A talk given at Jiangsu Normal University (March 22, 2012)
Workshop in Combinatorics and Graph (Changsha, June 10, 2012)
The 5th National Conferfence on Combinatorics
and Graph theory (Luoyang, July 18, 2012)

Primes from the viewpoint of combinatorics

Zhi-Wei Sun

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

July 18, 2012

Abstract

Prime numbers play a central role in number theory; many mathematicians ever tried in vain to find a nontrivial number -theoretic function whose values are always primes. In this talk we will introduce the speaker's recent work on primes from the viewpoint of combinatorics. We will generate primes in a combinatorial manner and pose many new challenging conjectures on primes. A positive integer n is said to be *good* if the total number of prime factors (counted with multiplicity) of n has the same parity with n; we find that the statistics of good numbers is closely related to the famous Riemann Hypothesis.

Part I. Classical results on functions with prime values

Prime numbers

An integer $p > 1$ is said to be a *prime* if p cannot be written as ab with $a, b \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ and $a, b > 1$.

Prime numbers not more than 100:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Fundamental Theorem on Arithmetic. Any integer $n > 1$ can be written as a product of finitely many primes and the factorization is unique if we ignore the order of factors.

Thus, prime numbers are quite essential in number theory.

Euclid: There are infinitely many primes.

A Sketch of the Proof. Let $p_1, \ldots, p_n$ be the first n primes. Then the smallest prime divisor of $\prod_{k=1}^{n} p_k + 1$ is a prime different from $p_1, \ldots, p_n$.

Fortune's Conjecture and Firoozbakht's Conjecture

Let p_k denote the kth prime. *Primorial*: $p_n\# := p_1 \cdots p_n$.

Fortune's Conjecture. Let q_n be the least prime greater than $p_n\# + 1$. Then $q_n - p_n\#$ is always a prime.

Remark. R. F. Fortune (1903-1979) was a social anthropologist at Cambridge University.

Lesser Fortune Conjecture (suggested by P. Carpenter). Let q_n be the greatest prime smaller than $p_n\# - 1$. Then $p_n\# - q_n$ is always a prime.

Example. $5\# = 2 \times 3 \times 5 = 30$. The least prime greater than 31 is 37 and the greatest prime smaller than 29 is 23. Clearly both $37 - 30$ and $30 - 23$ coincide with the prime 7.

Firoozbakht's Conjecture. $\sqrt[n]{p_n} > \sqrt[n+1]{p_{n+1}}$ for all $n = 1, 2, \ldots$.

The conjecture implies that $p_{n+1} - p_n < \log^2 p_n - \log p_n$ for sufficiently large n, which is stronger than Cramer's conjecture.

Euler's polynomial $x^2 - x + 41$

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

Theorem. 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 $x = 1, \ldots, p-1$.

General polynomials

Let $P(x_1, \ldots, x_n)$ be a non-constant polynomial with integer coefficients. If $P(a_1, \ldots, a_n)$ is a prime p, then

$$P(a_1 + pq_1, \ldots, a_n + pq_n) \equiv P(a_1, \ldots, a_n) = p \equiv 0 \pmod{p}.$$

Thus $P(x_1, \ldots, x_n)$ cannot be primes for all $x_1, \ldots, x_n \in \mathbb{Z}$.

The following result comes from Matijasevič's negative solution of Hilbert's tenth problem and later refinements.

Theorem. There exists a polynomial $P(x_1, \ldots, x_{10})$ with integer coefficients such that the set of positive integers in the range of $P(x_1, \ldots, x_{10})$ (with $x_1, \ldots, x_{10} \in \mathbb{N} = \{0, 1, 2, \ldots\}$) is exactly the set of all prime numbers.

Fermat numbers

If m has an odd prime divisor p, then $2^{m/p}+1$ is a proper divisor of 2^m+1 and hence 2^m+1 is composite.

Fermat (1640) introduced the Fermat numbers

$$F_n = 2^{2^n}+1 \quad (n = 0, 1, 2, \ldots).$$

He observed that

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

are primes. Then he conjectured that F_n is always a prime.

Euler (1732). $F_5 = 2^{32} = 1 = 641 \times 6700417$.
Euler (1770). Any divisor of F_n has the form $2^{n+1}q+1$.

No more Fermat primes are found.

Mills' Theorem

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

Proof. By a result of A. E. Ingham [Quart. J. Math. Oxford Ser. 8(1937)], $p_{n+1} - p_n < K p_n^{5/8}$ for $n = 1, 2, 3, \ldots$, where K is a fixed positive integer. Suppose that $N > K^8$ and p_n is the largest prime not more than N^3. Then

$$N^3 < p_{n+1} < p_n + K p_n^{5/8} < N^3 + N^{1/8}(N^3)^{5/8} = N^3 + N^2 < (N+1)^3 - 1.$$

Let P_0 be a prime greater than K^8. Then we can find an infinite sequence of primes, $P_0, P_1, P_2, \ldots$ such that

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

Mills' Theorem (continued)

Let $u_n = P_n^{3^{-n}}$ and $v_n = (P_n + 1)^{3^{-n}}$. Then $u_n < v_n$,

$$u_{n+1} = P_{n+1}^{3^{-(n+1)}} > (P_n^3)^{3^{-n-1}} = P_n^{3^{-n}} = u_n$$

and

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

Let $A = \lim_{n\to\infty} u_n$ and $B = \lim_{n\to\infty} v_n$. Then

$$u_n < A \leqslant B < v_n \quad \text{and thus} \quad P_n < A^{3^n} < P_n + 1.$$

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

Inspired by Mills' theorem, E. M. Wright proved that there is a real number α such that integral parts of those

$$\alpha_0 = \alpha, \ \alpha_1 = 2^{\alpha_0}, \ \alpha_2 = 2^{\alpha_1}, \ \ldots$$

are all primes.

Part II. My recent work on generating primes

Classical way to generate primes

If p is the smallest prime divisor of a composite number $m = pq$, then $n \geqslant p^2$ and hence $p \leqslant \sqrt{m}$. So, an integer $n > 1$ is a prime if and only if it is divisible by none of those primes not exceeding $\sqrt{n}$.

A classical way to generate primes in $(\sqrt{N}, N]$ is as follows:

Delete all those $m \in (\sqrt{N}, N]$ which are multiples of some primes not exceeding $\sqrt{N}$. Those remaining numbers in $(\sqrt{N}, N]$ are just primes in the interval.

This method to generate primes is called the *Eratosthenes sieving method*.

Example. Deleting multiples of 2 or 3 or 5 or 7 from $11, \ldots, 100$ we then obtain all the primes in $(10, 100]$.

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

Theorem 1 (Sun, Feb. 29, 2012) (i) For $n \in \mathbb{Z}^+$ let $S(n)$ denote the smallest integer $m > 1$ such that those $2k(k-1)$ mod m for $k = 1, \ldots, n$ are pairwise distinct. Then $S(n)$ is the least prime greater than $2n-2$.
(ii) For $n \in \mathbb{Z}^+$ let $T(n)$ denote the least integer $m > 1$ such that those $k(k-1)$ mod m with $1 \leqslant k \leqslant n$ are pairwise distinct. Then we have

$$T(n) = \min\{m \geqslant 2n-1 : \ m \text{ is a prime or a positive power of } 2\}.$$

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 3 (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 $p \not\equiv 1 \pmod{q}$.

Previous results by others

Theorem 1 (L. K. Arnold, S. J. Benkoski and B. J. McCabe, 1985). Let $n > 4$ be an integer. Then the least positive integer m (denoted by $D(n)$) such that $1^1, 2^2, \ldots, n^2$ 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 $n!$ is congruent to none of $1!, \ldots, (n-1)!$ modulo m, 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.

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 $P_k \pm P_{k+1} \equiv 0 \pmod{p_k}$. 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 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. The speaker has 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! They all keep silent on this mysterious recurrence.

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 $2m + 2.2\sqrt{m}$ such that

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

Examples.

$$10 = 17 - 13 + 11 - 7 + 5 - 3;$$
$$20 = 41 - 37 + 31 - 29 + 23 - 19 + 17 - 13 + 11 - 7 + 5 - 3;$$
$$2382 = p_{652} - p_{651} + \cdots + p_{44} - p_{43},$$
$$p_{652} = 4871 = \lfloor 2 \cdot 2382 + 2.2\sqrt{2382} \rfloor.$$

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 III. My recent hypothesis related to the Riemann Hypothesis

Liouville's function

$\Omega(n)$: the *total* number of prime factors of n (counted with multiplicity).

For example, $12 = 2^2 \times 3$ and so $\Omega(12) = 3$.

Liouville's function: $\lambda(n) = (-1)^{\Omega(n)}$.

It is known that

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}.$$

If $\Re(s) > 1$, then

$$\sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)},$$

where

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The Riemann Hypothesis

If $\Re(s) > 1$, then

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} + \sum_{n=1}^{\infty} \frac{1}{n^s} = 2 \sum_{m=1}^{\infty} \frac{1}{(2m)^s}$$

and hence

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} = (2^{1-s} - 1)\zeta(s).$$

If $0 < \Re(s) \leqslant 1$ and $s \neq 1$, then we define $\zeta(s)$ by the last equality since $\sum_{n=1}^{\infty}(-1)^n/n^s$ converges.

Riemann Hypothesis (B. Riemann 1859): If $0 < \Re(s) \leqslant 1$ and $\zeta(s) = 0$, then $\Re(s) = 1/2$.

RH is one of the most challenging problems in number theory!

Littlewood's comment (1962): *"There is no evidence whatever for it and no imaginable reason for it to be true."*

Pólya's conjecture and Turán's conjecture

Pólya's Conjecture (1919). $L(x) = \sum_{n \leqslant x} \lambda(n) < 0$ for all $x \geqslant 1$.

Pólya showed that his conjecture implies RH. Unfortunately, in 1958 C. B. Haselgrove showed that $L(x)$ changes its sign infinitely often. Now it is known that the smallest x with $L(x) > 0$ is $x = 906150257$.

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

Turán showed that his conjecture implies RH. Unfortunately, C. B. Haselgrove also disproved this conjecture. Now it is known that the smallest x with $\sum_{n \leqslant x} \lambda(n)/n < 0$ is $x = 72185376951205$.

Good numbers VS bad numbers

Both Pólya's conjecture and Turán's conjecture fail. But, why their first counterexamples are very large? In my opinion this reminds that they should contain certain *positive* information.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\Omega(n)$	0	1	1	2	1	2	1	3	2	2	1	3	1	2	2	4	1	3	1	3

We say that a positive integer n is *good* if n and $\Omega(n)$ have the same parity (i.e., $n \equiv \Omega(n) \pmod 2$), and n is *bad* otherwise.

Among $1, \ldots, 20$ there are only 8 bad numbers: 1, 2, 8, 9, 12, 15, 18, 20.

Are there more good numbers than bad numbers??

A new hypothesis

Hypothesis (Sun, May 16, 2012). We have

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

and

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

Moreover,

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

and

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

Remark. (a) I have showed that RH follows if $S(x) > 0$ for $x \geqslant 5$ or $T(x) < 0$ for $x \geqslant 1$.
(b) I have verified the hypothesis about $S(x)$ and $T(x)$ for x up to 10^{11} and 2×10^9 respectively.

Some numerical evidence

$$S(10) = 2,\ S(100) = 14,\ S(1000) = 54,\ S(10000) = 186,$$
$$S(10^5) = 464,\ S(10^6) = 1302,\ S(10^7) = 5426,\ S(10^8) = 62824,$$
$$S(10^9) = 62824,\ S(5 \times 10^9) = 105476,\ S(10^{10}) = 172250,$$

$$S(2 \times 10^{10}) = 252292,\quad S(3 \times 10^{10}) = 292154,\quad S(4 \times 10^{10}) = 263326,$$
$$S(5 \times 10^{10}) = 360470,\quad S(6 \times 10^{10}) = 363152,\quad S(7 \times 10^{10}) = 406260,$$
$$S(8 \times 10^{10}) = 559558,\quad S(9 \times 10^{10}) = 491100,\quad S(10^{11}) = 457588.$$

Let $q(x) = S(x)/\sqrt{x}$. Then

$$\max_{1 \leqslant x \leqslant 10^{11}} q(x) = q(17593752) \approx 2.28251789,$$
$$\max_{604520021 < x \leqslant 10^{11}} q(x) = q(3731064314) \approx 2.213795;$$
$$\min_{324 < x \leqslant 10^{11}} q(x) = q(123579784) \approx 1.046179,$$
$$\min_{1812913634 < x \leqslant 10^{11}} q(x) = q(62567895568) \approx 1.133624.$$

Some comments from others

Peter Humphries (June 3, 2012): *The only way your conjecture could be true would be if the Riemann hypothesis is true but the Linear Independence hypothesis is not, which seems extremely unlikely.*

Linear Independence Hypothesis. Those reals t such that $\zeta(\frac{1}{2} + it) = 0$ are linearly independent over the rational field $\mathbb{Q}$.

Andrew Odlyzko (July 9, 2012). *Your conjecture is a very interesting one, but I am quite confident that it is false.*

It appears very unlikely that the analytic and computational methods that disproved Mertens' conjecture would disprove your conjecture.

Your conjecture will likely be true for quite a ways. It is likely another case where even a lot of evidence from an initial segment is misleading.

Two references

1. Z. W. Sun, *On functions taking only prime values*, preprint, 2012, `arXiv:1202.6589`

2. Z. W. Sun, *On a pair of zeta functions*, preprint, 2012, `arXiv:1204.6689`

You are welcome to solve my conjectures!

Thank you!