ON AN ASSERTION OF ERDŐS CONCERNING THE GREATEST COMMON DIVISOR OF n AND $\sigma(n)$

PAUL POLLACK

Abstract. In 1956, Erdős published (without proof) the theorem that if f is an increasing function with $f(x) \geq (\log x)^{\beta}$ (for some fixed $\beta > 0$), then the number $n \leq x$ for which $\gcd(n, \sigma(n)) > f(x)$ is at most $x/f(x)^c$, where c is a positive constant depending only on β. He claimed that this result was best possible, in that one cannot save a fixed power of f if $f(x)$ grows slower than each fixed power of $\log x$. We prove an extension of Erdős's theorem which contradicts this latter claim. Moreover, we prove that our result is best possible.

1. Introduction

A natural number n is called *perfect* if $\sigma(n) = 2n$ and *multiply perfect* if $\sigma(n)$ is a multiple of n. In 1956, Erdős published improved bounds on the distribution of perfect and multiply perfect numbers [Erd56]. These estimates were soon superseded by those of Wirsing [Wir59]; even so, Erdős's methods remain of interest because they can be adapted to show that $\gcd(n, \sigma(n))$ is seldom 'large.' A result of this type appears without proof as [Erd56, Theorem 3], accompanied by a claim that this theorem is best possible. Here we show that Erdős's result is *not* best possible, and we prove a best possible result in the same direction.

We show the following:

Theorem 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 very similar to 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 shows that this final assertion is not correct. We can however prove

2000 *Mathematics Subject Classification.* 11N37.

The author is supported by NSF award DMS-0802970.

a result in the same direction which shows that Theorem 1 is best possible.

Theorem 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 $2 \le A \le \exp((\log_2 x)^\beta)$, then the number of $n \le x$ with $\gcd(n, \sigma(n)) > A$ is at least x/A^ϵ.*

Notation. Let $\log_1 x := \max\{1, \log x\}$, and for $k > 1$, inductively define $\log_k x := \max\{1, \log(\log_{k-1}(x))\}$. Other notation is either standard or is introduced as necessary.

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

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. □

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

Lemma 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 4. *Let d be a squarefree integer. Then the number of squarefree $n \le x$ 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 $d \mid \sigma(n)$ while d and n are squarefree, we have that

$$d = \gcd(d, \sigma(n)) = \gcd(d, \prod_{p \mid n} (p+1)) = \prod_{\substack{p \mid n \\ \gcd(d, p+1) > 1}} \gcd(d, p+1).$$

In this way n induces a factorization of d, where by a *factorization of d* we mean a decomposition of d as a product of integers 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 $n \le x$ as in the lemma statement which induce this factorization.

Let "$d = a_1 a_2 \cdots a_k$" be a factorization of d. Note that necessarily $k \le \omega(d)$. 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 $1 \le i \le k$. So by Lemma 3, the number of such $n \le x$ is

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

where C is an absolute positive constant. 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 4. □

The last part of our preparation consists in reducing the proof of Theorem 1 to that of the following squarefree version:

Theorem 3. *For each $\beta > 0$, for $x > x_1(\beta)$ and $A > \exp((\log_2 x)^\beta)$, the number of* squarefree *$n \le x$ with $\gcd(n, \sigma(n)) > A$ is at most $x/A^{c'}$, where $c' = c'(\beta)$.*

Lemma 5. *Theorem 1 follows from Theorem 3.*

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 Theorem 3 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 (3) 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 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 Theorem 3 (and so also Theorem 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 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 (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 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 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 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 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 6. *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 7. *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 8. *Let $x \geq 3$ and let m be a positive integer. The number of $n \leq x$ 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 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 9. *If x is sufficiently large (depending on the choice of the function β), then all but at most x/A numbers $n \leq x$ are such that $\sigma(n)$ is divisible by every prime $p \leq y$.*

Proof. By Lemma 8, the number of exceptional n is

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

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

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

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

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 7, we have that $\Psi_2(A^2, y) \sim (6/\pi^2)\Psi(A^2, y)$. Since $\log(A^2) = y^{o(1)}$, Lemma 6 implies that

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

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 2 follows immediately from Lemmas 9 and 10: Indeed, with at most x/A exceptions, any n with a divisor of the form prescribed in Lemma 10 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 2.

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.

[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.

[Nai88] M. Naimi, *Les entiers sans facteurs carré $\le x$ dont leurs facteurs premiers $\le y$*, 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.

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

E-mail address: pppollac@illinois.edu