On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ

Kevin Ford
*Sergei Konyagin**

Dedicated to Professor Andrzej Schinzel on the occasion of his 60th birthday.

Abstract. Let $\sigma(n)$ denote the sum of the positive divisors of n. In this note it is shown that for any positive integer k, there is a number m for which the equation $\sigma(x) = m$ has exactly k solutions, settling a conjecture of Sierpiński. Additionally, it is shown that for every positive even k, there is a number m for which the equation $\phi(x) = m$ has exactly k solutions, where ϕ is Euler's function.

1991 Mathematics Subject Classification: Primary 11A25, 11N64; Secondary 11N36.

1. Introduction

For each natural number m, let $A(m)$ denote the number of solutions of $\phi(x) = m$ and let $B(m)$ denote the number of solutions of $\sigma(x) = m$. Here $\phi(x)$ is Euler's function and $\sigma(x)$ is the sum of divisors function. About 40 years ago, Sierpiński made two conjectures about the possible values of $A(m)$ and $B(m)$ (see [S1], [E,p. 12] and Conjectures C_{14} and C_{15} of [S2]).

Conjecture 1 (Sierpiński). *For each $k \geqslant 2$, there is a number m with $A(m) = k$.*

Conjecture 2 (Sierpiński). *For each $k \geqslant 1$, there is a number m with $B(m) = k$.*

An older conjecture of Carmichael [C1,C2] states that $A(m)$ can never equal 1. Carmichael's Conjecture remains unproven, however it is known that a counterexample m must exceed $10^{10^{10}}$ (c.f. Theorem 6 and section 7 of [F1]).

Both of Sierpiński's conjectures were deduced by Schinzel [S1] as a consequence of his Hypothesis H [SS].

Schinzel's Hypothesis H. *Suppose $f_1(n), \dots, f_k(n)$ are irreducible, integer valued polynomials (for integral n) with positive leading coefficients. Also suppose*

* The second author was supported by NSF grant DMS 9304580.

that for every integer $q \geqslant 2$, there is an integer n for which q does not divide $f_1(n) \cdots f_k(n)$. Then the numbers $f_1(n), \ldots, f_k(n)$ are simultaneously prime for infinitely many positive integers n.

By an inductive approach, the first author [F1,Lemma 7.1] has shown that Conjectures 1 and 2 follow from Dickson's Prime k-tuples Conjecture [D], which is the special case of Hypothesis H when each $f_i(n)$ is linear.

Although Hypothesis H has not been proved in even the simplest case of two linear polynomials (generalized twin primes), sieve methods have shown the conclusion to hold if the numbers $f_1(n), \ldots, f_k(n)$ are allowed to be primes or "almost primes" (non-primes with few prime factors). See [HR] for specifics. Taking a new approach we utilize these almost primes to prove Conjecture 2 unconditionally. The same method is applicable to Conjecture 1, but falls short of a complete proof because of the (probable) non-existence of a number with $A(m) = 1$. The fact that $B(1) = 1$ is crucial to the proof of Conjecture 2.

Theorem 1. *For every $k \geqslant 1$, there is a number m with $B(m) = k$.*

Theorem 2. *Suppose r is a positive integer and $A(m) = k$. Then there is a number l for which $A(lm) = rk$.*

Corollary 3. *If $A(m) = k$ is known to be solvable for $2 \leqslant k \leqslant C$, then $A(m) = k$ has a solution for every k divisible by a prime $\leqslant C$. In particular, $A(m) = k$ is solvable for all even k.*

The first author has succeeded in proving Conjecture 1 for all $k \geqslant 2$ by combining the inductive approach in [F1] with the theory of almost primes. The details are very complex and will appear in a forthcoming paper [F2].

2. Preliminary lemmas

Let $\omega(n)$ denote the number of distinct prime factors of n, let $P^-(n)$ denote the smallest prime factor of n, and let $[x]$ denote the greatest integer $\leqslant x$. The first two lemmas provide the construction of numbers m with a desired value of $A(m)$ or $B(m)$.

Lemma 1. *Suppose $A(m) = k$, $r \geqslant 2$, $n \geqslant 2$ and $p_{i,j}$ $(i = 1, \ldots, r; j = 1, \ldots, n)$ are primes larger than $2^r m + 1$. For each i, let $q_i = p_{i,2} p_{i,3} \cdots p_{i,n}$, and let t be the product of all primes $p_{i,j}$. Suppose further that*

(i) *$2p_{i,1} q_j + 1$ is prime whenever $i = 1$, $j = 1$ or $j = i$,*

(ii) *no $p_{i,j}$ equals any of the primes listed in (i),*

(iii) *except for the numbers listed in (i), for each $d_1 | t$ with $d_1 > 1$ and $d_2 | 2^{r-1} m$, $2d_1 d_2 + 1$ is composite.*

Then $A(2^r tm) = rk$.

Proof. Suppose that $\phi(x) = 2^r tm$. No $p_{i,j}$ may divide x, for otherwise $p_{i,j} - 1 | 2^r tm$, which is impossible by conditions (ii), (iii) and the fact that each $p_{i,j} > 2^r m + 1$. Therefore, each $p_{i,j}$ divides a number $s_{i,j} - 1$, where $s_{i,j}$ is a prime divisor of x. Therefore, $s_{i,j} = dp_{i,j} + 1$, where $d | 2^r mt / p_{i,j}$ and $2 | d$. By condition (iii), $s_{i,j}$ must be one of the primes listed in (i) and by condition (ii), each prime $s_{i,j}$ divides x to the first power only. By (i), there are r choices for $s_{1,1}$ and once $s_{1,1}$ is chosen the other primes $s_{i,j}$ are uniquely determined. For each choice,

$$\phi(s_{1,1} s_{2,1} \cdots s_{r,1}) = 2^r t,$$

and thus $\phi(x/(s_{1,1} \cdots s_{r,1})) = m$, which has exactly k solutions. □

Lemma 2. *Suppose* $r \geqslant 2$, $n \geqslant 2$ *and* $p_{i,j}$ $(i = 1, \ldots, r; j = 1, \ldots, n)$ *are primes larger than* $2^r + 1$. *For each* i, *let* $q_i = p_{i,2} p_{i,3} \cdots p_{i,n}$, *and let* t *be the product of all primes* $p_{i,j}$. *Suppose further that*
(i) $2 p_i q_j - 1$ *is prime whenever* $i = 1$, $j = 1$ *or* $j = i$,
(ii) $\sigma(\pi^b) \nmid 2^r t$ *for every prime* π *and integer* $b \geqslant 2$ *with* $\sigma(\pi^b) > 2^r$,
(iii) *except for the numbers listed in (i), for each* $d_1 | t$ *with* $d_1 > 1$ *and* $d_2 | 2^{r-1}$, $2 d_1 d_2 - 1$ *is composite.*
Then $B(2^r t) = r$.

Proof. Suppose that $\sigma(x) = 2^r t$. Each $p_{i,j}$ divides a number $\sigma(s_{i,j}^b)$, where $s_{i,j}^b$ is a prime power divisor of x. Condition (ii) implies $b = 1$, so $s_{i,j} = dp_{i,j} - 1$, where d is an even divisor of $2^r t / p_{i,j}$. By condition (iii), $s_{i,j}$ must be one of the primes listed in (i). There are r choices for $s_{1,1}$ and once $s_{1,1}$ is chosen the other primes $s_{i,j}$ are uniquely determined. For each choice,

$$\sigma(s_{1,1} s_{2,1} \cdots s_{r,1}) = 2^r t,$$

which forces $x = s_{1,1} \cdots s_{r,1}$. □

To show such sets of primes $(p_{i,j})$ exist, the first tool we require is a lower bound on the density of primes s for which $\frac{s-1}{2}$ (or $\frac{s+1}{2}$) is an almost prime.

Lemma 3. *Let* $a = 1$ *or* $a = -1$. *For some positive* α *and* x *sufficiently large, there are* $\gg x / \log^2 x$ *primes* $x/2 < s \leqslant x$ *for which* $s = 2u + a$, u *has at least 2 prime factors and every prime factor of* u *exceeds* x^α.

Proof. This follows from the linear sieve and the Bombieri-Vinogradov prime number theorem (Lemma 3.3 of [HR]) to bound the error terms. By Theorem 8.4 of [HR], we have

$$\#\{x/2 < s \leqslant x : s, \tfrac{1}{2}(s - a) \text{ both prime}\} \leqslant (4 + o(1)) \frac{x}{\log^2 x}$$

and for $x \geqslant x_0(\alpha)$

$$\#\{x/2 < s \leqslant x : s \text{ prime }, P^-(\tfrac{1}{2}(s-a)) > x^\alpha\} \geqslant \left(\frac{e^{-\gamma}}{\alpha} f(1/(2\alpha)) + o(1)\right) \frac{x}{\log^2 x},$$

where f is the usual lower bound sieve function and γ is the Euler-Mascheroni constant. Taking $\alpha = \frac{1}{8}$ and noting that $f(4) = \frac{1}{2}e^\gamma \log 3$, the number of primes $x/2 < s \leqslant x$ for which $u = \frac{1}{2}(s-a)$ contains at least 2 prime factors and all prime factors of u exceed x^α is at least $0.39x/\log^2 x$ for large x. □

In the argument below it is critical that the numbers $\frac{1}{2}(s-a)$ have at least two prime factors. This may be the first application of lower bound sieve results where almost primes are desired and primes are not.

Lemma 4. *Suppose $g \geqslant 1$, and $a_i, b_i (i = 1, \ldots, g)$ are integers satisfying*

$$E := \prod_{i=1}^{g} a_i \prod_{1 \leqslant r < s \leqslant g} (a_r b_s - a_s b_r) \neq 0.$$

Let $\rho(p)$ denote the number of solutions of

$$\prod_{i=1}^{g} (a_i n + b_i) \equiv 0 \pmod{p},$$

and suppose $\rho(p) < p$ for every prime p. If $\log E \ll \log z$, then the number of n with $z < n \leqslant 2z$ and $P^-(a_i n + b_i) > z^\alpha$ for $i = 1, \ldots, g$ is

$$\begin{aligned} &\ll_{g,\alpha} \frac{z}{\log^g z} \prod_p \left(1 - \frac{\rho(p)-1}{p-1}\right)\left(1 - \frac{1}{p}\right)^{1-g} \\ &\ll_{g,\alpha} \frac{z}{\log^g z} \left(\frac{E}{\phi(E)}\right)^g \ll_{g,\alpha} \frac{z(\log\log z)^g}{\log^g z}. \end{aligned}$$

Proof. This is essentially Theorem 5.7 of [HR]. The second part follows from the fact that $\rho(p) = g$ unless $p|E$, in which case $\rho(p) < g$. □

Lemma 5. *For any real $\beta > 0$,*

$$\sum_{k \leqslant x} \left(\frac{k}{\phi(k)}\right)^\beta \ll_\beta x.$$

Proof. Write $(k/\phi(k))^\beta = \sum_{d|k} g(d)$, where g is the multiplicative function satisfying $g(p) = (p/(p-1))^\beta - 1$ for primes p and $g(p^a) = 0$ when $a \geqslant 2$. Then

$$\sum_{k \leqslant x} (k/\phi(k))^\beta = \sum_{d \leqslant x} g(d)[x/d] \leqslant x \prod_p (1 + g(p)/p) = c(\beta)x.$$

3. The main argument

Fix $a = 1$ or $a = -1$. The primes s counted in Lemma 3 have the property that $\omega(\frac{1}{2}(s-a)) \leqslant [1/\alpha]$. Therefore, there exists a number n $(1 \leqslant n \leqslant [1/\alpha] - 1)$ and some pair y, z with $x/16 \leqslant yz \leqslant x/2$, $y > x^\alpha$ such that

$$\#\{y < p \leqslant 2y, z < q \leqslant 2z : p, 2pq + a \text{ prime}, \omega(q) = n, P^-(q) > y\} \gg \frac{x}{\log^3 x}.$$

Denote by B the set of such pairs (p, q). From now on variables p, p_i will denote primes in $(y, 2y]$ and variables q, q_i will denote numbers in $(z, 2z]$ with n prime factors, each exceeding y. Implied constants in the following may depend on r, n or m.

Lemma 6. *The number of $2r$-tuples $(p_1, \dots, q_r)$ with each $(p_i, q_i) \in B$ which satisfy condition (i) but fail condition (ii) or (iii) (referring either to Lemma 1 or Lemma 2 and writing $p_i = p_{1,i}$ and $q_i = p_{i,2} \cdots p_{i,n}$) is*

$$\ll \frac{x^r (\log\log x)^{rn+4r-1}}{(\log x)^{5r-1}}.$$

Proof. We first count those $2r$-tuples satisfying (i) but failing (ii). When $a = 1$, all of the $2r$-tuples satisfy condition (ii) in Lemma 1, since $2p_{i,1}q_j + 1 \gg x$ and each $p_{i,j} \ll x^{1-\alpha}$. If condition (ii) of Lemma 2 fails, then $y/2 \leqslant \pi^b \leqslant 2^r t \leqslant (2x)^r$. Therefore, the number of $2r$-tuples not satisfying (ii) is bounded above by

$$\sum_{y/2 \leqslant \pi^b \leqslant (2x)^r} \frac{(2x)^r}{\pi^b} \ll x^r \sum_{b=2}^{\infty} \sum_{\pi \geqslant (y/2)^{1/b}} \frac{1}{\pi^b} \ll x^{r-\alpha/2}.$$

Counting the $2r$-tuples satisfying (i) but failing (iii) is a straightforward application of Lemma 4. First fix d_2 and the set of pairs (i, j) for which $p_{i,j} | d_1$ (there are finitely many such choices). Each of the numbers listed in (i) and (iii) are linear in all the variables $p_{i,j}$, thus applying Lemma 4 successively with the variables $p_{i,j}$ (in some order) gives the desired upper bound on their number.

We illustrate this process in the case $r = 3$, $n = 2$, $d_1 = p_{2,2}p_{2,3}p_{3,3}$, d_2 arbitrary. Fix distinct primes $p_{1,2}, p_{1,3}, p_{2,2}, p_{2,3}, p_{3,2}$. Since $p_{3,2} \ll z/y$, by Lemma 4 the number of primes $p_{3,3}$ such that $2d_2p_{2,2}p_{2,3}p_{3,3} + a$ is prime is

$$\ll \frac{z(\log\log x)^2}{p_{3,2}\log^2 x}.$$

Given $p_{3,3}$ (i.e. q_1, q_2, q_3 are fixed), the number of p_1 with $2p_1q_j + a$ prime $(j = 1, 2, 3)$ is $O(y(\log\log x)^4/\log^4 x)$, the number of p_2 with $2p_2q_j + a$ prime $(j = 1, 2)$ is $O(y(\log\log x)^3/\log^3 x)$ and the number of p_3 with $2p_3q_j + a$ prime $(j = 1, 3)$ is $O(y(\log\log x)^3/\log^3 x)$. Multiplying these together and summing over all $p_{i,j}$ $(i = 1, 2, 3; j = 2, 3)$ gives an upper bound of $O(x^3(\log\log x)^{13}/\log^{14} x)$ 6-tuples. □

Lemma 7. *The number of* $2r$*-tuples* $(p_1, \ldots, q_r)$*, with each* $(p_i, q_i) \in B$*, satisfying condition (i) of Lemma 1 or Lemma 2 is*

$$\gg \frac{x^r}{(\log x)^{5r-2}}.$$

Proof. Denote by P_j a generic j-tuple $(p_1, \ldots, p_j)$ with $p_1, \ldots, p_j$ distinct. Let $N_j(q)$ be the number of P_j such that $2p_iq + a$ is prime for each i, and let $M_j(P_j)$ be the number of q such that $2p_iq + a$ is prime for each i.

By the definition of B, we have

$$\sum_q N_1(q) = |B| \gg x/\log^3 x.$$

Therefore, by Hölder's inequality,

$$\begin{aligned} S := \sum_{P_r} M_r(P_r) = \sum_q N_r(q) = r! \sum_q \binom{N_1(q)}{r} \\ \gg \sum_{N_1(q) \geqslant r+1} N_1(q)^r \gg (z/\log z)^{1-r} \left(\sum_{N_1(q) \geqslant r+1} N_1(q) \right)^r \quad (1) \\ \gg \frac{x^r}{z^{r-1}(\log x)^{2r+1}}. \end{aligned}$$

Lemma 4 gives

$$M_r(P_r) \ll L(P_r) \frac{z}{(\log x)^{r+1}}, \tag{2}$$

where

$$L(P_j) := \prod_{1 \leqslant g < h \leqslant j} \frac{|p_g - p_h|}{\phi(|p_g - p_h|)}. \tag{3}$$

This follows from the fact that $r + 1 \geqslant \rho(p) \geqslant r + 1 - k_p$, where k_p is the number of pairs (i, j) with $i > j$ and $|p_i - p_j|$ divisible by p. Let A be the number of p, so that $A \asymp y/\log x$. Let $R(k; x)$ denote the number of primes $p \leqslant x - k$ for which $p + k$ is also prime. By Lemma 4, when $k \leqslant x/2$ we have

$$R(k; x) \ll \frac{x}{\log^2 x} \frac{k}{\phi(k)}.$$

Lemma 5 now gives

$$\sum_{y < p_1 < p_2 \leqslant 2y} L(p_1, p_2)^\beta \leqslant \sum_{k \leqslant y} \left(\frac{k}{\phi(k)} \right)^\beta R(k; 2y) \ll_\beta A^2.$$

Let $H = \binom{j}{2}$. Together with (3) and Hölder's inequality, we have

$$j!\binom{A}{j} \leqslant \sum_{P_j} L(P_j) \leqslant \prod_{1\leqslant g<h\leqslant j} \left(A^{j-2} \sum_{p_g, p_h} L(p_g, p_h)^H \right)^{1/H} \ll_j A^j \tag{4}$$

and similarly

$$\sum_{P_j} L^2(P_j) \ll_j A_j.$$

The upper bounds

$$S \ll \frac{zA^r}{(\log x)^{r+1}}$$

and

$$\sum_{P_r} M_r^2(P_r) \ll S^2 A^{-r} \tag{5}$$

now follow from (1), (2) and (4). Choose $\delta_0 > 0$ small enough so that

$$r!\binom{A}{r} \frac{\delta_0 z}{(\log x)^{r+1}} \leqslant \frac{S}{2}$$

and let P denote the set of P_r with

$$M_r(P_r) \geqslant \frac{\delta_0 z}{(\log x)^{r+1}}.$$

By (5) and the Cauchy-Schwarz inequality,

$$\begin{aligned} S &\leqslant \left(r!\binom{A}{r} - |P| \right) \frac{\delta_0}{(\log x)^{r+1}} + \sum_{P_r \in P} M_r(P_r) \\ &\leqslant \frac{S}{2} + O\left(|P|^{1/2} S A^{-r/2} \right), \end{aligned}$$

whence

$$|P| \gg A^r. \tag{6}$$

For each P_j, let $J_j(P_j)$ denote the number of P_{r-j} with $P_{r-j} \cap P_j = \emptyset$ and $(P_j, P_{r-j}) \in P$. Let δ_1 and δ_2 be sufficiently small positive constants, depending on r, but not on A. Let R denote the set of p such that $J_1(p) \geqslant \delta_1 A^{r-1}$. By (6), if δ_1 is small enough then $|R| \gg A$. If $p \in R$, denote by $T(p)$ the set of p' such that $J_2(p, p') \geqslant \delta_2 A^{r-2}$. If δ_2 is small enough, $|T(p)| \gg A$ uniformly in p. Choose δ_2 so that $\delta_2 < \frac{1}{2r}\delta_1$. We first show that

$$\sum_{\substack{p_1 \in R \\ p_2, \dots, p_r \in T(p_1) \\ (p_1, \dots, p_r) \in P}} M_r(p_1, p_2, \dots, p_r) \gg A^r \frac{z}{(\log x)^{r+1}}. \tag{7}$$

The functions M_j are symmetric in all variables, hence

$$\begin{aligned}\#\{(p_1,\cdots,p_r)\in P : p_1\in R; p_2,\dots,p_r\in T(p_1)\}\\ \geqslant \sum_{p_1\in R} J_1(p_1) - r \sum_{\substack{p_1\in R\\ p_2\notin T(p_1)}} J_2(p_1,p_2)\\ \geqslant |R|\delta_1 A^{r-1} - r|R|A(\delta_2 A^{r-2})\\ \geqslant \tfrac{1}{2}|R|\delta_1 A^{r-1} \gg A^r.\end{aligned}$$

Together with the definition of P, this proves (7). Next, if $p_1 \in R$ and $p_2 \in T(p_1)$, then by Lemma 4,

$$\begin{aligned}J_2(p_1,p_2)\delta_0 \frac{z}{(\log x)^{r+1}} &\leqslant \sum_{p_3,\cdots,p_r} M_r(p_1,\dots,p_r)\\ &= \sum_{q \text{ counted in } M_2(p_1,p_2)} N_{r-2}(q)\\ &\ll \left(\frac{y}{\log^2 x}\right)^{r-2} M_2(p_1,p_2),\end{aligned}$$

whence

$$M_2(p_1,p_2) \gg \frac{z}{\log^3 x}. \tag{8}$$

Let E denote the number of $2r$-tuples $(p_1,\dots,q_r)$ with $\gcd(q_i,q_j) > 1$ for some $i \neq j$. Using (7) and (8), the number of $2r$-tuples satisfying condition (i) of either Lemma 1 or Lemma 2 is at least

$$\begin{aligned}&\sum_{p_1,\cdots,p_r} M_r(p_1,\dots,p_r)\prod_{j=2}^{r} M_2(p_1,p_j) - E\\ &\geqslant \sum_{\substack{p_1\in R\\ p_2,\dots,p_r\in T(p_1)}} M_r(p_1,\dots,p_r)\prod_{j=2}^{r} M_2(p_1,p_j) - E\\ &\gg \left(\frac{z}{\log^3 x}\right)^{r-1} \sum_{\substack{p_1\in R\\ p_2,\dots,p_r\in T(p_1)}} M_r(p_1,\dots,p_r) - E\\ &\gg \frac{x^r}{(\log x)^{5r-2}} - E.\end{aligned}$$

Trivially $E \ll \frac{x^r}{y}$ and the lemma follows. □

For every $r \geqslant 2$, Lemmas 6 and 7 guarantee the existence of a set of primes $(p_{i,j})$ satisfying the hypotheses of Lemma 1 or Lemma 2. This completes the proof of Theorems 1 and 2.

The methods of this paper also apply to a wide class of multiplicative arithmetic functions. An exposition of some results will appear in section 9 of [F1].

References

[C1] Carmichael, R. D., *On Euler's ϕ-function.* Bull. Amer. Math. Soc. **13** (1907), 241–243.

[C2] — *Note on Euler's ϕ-function.* Bull. Amer. Math. Soc. **28** (1922), 109–110.

[D] Dickson, L. E., *A new extension of Dirichlet's theorem on prime numbers.* Messenger of Math. **33** (1904), 155–161.

[E] Erdös, P, *Some remarks on Euler's ϕ-function.* Acta Arith. **4** (1958), 10–19.

[F1] Ford, K, *The distribution of totients.* The Ramanujan J. **2**, nos. 1–2 (1998), 67–151.

[F2] — *The number of solutions of $\phi(x) = m$* Annals of Math. (to appear)

[HR] Halberstam, H., Richert, H.-E., Sieve Methods Academic Press, London 1974.

[SS] Schinzel, A.,Sierpiński, W., *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208.

[S1] Schinzel, A., *Sur l'equation $\phi(x) = m$*, Elem. Math. **11** (1956), 75–78.

[S2] — *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. **7** (1961/62), 1–8.