ON THE GREATEST COMMON DIVISOR OF A NUMBER AND ITS SUM OF DIVISORS

PAUL POLLACK

Abstract. As usual, let $\sigma(n)$ denote the sum of the positive divisors of n. We investigate the distribution of $\gcd(n, \sigma(n))$ on the natural numbers $n \leq x$. In particular, we both sharpen and correct some unproved assertions of Erdős, and we show that the average of $\gcd(n, \sigma(n))$ on the natural numbers $n \leq x$ is $x^{o(1)}$.

1. Introduction

A natural number n is called *perfect* if $\sigma(n) = 2n$ and *multiply perfect* whenever $\sigma(n)$ is a multiple of n. In 1956, Erdős published improved upper bounds on the counting functions of the perfect and multiply perfect numbers [Erd56]. These estimates were soon superseded by a theorem of Wirsing [Wir59] (Theorem B below), but Erdős's methods remain of interest as they are applicable to more general questions concerning the distribution of $\gcd(n, \sigma(n))$. Erdős describes some applications of this type (op. cit.) but omits the proofs. In this paper we prove corrected versions of his results, and we establish some new results in the same direction.

Our first theorem is the following:

Theorem 1.1. *Let $\beta > 0$. If $x > x_0(\beta)$ and $A > \exp((\log\log x)^\beta)$, then the number of $n \leq x$ for which $\gcd(n, \sigma(n)) > A$ is at most x/A^c, where $c = c(\beta) > 0$.*

This is (more or less) Theorem 3 of [Erd56], except that Erdős's assumptions correspond to the stronger hypothesis that $A > (\log x)^\beta$. After stating Theorem 3, Erdős asserts that if A grows slower than any power of $\log x$, then one cannot save a fixed power of A. Theorem 1.1 shows that this final assertion is not correct. We can however prove a result in the same direction which shows that Theorem 1.1 is best possible.

2000 *Mathematics Subject Classification.* 11N37.

The author is supported by NSF award DMS-0802970.

Theorem 1.2. *Let $\beta = \beta(x)$ be a positive real-valued function of x satisfying $\beta(x) \to 0$ as $x \to \infty$. Let $\epsilon > 0$. If x is sufficiently large (depending on ϵ and the choice of function β) and $2 \leq A \leq \exp((\log\log x)^{\beta})$, then the number of $n \leq x$ with $\gcd(n, \sigma(n)) > A$ is at least x/A^{ϵ}.*

If A is large, we obtain a stronger result than that furnished by Theorem 1.1 by estimating the mean value of $\gcd(n, \sigma(n))$:

Theorem 1.3. *For each $x \geq 3$, we have*

$$\sum_{n \leq x} \gcd(n, \sigma(n)) \leq x^{1+c_1/\sqrt{\log\log x}},$$

where c_1 is an absolute positive constant.

For example, it follows immediately from Theorem 1.3 that if $A \geq x^{\delta}$ (for a fixed $\delta > 0$), then the number of solutions to $\gcd(n, \sigma(n)) > A$ is at most $x/A^{1+o(1)}$ as $x \to \infty$.

For large A the above results supply no lower bound on the number of solutions to $\gcd(n, \sigma(n)) > A$. In fact, it is possible to establish such a bound in a wide range of A:

Theorem 1.4. *Fix $\epsilon > 0$. The number of $n \leq x$ with $\gcd(n, \sigma(n)) > A$ is at least $x/A^{1+o(1)}$ as $x \to \infty$, uniformly for $2 \leq A \leq x^{1-\epsilon}$.*

It seems interesting to observe that Theorems 1.3 and 1.4 have the following immediate consequence:

Corollary 1.5. *For each fixed $\delta \in (0, 1)$, the number of $n \leq x$ for which $\gcd(n, \sigma(n)) > x^{\delta}$ is $x^{1-\delta+o(1)}$ as $x \to \infty$.*

Notation. For the most part we use standard notation of analytic number theory. As usual, we write $\omega(n)$ for the number of distinct prime factors of n, $\mathrm{rad}(n)$ for the product of the distinct primes dividing n, and $\Psi(x, y)$ for the number of $n \leq x$ all of whose prime divisors are $\leq y$. We put $\log_1 x := \max\{\log x, 1\}$, and we define inductively $\log_k x = \max\{1, \log_{k-1} x\}$. We emphasize that when 'c' is used with a subscript, it always refers to an absolute positive constant.

2. Proof of Theorem 1.1

We require several preliminaries. Theorem A below assembles results due to Kátai & Subbarao (see [KS06, Theorem 1]) and Erdős, Luca, and Pomerance (cf. [ELP08, Theorem 8, Corollary 10]). See also [Erd56, Theorem 4].

Theorem A. *For all natural numbers n outside of a set of density zero,* $\gcd(n, \sigma(n))$ *is the largest divisor of n supported on the primes not exceeding* $\log\log n$*.*

For each real u, the set of n with $\gcd(n, \sigma(n)) > (\log\log n)^u$ *possesses a natural density $g(u)$. The function $g(u)$ is continuous everywhere, strictly decreasing on $[0, \infty)$ and satisfies $g(0) = 1$ and $\lim_{u\to\infty} g(u) = 0$. Explicitly we have*

$$g(u) := e^{-\gamma} \int_u^\infty \rho(t)\, dt$$

for all $u > 0$, where γ is the Euler-Mascheroni constant and ρ is the Dickman-de Bruijn function.

The next lemma is proved by Erdős and Nicolas as [EN80, Théorème 2], except for the statement concerning uniformity, which however is clear from their proof.

Lemma 2.1. *For each fixed $c \in (0, 1]$, the number of $n \le x$ with*

$$\omega(n) > c\frac{\log x}{\log_2 x}$$

is $x^{1-c+o(1)}$ as $x \to \infty$. Moreover, the convergence of the $o(1)$ term to zero is uniform if c is restricted to any compact subset of $(0, 1]$.

The next result is implicit in the proof of [Erd56, Theorem 1]; for the convenience of the reader we repeat the argument here.

Lemma 2.2. *Let $\epsilon > 0$. If $m > m_0(\epsilon)$ is squarefree, then there exists $d \mid m$ with $\gcd(d, \sigma(d)) = 1$ and $d \ge m^{1/2-\epsilon}$.*

Proof. By replacing m by $m/2$ if necessary, we may assume that m is odd. We now run the following algorithm: Put $d_0 = 1$ and $d_0' = m$. Having defined d_i and d_i' so that $d_i d_i' = m$ and $\gcd(d_i, \sigma(d_i)) = 1$, we proceed as follows: If there is a prime dividing d_i' which does not divide $\sigma(d_i)$, then let p be the largest such prime and set $d_{i+1} = d_i p$ and $d_{i+1}' = d_i'/p$. (If there is no such prime, terminate the algorithm.) Then $d_{i+1}d_{i+1}' = m$ and

$$\begin{aligned}\gcd(d_{i+1}, \sigma(d_{i+1})) &= \gcd(d_i p, \sigma(d_i)(p + 1)) \\ &= \gcd(d_i, p + 1),\end{aligned}$$

since $p \nmid \sigma(d_i)$ and $\gcd(d_i, \sigma(d_i)) = 1$. Since p is odd (by our assumption that m is odd), every prime factor q of $p+1$ is smaller than p. None of these q can divide d_i: Indeed, if q divides d_i, then there must be some $j < i$ for which q is the largest prime divisor of d_j' not dividing $\sigma(d_j)$. But this is absurd: $q < p$, p is a divisor of d_j' (since d_i' divides d_j') and

$p \nmid \sigma(d_j)$ (since $d_j \mid d_i$ and $p \nmid \sigma(d_i)$). Thus $\gcd(d_i, p+1) = 1$ and so $\gcd(d_{i+1}, \sigma(d_{i+1})) = 1$.

At the end of this algorithm we have numbers d_k, d_k' with $d_k d_k' = m$ and $\gcd(d_k, \sigma(d_k)) = 1$. Moreover, d_k' must divide $\sigma(d_k)$, otherwise we could continue the algorithm. It follows immediately that

$$d_k^2 \geq \sigma(d_k) \geq d_k', \quad \text{whence} \quad d_k^3 \geq d_k d_k' = m,$$

so that $d_k \geq m^{1/3}$. This shows that d_k is large whenever m is large. As a consequence, $\sigma(d_k) \leq d_k^{1+\epsilon}$ for large m, and now we can deduce that

$$d_k^{1+\epsilon} \geq \sigma(d_k) \geq d_k', \quad \text{whence} \quad d_k^{2+\epsilon} \geq m,$$

so that $d_k \geq m^{1/(2+\epsilon)} \geq m^{1/2-\epsilon}$ if ϵ is small (which may be assumed). So if we choose $d = d_k$, then we have the lemma. $\square$

The next lemma is an easy consequence of the Brun-Titchmarsh inequality; for a proof see, e.g., [Kát91, Lemma 6].

Lemma 2.3. *Let m be a positive integer. For all $x \geq 1$, we have*

$$\sum_{\substack{p \leq x \\ p \equiv -1 \pmod m}} \frac{1}{p} \ll \frac{\log_2 x}{\varphi(m)}.$$

Here the implied constant is absolute.

Lemma 2.4. *Let d be a squarefree integer. For $x \geq 1$, the number of squarefree $n \leq x$ for which for which d divides $\sigma(n)$ is at most*

$$\omega(d)^{\omega(d)} \frac{x}{\varphi(d)} (C \log_2 x)^{\omega(d)},$$

where C is an absolute positive constant.

Proof. Since d divides $\sigma(n) = \prod_{p \mid n} (p+1)$, we can write $d = \prod_{p \mid n} a_p$, where each a_p divides $p+1$. Throwing away those $a_p = 1$, we see that n induces a (not necessarily unique) factorization of d, where by a *factorization* of d we mean a decomposition of d as a product of factors strictly larger than 1, where the order of the factors is not taken into account. For each possible factorization of d, we estimate the number of $n \leq x$ as in the lemma statement which induce this factorization.

Let $d = a_1 a_2 \cdots a_k$ be a factorization of d. If n induces this factorization, then there are distinct primes $p_1, \dots, p_k$ dividing n with $p_i \equiv -1 \pmod{a_i}$ for each $1 \leq i \leq k$. So by Lemma 2.3, with C an appropriate absolute positive constant, the number of such $n \le x$ is

$$\begin{aligned}\le \sum_{p_1 \equiv -1 \pmod{a_1}} \cdots \sum_{p_k \equiv -1 \pmod{a_k}} \frac{x}{p_1 \cdots p_k} \\ \le x \prod_{i=1}^{k} \frac{C \log_2 x}{\varphi(a_i)} = \frac{x}{\varphi(d)} (C \log_2 x)^k \le \frac{x}{\varphi(d)} (C \log_2 x)^{\omega(d)}.\end{aligned}$$

(The last inequality uses the observation that each factorization of d involves at most $\omega(d)$ factors.) Since d is squarefree, the number of factorizations of d is given by $B_{\omega(d)}$, where B_l (the lth *Bell number*) stands for the number of set-partitions of an l-element set.

Since any partition of an l-element set involves at most l components, we have always have $B_l \le l^l$. Taking $l = \omega(d)$ completes the proof of Lemma 2.4. □

The last part of our preparation consists in reducing the proof of Theorem 1.1 to that of the following squarefree version:

Proposition 2.5. *Let $\beta > 0$. If $x > x_1(\beta)$ and $A > \exp((\log_2 x)^\beta)$, then the number of* squarefree $n \le x$ *with* $\gcd(n, \sigma(n)) > A$ *is at most $x/A^{c'}$, where $c' = c'(\beta)$.*

Lemma 2.6. *Theorem 1.1 follows from Proposition 2.5.*

Proof. Let $\beta > 0$. Suppose that $n \le x$ and $\gcd(n, \sigma(n)) > A$ where $A > \exp((\log_2 x)^\beta)$. Write $n = n_0 n_1$, where n_0 is squarefree, n_1 is squarefull, and $\gcd(n_0, n_1) = 1$. If $n_1 > A^{1/4}$, then n belongs to a set of size at most $x \sum_{\substack{m > A^{1/4} \\ m \text{ squarefull}}} 1/m \ll x/A^{1/8}$. Otherwise, since

$$\begin{aligned}A &< \gcd(n_0 n_1, \sigma(n_0)\sigma(n_1)) \\ &\le \gcd(n_0, \sigma(n_0)) \gcd(n_0, \sigma(n_1)) \gcd(n_1, \sigma(n_0)\sigma(n_1)) \\ &\le \gcd(n_0, \sigma(n_0)) n_1 \sigma(n_1) \le \gcd(n_0, \sigma(n_0)) n_1^3,\end{aligned}$$

it follows that

$$\gcd(n_0, \sigma(n_0)) \ge A/n_1^3 \ge A^{1/4}.$$

The number of such $n \le x$ is therefore at most

$$\sum_{\substack{n_0 \le x \\ n_0 \text{ squarefree} \\ \gcd(n_0, \sigma(n_0)) > A^{1/4}}} \sum_{\substack{n_1 \le x/n_0 \\ n_1 \text{ squarefull} \\ \gcd(n_0, n_1) = 1}} 1 \ll \sqrt{x} \sum_{\substack{n_0 \le x \\ n_0 \text{ squarefree} \\ \gcd(n_0, \sigma(n_0)) > A^{1/4}}} \frac{1}{\sqrt{n_0}}. \tag{1}$$

Define

$$B(u) := \sum_{\substack{m \le u \\ m \text{ squarefree} \\ \gcd(m,\sigma(m)) > A^{1/4}}} 1.$$

Since $A^{1/4} > \exp(\frac{1}{4}(\log_2 x)^{\beta}) > \exp((\log_2 x)^{\beta/2})$ for large x, we can apply Proposition 2.5 with β replaced by $\beta/2$ to find that $B(u) \le u/A^{c'/4}$, where $c' = c'(\beta/2)$ and the inequality holds for all $u \le x$ which are large enough (depending just on β). Partial summation now shows that for sufficiently large x (depending just on β), the final sum in (2.5) is $\ll x^{1/2}/A^{c'/4}$, so that the double sum in (1) is $\ll x/A^{c'/4}$.

It follows that Theorem 1.1 holds if $c = c(\beta)$ is chosen as any constant smaller than $\min\left\{\frac{1}{8}, \frac{1}{4}c'(\beta/2)\right\}$. $\square$

We now prove Proposition 2.5 (and so also Theorem 1.1). Assume $\beta > 0$, $A > \exp((\log_2 x)^{\beta})$, and n is a squarefree integer with $\gcd(n, \sigma(n)) > A$. Put $D := \gcd(n, \sigma(n))$.

If there is a prime $p > A^{1/2}$ dividing D, then n has the form pr, where $p \mid \sigma(r)$. By Lemma 2.4, the number of possible r is

$$\ll \frac{x/p}{\varphi(p)} \log_2 x \ll \frac{x \log_2 x}{p^2},$$

so that the number of n that can arise this way is

$$\ll x \log_2 x \sum_{p > A^{1/2}} \frac{1}{p^2} \ll \frac{x \log_2 x}{A^{1/2}}.$$

This number is smaller than $x/A^{1/3}$ for large x (depending on β).

We may therefore assume that the largest prime dividing D is at most $A^{1/2}$. Since $D > A$, successively stripping primes from D, we must eventually discover a divisor of D in the interval $(A^{1/2}, A]$. If x (and hence A) is large, we can apply Lemma 2.2 (with $\epsilon = 1/6$) to this divisor to obtain a divisor d of D with $d \in (A^{1/6}, A]$ having the property that $\gcd(d, \sigma(d)) = 1$.

Write $n = de$. Since $d \mid \sigma(n)$ and $\gcd(d, \sigma(d)) = 1$, it follows that $e \le x/d$ and $d \mid \sigma(e)$. By Lemma 2.4, the number of such e is at most

$$\frac{x}{d\varphi(d)} (C\omega(d) \log_2 x)^{\omega(d)} \tag{2}$$

The strategy for the remainder of the proof is as follows: First, if d does not have too many distinct prime divisors, then the bound (2) is manageable, and summing over such d yields an acceptable bound on the number of corresponding n. Otherwise, n is divisible by some

$d \in (A^{1/6}, A]$ with an abnormally large number of prime divisors, and Lemma 2.1 implies that such n are rare.

Let c be a small constant whose value will be chosen momentarily. Suppose that

$$\omega(d) < c\frac{\log A}{\log\log A}.$$

Then (for large x)

$$(C\omega(d)\log_2 x)^{\omega(d)} \le \exp\left(c\frac{\log A}{\log_2 A}(\log_2 A + \log_3 x)\right).$$

Since $A > \exp((\log_2 x)^\beta)$, we have $\log_2 A > \beta \log_3 x$, so this upper bound is at most

$$\exp(c(1+\beta^{-1})\log A) = A^{c(1+\beta^{-1})}.$$

We now assume $c > 0$ is small enough that $c(1+\beta^{-1}) \le 1/12$. Then summing (2) over these values of d, we obtain an upper bound on the number of corresponding n which is at most

$$xA^{1/12}\sum_{d>A^{1/6}}\frac{1}{d\varphi(d)} \ll x/A^{1/12}.$$

The remaining n have a divisor $d \in (A^{1/6}, A]$ for which $\omega(d) > c\log A/\log\log A$, and the number of such n is at most $x\sum 1/d$ taken over these d. Let

$$B(u) := \sum_{\substack{m\le u\\ \omega(m)>c\log A/\log_2 A}} 1.$$

For $A^{1/6} \le u \le A$, define d_u so that

$$d_u\frac{\log u}{\log_2 u} = \frac{\log A}{\log_2 A}, \quad \text{so that} \quad d_u = (1+o(1))\frac{\log A}{\log u}.$$

By Lemma 2.1, for these u we have

$$B(u) = u^{1-cd_u+o(1)} = u^{1-c\log A/\log u}A^{o(1)} = (u/A^c)A^{o(1)} \le u/A^{c/2},$$

say. (Note that for large x, the real number cd_u belongs to the compact subinterval $[c/2, 12c]$ of $(0,1]$.) Thus

$$\sum_{\substack{d\in(A^{1/6},A]\\ \omega(d)>c\log A/\log_2 A}}\frac{1}{d} = \frac{B(A)}{A} - \frac{B(A^{1/6})}{A^{1/6}} + \int_{A^{1/6}}^{A}\frac{B(t)}{t^2}\,dt$$

$$\ll A^{-c/2} + (\log A)A^{-c/2} \ll A^{-c/3},$$

say.

Piecing everything together, it follows that the number of $n \le x$ with $\gcd(n, \sigma(n)) > A$ is at most $x/A^{c'(\beta)}$ for large x, if we choose $c'(\beta) < \min\left\{\frac{1}{3}c, \frac{1}{12}\right\}$.

3. Proof of Theorem 1.2

We begin by recalling some results from the theory of smooth numbers. Let $\Psi(x, y)$ denote the number of y-smooth positive integers $n \le x$, where n is called *y-smooth* if each prime p dividing n satisfies $p \le y$. Let $\Psi_2(x, y)$ denote the number of squarefree y-smooth numbers $n \le x$. The following estimate of de Brujin appears as [Ten95, Theorem 2, p. 359]:

Lemma 3.1. *Uniformly for $x \ge y \ge 2$,*

$$\log \Psi(x, y) = Z\left(1 + O\left(\frac{1}{\log y} + \frac{1}{\log_2 2x}\right)\right),$$

where

$$Z := \frac{\log x}{\log y} \log\left(1 + \frac{y}{\log x}\right) + \frac{y}{\log y} \log\left(1 + \frac{\log x}{y}\right).$$

The following result is due to Ivić and Tenenbaum [IT86] and Naimi [Nai88] (independently).

Lemma 3.2. *Whenever $x, y \to \infty$, and $\log y/\log_2 x \to \infty$, we have $\Psi_2(x, y) = (6/\pi^2 + o(1))\Psi(x, y)$.*

The next lemma is due to Pomerance (cf. [Pom77, Theorem 2]).

Lemma 3.3. *Let $x \ge 3$ and let m be a positive integer. The number of $n \le x$ for which $m \nmid \sigma(n)$ is $\ll x/(\log x)^{1/\varphi(m)}$, where the implied constant is absolute.*

We now have all the tools at our disposal necessary to prove Theorem 1.2. By Theorem A we may assume that

$$\log_2 x < A < \exp((\log_2 x)^{\beta(x)}). \tag{3}$$

Put $y := (\log_2 x)^{1-\sqrt{\beta(x)}}$.

Lemma 3.4. *If x is sufficiently large (depending on the choice of the function β), then all but at most x/A numbers $n \le x$ are such that $\sigma(n)$ is divisible by every prime $p \le y$.*

Proof. By Lemma 3.3, the number of exceptional n is

$$\ll y \frac{x}{(\log x)^{1/y}} \le (\log_2 x) \frac{x}{\exp((\log_2 x)^{\sqrt{\beta}})}.$$

To see that this is at most x/A, note that by the upper bound on A in (3) and a short computation, it is enough to prove that

$$\log_3 x - (\log_2 x)^{\sqrt{\beta}} < -(\log_2 x)^{\beta}.$$

From (3), we have that that $(\log_2 x)^{\beta} > \log_3 x$, so that for large x,

$$\begin{aligned}(\log_2 x)^{\sqrt{\beta}} - (\log_2 x)^{\beta} &= ((\log_2 x)^{\beta})^{1/\sqrt{\beta}} - (\log_2 x)^{\beta} \\ &> ((\log_2 x)^{\beta})^2 - (\log_2 x)^{\beta} \\ &> (\log_3 x)^2 - \log_3 x > \log_3 x,\end{aligned}$$

which gives the lemma. □

Lemma 3.5. *If x is sufficiently large (depending on β and ϵ), then the number of positive integers $n \le x$ which have a squarefree, y-smooth divisor in the interval $(A, A^2]$ is at least $x/A^{\epsilon/2}$.*

Proof. Let $P_y := \prod_{p \le y} p$ be the product of the primes not exceeding y. The number of $n \le x$ with a squarefree, y-smooth divisor $d \in (A, A^2]$ is at least

$$\sum_{\substack{d \mid P_y \\ A < d \le A^2}} \sum_{\substack{n \le x \\ d \mid n, (n/d, P_y) = 1}} 1. \tag{4}$$

By inclusion-exclusion and Mertens's theorem, for each d in the outer sum, the inner sum is

$$(x/d)\frac{e^{-\gamma}}{\log y} + O(2^{\log_2 x}) = (e^{-\gamma} + o(1))\frac{x}{d \log_3 x},$$

and so the double-sum (4) is

$$\gg \frac{x}{\log_3 x} \sum_{\substack{d \mid P_y \\ A < d \le A^2}} \frac{1}{d} \ge \frac{x}{\log_3 x}\frac{1}{A^2}(\Psi_2(A^2, y) - A). \tag{5}$$

We have

$$\log y / \log_2(A^2) \ge (1 + o(1)) \log_3 x / (\beta(x) \log_3 x + \log 2),$$

which tends to infinity with x since $\beta(x)$ tends to zero. So by Lemma 3.2, we have that $\Psi_2(A^2, y) \sim (6/\pi^2)\Psi(A^2, y)$. Since $\log(A^2) = y^{o(1)}$, Lemma 3.1 implies that

$$\Psi(A^2, y) \ge \exp\left((1 + o(1)) \log\left(A^2\right)\right) = A^{2+o(1)}.$$

Referring back to (5), we find that the double sum (4) is bounded below by $(x/\log_3 x)A^{o(1)}$, which is at least $xA^{o(1)}$ since $A \ge \log_2 x$. □

Theorem 1.2 follows immediately from Lemmas 3.4 and 3.5: Indeed, with at most x/A exceptions, any n with a divisor of the form prescribed in Lemma 3.5 will satisfy $\gcd(n, \sigma(n)) > A$. Since there are at least

$$x/A^{\epsilon/2} - x/A > x/A^{\epsilon}$$

such n, we have Theorem 1.2.

4. Proof of Theorem 1.3

The proof rests on the following theorem of Wirsing [Wir59]:

Theorem B. *For each $x \geq 3$ and every pair of positive integers a and b, the number of $n \leq x$ for which $a(n) = a$ and $b(n) = b$ is at most*

$$x^{c_2/\log\log x}.$$

Here c_2 denotes an absolute positive constant.

For our purposes, we require a variant of Theorem A where only the denominator is specified. Perhaps surprisingly, such a variant can be derived from Theorem A by a simple inductive argument:

Theorem 4.1. *For each $x \geq 3$ and each positive integer b, the number of $n \leq x$ for which $b(n) = b$ is at most*

$$x^{c_3/\sqrt{\log\log x}}.$$

Here c_3 is an absolute positive constant.

Let us suppose temporarily that Theorem 4.1 has been established. Then we can quickly dispense with Theorem 1.3 following a method of Erdős, Luca, and Pomerance (cf. the proof of the upper bound in [ELP08, Theorem 11]). Indeed, for $x \geq 1$,

$$\begin{aligned} \frac{1}{x}\sum_{n \leq x} \gcd(n, \sigma(n)) \leq \sum_{n \leq x} \frac{\gcd(n, \sigma(n))}{n} &= \sum_{b \leq x} \frac{1}{b} \sum_{\substack{n \leq x \\ b(n) = b}} 1 \\ &\leq (1 + \log x) x^{c_3/\sqrt{\log_2 x}} \leq x^{c_1/\sqrt{\log_2 x}} \end{aligned}$$

for an appropriate constant c_1. So it is enough to prove Theorem 4.1.

Lemma 4.2. *Suppose $x \geq 1$. For each positive integer $b \leq x$, the number of $n \leq x$ with $\mathrm{rad}(n) \mid b$ is at most $x^{c_4/\log_2 x}$.*

Lemma 4.2 is proved by Erdős et al. in the course of demonstrating [ELP08, Theorem 11]. For the convenience of the reader we extract their argument and present it here:

Proof of Lemma 4.2. The number of such $n \le x$ is maximized when b is the largest product of consecutive primes (starting at 2) not exceeding x. In this case the number of such n is precisely $\Psi(x,p)$, where p is the largest prime divisor of b. By the prime number theorem, $p \sim \log x$, and by Lemma 3.1, $\Psi(x,p) = x^{(\log 4+o(1))/\log_2 x}$ as $x \to \infty$. $\square$

Proof of Theorem 4.1. It is well-known (see, e.g., [HW79, Theorem 323]) that $\sigma(n)/n \le (e^\gamma + o(1))\log_2 n$. Fix $x_0 > e^{2e}$ with the property that for all $x \ge x_0$, we have

$$\sigma(n)/n \le 2\log_2 x$$

for all positive integers $n \le x$. We prove that for each integer $N \ge 2$, each $x > x_0^{N/2}$ and each positive integer b, the number of $n \le x$ for which $b(n) = b$ is bounded by

$$x^{1/N + c_5 N/\log_2 x}.$$

Theorem 4.1 follows for large x upon choosing $N = \lfloor \sqrt{\log_2 x} \rfloor$. This implies the same result for all $x \ge 3$ with a possibly different constant in the exponent.

We proceed by induction on N. Suppose first that $N = 2$. If $b(n) = b$, then b divides n, and so we can assume $b \le x^{1/2}$ since otherwise we obtain an even sharper upper bound of $x^{1/2}$. Since $x > x_0$, the relation $b(n) = b$ implies that

$$\sigma(n)/n \in \{a/b : b \le a \le 2x^{1/2}\log_2 x\}.$$

By Wirsing's theorem (Theorem B), we know that the number of $n \le x$ with this property is at most

$$2x^{1/2}(\log_2 x)x^{c_2/\log_2 x} \le x^{1/2}x^{2c_5/\log_2 x}$$

if c_5 is chosen appropriately (depending on x_0 and c_2).

Suppose the estimate is known for N; we prove it holds also for $N+1$. If $b \le x^{1/(N+1)}$, then we can apply Wirsing's theorem as above to obtain that the number of $n \le x$ with $b(n) = b$ is bounded by

$$2x^{1/(N+1)}(\log_2 x)x^{c_2/\log_2 x} \le x^{1/(N+1)}x^{(N+1)c_5/\log_2 x}.$$

So we may suppose $b \ge x^{1/(N+1)}$. We also assume $b \le x$, since otherwise there are no solutions $n \le x$ to $b(n) = b$. Let d denote the largest divisor of n supported on the primes dividing b. Since $b \mid n$, we have $b \mid d$. Moreover, if $n = dn'$, then

$$n' = n/d \le x/b \le x^{N/(N+1)}$$

and

$$\frac{\sigma(n')}{n'} = \frac{d}{\sigma(d)}\frac{\sigma(n)}{n} = \frac{d}{\sigma(d)}\frac{a}{b}$$

where $a = a(n)$. In particular, $b(n')$ divides $\sigma(d)b$. Let b' be a divisor of $\sigma(d)b$. Since

$$x^{N/(N+1)} \geq (x_0^{(N+1)/2})^{N/(N+1)} = x_0^{N/2},$$

the induction hypothesis implies that for each b' dividing $\sigma(d)b$, there are at most

$$(x^{N/(N+1)})^{1/N} x^{c_5 N/\log_2 x} = x^{1/(N+1)} x^{c_5 N/\log_2 x}$$

choices for $n' \leq x^{N/(N+1)}$ with $b(n') = b'$. (We have also used here that $x^{N/(N+1)} > e^e$, and that the function $t^{1/\log_2 t}$ is increasing for $t > e^e$.) The maximal order of the divisor function (see, e.g., [HW79, Theorem 317]) guarantees that the number of choices for b', given d, is bounded by $x^{c_6/\log_2 x}$, while by Lemma 4.2, the number of choices for d is bounded by $x^{c_4/\log_2 x}$. It follows that the number of choices for $n = dn'$ is at most

$$x^{1/(N+1)} x^{(c_5 N + (c_6 + c_4))/\log_2 x} \leq x^{1/(N+1)} x^{c_5(N+1)/\log_2 x},$$

if we choose c_5 so that $c_5 \geq c_6 + c_4$. □

Remark. Suppose $f\colon \mathbf{N} \to \mathbf{N}$ is a multiplicative function. Say that f has *property* W if the following holds (for each $\epsilon > 0$):

> For $x > x_0(\epsilon)$, the number of $n \leq x$ with $f(n)/n = a/b$ is bounded by x^ϵ, uniformly in the choice of positive integers a and b.

Say that f has *property* W' if the following holds (for each $\epsilon > 0$):

> For $x > x_1(\epsilon)$, the number of $n \leq x$ for which n divides $bf(n)$ is bounded by x^ϵ, uniformly for positive integers $b \leq x$.

Wirsing's argument establishes that *property* W holds for a large class of multiplicative functions (see, e.g., [Luc76] for a general statement as well an extension to to certain compositions of multiplicative functions). The proof of Theorem 4.1 shows that if f has property W and $f(n) \ll_\rho n^{1+\rho}$ for each $\rho > 0$, then f also has property W'.

5. Proof of Theorem 1.4

It is convenient to divide the proof of Theorem 1.4 into two parts depending on the size of A. Clearly the theorem will follow from the following two propositions:

Proposition 5.1. *There is an absolute constant $c_7 > 0$ for which the following holds: For each fixed $\epsilon > 0$ and each $A \in [2, x^{c_7}]$, the number of $n \leq x$ for which $\gcd(n, \sigma(n)) > A$ is at least $x/A^{1+\epsilon}$ if x is sufficiently large (depending only on ϵ).*

Proposition 5.2. *Fix $\epsilon > 0$. The number of $n \le x$ for which*

$$\gcd(n, \sigma(n)) > A \tag{6}$$

is at least $x/A^{1+o(1)}$ as $x \to \infty$, uniformly for $x^{\epsilon} \le A \le x^{1-\epsilon}$.

We begin with the proof of Proposition 5.1.

Proof. Fix $0 < \epsilon < 1$. As in the proof of Theorem 1.2, we can assume $A \ge \log_2 x$, since for smaller A the result follows from Theorem A. We claim that there is an absolute constant $c_7 > 0$ for which the following holds: If x is sufficiently large (depending on ϵ), then there are at least $x/A^{1+2\epsilon}$ positive integers $m \le x/A^{1+\epsilon}$ possessing both of the following properties:

(1) there is a prime $q \parallel m$ for which $q + 1$ has a prime divisor in $(A, A^{1+\epsilon}]$,
(2) the least prime divisor of m exceeds $A^{1+\epsilon}$.

Once this is proved the theorem follows easily: Indeed, for each such m, choose a prime $q \parallel m$ for which $q + 1$ has a prime divisor $p \in (A, A^{1+\epsilon}]$ and form the number $n = mp$. Then $n \le x$,

$$p \mid n \quad \text{and} \quad p \mid q + 1 \mid \sigma(n), \quad \text{so that} \quad \gcd(n, \sigma(n)) \ge p > A.$$

Moreover, condition (2) guarantees that the numbers n formed in this way are all distinct. Thus there are at least $x/A^{1+2\epsilon}$ values of $n \le x$ for which $\gcd(n, \sigma(n)) > A$. Replacing ϵ by $\epsilon/2$ we have the theorem.

The proof of the claim proceeds in stages. Put

$$\mathcal{Q} := \{q \text{ prime} : q + 1 \text{ has a prime divisor in } (A, A^{1+\epsilon}]\},$$

and let $Q(y) := \#(\mathcal{Q} \cap [1, y])$. Let us estimate the number of $q \le y$ which are *not* in $\mathcal{Q}$. Suppose M is fixed; then by the fundamental lemma of the sieve (see, e.g., [HR74, Theorem 2.5′]), for $y \ge A^{2M}$ and x sufficiently large, the number of such q is

$$\le (1 + \delta_M) \left(\prod_{A < p \le A^{1+\epsilon}} \frac{p-2}{p-1} \right) \mathrm{Li}(y),$$

where $\delta_M \to 0$ as $M \to \infty$. Since ϵ is fixed, the product here tends to a constant $B(\epsilon) < 1$ as x (and hence A) tends to infinity. We now fix M so large that $(1 + \delta_M)B(\epsilon) < 1$. For this choice of M, the proportion of primes $\le y$ not in $\mathcal{Q}$ is strictly less than 1; thus $Q(y) \gg \mathrm{Li}(y)$ whenever $y \ge A^M$ and x is sufficiently large.

This lower bound is used to estimate the number of $m \le x/A^{1+\epsilon}$ having properties (1) and (2) above. By the fundamental lemma of the sieve (this time see, e.g., [HR74, Theorem 2.5]), if $A \le x^{c_7}$ where c_7 is a sufficiently small absolute constant, then the number of $m \le x/A^{1+\epsilon}$ having property (2) above is at least

$$\frac{1}{2}\frac{x}{A^{1+\epsilon}}\prod_{p\le A^{1+\epsilon}}(1-1/p) \tag{7}$$

for large x.

If we require that m not only have property (2) but also have no prime divisors in $\mathcal{Q}$ exceeding A^M, then the number of such $m \le x/A^{1+\epsilon}$ is (by Brun's sieve; see, e.g., [HR74, Theorem 2.2])

$$\ll \frac{x}{A^{1+\epsilon}}\prod_{p\le A^{1+\epsilon}}(1-1/p)\prod_{\substack{A^M\le q\le x/A^{1+\epsilon}\\ q\in\mathcal{Q}}}(1-1/q),$$

where the implied constant is absolute. Here the product over the primes in $\mathcal{Q}$ is

$$\le \exp\Bigg(-\sum_{\substack{A^M\le q\le x/A^{1+\epsilon}\\ q\in\mathcal{Q}}}\frac{1}{q}\Bigg).$$

Since $\mathcal{Q}(y) \gg \mathrm{Li}(y)$ for $y \ge A^M$, partial summation shows that the sum inside the exponential can be made arbitrarily large by choosing c_7 sufficiently small (perhaps depending on M). So if c_7 is fixed sufficiently small, the number of m satisfying both conditions is at most

$$\frac{1}{4}\frac{x}{A^{1+\epsilon}}\prod_{p\le A^{1+\epsilon}}(1-1/p).$$

Comparing this with (7), we see that there are at least

$$\frac{1}{4}\frac{x}{A^{1+\epsilon}}\prod_{p\le A^{1+\epsilon}}(1-1/p) \gg \frac{x}{A^{1+\epsilon}\log A} \tag{8}$$

positive integers $m \le x/A^{1+\epsilon}$ with property (2) and which have some prime divisor in $\mathcal{Q}$ exceeding A^M. But such an m has property (1) unless m is divisible by q^2 for some $q \in \mathcal{Q}$ exceeding A^M, and the number of such m is

$$\ll \frac{x}{A^{1+\epsilon}}\sum_{q>A^M}\frac{1}{q^2} \ll \frac{x}{A^{1+\epsilon+M}},$$

which is negligible compared to the lower bound (8).

So there are $\gg x/(A^{1+\epsilon}\log A)$ values of $m \le x/A^{1+\epsilon}$ with both properties (1) and (2), which suffices to yield the claim. $\square$

The proof of Proposition 5.2 requires some preliminary results. Let ψ denote the Dedekind ψ function, which is the arithmetic function defined by $\psi(n) := n\prod_{p|n}(1+1/p)$. (Thus $\psi \le \sigma$ pointwise, and ψ and σ agree on squarefree arguments.) For each integer $K \ge 0$, define

$$F_K(n) := \prod_{0\le k\le K} \psi_k(n),$$

where ψ_k denotes the kth iterate of ψ. We need the following lemma:

Lemma 5.3. *Let K be a fixed nonnegative integer. For each positive integer n, write*

$$F_K(n) = MN, \quad \textit{where} \quad M := \prod_{\substack{p^e \| F_K(n) \\ p\le \log^3 x}} p^e \textit{ and } N := \prod_{\substack{p^e \| F_K(n) \\ p> \log^3 x}} p^e.$$

Then for all but $o(x)$ values of $n \le x$, we have that N is squarefree and

$$M \le \exp(2(5\log_2 x)^{K+2}) = x^{o(1)}.$$

With the Euler function φ in place of ψ, this is established by Luca and Pomerance (see [LP07, §3.2]). The same argument applies, with obvious changes, to prove Lemma 5.3.

Put $R_K(n) := \mathrm{rad}(F_K(n))$.

Lemma 5.4. *Let K be a fixed positive integer. Then for all but $o(x)$ values of $n \in [x/2, x]$, we have*

$$R_K(n) = x^{K+1+o(1)}$$

and

$$\gcd(R_K(n), \psi(R_K(n))) > x^{K+o(1)}.$$

Proof. For all but $o(x)$ values of $n \in [x/2, x]$, the conclusion of Lemma 5.3 holds. For these typical n, we have

$$R_K(n) \ge \frac{F_K(n)}{M} \ge \frac{n^{K+1}}{M} \ge \frac{1}{2^{K+1}M}x^{K+1} = x^{K+1+o(1)},$$

and

$$R_K(n) \le F_K(n) \le x^{K+1}(2\log_2 x)^{1+2+\dots+K} \le x^{K+1+o(1)}.$$

(Here we use the maximal order of the sigma function.) This gives the first assertion of the lemma.

Moreover, in the notation of Lemma 5.3, N divides $R_K(n)$ for these n, so that $\psi(N)$ divides $\psi(R_K(n))$ and hence $\gcd(R_K(n), \psi(R_K(n))) \ge \gcd(N, \psi(N))$. Thus it is enough to show that for these n, we have $\gcd(N, \psi(N)) \ge x^{K+o(1)}$.

For a positive integer m, define $\mathrm{rad}'(m)$ to be the product of the distinct primes dividing m that exceed $\log^3 x$. Since N is squarefree, it follows that

$$N = \mathrm{rad}'(F_K(n)) = \prod_{k=0}^{K} \mathrm{rad}'(\psi_k(n)).$$

Hence

$$\begin{aligned}\gcd(N, \psi(N)) &= \prod_{k=0}^{K} \gcd(\mathrm{rad}'(\psi_k(n)), \psi(N)) \\ &\geq \prod_{k=1}^{K} \gcd(\mathrm{rad}'(\psi_k(n)), \psi(\mathrm{rad}'(\psi_{k-1}(n)))).\end{aligned}$$

Now we observe that

$$\mathrm{rad}'(\psi_k(n)) \mid \psi(\mathrm{rad}'(\psi_{k-1}(n))).$$

Indeed, suppose p divides $\psi_k(n)$ and $p > \log^3 x$. Then either p^2 divides $\psi_{k-1}(n)$ or $q \mid \psi_{k-1}(n)$ for some prime $q \equiv -1 \pmod p$. Since N is squarefree, only the latter is possible. Then q divides $\mathrm{rad}'(\psi_{k-1}(n))$ and so

$$p \mid q + 1 = \psi(q) \mid \psi(\mathrm{rad}'(\psi_{k-1}(n))).$$

Hence

$$\begin{aligned}\gcd(N, \psi(N)) &\geq \prod_{k=1}^{K} \mathrm{rad}'(\psi_k(n)) = N/\mathrm{rad}'(\psi_0(n)) \\ &\geq \frac{N}{n} = \frac{F_K(n)}{Mn} \geq \frac{n^K}{M} \geq \frac{1}{2^K M} x^K = x^{K+o(1)}.\end{aligned}$$

This completes the proof of Lemma 5.4. □

Proof of Proposition 5.2. Fix a positive integer K large enough that $1/K < \epsilon/2$. We let δ denote a fixed small positive real number (to be specified more precisely shortly) and we put

$$\mathcal{I} := \left[\frac{1}{2} A^{1/K+\delta}, A^{1/K+\delta}\right].$$

Then by Lemma 5.4, for almost all $n \in \mathcal{I}$, we have

$$R_K(n) \leq A^{1+1/K+(K+1)\delta+o(1)} \tag{9}$$

and

$$\gcd(R_K(n), \sigma(R_K(n))) \geq \left(\frac{1}{2} A^{1/K+\delta_0}\right)^{K+o(1)} > A.$$

Let $\mathcal{R}$ be the set of values $R_K(n)$ that arise from these typical $n \in \mathcal{I}$. Since $\operatorname{rad}(n) \mid R_K(n)$, each element of $\mathcal{R}$ arises from at most $x^{o(1)}$ values of n (by Lemma 4.2), and hence

$$\#\mathcal{R} \geq A^{1/K+\delta} x^{o(1)} = A^{1/K+\delta+o(1)}.$$

For each $r \in \mathcal{R}$, define

$$\mathcal{A}(r) := \{br : 1 \leq b \leq x/r \text{ and } \gcd(b,r) = 1\} \quad \text{and} \quad \mathcal{A} := \bigcup_{r \in \mathcal{R}} \mathcal{A}(r).$$

Note that every element of $\mathcal{A}$ satisfies (6), since

$$\gcd(br, \sigma(br)) = \gcd(br, \sigma(b)\sigma(r)) \geq \gcd(r, \sigma(r)) > A.$$

So the proof will be complete if we establish a suitable lower bound on $\#\mathcal{A}$. We suppose now that our small constant δ satisfies $(K+1)\delta < \epsilon/2$. Then by (9), each $r \in \mathcal{R}$ satisfies

$$r \leq A^{1+\epsilon+o(1)} \leq (x^{1-\epsilon})^{1+\epsilon+o(1)} \leq x^{1-\frac{1}{2}\epsilon^2},$$

say, once x is large enough. Using this estimate together with inclusion-exclusion, we see that

$$\#\mathcal{A}(r) = \frac{x}{r}\frac{\varphi(r)}{r} + O(2^{\omega(r)}) \geq \frac{x}{r} x^{o(1)},$$

since $2^{\omega(r)} = d(r) \ll x^{\epsilon^2/4}$, say. Moreover, each element $a \in \mathcal{A}$ is contained in at most $d(a) = x^{o(1)}$ such sets $\mathcal{A}(r)$. It follows that

$$\begin{aligned}\#\mathcal{A} &\geq x^{o(1)} \#\mathcal{R} \left(\min_{r \in \mathcal{R}} \#\mathcal{A}(r)\right) \\ &\geq x^{o(1)} \left(A^{1/K+\delta+o(1)}\right) \frac{x}{A^{1+1/K+(K+1)\delta+o(1)}} = x/A^{1+K\delta+o(1)}.\end{aligned}$$

Since we can take δ arbitrarily small, the theorem follows. □

Acknowledgements

The author takes pleasure in acknowledging helpful conversations with Kevin Ford and Carl Pomerance.

References

[ELP08] P. Erdős, F. Luca, and C. Pomerance, *On the proportion of numbers coprime to a given integer*, Anatomy of Integers, CRM Proceedings & Lecture Notes, vol. 46, Amer. Math. Soc., 2008, pp. 47–64.

[EN80] P. Erdős and J.-L. Nicolas, *Sur la fonction "nombre de facteurs premiers de n"*, Séminaire Delange-Pisot-Poitou, 20e année: 1978/1979. Théorie des nombres, Fasc. 2 (French), Secrétariat Math., Paris, 1980, pp. Exp. No. 32, 19.

[Erd56] P. Erdős, *On perfect and multiply perfect numbers*, Ann. Mat. Pura Appl. (4) **42** (1956), 253–258.

[HR74] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, vol. 4, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974.

[HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.

[IT86] A. Ivić and G. Tenenbaum, *Local densities over integers free of large prime factors*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 148, 401–417.

[Kát91] I. Kátai, *On the number of prime factors of* $\varphi(\varphi(n))$, Acta Math. Hungar. **58** (1991), no. 1-2, 211–225.

[KS06] I. Kátai and M. V. Subbarao, *Some further remarks on the* φ *and* σ*-functions*, Ann. Univ. Sci. Budapest. Sect. Comput. **26** (2006), 51–63.

[LP07] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 351–361.

[Luc76] L. Lucht, *Über die Hintereinanderschaltung mulitplikativer Funktionen*, J. Reine Angew. Math. **283/284** (1976), 275–281.

[Nai88] M. Naimi, *Les entiers sans facteurs carré* $\leq x$ *dont leurs facteurs premiers* $\leq y$, Groupe de travail en théorie analytique et élémentaire des nombres, 1986–1987, Publ. Math. Orsay, vol. 88, Univ. Paris XI, Orsay, 1988, pp. 69–76.

[Pom77] C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293/294** (1977), 217–222.

[Ten95] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995, Translated from the second French edition (1995) by C. B. Thomas.

[Wir59] E. Wirsing, *Bemerkung zu der Arbeit über vollkommene Zahlen*, Math. Ann. **137** (1959), 316–318.

Dept. of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, 273 Altgeld Hall, MC-382, Urbana, IL 61801

E-mail address: `pppollac@illinois.edu`