ON THE GREATEST COMMON DIVISOR OF AN INTEGER AND ITS SUM OF DIVISORS

PAUL POLLACK

Abstract. We show that for each fixed $\delta \in (0,1)$, the number of $n \le x$ for which $\gcd(n, \sigma(n)) > n^{\delta}$ is $x^{1-\delta+o(1)}$, as $x \to \infty$. This both substantiates and sharpens an estimate stated by Erdős without proof. In the course of establishing the upper bound we prove the following result, of independent interest: For each $x \ge 3$ and each $b \ge 1$, the number of $n \le x$ for which $\sigma(n)/n$ has denominator b in lowest terms is bounded above by $x^{c/\sqrt{\log\log x}}$, where c is an absolute positive constant.

1. Introduction

What is the greatest common divisor of n and its sum of divisors $\sigma(n)$? It was shown by Kátai and Subbarao ([KS06, Theorem 1]; cf. [ELP08, Theorem 8]) that for all n outside a set of density zero, one has

$$\gcd(n, \sigma(n)) = \prod_{\substack{p^e \| n \\ p \le \log\log n}} p^e.$$

In other words, $\gcd(n, \sigma(n))$ is almost always the largest divisor of n supported on the primes up to $\log\log n$. It follows (see [ELP08, Corollary 10]) that the density of n for which $\gcd(n, \sigma(n)) > (\log\log n)^u$ is a continuous, strictly decreasing function of u, which takes the value 1 when $u = 0$ and which tends to zero as $u \to \infty$.

Historically there has been great interest in much larger values of $\gcd(n, \sigma(n))$. For example, it is well-known that this greatest common divisor is sometimes n itself; in this case n is called *multiply perfect.* We expect, but cannot prove, that there are infinitely many such n. In 1956 Erdős [Erd56, p. 254] asserted that for each $\delta > 0$, there is a $\delta' > 0$ so that the number of $n \le x$ with $\gcd(\sigma(n), n) > n^{\delta}$ is at most $x^{1-\delta'}$. The primary purpose of this note is to prove the following sharpening of this result:

2000 *Mathematics Subject Classification.* 11N37.

The author is supported by NSF award DMS-0802970.

Theorem 1. *Fix $\delta \in (0,1)$. As $x \to \infty$, the number of $n \le x$ for which $\gcd(n, \sigma(n)) > n^{\delta}$ is $x^{1-\delta+o(1)}$.*

To establish the upper bound implicit in Theorem 1, we prove that the average of $\gcd(n, \sigma(n))$ on the positive integers $n \le x$ is $x^{o(1)}$. The analogous statement with the Euler function φ in place of σ was established by Erdős, Luca, and Pomerance in [ELP08, Theorem 11]. Their argument makes use of the fact that $\varphi(n)/n$ depends only on the set of primes dividing n, and so does not seem to apply to σ.

To work around this difficulty we employ a result of Wirsing [Wir59]. If n is a positive integer, define $a(n)$ and $b(n)$ to be the unique pair of coprime positive integers with $\sigma(n)/n = a(n)/b(n)$.

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

$$x^{c_1/\log\log x}.$$

Here c_1 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. We state our result here, which seems to be of independent interest:

Theorem 2. *For each $x \ge 3$ and each positive integer b, the number of $n \le x$ for which $b(n) = b$ is at most*

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

Here c_2 is an absolute positive constant.

To establish the lower bound implicit in Theorem 1, we use ideas of Luca and Pomerance from [LP07] concerning "Euler-function chains." These ideas have been employed to study large values of $\gcd(n, \varphi(n))$ in [ELP08]; see, e.g., the proof of [ELP08, Theorem 7].

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 $n \le x$ all of whose prime divisors are $\le y$. 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 the c_i always denote *absolute* positive constants.

2. Proof of Theorem 2

Lemma 1. *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 $x^{c_3/\log_2 x}$.*

Lemma 1 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 1. The number of such $n \leq x$ 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 work of de Bruijn (see, e.g., [Ten95, Theorem 2, p. 359]), $\Psi(x, p) = x^{(\log 4 + o(1))/\log_2 x}$ as $x \to \infty$. $\square$

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

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

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

$$x^{1/N + c_4 N/\log_2 x}.$$

Theorem 2 follows for large x upon choosing $N = \lfloor \sqrt{\log_2 x} \rfloor$. This implies the same result for all $x \geq 3$ 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 $b \leq x^{1/2}$ since otherwise we obtain an even sharper upper bound of $x^{1/2}$. Since $x > x_0$, the relation $b(n) = b$ implies that

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

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

$$2x^{1/2} (\log_2 x) x^{c_1/\log_2 x} \leq x^{1/2} x^{2c_4/\log_2 x}$$

if c_4 is chosen appropriately (depending on x_0 and c_1).

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

$$2x^{1/(N+1)} (\log_2 x) x^{c_1/\log_2 x} \leq x^{1/(N+1)} x^{(N+1)c_4/\log_2 x}.$$

So we may suppose $b \geq x^{1/(N+1)}$. We also assume $b \leq x$, since otherwise there are no solutions $n \leq x$ 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

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

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

$$(x^{N/(N+1)})^{1/N} x^{c_4 N/\log_2 x} = x^{1/(N+1)} x^{c_4 N/\log_2 x}$$

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 $x^{c_5/\log_2 x}$, while by Lemma 1, the number of choices for d is bounded by $x^{c_6/\log_2 x}$. It follows that the number of choices for $n = dn'$ is at most

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

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

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 2 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'.

3. Proof of Theorem 1

By considering the contribution of those n in $(x/2, x], (x/4, x/2]$, etc., it is enough to prove that the number of $n \leq x$ which satisfy the relation

$$\gcd(n, \sigma(n)) > x^{\delta} \tag{1}$$

is

$$x^{1-\delta+o(1)}.$$

That this is an upper bound on the number of solutions follows immediately from the following estimate for the average of $\gcd(n, \sigma(n))$:

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

$$\frac{1}{x} \sum_{n \leq x} \gcd(n, \sigma(n)) < x^{c_7/\sqrt{\log_2 x}}.$$

Proof. Having established Theorem 2, we may (and do) follow the proof of the upper bound of [ELP08, Theorem 11]. We have

$$\begin{aligned} \frac{1}{x} \sum_{n \leq x} \gcd(n, \sigma(n)) &\leq \sum_{n \leq x} \frac{\gcd(n, \sigma(n))}{n} = \sum_{b \leq x} \frac{1}{b} \sum_{\substack{n \leq x \\ b(n) = b}} 1 \\ &\leq (1 + \log x) x^{c_2/\sqrt{\log_2 x}} \leq x^{c_7/\sqrt{\log_2 x}}. \end{aligned}$$ □

Thus we focus attention on a lower bound for the number of solutions to (1). Let ψ denote the Dedekind ψ function, which is the arithmetic function defined by $\psi(n) := n \prod_{p|n} (1 + 1/p)$. (Thus $\psi \leq \sigma$ pointwise, and ψ and σ agree on squarefree arguments.) For each integer $K \geq 0$, define

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

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

Lemma 2. *Let K be a fixed nonnegative integer. For each positive integer n, write*

$$F_K(n) = AB, \quad \text{where} \quad A := \prod_{\substack{p^e \| F_K(n) \\ p \leq \log^3 x}} p^e \text{ and } B := \prod_{\substack{p^e \| F_K(n) \\ p > \log^3 x}} p^e.$$

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

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

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

Lemma 3. *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 2 holds. For these typical n, we have

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

and

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

This gives the first assertion of the lemma. Moreover, for these n we have that B divides $R_K(n)$, so that $\psi(B)$ divides $\psi(R_K(n))$ and hence $\gcd(R_K(n), \psi(R_K(n))) \geq \gcd(B, \psi(B))$. Thus it is enough to show that for these n, we have $\gcd(B, \psi(B)) \geq x^{K+o(1)}$.

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 B is squarefree, it follows that

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

Hence

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

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 B 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

$$\gcd(B,\psi(B)) \geq \prod_{k=1}^{K} \mathrm{rad}'(\psi_k(n)) = B/\mathrm{rad}'(\psi_0(n))$$
$$\geq \frac{B}{n} = \frac{F_K(n)}{An} \geq \frac{n^K}{A} \geq \frac{1}{2^K A} x^K = x^{K+o(1)}.$$

This completes the proof of Lemma 3. □

We now prove the lower bound for the number of solutions to (1). Given $\delta \in (0,1)$, fix an integer $K \geq 1$ for which $\delta \in (0, K/(K+1))$. For small enough $\epsilon > 0$, we may define $\alpha = \alpha(\epsilon) \in (0,1)$ so that

$$\alpha K/(K+1) = \delta + (K+1)\epsilon.$$

Having fixed such an ϵ, we define the closed interval $\mathcal{I}$ by

$$\mathcal{I} := \left[\frac{1}{2} x^{\alpha/(K+1)-\epsilon}, x^{\alpha/(K+1)-\epsilon}\right].$$

Then by Lemma 3, for almost all $n \in \mathcal{I}$, we have

$$x^{\alpha-(K+1)\epsilon} \leq R_K(n) \leq x^{\alpha},$$

say, and

$$\gcd(R_K(n), \sigma(R_K(n))) \geq \frac{1}{2^K} x^{\alpha K/(K+1) - K\epsilon + o(1)} > x^{\delta}.$$

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

$$\#\mathcal{R} \geq x^{\alpha/(K+1)-\epsilon+o(1)} \geq x^{\alpha/(K+1)-2\epsilon},$$

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

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

Note that every element of $\mathcal{A}$ satisfies (1), since

$$\gcd(br, \sigma(br)) = \gcd(br, \sigma(b)\sigma(r)) \geq \gcd(r, \sigma(r)) > x^{\delta}.$$

So the proof will be complete if we establish a suitable lower bound on $\#\mathcal{A}$. By inclusion-exclusion, for each $r \in \mathcal{R}$ we have that

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

for large enough x. Moreover, each element $a \in \mathcal{A}$ is contained in at most $d(a) \le x^{\epsilon}$ such sets $\mathcal{A}(r)$. It follows that

$$\begin{aligned}\#\mathcal{A} \ge x^{-\epsilon}\#\mathcal{R}\left(\min_{r\in\mathcal{R}}\#\mathcal{A}(r)\right) &\ge x^{-\epsilon}x^{\alpha/(K+1)-2\epsilon}x^{1-\alpha-\epsilon}\\ &= x^{1-\alpha K/(K+1)-4\epsilon} = x^{1-\delta-(K+5)\epsilon}.\end{aligned}$$

Since we can take ϵ arbitrarily small, the theorem is proved.

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.

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

[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.

[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.

[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.

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801

E-mail address: pppollac@illinois.edu