additive chain.

Remark. I have verified that for each $n = 2, \ldots, 10^5$ we can write $s(n)$ as $s(k) + s(m)$ for some $k, m \in \mathbb{Z}^+$.

A conjecture on $\varphi(n)\pi(n^2)$ and $\sigma(n)\pi(n^2)$

For any positive integer n, define

$$\varphi(n)=|\{1\leqslant a\leqslant n:\ (a,n)=1\}|\ \text{ and }\sigma(n)=\sum_{d|n}d.$$

Conjecture (Sun, 2014-10-14). All the numbers

$$\varphi(n)\pi(n^2)\ \ (n=1,2,3,\ldots)$$

are pairwise distinct. Also, all the numbers

$$\sigma(n)\pi(n^2)\ \ (n=1,2,3,\ldots)$$

are pairwise distinct.

Remark. I have verified that all the numbers $\varphi(n)\pi(n^2)$ (or $\sigma(n)\pi(n^2)$) $(n=1,2,\ldots,4\times10^5)$ are indeed pairwise distinct!

On representations involving $\pi(x^2)$

By the Prime Number Theorem,

$$\pi(x^2) \sim \frac{x^2}{\log x^2} = \frac{x^2}{2\log x} \text{ for } x \geqslant 2.$$

Conjecture (Sun, 2015-10-09). (i) Any positive integer n can be written as $\pi(x^2) + \pi(y^2/2)$, where x and y are positive integers.

(ii) Any positive integer n can be written as $\pi(x^2/2) + \pi(3y^2/2)$, where x and y are positive integers.

Remark. I have verified this for n up to 4×10^5. For example,

$$28 = 11 + 17 = \pi(6^2) + \pi\left(\frac{11^2}{2}\right)$$

and

$$100407 = 7554 + 92853 = \pi\left(\frac{392^2}{2}\right) + \pi\left(\frac{3 \times 894^2}{2}\right).$$

A challenging conjecture on the prime sequence

Conjecture (Z.-W. Sun, 2014-09-25) Let m be any positive integer. Then $m+n$ divides p_m+p_n for some $n\in\mathbb{Z}^+$. Moreover, we may require $n<m(m-1)$ if $m>2$.

Remark. We have verified this for all $m=1,\ldots,10^5$, see `http://oeis.org/A247824` for related data.

Example. The least $n\in\mathbb{Z}^+$ with $2+n$ dividing p_2+p_n is 5. For $m=79276$, the least $n\in\mathbb{Z}^+$ with $m+n$ dividing p_m+p_n is $3141281384>3\times 10^9$.

Heuristic Argument (not rigorous). The probability for $p_m+p_n\equiv 0\pmod{m+n}$ is around $1/(m+n)$. Note that

$$\sum_{n=1}^{m(m-1)}\frac{1}{n+m}=\sum_{k=1}^{m^2}\frac{1}{k}-\sum_{k=1}^{m}\frac{1}{k}\sim\log m^2-\log m=\log m\to\infty$$

as $m\to+\infty$.

A conjecture on unit fractions involving primes

It is well known that any positive rational number can be written as the sum of some distinct unit fractions (via the simple fact $1/n = 1/(n+1) + 1/(n(n+1))$). For example,

$$\frac{2}{3} = \frac{1}{3} + \frac{1}{3} = \frac{1}{3} + \left(\frac{1}{4} + \frac{1}{3\times 4}\right) = \frac{1}{3} + \frac{1}{4} + \frac{1}{12}.$$

As Euler proved, the series $\sum_p 1/p$ diverges, where p runs over all the primes.

Conjecture (Z.-W. Sun, 2015-09-09). Let r be any positive rational number. For $d = \pm 1$, there are finitely many distinct primes $q_1, \ldots, q_k$ such that $r = \sum_{j=1}^{k} 1/(q_j + d)$.

Remark. On Nov. 4, 2015 I announced a prize of 1000 US dollars for the first correct proof. The conjecture has been verified for all those rational numbers $r \in (0, 1]$ with denominators not exceeding 100. (`http://math.nju.edu.cn/~zwsun/UnitFraction.pdf`.)

Examples:

$$1 = \frac{1}{2-1} = \frac{1}{3-1} + \frac{1}{5-1} + \frac{1}{7-1} + \frac{1}{13-1},$$

$$1 = \frac{1}{2+1} + \frac{1}{3+1} + \frac{1}{5+1} + \frac{1}{7+1} + \frac{1}{11+1} + \frac{1}{23+1},$$

$$\begin{aligned}\frac{1}{19} =& \frac{1}{37-1} + \frac{1}{137-1} + \frac{1}{191-1} + \frac{1}{229-1} \\ &+ \frac{1}{331-1} + \frac{1}{397-1} + \frac{1}{761-1} + \frac{1}{1021-1} \\ =& \frac{1}{37+1} + \frac{1}{107+1} + \frac{1}{227+1} + \frac{1}{239+1} \\ &+ \frac{1}{311+1} + \frac{1}{359+1} + \frac{1}{701+1} + \frac{1}{911+1}\end{aligned}$$ (Z.-W. Sun).

$$\begin{aligned}\frac{6}{29} =& \frac{1}{7-1} + \frac{1}{29-1} + \frac{1}{281-1} + \frac{1}{2437-1} + \frac{1}{2521-1} + \frac{1}{7309-1} \\ =& \frac{1}{5+1} + \frac{1}{29+1} + \frac{1}{271+1} + \frac{1}{509+1} + \frac{1}{1217+1} \\ &+ \frac{1}{4079+1} + \frac{1}{7307+1} + \frac{1}{17747+1}\end{aligned}$$ (Qing-Hu Hou, Nov. 6).

Write $n = x + y$ with $2^x + y$ prime

Conjecture (Sun, Nov. 10, 2013). Any integer $n > 1$ can be written as $x + y$ with $2^x + y$ prime, where x and y are positive integers.

Examples: $8 = 3 + 5$ with $2^3 + 5 = 13$ prime, and $53 = 20 + 33$ with $2^{20} + 33 = 1048609$ prime.

In 2013, I verified the conjecture for n up to 2×10^6 except for $n = 1657977$. For $n = 1657977$ the least $x \in \mathbb{Z}^+$ with $2^x + (n - x)$ prime is greater than 2×10^5.

Write $n = x + y$ with $2^x + y$ prime

Conjecture (Sun, Nov. 10, 2013). Any integer $n > 1$ can be written as $x + y$ with $2^x + y$ prime, where x and y are positive integers.

Examples: $8 = 3 + 5$ with $2^3 + 5 = 13$ prime, and $53 = 20 + 33$ with $2^{20} + 33 = 1048609$ prime.

In 2013, I verified the conjecture for n up to 2×10^6 except for $n = 1657977$. For $n = 1657977$ the least $x \in \mathbb{Z}^+$ with $2^x + (n - x)$ prime is greater than 2×10^5.

On August 30, 2015 I found that $1657977 = 205494 + 1452483$ with $2^{205494} + 1452483$ a prime of 61860 decimal digits.

Write $n = x + y$ with $2^x + y$ prime

Conjecture (Sun, Nov. 10, 2013). Any integer $n > 1$ can be written as $x + y$ with $2^x + y$ prime, where x and y are positive integers.

Examples: $8 = 3 + 5$ with $2^3 + 5 = 13$ prime, and $53 = 20 + 33$ with $2^{20} + 33 = 1048609$ prime.

In 2013, I verified the conjecture for n up to 2×10^6 except for $n = 1657977$. For $n = 1657977$ the least $x \in \mathbb{Z}^+$ with $2^x + (n - x)$ prime is greater than 2×10^5.

On August 30, 2015 I found that $1657977 = 205494 + 1452483$ with $2^{205494} + 1452483$ a prime of 61860 decimal digits.

Until today, I have verified the conjecture for all $n \leqslant 7292138$. On Nov. 16, 2015, I found that $5120132 = 250851 + 4869281$ with

$$2^{250851} + 4869281$$

a prime of 75514 decimal digits!

Two new kinds of primes

Conjecture. (Sun, Nov. 26-27, 2015) (i) There are infinitely many primes p in the form $2^x + y$ with $0 \leqslant y < 2^x$ such that all those numbers $2^{x-a} + (y + a)$ $(0 < a \leqslant x)$ are composite.

(ii) There are infinitely many primes p in the form $2^x + y$ with $0 \leqslant y < 2^x$ such that all those numbers $2^{x+a} + (y - a)$ $(0 < a \leqslant y)$ are composite.

Those primes having the property described in part (i) are

$$5, 7, 13, 19, 31, 47, 61, 71, 101, 211, 239, 241, 271, 281, \ldots$$

(see `http://oeis.org/A264865`). I call such numbers *the first kind of primes*.

Those primes having the property described in part (ii) are

$$2, 3, 5, 11, 13, 17, 19, 23, 41, 71, 131, 149, 257, 277, 523, \ldots$$

(see `http://oeis.org/A264866`). I call such numbers *the second kind of primes*.

Concluding remarks

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

Zhi-Wei Sun, *Problems on combinatorial properties of primes*, in: M. Kaneko, S. Kanemitsu and J. Liu (eds.), Number Theory: Plowing and Starring through High Wave Forms, Proc. 7th China-Japan Seminar(Fukuoka, Oct. 28–Nov. 1, 2013), Ser. Number Theory Appl., Vol. 11, World Sci., Singapore, 2015, pp. 169–187. [This paper contains 60 conjectures on primes. It is also available from `http://arxiv.org/abs/1402.6641`.]

and

Zhi-Wei Sun, *Conjectures on representations involving primes*, in: Combinatorial and Additive Number Theory (edited by M. B. Nathanson), Springer, to appear. [This paper contains 100 conjectures.]

Thank you!