New York Journal of Mathematics

New York J. Math. **16** (2010) 23–30.

On the radical of a perfect number

Florian Luca and **Carl Pomerance**

Abstract. In this note, we look at the radical (that is, the squarefree kernel) of perfect numbers. We raise the question of whether large perfect numbers have the tendency to become far apart from each other and prove several results towards this under the ABC conjecture.

Contents

1. Introduction

A positive integer n is perfect if $\sigma(n) = 2n$, where σ is the sum-of-divisors function. The two outstanding problems are whether there are infinitely many even perfect numbers and whether there are any odd perfect numbers at all. Studied since Pythagoras and Euclid, the subject has a colorful history. A conventional view is that the study of perfect numbers maintains a certain isolation from the rest of mathematics and number theory. However, looking deeper, one finds the introduction of finite fields to primality testing (the Lucas–Lehmer test, culminating in the recent polynomial-time test of Agrawal, Kayal, and Saxena), advances in factoring large numbers, the study of primitive sequences in combinatorial number theory, distribution functions in probabilistic number theory, and so on. In this note, we make an attempt to relate the study of perfect numbers to the celebrated ABC conjecture. We begin by proving an unconditional inequality bounding the radical of a perfect number. We next show some consequences of this inequality under assumption of the ABC conjecture, and in particular show that for each k there can be at most finitely many triples of perfect numbers that can lie in some interval of length k.

Received November 10, 2009.

2000 *Mathematics Subject Classification.* 11A25.

Key words and phrases. perfect number, ABC conjecture.

F. L. was supported in part by grants SEP-CONACyT 79685 and PAPIIT 100508.

C. P. was supported in part by NSF grant DMS-0703850.

ISSN 1076-9803/2010

2. The radical of a perfect number

For a positive integer n we put

$$\operatorname{rad}(n) = \prod_{p \mid n} p,$$

where p runs over primes. The number $\operatorname{rad}(n)$ is called the *radical* of n, or the *squarefree kernel* of n. Let x be a perfect number. If x is even, then by a result of Euclid and Euler, $x = 2^{p-1}(2^p - 1)$ for some prime p such that $2^p - 1$ is also prime. Thus,

$$\operatorname{rad}(x) = 2(2^p - 1) < \sqrt{8x}. \tag{1}$$

Our first result in this note removes the restriction that x is even, at the cost of a somewhat weaker inequality.

Proposition 1. *The inequality*

$$\operatorname{rad}(x) < 2x^{17/26}$$

holds for all perfect numbers x.

Proof. In light of inequality (1), we may assume that x is odd. It has been known since Euler that $x = q^\alpha m^2$, where $q \equiv 1 \pmod 4$ is a prime, $\alpha \equiv 1 \pmod 4$, and m is coprime to q. Obviously

$$\operatorname{rad}(x) \le qm = q\left(\frac{x}{q^\alpha}\right)^{1/2} = x^{1/2} q^{1-\alpha/2}. \tag{2}$$

So, if $\alpha \ne 1$, it then follows that $\operatorname{rad}(x) < x^{1/2}$. Assume now that $\alpha = 1$, therefore $q \| x$. By (2), we may also assume that $q \ge 4x^{4/13}$.

Since x is perfect, there is a prime power $p^{2a} \| x$ with $q \mid \sigma(p^{2a})$. Write x as $qp^{2a}v^2$. Suppose that $p \nmid \sigma(q)$, so that $qp^{2a} \mid \sigma(p^{2a}v^2)$. Thus,

$$qp^{2a} < 2p^{2a}v^2; \quad \text{that is,} \quad v > (q/2)^{1/2}.$$

Also, since p is an odd prime,

$$q \le \sigma(p^{2a}) < \frac{3}{2}p^{2a}, \quad \text{so} \quad p^a > (2q/3)^{1/2}.$$

Thus,

$$\operatorname{rad}(x) \le \frac{x}{p^{2a-1}v} \le \frac{x}{p^a v} < 3^{1/2}\frac{x}{q}. \tag{3}$$

Next, consider the case when $p \mid \sigma(q) = q+1$. Then $q \equiv -1 \pmod p$, and since $\sigma(p^{2a}) \equiv 1 \pmod p$, we have $\sigma(p^{2a}) = qu$, where $u \equiv -1 \pmod p$. In particular, this forces $q, u \ge 2p - 1$ (and so $a \ge 2$). In any event, we have $q \le \sigma(p^{2a})/(2p-1) < p^{2a-1}$, so that

$$\operatorname{rad}(x) \le \frac{x}{p^{2a-1}} < \frac{x}{q},$$

and (3) holds in this case as well.

By (3), we may assume that q is not too large, so that with our earlier assumed lower bound for q, we have

$$4x^{4/13} \le q < x^{9/26}. \tag{4}$$

Factor $p^a v$ as nk where $(n,k)=1$, n is squarefree, and k is squarefull (i.e., each prime dividing k appears with exponent at least 2). Thus, $x = qn^2k^2$. It follows that $n = (x/q)^{1/2}k^{-1}$, so by (4),

$$\operatorname{rad}(x) \le qnk^{1/2} = (qx)^{1/2}k^{-1/2} < x^{35/52}k^{-1/2}.$$

Therefore, we are done unless

$$k^2 < \frac{1}{16}x^{1/13}. \tag{5}$$

Since (5) implies $\sigma(k^2) < \frac{1}{8}x^{1/13}$, we have $q \nmid \sigma(k^2)$ by the lower bound in (4). Thus, $q \mid \sigma(n^2)$; that is, $p^{2a} \| n^2$ and $a = 1$. By the observation above, this forces $p \nmid \sigma(q)$.

Since (using p odd and (4))

$$p^2 > \frac{2}{3}\sigma(p^2) \ge \frac{2}{3}q \ge \frac{8}{3}x^{4/13}, \tag{6}$$

we have by (5) that $p \nmid \sigma(k^2)$, so either

(i) $p^2 \mid \sigma(r^2)$ for some prime $r \mid n$, or
(ii) $p \mid \sigma(r^2)$, $p \mid \sigma(s^2)$ for some primes $r, s \mid n$, $r \ne s$.

In case (i),

$$r^2 > \frac{2}{3}\sigma(r^2) \ge \frac{2}{3}p^2 \ge \frac{16}{9}x^{4/13},$$

using (6). Then

$$qp^2r^2 > 4x^{4/13} \cdot \frac{8}{3}x^{4/13} \cdot \frac{16}{9}x^{4/13} = \frac{512}{27}x^{12/13},$$

so $\sigma(x/qp^2r^2) < (27/256)x^{1/13}$ which is too small to be divisible by r. Thus, $qp^2r^2 \mid \sigma(qp^2r^2)$, which implies that $\sigma(qp^2r^2)/qp^2r^2$ is an integer in the interval $(1,2]$; that is, it is 2 and $x = qp^2r^2$ is perfect. But by a theorem of Sylvester [4], each odd perfect number has at least 5 distinct prime factors. Thus, case (i) does not occur.

If we are in case (ii), then again by (6),

$$r^2 > \frac{2}{3}\sigma(r^2) \ge \frac{2}{3}p \quad \text{and} \quad s^2 > \frac{2}{3}\sigma(s^2) \ge \frac{2}{3}p, \quad \text{so} \quad r^2s^2 > \frac{32}{27}x^{4/13}.$$

Hence, by (4) and (6),

$$qp^2r^2s^2 > 4x^{4/13} \cdot \frac{8}{3}x^{4/13} \cdot \frac{32}{27}x^{4/13} = \frac{1024}{81}x^{12/13}.$$

So $\sigma(x/qp^2r^2s^2) < (81/512)x^{1/13}$, which is too small to be divisible by r or s, which are each larger than $x^{1/13}$. Hence, $qp^2r^2s^2 \mid \sigma(qp^2r^2s^2)$, which implies as above that $x = qp^2r^2s^2$ is perfect. This contradicts Sylvester's theorem quoted above, so this case does not occur either. We conclude that the proposition holds. □

3. The *ABC* conjecture and the distance between two perfect numbers

Luca proposed as a problem (see [3]) to prove that two consecutive numbers cannot be both perfect. This raises the question of whether perfect numbers should be far apart from each other. More formally, given $k \neq 0$, is it true that the equation

$$x - y = k \tag{7}$$

has only finitely many solutions in perfect numbers x and y? This is clear if x and y are both even since even perfect numbers are, in particular, members of a binary recurrent sequence so they increase at an exponential rate, but what if one is even and one is odd, or if both are odd? In what follows, we prove some conditional results on this problem. Recall that the ABC conjecture asserts that for each $\varepsilon > 0$ there exists a constant C_ε depending only on ε such that whenever a, b and c are coprime nonzero integers with $a + b = c$ the inequality

$$\max\{|a|, |b|, |c|\} \leq C_\varepsilon \text{rad}(abc)^{1+\varepsilon}$$

holds.

Proposition 2. *The ABC conjecture implies that for every odd integer k, the equation*

$$x - y = k$$

has only finitely many solutions in perfect numbers x and y.

Proof. Let us assume that there are solutions to the equation $x - y = k$ in perfect numbers x and y with an arbitrarily large x.

We use the following well-known consequence of the ABC conjecture: Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d \geq 1$ without repeated roots. Fix $\varepsilon > 0$. Then the ABC conjecture implies that

$$\text{rad}(f(n)) \gg |n|^{d-1-\varepsilon}. \tag{8}$$

The implied constant here depends on the polynomial $f(X)$ and ε. For a proof of this result, see [1] or [2]. [1]

Since k is odd, if follows that one of the numbers x and y is odd and the other is even. Up to changing k to $-k$, we may assume that x is even. Assume that $x = 2^{p-1}(2^p - 1)$. Let d be some fixed positive integer to be chosen later. There are nonnegative integers a, t with $a < d$ and $p = a + dt$. Then

$$y = x - k = 2^{2p-1} - 2^{p-1} - k = 2^{2a-1}m^{2d} - 2^{a-1}m^d - k,$$

[1]We recall that the expressions $A \ll B$ and $B \gg A$ are synonymous with $A = O(B)$.

where $m := 2^t$. Let us take a look at the polynomial

$$f(X) = 2^{2a-1}X^{2d} - 2^{a-1}X^d - k.$$

We shall show that it has no repeated roots. Note that

$$f'(X) = d2^{2a}X^{2d-1} - d2^{a-1}X^{d-1} = d2^{a-1}X^{d-1}(2^{a+1}X^d - 1).$$

Thus, assuming that z is a double root of $f(X)$, we then get that

$$z^{d-1}(2^{a+1}z^d - 1) = 0.$$

Clearly, $z \neq 0$ because $f(0) = -k \neq 0$. Thus, $z^d = 2^{-a-1}$, and now for such z we have

$$f(z) = 2^{a-1}z^d(2^a z^d - 1) - k = 2^{-2}(2^{-1} - 1) - k = -2^{-3} - k \neq 0.$$

Thus, the polynomial $f(X)$ has only simple roots. By (8) and $x \gg m^{2d}$, it follows that

$$\text{(9)} \quad \operatorname{rad}(y) = \operatorname{rad}(f(m)) \gg m^{2d-1-\varepsilon} = (m^{2d})^{1-1/2d-\varepsilon/2d} \gg x^{1-1/2d-\varepsilon/2d}.$$

However, assuming say that $x > 2|k|$, it follows that $y \ll x$, and by Proposition 1, we get that

$$\operatorname{rad}(y) \ll y^{17/26} \ll x^{17/26}. \tag{10}$$

Putting together relations (9) and (10), we get

$$x^{17/26} \gg x^{1-1/2d-\varepsilon/2d}.$$

Taking $d = 3$ and $\varepsilon = 1$, we get that $x = O(1)$, contradicting that x was arbitrarily large. This completes the proof of Proposition 2. □

We give another result in the same spirit as Proposition 2.

Proposition 3. *The ABC conjecture implies that for every nonzero integer k, the equation*

$$x - y = k$$

has only finitely many solutions in squarefull perfect numbers x and y.

Proof. Observe first that since even perfect numbers are never squarefull, it follows that x and y are both odd. Without restricting the generality, we may assume that $k > 0$ (otherwise we replace k by $-k$), and that $y > k$. Thus, $y < x < 2y$. Observe that if $x = p^{1+4a_p}m^2$ and $y = q^{1+4b_q}n^2$, then $a_p \geq 1$ and $b_q \geq 1$. Write

$$x = u^2 m_1 \qquad \text{and} \qquad y = v^2 n_1, \tag{11}$$

where u and v are squarefree and m_1 and n_1 are fourth power full, meaning that whenever r is a prime factor of m_1 (or n_1), then $r^4 \mid m_1$ (or $r^4 \mid n_1$), respectively. Observe that

$$\operatorname{rad}(x) \leq u m_1^{1/4} = u\left(\frac{x}{u^2}\right)^{1/4} = u^{1/2}x^{1/4},$$

and similarly

$$\operatorname{rad}(y) \le v^{1/2} y^{1/4} \ll v^{1/2} x^{1/4}.$$

Let $D := \gcd(x, y)$. Then $D \mid k$, and

$$\frac{x}{D} - \frac{y}{D} = \frac{k}{D}. \tag{12}$$

The ABC conjecture applied to equation (12) shows that

$$\frac{x}{k} \le \frac{x}{D} \ll (\operatorname{rad}(x)\operatorname{rad}(y))^{1+\varepsilon} \ll (uv)^{1/2+\varepsilon} x^{1/2+\varepsilon} \ll (uv)^{1/2} x^{1/2+2\varepsilon},$$

where we used the fact that $u \le x^{1/2}$ and $v \le y^{1/2} \ll x^{1/2}$. Thus,

$$x^{1-4\varepsilon} \ll uv, \tag{13}$$

where the constant implied in the above Vinogradov symbol depends on both ε and k.

We shall now choose $\varepsilon > 0$ in the following way. First choose a number T so large that $3^T > k$. Next choose $\varepsilon > 0$ so small that $17 \cdot 3^{T+1}\varepsilon < 1/2$. From, now on, we will work under this assumption. Since both $v \ll x^{1/2}$ and $u \le x^{1/2}$ hold, from the above inequality (13) we read that

$$u \gg x^{1/2-4\varepsilon}, \qquad \text{and} \qquad v \gg x^{1/2-4\varepsilon},$$

and by equations (11) we learn that $m_1 \ll x^{8\varepsilon}$ and $n_1 \ll x^{8\varepsilon}$. Now

$$2u^2 m_1 = 2x = \sigma(x) = \sigma(u^2)\sigma(m_1),$$

and $\sigma(m_1) \le 2m_1 \ll x^{8\varepsilon}$. This shows that $\gcd(u^2, \sigma(u^2)) \gg x^{1-16\varepsilon}$. Similarly, $\gcd(v^2, \sigma(v^2)) \gg x^{1-16\varepsilon}$. Write

$$U_0 = \gcd(u^2, \sigma(u^2)) = \prod_{i=1}^{t} p_i^{a_i}, \qquad V_0 = \operatorname{rad}(U_0)^2, \qquad W_0 = \frac{x}{V_0},$$

where $a_i \in \{1, 2\}$ for $i = 1, \ldots, t$.

We next show that $t \ge T + 1$ holds assuming that x is sufficiently large. Indeed observe that V_0 and W_0 are coprime. Assume that there exists a prime dividing $\gcd(U_0, \sigma(W_0))$ which we take to be p_1. Then

$$p_1 \le \sigma(W_0) \le 2W_0 = 2x/V_0 \le 2x/U_0 < c_1 x^{16\varepsilon},$$

where $c_1 > 0$ is some constant depending on k and ε. Assuming that x is sufficiently large, we have that $\max\{p_1, W_0\} < 2x^{17\varepsilon}$. Let

$$U_1 = \frac{U_0}{p_1^{a_1}} = \prod_{i=2}^{t} p_i^{a_i}, \qquad V_1 = \operatorname{rad}(U_1)^2, \qquad W_1 = \frac{x}{V_1} = W_0 p_1^2 \le 2^3 x^{51\varepsilon}.$$

Assume next that there is a prime dividing $\gcd(U_1, \sigma(W_1))$ which we take to be p_2. Then $p_2 \le 2W_1 \le 2^4 x^{51\varepsilon}$. Repeating the above construction, we get

$$U_2 = \frac{U_1}{p_2^{a_2}} = \prod_{i=3}^{t} p_i^{a_i}, \qquad V_2 = \operatorname{rad}(U_2)^2, \qquad W_2 = \frac{x}{V_2} = W_1 p_2^2 \le 2^{11} x^{153\varepsilon}.$$

Let us continue in this way. Then at step j, where $1 \le j \le t$, we end up with the three numbers

$$U_j = \prod_{i=j+1}^{t} p_i^{a_i}, \quad V_j = \mathrm{rad}(U_j)^2, \quad W_j = \frac{x}{V_j} = W_{j-1}p_j^2 \le 2^{4\cdot 3^{j-1}-1} \cdot x^{17\cdot 3^j \varepsilon}.$$

Assume that we have reached some $j \le T+1$ such that for $i \in \{j+1, \ldots, t\}$ we have that no p_i divides $\sigma(W_j)$. Then since $\sigma(V_j W_j) = \sigma(V_j)\sigma(W_j) = 2V_j W_j$ (observe that V_j and W_j are coprime), we get that each $p_i^2 \mid \sigma(V_j)$. This shows that $V_j \mid \sigma(V_j)$. In particular, either V_j is perfect, which is false since $V_j = \mathrm{rad}(U_j)^2$ is a square, and there are no "perfect squares", or $V_j = 1$, which is again false for large x because

$$V_j \ge 2^{-4\cdot 3^{j-1}-1} x^{1-17\cdot 3^j \varepsilon} \ge 2^{-4\cdot 3^T - 1} x^{1-17\cdot 3^{T+1}\varepsilon} \ge 2^{-4\cdot 3^T-1} x^{1/2} > 1,$$

where the last inequality holds for large enough x. So, the conclusion is that the above process must continue at least until $j > T+1$ is reached. Thus, $\omega(U_0) = t \ge j \ge T+1$. Now every prime p_i dividing U_0 also divides $\sigma(u^2)$, so it divides q^2+q+1 for some prime $q \mid u$. Thus, either $p_i = 3$, or $p_i \equiv 1 \pmod 3$. Thus, u has at least T distinct primes $p \equiv 1 \pmod 3$ and such that $p^2 \| x$; therefore $3^T \mid \sigma(x) = 2x$, so $3^T \mid x$.

A similar argument shows that $3^T \mid y$. Hence, $3^T \mid (x-y) = k$, which is false, because $3^T > k$. $\square$

Let $(a_n)_{n\ge 1}$ be the increasing sequence of perfect numbers. While we cannot prove in its full generality that for every fixed positive integer k the equation

$$a_{n+1} - a_n \le k$$

has only finitely many solutions, we can show that there are no three perfect numbers close together infinitely often assuming again the ABC conjecture.

Proposition 4. *Under the ABC conjecture, for every fixed positive integer k the inequality*

$$a_{n+2} - a_n \le k$$

has only finitely many solutions n.

Proof. Assume that $2 \le k_1 < k_2 \le k$ are fixed and that $a_{n+1} = a_n + k_1$ and $a_{n+2} = a_n + k_2$. Let $x := a_n$. Consider the polynomial

$$f(X) = X(X+k_1)(X+k_2),$$

which obviously has only simple roots. By (8), we have that

$$\mathrm{rad}(a_n a_{n+1} a_{n+2}) = \mathrm{rad}(f(x)) \gg x^{2-\varepsilon}.$$

On the other hand, by Proposition 1, we have that

$$\mathrm{rad}(a_n a_{n+1} a_{n+2}) \le \mathrm{rad}(a_n)\mathrm{rad}(a_{n+1})\mathrm{rad}(a_{n+2}) \le 8x^{51/26}.$$

Thus, $x^{51/26} \gg x^{2-\varepsilon}$, and choosing $\varepsilon = 1/27$, we get that $x = O(1)$. $\square$

Acknowledgements. The authors thank the anonymous referee for comments which improved the quality of the paper. They also thank Bill Banks, Kevin Ford, Hendrik Lenstra, and Paul Pollack for useful suggestions.

References

[1] Elkies, Noam D. *ABC* implies Mordell. *Internat. Math. Res. Notices* **1991**, no. 7, 99–109. MR1141316 (93d:11064), Zbl 0763.11016.

[2] Langevin, Michel. Partie sans facteur carré de $F(a,b)$ (modulo la conjecture (abc)). *Séminaire de Théorie des Nombres* (1993–1994), *Publ. Math. Univ. Caen*, 1995.

[3] Luca, Florian. Problem 10711. *Amer. Math. Monthly* **106** (1999) 781–782; solution **108** (2001) 80–81. MR1543406, MR1543804.

[4] Sylvester, James Joseph. Sur l'impossibilité de l'existence d'un nombre parfait impair qui ne contient pas au moins 5 diviseurs premiere distincte, *Compte Rendus* **CVI** (1888), 522–526. JFM 20.0173.04

Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Mathematics Department, Dartmouth College, Hanover, NH 03755, USA
carl.pomerance@dartmouth.edu

This paper is available via http://nyjm.albany.edu/j/2010/16-3.html.