A talk given at Univ. of Illinois at Urbana-Champaign (August 28, 2012)
and the 6th National Number Theory Confer. (October 20, 2012)
and the China-Korea Number Theory Seminar (October 27, 2012)

Various new observations about primes

Zhi-Wei Sun

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

October 27, 2012

Abstract

This talk focuses on the speaker's recent discoveries about primes. We will talk about the speaker's new way to generate all primes or primes in certain arithmetic progressions, and his various conjectures for products of primes, sums of primes, recurrence for primes, representations of integers as alternating sums of consecutive primes. We will also mention his new observations (mainly made in August 2012 at UIUC) about twin primes, squarefree numbers, and primitive roots modulo primes.

Part I. On functions taking only prime values

Representing primes by polynomials

Euler: $x^2 - x + 41$ is prime for every $x = 1, \ldots, 40$.

Theorem (Rabinowitz, 1913). Let $p > 1$ be an integer and let K be the imaginary quadratic field $\mathbb{Q}(\sqrt{1-4p})$. Let O_K be the ring of algebraic integers in K. Then $x^2 - x + p$ is a prime for all $x = 1, \ldots, p-1$ if and only if K has class number one, i.e., O_K is a principal ideal domain.

Theorem (conjectured by Gauss and proved by H. Stark). The only imaginary quadratic field having class number one are those $\mathbb{Q}(\sqrt{-d})$ with $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

Thus, for any $p > 41$, $x^2 - x + p$ **cannot** take prime values for all $x = 1, \ldots, p-1$.

In general, any non-constant polynomial $P(x_1, \ldots, x_n)$ with integer coefficients cannot take primes for all $x_1, \ldots, x_n \in \mathbb{Z}$.

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 $n = 1, 2, 3, \ldots$.

A problem on central binomial coefficients

Let p be an odd 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 (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. Moreover, if $p > 11$ then $\binom{2k}{k}$ $(k = 1, \ldots, (p-3)/2)$ cannot be pairwise distinct modulo 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. If $a \in \mathbb{Z}$ is not divisible by p and $a^k \not\equiv 1 \pmod{p}$ for $k = 1, \ldots, p-2$, then we say that a is a *primitive root* mod p (or the order of a mod p is $p-1$).

Artin's Conjecture (1927). 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 (moreover, the set of such primes has a positive asymptotic density inside the set of all primes).

Progress:

(1) C. Hooley (1967): The conjecture follows from the Generalized Riemann Hypothesis.

(2) R. Gupta & M. R. Murty (1984): The conjecture holds for infinitely many a (with help of sieve methods).

(3) R. Heath-Brown (1986): There are at most two exceptional primes a for which Artin's conjecture fails.

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.

Motivation. By Stirling's formula, $\binom{2k}{k} \sim 4^k/\sqrt{k\pi}$.

Conjectures on Lucas sequences

Let A be an integer with $|A| > 2$. Define

$$u_0(A) = 0,\ u_1(A) = 1,\ \text{and } u_{n+1}(A) = Au_n(A) - u_{n-1}(A);$$
$$v_0(A) = 2,\ v_1(A) = A,\ \text{and } v_{n+1}(A) = Av_n(A) - v_{n-1}(A).$$

Conjecture (Sun, Feb. 26, 2012). (i) If $2 + A$ is not a square, then there are infinitely many odd primes p such that those $v_k(A) \bmod p$ with $k = 1, ..., (p - \varepsilon_p)/2$ are pairwise distinct, where $\varepsilon_p = (\frac{A^2-4}{p})$.

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

Conjecture (Sun, Feb. 26, 2012). Let $n \in \mathbb{Z}^+$ be sufficiently large ($n > 2|A|$ or $n > 100$ may suffice). Then $t_A(n)$ (the smallest integer $m > 1$ such that $v_k(A)$ $(k = 1, ..., (p - \varepsilon_p)/2)$ are pairwise distinct modulo m) is 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 $v_k(A) \bmod p$ $(k = 1, ..., (p - \varepsilon_p)/2)$ are pairwise distinct.

Generate all primes in a combinatorial manner

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

(c) I 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.

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 $(2k-1)^d$ $(k = 1, \ldots, n)$ 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 $p \not\equiv 1 \pmod{q}$.

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

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

Previous results by others

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 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.

Another conjecture involving factorials

Conjecture (Sun, March 25, 2012). The least integer $m > 1$ such that $n! \not\equiv k! \pmod{m}$ for all $0 < k < n$, is a prime in $[n, 2n)$ unless $n \in \{4, 6\}$.

Remark. The Bertrand Postulate confirmed by Chebyshev states that for any $x > 1$ the interval $[x, 2x)$ contains a prime.

For Euler number $E_0, E_1, E_2, \ldots$, I have a similar conjecture.

Conjecture (Sun, March, 2012). Let $e(n)$ be the least integer $m > 1$ such that $2E_{2n} \not\equiv 2E_{2k} \pmod{m}$ for all $0 < k < n$. Then $e(n)$ is a prime in the interval $[2n, 3n]$ with the only exceptions as follows:

$$e(4) = 13,\ e(7) = 23,\ e(10) = 5^2,\ e(55) = 11^2.$$

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) 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. If $w_i(n) = p_k$, then $k \geqslant n$ since $p_k \mid P_k \pm P_{k+1}$. I'm even unable to prove $w_2(n) > n$.

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 $n = 1, 2, 3, \ldots$. 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 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, 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}.

No comments from number theorists though I made the conjecture public via a message to Number Theory List! They all keep silent on this mysterious recurrence.

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 $p_k, \ldots, p_n$ $(k \leqslant n)$ 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. 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. Inequalities involving primes

Firoozbakht's Conjecture

In 1982 Faride Firoozbakht (from Iran) posed the following challenging conjecture while he was studying a proof of the Prime Number Theorem.

Firoozbakht's Conjecture. $\sqrt[n]{p_n} > \sqrt[n+1]{p_{n+1}}$ for all $n = 1, 2, \ldots$, i.e., the sequence $(\sqrt[n]{p_n})_{n\geqslant 1}$ is strictly decreasing

Remark. The conjecture implies that

$$p_{n+1} - p_n < \log^2 p_n - \log p_n + 1$$

for all $n > 4$, which is stronger than Cramer's conjecture that $c := \limsup(p_{n+1} - p_n)/\log^2 p_n$ coincides with 1 (A. Granville thought that c should be $2/e^\gamma \approx 1.122918$.)

Verification record. Verified for all primes less than 4×10^{18}.

Comments. Since $\log \sqrt[n]{p_n} \sim (\log n)/n$, the conjecture seems reasonable. I saw it few years ago but soon forgot the reference and the proposer's long name.

A refinement of Firoozbakht's Conjecture

By the Prime Number Theorem, $p_n \sim n \log n$. Note that

$$\log \frac{\sqrt[n+1]{(n+1)\log(n+1)}}{\sqrt[n]{n\log n}} = -\frac{\log n}{n^2} - \frac{\log\log n}{n^2} + O\left(\frac{1}{n^2}\right).$$

This led me to make the following conjecture.

Conjecture (Sun, 2012-09-11) For any integer $n > 4$, we have the inequality

$$\frac{\sqrt[n+1]{p_{n+1}}}{\sqrt[n]{p_n}} < 1 - \frac{\log\log n}{2n^2}.$$

Remark. We have verified the conjecture for all $n \leqslant 3500000$ and all those n with $p_n < 4 \times 10^{18}$ and $p_{n+1} - p_n \neq p_{k+1} - p_k$ for all $1 \leqslant k < n$. If $n = 49749629143526$, then $p_{n+1} - p_n = 1132$, $p_n = 1693182318746371$, and

$$(1 - \sqrt[n+1]{p_{n+1}}/\sqrt[n]{p_n})n^2/\log\log n \approx 0.5229.$$

Some easy facts

Easy things:

$(\sqrt[n]{n})_{n\geqslant 3}$ is strictly decreasing,

$(\sqrt[n+1]{n+1}/\sqrt[n]{n})_{n\geqslant 4}$ is strictly increasing.

Reason: For the function $f(x) = (\log x)/x$ on the interval $[4.5, +\infty)$, we have

$$f'(x) = \frac{1-\log x}{x^2} < 0 \text{ and } f''(x) = \frac{2\log x - 3}{x^3} > 0,$$

and hence $f(x)$ is strictly decreasing and strictly convex.

For

$$P_n = p_1 p_2 \cdots p_n \quad \text{and} \quad S_n = p_1 + p_2 + \cdots + p_n,$$

$(\sqrt[n]{P_n})_{n\geqslant 1}$ and $(S_n/n)_{n\geqslant 1}$ are strictly increasing (easy to prove).

$\sqrt[n]{P_n}$ —— the *geometric mean* of $p_1, p_2, \ldots, p_n$.

S_n/n —— the *arithmetic mean* of $p_1, p_2, \ldots, p_n$.

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

Theorem (Sun). (i) (July 28-31) $(\sqrt[n]{S_n})_{n\geqslant 2}$ and $(\sqrt[n]{S_n/n})_{n\geqslant 1}$ are strictly decreasing.

(ii) (Discovered on July 29 and proved on August 25)

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

are strictly increasing.

A general theorem

For $S_n^{(\alpha)} = \sum_{k=1}^{n} p_k^{\alpha}$, we have

Theorem (Sun, Bull. Aust. Math. Soc., in press). Let $\alpha \geqslant 1$.

(i) If $n \geqslant \max\{100, e^{2\times 1.348^{\alpha}+1}\}$, then

$$\sqrt[n]{\frac{S_n^{(\alpha)}}{n}} > \sqrt[n+1]{\frac{S_{n+1}^{(\alpha)}}{n+1}}$$

and hence

$$\sqrt[n]{S_n^{(\alpha)}} > \sqrt[n+1]{S_{n+1}^{(\alpha)}}.$$

(ii) The sequence

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

is strictly increasing, where

$$N(\alpha) = \max\left\{350000,\ \lceil e^{((\alpha+1)^2 1.2^{2\alpha+1}+(\alpha+1)1.2^{\alpha+1})/\alpha} \rceil \right\}.$$

The cases $\alpha = 2, 3, 4$

Corollary. 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.

On squarefree numbers

A positive integer n is called *squarefree* if $p^2 \nmid n$ for any prime p. Here is the list of all squarefree positive integers not exceeding 30 in alphabetical order:

1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30.

Conjecture (Sun, 2012-08-14) (i) For $n = 1, 2, 3, \ldots$ let s_n be the n-th squarefree positive integer. Then the sequence $(\sqrt[n]{s_n})_{n\geqslant 7}$ is strictly decreasing.

(ii) For $n = 1, 2, 3, \ldots$ let $S(n)$ be the sum of the first n squarefree positive integers. Then the sequence $(\sqrt[n+1]{S(n+1)}/\sqrt[n]{S(n)})_{n\geqslant 7}$ is strictly increasing.

Remark. I have checked both parts of the conjecture via `Mathematica`; for example, $\sqrt[n]{s_n} > \sqrt[n+1]{s_{n+1}}$ for all $n = 7, \ldots, 500000$. Note that $\lim_{n\to\infty} \sqrt[n]{S(n)} = 1$ since $S(n)$ does not exceed the sum of the first n primes.

Conjecture on primitive roots modulo primes

Conjecture (Sun, 2012-08-17). Let $a \in \mathbb{Z}$ be not a perfect power (i.e., there are no integers $m > 1$ and x with $x^m = a$).

(i) Assume that $a > 0$. Then there are infinitely many primes p having a as the *smallest positive* primitive root modulo p. Moreover, if $p_1(a), \ldots, p_n(a)$ are the first n such primes, then the next such prime $p_{n+1}(a)$ is smaller than $p_n(a)^{1+1/n}$.

(ii) Suppose that $a < 0$. Then there are infinitely many primes p having a as the *largest negative* primitive root modulo p. Moreover, if $p_1(a), \ldots, p_n(a)$ are the first n such primes, then the next such prime $p_{n+1}(a)$ is smaller than $p_n(a)^{1+1/n}$ with the only exception $a = -2$ and $n = 13$.

(iii) The sequence $(\sqrt[n+1]{P_{n+1}(a)}/\sqrt[n]{P_n(a)})_{n\geqslant 3}$ is strictly increasing with limit 1, where $P_n(a) = \sum_{k=1}^{n} p_k(a)$.

Remark. The first 5 primes having 24 as the smallest positive primitive root are

$$533821,\ 567631,\ 672181,\ 843781,\ 1035301.$$

Conjecture on twin primes

It is conjectured that there are infinitely many twin primes.

Conjecture (Sun, 2012-08-18) (i) If $\{t_1, t_1+2\}, \ldots, \{t_n, t_n+2\}$ are the first n pairs of twin primes, then the first prime t_{n+1} in the next pair of twin primes is smaller than $t_n^{1+1/n}$, i.e., $\sqrt[n]{t_n} > \sqrt[n+1]{t_{n+1}}$.

(ii) The sequence $(\sqrt[n+1]{T(n+1)}/\sqrt[n]{T(n)})_{n\geqslant 9}$ is strictly increasing with limit 1, where $T(n) = \sum_{k=1}^{n} t_k$.

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

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

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

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

Conjecture on Sophie Germain primes

A prime p is called a Sophie Germain prime if $2p+1$ is also a prime. It is conjectured that there are infinitely many Sophie Germain primes, but this has not been proved yet.

Conjecture (Sun, 2012-08-18) (i) If $g_1, \ldots, g_n$ are the first n Sophie Germain primes, then the next Sophie Germain prime g_{n+1} is smaller than $g_n^{1+1/n}$ (i.e., $\sqrt[n]{g_n} > \sqrt[n+1]{g_{n+1}}$) with the only exceptions $n = 3, 4$.

(ii) The sequence $(\sqrt[n+1]{G(n+1)}/\sqrt[n]{G(n)})_{n\geqslant 13}$ is strictly increasing with limit 1, where $G(n) = \sum_{k=1}^{n} g_k$.

Remark. Via `Mathematica` I verified that $\sqrt[n]{g_n} > \sqrt[n+1]{g_{n+1}}$ for all $n = 5, \ldots, 200000$, and

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

for all $n = 13, 14, \ldots, 200000$. Note that $g_{200000} = 42721961$.

A general conjecture related to Hypothesis H

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

General Conjecture (Sun, 2012-09-08) Let $f_1(x), \ldots, f_k(x)$ be irreducible polynomials with integer coefficients and positive leading coefficients such that there is no prime dividing $\prod_{j=1}^k f_j(q)$ for all $q \in \mathbb{Z}$. Let $q_1, q_2, \ldots$ be the list (in ascending order) of those $q \in \mathbb{Z}^+$ such that $f_1(q), \ldots, f_k(q)$ are all primes. Then, for all sufficiently large positive integers n, we have

$$q_{n+1} < q_n^{1+1/n}, \text{ i.e., } \sqrt[n]{q_n} > \sqrt[n+1]{q_{n+1}}.$$

Also, there is a positive integer N such that the sequence $(\sqrt[n+1]{Q(n+1)}/\sqrt[n]{Q(n)})_{n \geqslant N}$ is strictly increasing with limit 1, where $Q(n) = \sum_{k=1}^n q_k$.

Conjecture on Proth primes

Proth numbers: $k \times 2^n + 1$ with k odd and $0 < k < 2^n$.

F. Proth (1878): A Proth number p is a prime if (and only if) $a^{(p-1)/2} \equiv -1 \pmod{p}$ for some integer a.

A *Proth prime* is a Proth number which is also a prime number; the Fermat primes are a special kind of Proth primes.

Conjecture (Sun, 2012-09-07) (i) The number of Proth primes not exceeding a large integer x is asymptotically equivalent to $c\sqrt{x}/\log x$ for a suitable constant $c \in (3, 4)$.

(ii) If $\mathrm{Pr}(1), \ldots, \mathrm{Pr}(n)$ are the first n Proth primes, then $\mathrm{Pr}(n+1) < \mathrm{Pr}(n)^{1+1/n}$ (i.e., $\sqrt[n]{\mathrm{Pr}(n)} > \sqrt[n+1]{\mathrm{Pr}(n+1)}$) unless $n = 2, 4, 5$. If we set $\mathrm{PR}(n) = \sum_{k=1}^{n} \mathrm{Pr}(k)$, then the sequence $(\sqrt[n+1]{\mathrm{PR}(n+1)}/\sqrt[n]{\mathrm{PR}(n)})_{n \geqslant 34}$ is strictly increasing with limit 1.

Remark. I have checked the conjecture for the first 4000 Proth primes.

On irreducible polynomials over finite fields

Let $q > 1$ be a prime power and let $\mathbb{F}_q$ denote the finite field of order q. For $n = 1, 2, 3, \ldots$ let $N_n(q)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$.

Theorem (Sun, October 2012)
(i) The sequence $(N_{n+1}(q)/N_n(q))_{n\geqslant 1}$ is strictly increasing if $q \geqslant 9$, and $(N_{n+1}(q)/N_n(q))_{n\geqslant 19}$ is strictly increasing if $q < 9$.

(ii) The sequence $(\sqrt[n]{N_n(q)})_{n>e^{3+7/(q-1)^2}}$ is strictly increasing, and the sequence

$$(\sqrt[n+1]{N_{n+1}(q)}/\sqrt[n]{N_n(q)})_{n\geqslant 5.835\times 10^{14}}$$

is strictly decreasing.

On partitions of integers

A partition of a positive integer n is a way of writing n as a sum of positive integers with the order of addends ignored. Let $p(n)$ denote the number of partitions of n. It is known that

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4\sqrt{3}n} \quad \text{(Hardy and Ramanujan)}$$

and hence $\lim_{n\to\infty} \sqrt[n]{p(n)} = 1$.

Conjecture (Sun, 2012-08-02) The sequence $(\sqrt[n]{p(n)})_{n\geqslant 6}$ is strictly decreasing. Moreover, the sequence $(\sqrt[n+1]{p(n+1)}/\sqrt[n]{p(n)})_{n\geqslant 26}$ is strictly increasing.

Remark. I have verified the conjecture for n up to 10^5.

I have many other conjectures on monotonicity of $(\sqrt[n]{a_n})_{n\geqslant 1}$ or $(\sqrt[n+1]{a_{n+1}}/\sqrt[n]{a_n})_{n\geqslant 1}$ for various combinatorial sequences $(a_n)_{n\geqslant 1}$ of positive integers.

Part III. Selected conjectures on primes made before 2012

Selected conjectures made before 2012

Conjecture (Sun, 2009). Any natural number $n \neq 216$ can be written in the form $p + T_x$, where p is a prime or zero, and $T_x = x(x+1)/2$ is a triangular number.

Conjecture (Sun, 2010). For any prime $p > 3$ we have

$$\sum_{k=0}^{p-1} \frac{\binom{4k}{2k+1}\binom{2k}{k}}{48^k} \equiv 0 \pmod{p^2}.$$

Conjecture (Sun, 2010). For any odd prime p we have

$$\sum_{n=0}^{p-1} A_n \equiv \begin{cases} 4x^2 - 2p \pmod{p^2} & \text{if } p = x^2 + 2y^2, \\ 0 \pmod{p^2} & \text{if } p \equiv 5, 7 \pmod{8}, \end{cases}$$

where $A_0, A_1, \ldots$ are Apéry numbers defined by

$$A_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2.$$

Remark. I have proved the congruence modulo p.

Selected conjectures made before 2012

Conjecture (Sun, 2011). For any odd prime p and $n = 1, 2, 3, \ldots$,

$$\frac{1}{n\binom{2n}{n}} \sum_{k=0}^{n-1} \binom{(p-1)k}{k, \ldots, k} \text{ is always a } p\text{-adic integer.}$$

Conjecture (Sun, 2011). Let $p > 3$ be a prime and let $T_k(b, c)$ denote the coefficient of x^k in $(x^2 + bx + c)^k$. Then

$$\sum_{k=0}^{p-1} \frac{\binom{2k}{k} T_k^2(3, -3)}{(-108)^k}$$

$$\equiv \begin{cases} 4x^2 - 2p \pmod{p^2} & \text{if } (\frac{-1}{p}) = (\frac{p}{3}) = (\frac{p}{7}) = 1,\ p = x^2 + 21y^2, \\ 12x^2 - 2p \pmod{p^2} & \text{if } (\frac{-1}{p}) = (\frac{p}{7}) = -1, (\frac{p}{3}) = 1,\ p = 3x^2 + 7y^2, \\ 2x^2 - 2p \pmod{p^2} & \text{if } (\frac{-1}{p}) = (\frac{p}{3}) = -1, (\frac{p}{7}) = 1, 2p = x^2 + 21y^2, \\ 6x^2 - 2p \pmod{p^2} & \text{if } (\frac{-1}{p}) = 1, (\frac{p}{3}) = (\frac{p}{7}) = -1, 2p = 3x^2 + 7y^2, \\ 0 \pmod{p^2} & \text{if } (\frac{-21}{p}) = -1. \end{cases}$$

Remark. The quadratic field $\mathbb{Q}(\sqrt{-21})$ has class number four.

Few of my 181 conjectural series

Motivated by congruences modulo primes, I found:

$$\sum_{k=1}^{\infty}\frac{(28k^2-18k+3)(-64)^k}{k^5\binom{2k}{k}^4\binom{3k}{k}}=-14\zeta(3),$$

$$\sum_{n=0}^{\infty}\frac{40n^2+26n+5}{(-256)^n}\binom{2n}{n}^2\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{k}\binom{2(n-k)}{n-k}=\frac{24}{\pi^2},$$

$$\sum_{k=0}^{\infty}\frac{66k+17}{(2^{11}3^3)^k}T_k^3(10,11^2)=\frac{540\sqrt{2}}{11\pi},$$

$$\sum_{k=0}^{\infty}\frac{126k+31}{(-80)^{3k}}T_k^3(22,21^2)=\frac{880\sqrt{5}}{21\pi},$$

$$\sum_{k=0}^{\infty}\frac{3990k+1147}{(-288)^{3k}}T_k^3(62,95^2)=\frac{432}{95\pi}(195\sqrt{14}+94\sqrt{2}).$$

Remark. I would like to offer \$300 for the person (not joint authors) who could prove the last three identities.

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

You are welcome to solve my conjectures and win the prizes!

Thank you!