New Conjectures on Primes and Related Motivations

Zhi-Wei Sun

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

May 5, 2026

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)

Abstract. In this talk we introduce various new conjectures involving primes posed by the speaker and the stories behind them. For example, in 2025 the speaker found a surprising recurrence for primes which states that for any integer $n > 9$ the least positive integer m such that $(p_1 - 1)^2, \ldots, (p_n - 1)^2$ are distinct modulo m is just the $(n+1)$-th prime p_{n+1}.

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

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

A problem on central binomial coefficients

Let p be a prime. For $k = 0, \ldots, (p-1)/2$ we have

$$\binom{2k}{k} = \frac{(2k)!}{k!^2} \not\equiv 0 \pmod{p};$$

but for $k = (p+1)/2, \ldots, p-1$ we have

$$\binom{2k}{k} = \frac{(2k)!}{k!^2} \equiv 0 \pmod{p}.$$

Conjecture (Z. W. Sun, Feb. 20, 2012). Let $p > 5$ be a prime. Then

$$\left\{ \pm\binom{2k}{k} : \ k = 1, \ldots, \frac{p-1}{2} \right\}$$

cannot be a reduced system of residues modulo p.

A conjecture on central binomial coefficients

Conjecture (Z. W. Sun, Feb. 20, 2012). Let $p > 11$ be a prime. Then

$$\binom{2k}{k} \quad \left(k = 1, \ldots, \frac{p-3}{2}\right)$$

cannot be pairwise distinct modulo p, i.e.,

$$\binom{2s}{s} \equiv \binom{2t}{t} \pmod{p} \qquad \text{for some } 0 < s < t < \frac{p-1}{2}.$$

When $p > 90$, there are $0 < r < s < t < (p-1)/2$ such that

$$\binom{2r}{r} \equiv \binom{2s}{s} \equiv \binom{2t}{t} \pmod{p}.$$

Remark. Later I realized that for any positive integer m the largest n such that $\binom{2k}{k}$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m should be $O(\sqrt{m})$ and probably less than $4.53\sqrt{m}$.

A function taking only prime values

Conjecture (Z. W. Sun, Feb. 21, 2012). For $n = 1, 2, 3, \ldots$ define $s(n)$ as the least integer $m > 1$ such that $\binom{2k}{k}$ $(k = 1, \ldots, n)$ are pairwise distinct modulo m. Then $s(n)$ is always a prime!

I also guessed that $s(n) < n^2$ for $n = 2, 3, 4, \ldots$. I calculated $s(n)$ for $n = 1, \ldots, 2065$. For example,

$$s(1) = 2,\ s(2) = 3,\ s(3) = 5,\ s(4) = s(5) = s(6) = 11,$$
$$s(7) = s(8) = s(9) = 23,\ s(10) = 31,\ s(11) = \cdots = s(14) = 43,$$
$$s(15) = s(16) = s(17) = s(18) = 59,\ s(19) = 107,\ s(20) = 149.$$

After I made the conjecture public via a message to `Number Theory List`, Laurent Bartholdi computed $s(n)$ for $n = 2001, \ldots, 5000$, and his computational result supports my conjecture.

Artin's conjecture

Let p be an odd prime. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ for any integer $a \not\equiv 0 \pmod{p}$. If $g \in \mathbb{Z}$ is not divisible by p and $g^n \not\equiv 1 \pmod{p}$ for $n = 1, \ldots, p-2$, then we say that g is a *primitive root* mod p (or the order of g mod p is $p-1$).

Artin's Conjecture. If $a \in \mathbb{Z}$ is neither -1 nor a square, then there are infinitely many primes p having a as a primitive root modulo p.

Remark. This conjecture was made by Artin in 1927 and it remains open.

A conjecture implying Artin's conjecture

Conjecture (Sun, Feb. 22-23, 2012). Let $a \in \mathbb{Z}$ with $|a| > 1$. For $n \in \mathbb{Z}^+$ define $f_a(n)$ as the least integer $m > 1$ such that those a^k $(k = 1, \ldots, n)$ are pairwise incongruent modulo m.

(i) $f_a(n)$ is a prime for all sufficiently large n.

(ii) If a is not a square, then for any sufficiently large n, $f_a(n)$ is the least prime $p > n$ having a as a primitive root mod p;

(iii) If a is a square, then for any sufficiently large n, $f_a(n)$ is just the least prime $p > 2n$ such that $a, a^2, \ldots, a^{(p-1)/2}$ are pairwise distinct modulo p.

Example. $f_{-3}(n)$ with $n \in \mathbb{Z}^+$ is the least prime $p > n$ such that -3 is a primitive root mod p.

Lucas sequences

Let $A, B \in \mathbb{Z}$. The Lucas sequence $u_n = u_n(A, B)$ $(n \in \mathbb{N})$ and its companion sequence $v_n = v_n(A, B)$ $(n \in \mathbb{N})$ are given by

$$u_0 = 0,\ u_1 = 1,\ \text{and } u_{n+1} = Au_n - Bu_{n-1}\ (n = 1, 2, 3, \ldots)$$

and

$$v_0 = 2,\ v_1 = A,\ \text{and } v_{n+1} = Av_n - Bv_{n-1}\ (n = 1, 2, 3, \ldots).$$

Let $\Delta = A^2 - 4B$, and $\alpha = (A + \sqrt{\Delta})/2$ and $\beta = (A - \sqrt{\Delta})/2$ be the two roots of the equation $x^2 - Ax + B = 0$. It is known that

$$(\alpha - \beta)u_n = \alpha^n - \beta^n \quad \text{and} \quad v_n = \alpha^n + \beta^n.$$

Those $F_n = u_n(1, -1)$ and $L_n = v_n(1, -1)$ are Fibonacci numbers and Lucas numbers respectively.

Conjectures on Lucas sequences

Let A be an integer with $|A| > 2$, and set $\varepsilon_p = (\frac{A^2-4}{p})$.

Conjecture (Sun, Feb. 26, 2012). (i) If $2 + A$ is not a square, then there are infinitely many odd primes p such that those $v_k(A, 1) \bmod p$ with $k = 1, ..., (p - \varepsilon_p)/2$ are pairwise distinct.

(ii) If $2 - A$ is not a square, then there are infinitely many odd primes p such that those $u_k(A, 1) \bmod p$ with $1 \leqslant k \leqslant (p - \varepsilon_p)/2$ are pairwise distinct.

For $n \in \mathbb{Z}^+$ **define** $t_A(n)$ as the smallest integer $m > 1$ such that

$$v_k(A, 1) \quad \left(k = 1, ..., \frac{p - \varepsilon_p}{2}\right)$$

are pairwise distinct modulo m.

Conjecture (Sun, Feb. 26, 2012). Let $n \in \mathbb{Z}^+$ be sufficiently large ($n > 2|A|$ or $n > 100$ may suffice). Then $t_A(n)$ is a prime. Moreover, if $A + 2$ is not a square, then $t_A(n)$ is the smallest odd prime p such that $p - \varepsilon_p \geqslant 2n$ and those $v_k(A, 1) \bmod p$ ($k = 1, ..., (p - \varepsilon_p)/2$) are pairwise distinct.

Some particular examples

Examples. (i) $t_3(n)$ with $n > 5$ is the smallest odd prime p such that $p - (\frac{p}{5}) \geqslant 2n$ and $v_k(3,1) = L_{2k}$ $(1 \leqslant k \leqslant \frac{1}{2}(p - (\frac{p}{5})))$ are pairwise incongruent modulo p.

(ii) $t_4(n)$ is a prime for any positive integer n. $t_4(n)$ with $n > 2$ is the smallest odd prime p such that $p - (\frac{3}{p}) \geqslant 2n$ and $T_k = v_k(4,1)$ $(k = 1, ..., (p - (\frac{3}{p}))/2)$ are pairwise incongruent mod p.

(iii) $t_{10}(n)$ and $t_{-10}(n)$ are always primes. For $n > 2$, $t_{10}(n)$ is the smallest odd prime p such that $p - (\frac{6}{p}) \geqslant 2n$ and $v_k(10,1)$ $(k = 1, ..., (p - (\frac{6}{p}))/2)$ are pairwise incongruent mod p, and $t_{-10}(n)$ is the smallest odd prime p such that $p - (\frac{6}{p}) \geqslant 2n$ and $v_k(-10,1) = (-1)^k v_k(10,1)$ $(k = 1, ..., (p - (\frac{6}{p}))/2)$ are pairwise distinct mod p.

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

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

A conjecture involving factorials

Recall that

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2}.$$

By Stirling's formula,

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

as $n \to +\infty$.

Conjecture (Sun, Feb. 27, 2012). For $n = 1, 2, 3, \ldots$ let $t(n)$ be the least integer $m > 1$ such that $1!, 2!, \ldots, n!$ are pairwise distinct mod m. Then $t(n)$ is a prime with the only exception $t(5) = 10$.

Examples. $t(1) = t(2) = 2$, $t(3) = 3$, $t(4) = 7$, $t(5) = 10$, $t(6) = t(7) = t(8) = 13$, $t(9) = 31$, $t(10) = t(11) = t(12) = 37$.

Qing-Hu Hou (Nankai Univ.) has verified the conjecture for $n \leqslant 10^4$.

I noted that if we replace $k!$ by $(k+1)!$ or $(2k)!$ in the definition of $t(n)$ then $t(n)$ will take only prime values.

A conjecture on products of consecutive primes

Conjecture (Sun, March 18, 2012). For $k \in \mathbb{Z}^+$ let P_k denote the product of the first k primes $p_1, \ldots, p_k$ (i.e., $P_k = p_k\#$).
(i) For $n \in \mathbb{Z}^+$ define $w_1(n)$ as the least integer $m > 1$ such that m divides none of those $P_i - P_j$ with $1 \leqslant i < j \leqslant n$. Then $w_1(n)$ is always a prime.
(ii) For $n \in \mathbb{Z}^+$ define $w_2(n)$ as the least integer $m > 1$ such that m divides none of those $P_i + P_j$ with $1 \leqslant i < j \leqslant n$. Then $w_2(n)$ is always a prime.
(iii) We have $w_1(n) < n^2$ and $w_2(n) < n^2$ for all $n = 2, 3, 4, \ldots$.

Remark. Clearly $w_i(n) \leqslant w_i(n+1)$ for $i = 1, 2$.

$$W_1 = \{w_1(n) : \ n \in \mathbb{Z}^+\} \ \text{ and } \ W_2 = \{w_2(n) : \ n \in \mathbb{Z}^+\}$$

are both infinite. (For $m > 1$, there is an odd prime $p_n \equiv -1 \pmod m$ and hence $P_{n-1} + P_n \equiv 0 \pmod m$.) If $w_i(n) = p_k$, then $k \geqslant n$ since $P_{k+1} \pm P_k \equiv 0 \pmod{p_k}$. So part (ii) of the conjecture implies the inequality $w_2(n) > n$ for all $n \in \mathbb{Z}^+$, i.e., for each $n > 1$ there are $1 \leqslant j < k \leqslant n$ such that $n \mid P_j + P_k$. This seems simple but I'm unable to prove it.

Respondences from others

One of my students: "*The conjecture might be wrong, it is not reasonable!*"

A Chinese professor in number theory: "*This seems to be incorrect*.

Other number theorists kept silent and made no comments.

In April, W. B. Hart (an English number theorist) verified the conjecture for n up to 10^5.

The following comment comes from
`http://tech.groups.yahoo.com/group/primenumbers/message/24181`

"As would be expected when coming from Zhi-Wei Sun, if he presents it as a conjecture, you can be sure of two things ... It's very likely true, and will be very hard to prove."

—Jack Brennen (March 21, 2012).

A conjecture on sums of consecutive prime

Conjecture (Sun, March 21, 2012). For $k \in \mathbb{Z}^+$ let S_k denote the sum of the first k primes $p_1, \ldots, p_k$.
(i) For $n \in \mathbb{Z}^+$ define $S^+(n)$ as the least integer $m > 1$ such that m divides none of $S_i! + S_j!$ with $1 \leqslant i < j \leqslant n$. Then $S^+(n)$ is always a prime not exceeding S_n.
(ii) For $n \in \mathbb{Z}^+$ define $S^-(n)$ as the least integer $m > 1$ such that m divides none of those $S_i! - S_j!$ with $1 \leqslant i < j \leqslant n$. Then $S^-(n)$ is always a prime not exceeding S_n.

Remark. When $n > 1$, clearly both $S^+(n)$ and $S^-(n)$ are greater than S_{n-1}. Thus, by the conjecture we should have $S^+(n) \leqslant S_n < S^+(n+1)$ and $S^-(n) \leqslant S_n < S^-(n+1)$ for all $n = 1, 2, 3, \ldots$. The conjecture implies that for any $n = 2, 3, \ldots$ the interval $(S_{n-1}, S_n]$ contains the primes $S^+(n)$ and $S^-(n)$ which are actually very close to S_{n-1}. However, it seems very challenging to prove that $(S_n, S_{n+1}]$ contains a prime for any $n \in \mathbb{Z}^+$. Note that

$$S_n \sim \sum_{k=1}^{n} k \log k \sim \int_1^n x \log x dx \sim \frac{n^2}{2} \log n.$$

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

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

Obviously $s_1 = p_1 = 2$. For $n = 2, 3, 4, \ldots$, we clearly have $s_n + s_{n-1} = p_n$ and hence $s_n < p_n$ since $s_{n-1} > 0$. 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).

$s_1, s_2, \ldots$ are pairwise distinct

Basic Fact. All the numbers $s_1, s_2, \ldots$ are pairwise distinct!

Proof. We show that $s_n \neq s_k$ for any $1 \leqslant k < n$.

If $n - k$ is even, then

$$s_n - s_k = (p_n - p_{n-1}) + \cdots + (p_{k+2} - p_{k+1}) > 0.$$

When $n - k$ is odd, we have

$$s_n - s_k = \sum_{l=k+1}^{n} (-1)^{n-l} p_l - 2 \sum_{j=1}^{k} (-1)^{k-j} p_j \equiv n - k \not\equiv 0 \pmod 2.$$

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}. In 2020 Chang Zhang (a student at Nanjing Univ.) extended the verification for $n \leqslant 3 \times 10^5$.

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

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

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 10^9. 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

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

Remark. For $d \in \{2, 3\}$ and integer $c \in (-d, d)$, I also have similar results involving the set of all primes $p \equiv c \pmod{d}$ and powers of d.

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 $p \geqslant (10n-r)/4$.

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

Rumely's result needed

Let $4 \leqslant d \leqslant 36$. 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

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

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

Part III. Other Conjectures and Results on Discriminators

A problem involving the cubic polynomial $x(x^2+1)$

Conjecture (Sun, 2013-04-21). For any positive integer n, the smallest positive integer m such that $k(k^2+1)$ $(k=1,\ldots,n)$ are incongruent modulo m^2 is just the first power of 3 not smaller than $\sqrt{n}$.

Remark. For $n = 244,245$, the least positive integer m such that $k(k^2+1)$ $(k=1,\ldots,n)$ are incongruent modulo m is $3^4\times 7$ which is not a power of three.

This conjecture was finally confirmed by Yuan-Hui Yang and Lilu Zhao via Kloosterman sums in the paper "On a conjecture of Sun involving powers of three" [Chin. Ann. Math. Ser. B, to appear].

Discriminators of polynomials of degree three or four

Conjecture (Sun, 2021-11-17). (i) For any integer $n > 1$, the smallest $m \in \mathbb{Z}^+$ such that those numbers $k^2(k^2-1)$ $(k = 1, \ldots, n)$ are distinct modulo m, coincides with the least prime $p > 2n$ dividing none of the numbers $a^2 + b^2 - 1$ $(1 \leqslant a < b \leqslant n)$.

(ii) For any integer $n \geqslant 15$, the smallest positive integer m such that $k(k^2+3)$ $(k = 1, \ldots, n)$ are distinct modulo m, is just the least power of 3 not smaller than $3n$.

(iii) For any $n \in \mathbb{Z}^+$, the smallest positive integer m such that those numbers $2k(k^2-2)$ $(k = 1, \ldots, n)$ are distinct modulo m, is just the least power of 3 not smaller than n.

Discriminators of polynomials of higher degrees

Conjecture (Sun, 2021-11-17). (i) Let

$$n \in \mathbb{Z}^+ \setminus \{26, 27, 28, 626, 627, 628, 629, 630\},$$

and define $D(n)$ as the least positive integer m such that the n numbers $k(k^4+1)$ $(k = 1, \ldots, n)$ are distinct modulo m. Choose $a \in \mathbb{N}$ such that $5^a < n \leqslant 5^{a+1}$. Then

$$D(n) = \begin{cases} 3 \times 5^a & \text{if } n \leqslant 3 \times 5^a, \\ 5^{a+1} & \text{if } n > 3 \times 5^a. \end{cases}$$

(ii) For any integer $n > 2$, the smallest positive integer m such that those numbers $33k^2(k^3+1)$ $(k = 1, \ldots, n)$ are distinct modulo m, must be a prime.

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 $(1 \leqslant i < j \leqslant 10)$.

A mysterious recurrence for primes

Conjecture (Mysterious Recurrence for Primes) [Sun, 2025-10-11]. For any integer $n > 2$ with $n \neq 4, 9$, the $(n+1)$-th prime p_{n+1} is just the least positive integer m such that the n numbers $(p_1-1)^2, \ldots, (p_n-1)^2$ are distinct modulo m.

The conjecture was announced in MathOverflow on Oct. 13, 2025 and later verified by J.-M. Lin for $n \leqslant 10^7$. See also the OEIS items A387959 and A387947 for some related data. For any positive integer n, define $s(n)$ as the smallest positive integer m such that the n distinct numbers $(p_1-1)^2, \ldots, (p_n-1)^2$ distinct modulo m. It is easy to check that

$$s(1) = 1,\ s(2) = 2,\ s(4) = 9 \text{ and } s(9) = 25.$$

Clearly $s(n) \leqslant s(n+1)$ for any $n \in \mathbb{Z}^+$. Note that $s(n) \neq p_k$ for every $k = 1, \ldots, n$ since $(p_k-1)^2 \equiv (p_1-1)^2 = 1 \pmod{p_k}$.

An equivalent version

We also have $s(n) \leqslant p_{n+1}$ since p_{n+1} does not divide

$$(p_k - 1)^2 - (p_j - 1)^2 = (p_k - p_j)(p_k + p_j - 2)$$

for any $1 \leqslant j < k \leqslant n$. Note that if $p_{n+1} = p_k + p_j - 2$ with $1 \leqslant j < k \leqslant n$ then we must have $p_j = 2$ (as p_{n+1} is odd) and hence $p_k = p_{n+1}$ which is impossible. Thus, we have reduced the conjecture to the following assertion: *For any composite number $m > 5$ with $m \neq 9, 25$, there are distinct primes p and q smaller than m such that*

$$(p-1)^2 - (q-1)^2 = (p-q)(p+q-2) \equiv 0 \pmod{m}.$$

If m is a positive even number with $m + 2 = p + q$ for some distinct primes p and q, then $(p-1)^2 \equiv (q-1)^2 \pmod{m}$. Thus the assertion with m even can be explained in the spirit of Goldbach's conjecture. However, we don't have any reasonable explanation for the assertion with m odd. For example, $\{43, 29\}$ is the unique prime pair $\{p, q\}$ with $49 \geqslant p > q$ such that $(p-1)^2 \equiv (q-1)^2 \pmod{49}$.

A conjecture involving $a^{k(k-1)/2}$

Conjecture (Z.-W. Sun, 2026-01-21). Let $a \in \mathbb{Z}$ with $|a| > 1$, and let $D(a, n)$ denote the least positive integer m such that

$$a^{k(k-1)/2} \ \ (k = 1, \ldots, n)$$

are pairwise incongruent modulo m.

(i) We have $\lim_{n\to+\infty} \frac{D(a,n)}{n} = 4$.

(ii) If $a \not\equiv \pm 3 \pmod 8$, then $D(a, n)$ is prime whenever $n > |a| + 1$.

(iii) When $a \equiv \pm 3 \pmod 8$, the set $\{D(a, n) : \ n \in \mathbb{Z}^+\}$ contains infinitely many powers of two, and the least $m \in \mathbb{Z}^+$ with $2a^{k(k-1)/2}$ $(1 \leqslant k \leqslant n)$ distinct modulo m is prime whenever $n \geqslant |a|$.

Remark. For related data, see https://oeis.org/A392732 and https://oeis.org/A392775.

On Ramanujan's tau function

The Ramanujan tau function given by

$$q\prod_{n=1}^{\infty}(1-q^n)^{24}=\sum_{n=1}^{\infty}\tau(n)q^n\quad(|q|<1)$$

is multiplicative, i.e., $\tau(mn)=\tau(m)\tau(n)$ whenever m and n are coprime. The values of $\tau(1),\tau(2),\ldots,\tau(10)$ are as follows:

$1,\ -24,\ 252,\ -1472,\ 4830,\ -6048,\ -16744,\ 84480,\ -113643,\ -115920.$

Lehmer's conjecture asserts that $\tau(n)\neq 0$ for all $n\in\mathbb{Z}^+$. In 2025, the speaker conjectured that for any $m,n\in\mathbb{Z}^+$ with $m\neq n$ we have

$$|\tau(m)+\tau(n)|\geqslant 23\ \text{ and }\ |\tau(m)-\tau(n)|\geqslant 25.$$

Conjecture (Z.-W. Sun, 2026-01-18) For any integer $n>1$ with $n\neq 37$, the least $m\in\mathbb{Z}^+$ such that $\tau(k)(\tau(k)-1)$ pairwise incongruent modulo m is a prime. (When $n=37$, the least $m\in\mathbb{Z}^+$ is $5^4=625$.)

Remark. For related data, see https://oeis.org/A392667.

Part IV. On combinatorial properties of primes

A combinatorial conjecture implying the twin prime conjecture

Conjecture 4.1 (Sun, 2013-09-08). For any positive integer n, there is a circular permutation $(i_0, i_1, \ldots, i_n)$ of $0, 1, \ldots, n$ such that all the adjacent sums

$$i_0 + i_1,\ i_1 + i_2,\ \ldots,\ i_{n-1} + i_n,\ i_n + i_0$$

belong to the set

$$T = \{k \in \mathbb{Z}^+ :\ 6k - 1 \text{ and } 6k + 1 \text{ are twin prime}\}.$$

Remark. I verified this for $n \leqslant 12$. For $n = 12$, we may take

$$(i_0, \ldots, i_{12}) = (0, 5, 2, 1, 6, 4, 3, 9, 8, 10, 7, 11, 12).$$

In 2013 Max Alekseyev extended the verification to $n \leqslant 25$. Later, Qing-Hu Hou at Tianjin Univ. verified the conjecture for $n \leqslant 100$.

The conjecture is stronger than the twin prime conjecture because it implies that for any $n \in \mathbb{Z}^+$ the set T contains an element not smaller than 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 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

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

Golomb's theorem

In 2014, at a conference in Taiwan organized by Winnie W.-C. Li, Carl Pomerance told me the following surprising result on exact values of the function $\pi(x)$.

Theorem 4.1 (S. Golomb [Amer. Math. Monthly 69 (1962)]). For any integer $m > 1$, there is an integer $n > 1$ such that $n/\pi(n) = m$, i.e., $\pi(n) = n/m$.

Proof. As $n/\pi(n) \sim \log n$, if n is sufficiently large then $n/\pi(n) \geqslant m$. Take the smallest integer $n > 1$ such that $n/\pi(n) \geqslant m$. If $n = 2$ then $n/\pi(n) = 2 = m$. If n is an odd prime, then

$$\frac{n}{\pi(n)} \geqslant m > \frac{n-1}{\pi(n-1)} = \frac{n-1}{\pi(n)-1}$$

and hence $\pi(n) > n$ which is impossible. If n is composite, then

$$\frac{n}{\pi(n)} \geqslant m > \frac{n-1}{\pi(n-1)} = \frac{n-1}{\pi(n)},$$

hence $n \geqslant m\pi(n) > n-1$ and thus $n = m\pi(n)$ as desired.

An extension

Theorem 4.2 (Sun [Ramanujan J. 42 (2017)]) (i) Let m be any positive integer. For the set

$$S_m := \left\{ a \in \mathbb{Z} : \ \pi(n) = \frac{n+a}{m} \text{ for some integer } n > 1 \right\},$$

we have $S_m = \{\ldots, -2, -1, \ldots, S(m)\}$, where

$$S(m) := \max\{km - p_k : \ k \in \mathbb{Z}^+\} = \max\{km - p_k : \ k = 1, 2, \ldots, \lfloor e^{m+1} \rfloor\}.$$

(ii) We have

$$(m-1)S(m+1) > mS(m) \quad \text{for any } m \in \mathbb{Z}^+.$$

Also,

$$\frac{e^{m-1}}{m-1} < S(m) < (m-1)e^{m+1} \quad \text{for all } m = 3, 4, \ldots,$$

and hence

$$\lim_{m \to +\infty} \sqrt[m]{S(m)} = e.$$

Corollaries

Corollary 4.1 (Sun [Ramanujan J. 42 (2017)]). Let $m > 0$ and $a \leqslant m^2 - m - 1$ be integers. Then there is an integer $n > 1$ with $\pi(n) = (n + a)/m$, i.e.,

$$\pi(mn - a) = n \quad \text{for some } n \in \mathbb{Z}^+.$$

Corollary 4.2 (Sun [Ramanujan J. 42 (2017)]). For any integer $m > 4$, there is a positive integer n such that $\pi(mn) = m + n$.

Let n be any positive integer. Clearly $\pi(n) < n + 1$ and $\pi(2n) \leqslant n < n + 2$. Observe that

$$\begin{aligned} 2n = \left\lfloor \frac{3n}{2} \right\rfloor + n - \left\lfloor \frac{n}{2} \right\rfloor &= |\{1 \leqslant k \leqslant 3n : \ \gcd(k, 6) > 1\}| \\ &\leqslant |\{1 \leqslant k \leqslant 3n : \ k \text{ is not prime}\}| + 1 = 3n - \pi(3n) + 1 \end{aligned}$$

and hence $\pi(3n) \leqslant n + 1 < n + 3$. As $k := \pi(4n) \geqslant 2$, we have $4n \geqslant p_k \geqslant k(\log k + \log\log k - 1)$. If $n \geqslant 45$, then $\log k + \log\log k \geqslant 5$ and hence $\pi(4n) = k \leqslant n < n + 4$. We can easily verify that $\pi(4n) < n + 4$ if $n \leqslant 44$.

One more corollary involving Fibonacci numbers

The well-known Fibonacci numbers F_n ($n \in \mathbb{N} = \{0, 1, 2, \ldots\}$) are given by

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

Corollary 4.3 (Sun [Ramanujan J. 42 (2017)]). For any integer $m > 3$, there is a positive integer n such that

$$\pi(mn) = F_m + n.$$

Examples.

$$\pi(4 \times 5) = F_4 + 5,\ \pi(5 \times 9) = F_5 + 9,\ \pi(6 \times 12) = F_6 + 12,$$
$$\pi(7 \times 16) = F_7 + 16,\ \pi(8 \times 25) = F_8 + 25,$$
$$\pi(9 \times 45) = F_9 + 45,\ \pi(10 \times 68) = F_{10} + 68.$$

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

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

is an additive chain.

Remark. It has been verified that for each $n = 2, 3, \ldots, 2^{24}$ we can write $f(n) = f(k) + f(m)$ for some $k, m \in \mathbb{Z}^+$.

Three more conjectures

Conjecture 4.3 (Sun, 2014-02-09). For any integer $n > 1$, $\pi(kn)$ is prime for some $k = 1, \ldots, n$.

Remark. For example, $\pi(6 \times 10) = 17$ is prime. Sun and Lilu Zhao [J. Comb. Number Theory 11 (2019)] proved that for any $n \in \mathbb{Z}^+$ the set $\{\pi(kn) : \ k = 1, 2, 3, \ldots\}$ contains infinitely many numbers P_2 which is a product of at most two primes.

Conjecture 4.4 (Sun, 2014-02-14). For any positive integer n, $\pi_2(kn)$ is a square for some $k = 1, \ldots, n$, where $\pi_2(x)$ denotes the number of twin prime pairs not exceeding x.

Remark. For example, $\pi_2(12660 \times 19939) = 10000^2$. The conjecture has been verified for $n \leqslant 40000$.

Conjecture 4.5 (Sun, 2014-02-08). For any integer $n > 4$, there is a prime $p < n$ such that $pn + \pi(p)$ is prime.

Remark. This has been verified for $n \leqslant 10^8$.

A challenging conjecture on the prime sequence

Conjecture 4.6 (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. This has been verified for all $m=1,\ldots,4\times 10^5$, 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 $m\to+\infty$.

On representations of positive rational numbers

Conjecture 4.7 (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. This has been verified for all those rational numbers $r=a/b$ with $a,b\in\{1,\ldots,1300\}$. For example, $2=20/10$ with $p_{20}+p_{10}=71+29=10^2$ a square.

Conjecture 4.8 (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. This has been verified this $r=a/b$ with $a,b\in\{1,\ldots,60\}$. For example,
$49/58=1076068567/1273713814$ with

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

Part V. On the functions $\varphi(n)$ and $\sigma(n)$

Euler's totient function φ

For $n \in \mathbb{Z}^+$ define

$$\varphi(n) = |\{1 \leqslant m \leqslant n : \ (m, n) = 1\}|.$$

Note that

$$\varphi(1) = \varphi(2) = 1 \text{ and } \varphi(3) = \varphi(4) = \varphi(6) = 2.$$

For any prime p and positive integer a, clearly

$$\varphi(p^a) = p^a - |\{1 \leqslant m \leqslant p^a : \ p \mid m\}| = p^a - p^{a-1} = p^{a-1}(p-1).$$

It is known that Euler's totient function φ is multiplicative, i.e.,

$$\varphi(mn) = \varphi(m)\varphi(n) \quad \text{for any } m, n \in \mathbb{Z}^+ \text{ with } (m, n) = 1.$$

Thus, if $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r \in \mathbb{Z}^+$, then

$$\varphi(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{i=1}^{r} \varphi(p_i^{a_i}) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1).$$

Three conjectures involving the function φ

Conjecture 5.1 (i) (Sun, 2014-10-08). For any integer $m > 1$, $\varphi(m+n) \mid n$ for some positive integer $n \leqslant m(m-1)$.

(ii) (Sun, 2014-09-29) For any integer $m > 6$, there is a positive integer n such that $m+n$ divides $\varphi(m)\varphi(n)$.

Examples. $\varphi(10+40) = 20$ divides 40. $10+14$ divides $\varphi(10)\varphi(14) = 24$.

Conjecture 5.2 (Sun, 2014-02-02). Any integer $n > 8$ can be written as $k+m$ $(k > m > 0)$ with $\varphi(k)\varphi(m)$ a square.

Example. $17 = 12+5$ with $\varphi(12)\varphi(5) = 4^2$.

Conjecture 5.3 (Sun, 2013-12-21). Any integer $n > 5$ can be written as $k+m$ $(k, m \in \mathbb{Z}^+)$ such that $\frac{\varphi(k)+\varphi(m)}{2}$ is prime.

Example. $13 = 3+10$ with $(\varphi(3)+\varphi(10))/2 = 3$ prime.

On $\varphi(n^2)$

If $n = p_1^{a_1} \cdots p_r^{a_r}$ with $p_1, \ldots, p_r$ distinct primes and $a_1, \ldots, a_r \in \mathbb{Z}^+$, then

$$\varphi(n^2) = \prod_{i=1}^{r} p_i^{2a_i-1}(p_i - 1) = n\varphi(n).$$

For positive integers m and n with $\varphi(m^2) = \varphi(n^2)$, we have $m = n$ by comparing the prime factorizations of $\varphi(m^2)$ and $\varphi(n^2)$. Thus, the numbers $\varphi(n^2)$ $(n = 1, 2, 3, \ldots)$ are pairwise distinct.

Conjecture 5.4 (Sun, 2015-10-01). Any integer $n > 1$ can be written as $x^2 + y^2 + \varphi(z^2)$, where $x, y \in \mathbb{N}$, $z \in \mathbb{Z}^+$, and $\max\{x, y\}$ or z is prime.

Remark. It is easy to see that $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$ for any $x, y, z \in \mathbb{Z}$.

A theorem of Krachun and Sun

Theorem 5.1 (D. Krachun and Z.-W. Sun [Amer. Math. Monthly 127 (2020)]) Each positive rational number can be written as $\varphi(m^2)/\varphi(n^2)$ with $m, n \in \mathbb{Z}^+$.

Examples. We have

$$\frac{19}{47} = \frac{19 \times 19673280}{47 \times 19673280} = \frac{\varphi(39330^2)}{\varphi(55836^2)}$$

with

$$39330 = 2 \times 3^2 \times 5 \times 19 \times 23 \quad \text{and} \quad 55836 = 2^2 \times 3^3 \times 11 \times 47.$$

Also,

$$\frac{47}{58} = \frac{47 \times 1700160}{58 \times 1700160} = \frac{\varphi(14476^2)}{\varphi(20010^2)}$$

with

$$14476 = 2^2 \times 7 \times 11 \times 47 \quad \text{and} \quad 20010 = 2 \times 3 \times 5 \times 23 \times 29.$$

Proof of Theorem 5.1

We claim a stronger result: If $p_1 < p_2 < \cdots < p_k$ are distinct primes and $a_1, \ldots, a_k$ are integers, then there are positive integers m and n with mn not divisible by any prime greater than p_k such that $p_1^{a_1} \cdots p_k^{a_k} = \varphi(m^2)/\varphi(n^2)$.

We prove the claim by induction on p_k.

The base of the induction is $p_k = 2$. For any $a \in \mathbb{Z}$, clearly

$$2^{2a} = \frac{2^{2(a+b)-1}}{2^{2b-1}} = \frac{\varphi(2^{2(a+b)})}{\varphi(2^{2b})}$$

for each integer $b > |a|$, and

$$2^{2a+1} = \begin{cases} \varphi(2^{2(a+1)})/\varphi(1^2) & \text{if } a \geq 0, \\ \varphi(1^2)/\varphi(2^{-2a}) & \text{if } a < 0. \end{cases}$$

Proof of Theorem 5.1 (continued)

Now let q be an odd prime and assume that the claim holds whenever $p_k < q$.

Let $q_1 < \cdots < q_k = q$ be distinct primes and let $r = \prod_{i=1}^{k} q_i^{a_i}$ with $a_1, \ldots, a_k \in \mathbb{Z}$. Set

$$r_0 = \begin{cases} r/q_k^{a_k} & \text{if } 2 \mid a_k, \\ r/((q_k - 1)q_k^{a_k}) & \text{if } 2 \nmid a_k. \end{cases}$$

Clearly, all the primes in the factorization of r_0 are smaller than $q_k = q$.

By the induction hypothesis, there are positive integers m_0 and n_0 with $m_0 n_0$ not divisible by any prime $p \geq q_k$ such that

$$\frac{\varphi(m_0^2)}{\varphi(n_0^2)} = r_0.$$

Obviously, we may take $m_0 = n_0 = 1$ if $r_0 = 1$.

Proof of Theorem 5.1 (continued)

Case 1. $2 \mid a_k$.
In this case, we take positive integers b and c with $b - c = a_k/2$, and set $m = m_0 q^b$ and $n = n_0 q^c$. Then

$$\frac{\varphi(m^2)}{\varphi(n^2)} = \frac{\varphi(m_0^2)}{\varphi(n_0^2)} \times \frac{q^{2b-1}(q-1)}{q^{2c-1}(q-1)} = r_0 q^{2(b-c)} = \prod_{i=1}^{k} q_i^{a_i} = r.$$

Case 2. $2 \nmid a_k$.
When $a_k > 0$, for $m = m_0 q^{(a_k+1)/2}$ and $n = n_0$, we have

$$\frac{\varphi(m^2)}{\varphi(n^2)} = \frac{\varphi(m_0^2)}{\varphi(n_0^2)} \times q^{a_k}(q-1) = r_0 q^{a_k}(q-1) = \prod_{i=1}^{k} q_i^{a_i} = r.$$

If $a_k < 0$, then there are positive integers m and n with mn not divisible by any prime greater than q_k such that $\prod_{i=1}^{k} q_i^{-a_i} = \varphi(n^2)/\varphi(m^2)$ and hence $\prod_{i=1}^{k} q_i^{a_i} = \varphi(m^2)/\varphi(n^2)$.

In view of the above, the claim holds and hence so does Th. 5.1.

The function $\sigma(n)$

For each $n \in \mathbb{Z}^+$, let $\sigma(n)$ be the sum of all (positive) divisors of n. For any prime p and $a \in \mathbb{Z}^+$, we have

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

The function σ is also multiplicative, thus

$$\sigma(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

if $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r \in \mathbb{Z}^+$.

For any odd prime p and $a \in \mathbb{Z}^+$, we have $\sigma(p^a) \equiv a + 1 \pmod 2$. It follows that

$$2 \nmid \sigma(n) \iff n \text{ is a square or twice a square.}$$

Two curious conjecture

Conjecture 5.5 (Sun, 2013-12-12). Any integer $n > 1$ can be written as $k^2 + m$ with $k, m \in \mathbb{Z}^+$ and $k^2 \leqslant m$ such that $\sigma(k^2) + \varphi(m)$ is prime.

This conjecture has been verified for $n < 5.12 \times 10^{10}$.

Examples.

$$24 = 4^2 + 18 \text{ with } \sigma(4^2) + \varphi(18) = 31 + 6 = 37 \text{ prime},$$

$$265 = 11^2 + 144 \text{ with } \sigma(11^2) + \varphi(144) = 133 + 48 = 181 \text{ prime}.$$

Conjecture 5.6 (Sun, 2015-07-08). Any positive rational number can be written as m/n with $m, n \in \mathbb{Z}^+$ such that both $\varphi(m)$ and $\sigma(n)$ are squares.

Remark. This has been verified for $r = a/b$ with $1 \leqslant a, b \leqslant 150$. For example,

$$\frac{149}{146} = \frac{142458436610}{139590145940}$$

with $\varphi(142458436610) = 214896^2$ and $\sigma(139590145940) = 596736^2$.

On the set $\{\sigma(n)/\varphi(n) : \ n \in \mathbb{Z}^+\}$

For any $\varepsilon > 0$, if p is a prime with $p > 1 + 2/\varepsilon$ then

$$\frac{\sigma(p)}{\varphi(p)} = \frac{p+1}{p-1} = 1 + \frac{2}{p-1} < 1 + \varepsilon.$$

On the other hand, $\sigma(n)/n = \sum_{d|n} \frac{1}{d}$ can be arbitrarily large.

Conjecture 5.7 (Sun, 2024-08-08).

$$\left\{\frac{\sigma(n)}{\varphi(n)} : \ n \in \mathbb{Z}^+\right\} = \{r \in \mathbb{Q} : \ r \geqslant 1\}.$$

Example. $41/2 = \sigma(25604040)/\varphi(25604040)$ with

$$25604040 = 2^3 \times 3 \times 5 \times 7 \times 11 \times 17 \times 163.$$

Remark. I verified that for $36 \geqslant a \geqslant b \geqslant 1$ we can write a/b as $\sigma(n)/\varphi(n)$ with $n \in \mathbb{Z}^+$ and posed the conjecture to MathOverflow as Question 476578 on August 8, 2024. One day later, Max Alekseyev reported that he had verified that for $100 \geqslant a > b \geqslant 1$ we can write a/b as $\sigma(n)/\varphi(n)$ with $n \in \mathbb{Z}^+$ squarefree.

On generators of the semigroup $\{a/b : \ a, b \in \mathbb{Z}^+ \ \& \ a > b\}$

For integers $a > b > 0$, clearly

$$\frac{a}{b} = \prod_{n=b}^{a-1} \frac{n+1}{n}.$$

In view of Conjecture 5.7 and Max Alekseyev's comment, it seems that each rational number $r > 1$ can be written as a product of distinct elements of the set

$$S_1 = \left\{ \frac{n+1}{n} : \ n \in \mathbb{Z}^+ \text{ and } 2n+1 \text{ is prime} \right\}$$
$$= \left\{ \frac{p+1}{p-1} : \ p \text{ is an odd prime} \right\}.$$

On generators of the semigroup $\{a/b : \ a, b \in \mathbb{Z}^+, \ a > b \text{ and } 2 \nmid ab\}$

For integers $m > k \geq 0$, it is apparent that

$$\frac{2m+1}{2k+1} = \prod_{n=k+1}^{m} \frac{2n+1}{2n-1}.$$

Motivated by the set S_1, we introduce the set

$$S_2 = \left\{ \frac{2n+1}{2n-1} : \ n \in \mathbb{Z}^+ \text{ and } 2n-3 \text{ is prime} \right\}$$
$$= \left\{ \frac{p+4}{p+2} : \ p \text{ is an odd prime} \right\}.$$

Conjecture 5.8 (Sun, 2024-08-11). For any $n \in \mathbb{Z}^+$, we can write $(2n+1)/(2n-1)$ as a product of distinct elements of S_2.

Remark. Perhaps, for any integers $m > k \geq 0$ we can write $(2m+1)/(2k+1)$ as a product of distinct elements of S_2.

On generators of the semigroup $\{a/b : \ a, b \in \mathbb{Z}^+, \ a > b \text{ and } 2 \nmid ab\}$

For each $n \in \mathbb{Z}^+$, let $a(n)$ denote the least odd squarefree number $m > 1$ such that

$$\prod_{p|m} \frac{p+4}{p+2} = \frac{2n+1}{2n-1}.$$

I have found the exact values of $a(1), \ldots, a(20), a(22), \ldots, a(53)$. For example,

$$\begin{aligned} a(1) &= 50234415 = 3 \times 5 \times 7 \times 11 \times 23 \times 31 \times 61, \\ a(2) &= 1085 = 5 \times 7 \times 31, \\ a(48) &= 165694433 = 131 \times 373 \times 3391, \\ a(51) &= 424958987 = 113 \times 1129 \times 3331. \end{aligned}$$

It seems that $a(n)$ is particularly large when n is divisible by 3. My computation indicates that

$$a(21) > 3 \times 10^{10} \quad \text{and} \quad a(54) > 1.3 \times 10^9.$$

Part VI. Conjectures involving primes and practical numbers

Practical numbers

A positive integer n is called a *practical* number if every $m = 1, \ldots, n$ can be written as a sum of some distinct divisors of n, i.e., there are distinct divisors $d_1, \ldots, d_k$ of n such that

$$\frac{m}{n} = \sum_{i=1}^{k} \frac{1}{d_i}.$$

For example, 6 is practical since $1, 2, 3, 6$ divides 6, and also $4 = 1 + 3$ and $5 = 2 + 3$. As any positive integer has a unique representation in base 2 with digits in $\{0, 1\}$, powers of 2 are all practical. 1 is the only odd practical number.

Practical numbers below 50:

1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, 30, 32, 36, 40, 42, 48.

Goldbach-type results for practical numbers

Theorem (Stewart [Amer. J. Math., 76(1954)]). If $p_1 < \cdots < p_r$ are distinct primes and $a_1, \ldots, a_r$ are positive integers then $m = p_1^{q_1} \cdots p_r^{a_r}$ is practical if and only if $p_1 = 2$ and

$$p_{s+1} - 1 \leqslant \sigma(p_1^{a_1} \cdots p_s^{a_s}) \quad \text{for all} \quad 0 < s < r,$$

where $\sigma(n)$ stands for the sum of all divisors of n.

The behavior of practical numbers is quite similar to that of primes. G. Melfi proved the following Goldbach-type conjecture of M. Margenstern.

Theorem (G. Melfi [J. Number Theory 56(1996)]).

(i) Each positive even integer is a sum of two practical numbers,

(ii) There are infinitely many practical numbers m with $m - 2$ and $m + 2$ also practical.

Primes VS Practical Numbers

In contrast with the Prime Number Theorem (which states that $\pi(x) = \sum_{p \le x} 1 \sim x/\log x$), A. Weingartner [Int. J. Number Theory 16 (2020)] proved that for the number $P(x)$ of practical numbers not exceeding $x > 1$ we have $P(x) \sim c\frac{x}{\log x}$, where $c \approx 1.336$.

Primes are odd except 2, and practical numbers are even except 1. Due to this, I would like to say that primes are *male* wile practical numbers are *female*. If one of n and $n+1$ is prime and the remaining one is practical, then I call $\{n, n+1\}$ a *couple*.

Conjecture (Sun, 2013). (i) For any integer $n > 2$, there is a practical number $p < n$ such that $n - p$ and $n + p$ are both prime or both practical.

(ii) Any even integer $2n > 4$ can be written as $p + q = (p+1) + (q-1)$, where p and q are primes with $p+1$ and $q-1$ both practical (thus $\{p, p+1\}$ and $\{q, q-1\}$ are couples).

Two kinds of sandwiches

I introduced two kinds of sandwiches.

First kind of sandwiches: $\{p-1, p, p+1\}$ with p prime and $p \pm 1$ practical.

Second kind of sandwiches: $\{q-1, q, q+1\}$ with q practical and $q \pm 1$ prime.

Conjecture (Sun, 2013).

(i) Each $n = 4, 5, \ldots$ can be written as $p + q$, where $\{p-1, p, p+1\}$ is a sandwich of the first kind, and q is either prime or practical.

(ii) Each even number $n > 8$ can be written as $p + q + r$, where $\{p-1, p, p+1\}$ and $\{q-1, q, q+1\}$ are sandwiches of the first kind, and $\{r-1, r, r+1\}$ is a sandwich of the second kind.

Main references

For sources of my above conjectures, you may visit my homepage `https://maths.nju.edu.cn`. In particular, you may loot at my following publications:

1. Zhi-Wei Sun, *On functions taking only prime values*, J. Number Theory **133** (2013), no. 8, 2794–2812.

2. Zhi-Wei Sun, *The least modulus for which consecutive polynomial values are distinct*, J. Number Theory **160** (2016), 108–116.

3. Zhi-Wei Sun, *A new theorem on the prime-counting function*, Ramanujan J. **42** (2017), 59–67.

4. Zhi-Wei Sun, Conjectures in Combinatorics and Number Theory, in English, Harbin Institute of Technology Press, 2026.

Thank you!