Even Perfect Numbers and A Bound on the Prime Factors of Odd Perfect Numbers, a summary and explanation of "On Prime Factors of Odd Perfect Numbers" a paper by Peter Acquaah and Sergei Konyagin

Timothy Gormley

June 6 2016

1 Introduction to Perfect Numbers

We define the function $\sigma(n)$ as the sum of the divisors of n.

We say a number n is perfect if and only if n is the sum of its divisors excluding itself, or equivalently, if and only if n is half of the sum of its divisors including itself.

$$\sigma(n) = 2n$$

We will divide perfect numbers into two types: perfect numbers which are even (divisible by two) and odd (not divisible by two). The even perfect numbers are all of the form:

$$2^{p-1}(2^p - 1)$$

where $(2^p - 1)$ is prime. Prime Numbers of the form $(2^p - 1)$ are called Mersenne primes, and only occur if p is prime, although they do not necessarily occur if p is prime. It is unknown whether or not there are infinitely many Mersenne primes. There were 27 Mersenne primes known at the time of [2] publication, but more have been discovered since, bringing the count to 49.

There are no known odd perfect numbers, but there is no proof that they do not exist. It was conjectured in 1496 that there are no odd perfect numbers.

In 2012, Peter Acquaah and Sergei Konyagin proved that for any odd perfect number x, any prime factor q satisfies $q < (3x)^{\frac{1}{3}}$, this paper will summarize their paper, explaining the details of their paper. This is useful because it simplifies the process of checking whether a number is an odd perfect number, because only prime numbers less than $(3x)^{\frac{1}{3}}$ need to be checked, accelerating the search for odd perfect numbers.

2 Notation

We'll define some notation that will be used throughout the rest of this paper.
$p|q$ means that p divides q evenly, q is a multiple of p. In other words, there is some n such that $np = q$.
$p \nmid q$ is the opposite, in other words p does not divide q.
For a prime p, natural number n, and nonegative integer u, $p^u || n$ if $p^u | n$ and $p^{u+1} \nmid n$, in other words, p divides n exactly u times.
As stated earlier, $\sigma(n) = \sum_{d|n} d$. In other words the sum of all the divisors of n. This function is multiplicative, that is $\sigma(MN) = \sigma(M)\sigma(N)$. This is because if $m|M$ and $n|N$, $mn|MN$. The converse is true because if $a|MN$, each of a's prime factors must divide either M or N, so there is some $b|M$, $c|N$, such that $bc = a$.

3 Mersenne Primes

Earlier we stated that primes of the form $(2^p - 1)$ are called Mersenne Primes, and occur only if p is prime.

Suppose $2^p - 1$ is prime. Suppose for a contradiction we can write $p = q_1 q_2$, where p and q are integers.

$$2^p - 1 = (2^{q_1})^{q_2} - 1$$

Applying the elephant teacup identity, we learn that

$$(2^p - 1) = (2^{q_1} - 1)((2^{q_1})^{q_2 - 1} + ... + 2^{q_1} + 1$$

So $(2^{q_1} - 1)|(2^p - 1)$, a contradiction, since we assumed $2^p - 1$ was prime.

Note that this is necessary but not sufficient, for example $2^1 1 - 1 = 2047$, but $23(89) = 2047$.

4 Cited Results on Perfect Numbers

In [1] Acquaah and Konyagin cite several properties of perfect numbers. They cite the form of the even perfect numbers from [2], which we will show below.

Acquaah and Konyagin then cite two other papers for three facts about the properties an odd perfect number must have, namely that if x is an odd perfect number, $x > 10^{1500}$ from [3], x has at least nine distinct prime factors from [4], and the total number of prime factors must be at least 101 from [3]. These facts do not play a large role in the paper.

One result by Euler that does play a crucial role in our proof regarding the prime factors of odd perfect numbers is that if x is an odd perfect number, $x = Q^\alpha m^2$, with Q and α both congruent to 1 modulo 4, and Q and m coprime.

5 Even Perfect Numbers

This section is an explanation of [2], which [1] cites. The form of even perfect numbers was first discovered by Euclid, who proved that if $(2^p - 1)$ is prime is then $2^{p-1}(2^p - 1)$ is perfect. I'll give a brief algebraic proof, although the fact is too elementary for any of the papers I'm citing to give the proof. Recall that $\sigma(NM) = \sigma(N)\sigma(M)$, by the multipicativity of σ shown earlier.

Suppose $(2^{a+1} - 1)$ is prime. Then consider $N = 2^a(2^{a+1} - 1)$. $\sigma(N) = \sigma(2^a)\sigma(2^{a+1} - 1) = \left(\sum_{k=0}^{a} 2^k\right)(2^{a+1} - 1 + 1) = (2^{a+1} - 1)2^{a+1} = 2N$

Euler was the first to prove the converse, that every even perfect number is of Euclid's type.

$$\sigma(n) = \sum_{d|n}(d)$$

$$\frac{\sigma(n)}{n} = \sum(1/d),$$

because for each divisor there is another such $d_1 d_2 = n$, so $\frac{d_1}{n} = \frac{1}{d_2}$ Let M be a proper divisor of N (proper divisor here means that $M|N$ and $N \neq M$.

$$\frac{\sigma(N)}{N} \geq \frac{\sigma(M)}{M},$$

because expressed as the summation above, $\frac{\sigma(N)}{N}$ will contain every term $\frac{\sigma(M)}{M}$ does, and at least one more $(\frac{N}{M})$.

Now assume $L = 2^a N$ is perfect $a > 0$.

$$\sigma(L) = 2L$$

by assumption

$$\sigma(2^a N) = 2^{a+1} N$$

$$\sigma(2^a)\sigma(N) = 2^{a+1} N$$

using the multiplicativity

$$\left(\sum_{k=0}^{a} 2^k\right) \sigma(N) = 2^{a+1} N$$

because all the factors of 2^a are the numbers 2^k $0 \leq k \leq a$.

$$(2^{a+1} - 1)\sigma(N) = 2^{a+1} N$$

this is from the formula for a finite geometric sum.

$$\frac{\sigma(N)}{N} = \frac{2^{a+1}}{2^{a+1} - 1}$$

Cohen also states at this stage that this implies $(2^{a+1} - 1)$ is a factor of N. This is because $\sigma(N)$ must be an integer. Now because $\frac{\sigma(N)}{N} \geq \frac{\sigma(M)}{M}$,

$$\frac{\sigma(N)}{N} \geq \frac{\sigma(2^{a+1} - 1)}{2^{a+1} - 1}$$

$$\frac{\sigma(2^{a+1} - 1)}{2^{a+1} - 1} \geq \frac{(2^{a+1} - 1) + 1}{2^{a+1} - 1}$$

because both $2^{a+1} - 1$ and 1 divide $2^{a+1} - 1$.

$$\frac{\sigma(N)}{N} \geq \frac{2^{a+1}}{2^{a+1} - 1}$$

But $\frac{\sigma(N)}{N} = \frac{2^{a+1}}{2^{a+1}-1}$ therefore:

$$\frac{\sigma(N)}{N} = \frac{\sigma(2^{a+1} - 1)}{2^{a+1} - 1} = \frac{2^{a+1}}{2^{a+1} - 1}$$

So by the inequality proved earlier, $N = 2^{a+1} - 1$ and $N = \sigma(2^{a+1} - 1) =$

$2^{a+1} - 1 + 1$, so $N = 2^{a+1} - 1$ must be prime. Therefore $L = 2^a(2^{a+1} - 1)$, $(2^{a+1}-1)$ prime. We observe that the inequality we will prove for Prime Factors of odd perfect numbers does not hold in this case, as $496 = 16 * 31$ is a perfect number, but $(3 * 496)^{1/3} < 31$.

6 Prime Factors of Odd Perfect Numbers

This section is a summary of Acquaah and Konyagin's paper, which proves that for any odd perfect number N, any prime factor q satisfies $q < (3x)^{\frac{1}{3}}$.

Let

$$n = \prod_{i=1}^{k} p_i^{r_i}$$

where p_i are all distinct primes. This is the prime factorization of n. By repeatedly using multiplicativity, as discussed in the section on even perfect numbers, we know that

$$\sigma(n) = \prod_{i=1}^{k} \sigma(p_i^{r_i})$$

$$\sigma(p_i^{r_i}) = \sum_{j=0}^{r_i} p_i^j,$$

a geometric series so

$$\sigma(p_i^{r_i}) = \frac{p_i^{r_i+1} - 1}{p_i - 1}$$

therefore

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{r_i+1} - 1}{p_i - 1}$$

For any odd prime power $y = p^r$, $\sigma(y) = \sum_{i=0}^{r} p^i = \frac{p^{r+1}-1}{p-1} = \frac{py-1}{p-1} < \frac{p}{p-1}y$. $\frac{p}{p-1} = (1 - \frac{1}{p})^{-1}$ as p increases, this decreases, so $\sigma(y) < \frac{3}{2}y$, the case where $p = 3$.

7 If the prime factor in question divides the odd perfect number more than once

Let x be an odd perfect number, and q be a divisor of x. Suppose $q^r||x$ and $r \geq 2$, q^r divides x, so $\frac{x}{q^r}$ is an integer, so $\sigma(\frac{x}{q^r}) = \frac{\sigma(x)}{\sigma(q^r)}$ by multiplicativity, so $\sigma(q^r)$ divides $\sigma(x)$. q^r and $\sigma(q^r)$ are also coprime, meaning they share no factors, because $\sigma(q^r) = \sum_{i=0}^{r} q^i$, the sum of 1 and terms all divisible by q, which is the only prime factor of q^r. Therefore, $\sigma(x)$ is divisible by $q^r\sigma(q^r)$. Therefore, $2x = \sigma(x) \geq q^r\sigma(q^r) > q^{2r} \geq q^4$. So $q < (2x)^{1/4}$, and we're done.

8 If the prime factor in question divides the odd perfect number only once

From Euler, $x = Q^\alpha m^2$, where Q is prime, $Q \equiv \alpha \equiv 1 \pmod 4$, and m and Q are coprime. Therefore, if q is a prime divisor of x, and $q \neq Q$, $q^2|x$, so the inequality shown above holds. Thus, assume $q = Q$ and $\alpha = 1$. So we can write $x = qm^2$.

The authors then state that since x is perfect, there is some prime power p such that $p^{2a}||x$ with $q|\sigma(p^{2a})$.

To prove this, first let $m = \prod_{i=1}^{k} p_i^{r_i}$. Then by multiplicativity $\sigma(m) = \prod_{i=1}^{k} \sigma(p_i^{r_i})$, and $\sigma(m^2) = \prod_{i=1}^{k} \sigma(p_i^{2r_i})$. Therefore,

$$2x = \sigma(x) = \sigma(q)\sigma(m^2) = \sigma(q)\prod_{i=1}^{k}\sigma(p_i^{2r_i})$$

We note that for any $p_i^{r_i}$, $p_i^{2r_i}||x$, because $m^2||x$, and m and q coprime.

$$qm^2 = \sigma(q)\prod_{i=1}^{k}\sigma(p_i^{2r_i})$$

q and $\sigma(q)$ are coprime, so $q|\prod_{i=1}^{k}\sigma(p_i^{2r_i})$. But q is prime, so it must divide as least one of the $\sigma(p_i^{2r_i})$ in order to divide the product, therefore, there exists some prime power p such that $p^{2a}||x$ with $q|\sigma(p^{2a})$.

Now we write x as $qp^{2a}v^2$.

First suppose that $p \nmid \sigma(q)$.

$$2qp^{2a}v^2 = 2x = \sigma(x) = \sigma(q)\sigma(p^{2a})\sigma(v^2)$$

by hypothesis, $p^{2a} \nmid \sigma(q)$ and $p^{2a} \nmid \sigma(p^{2a})$ because prime powers do not divide the sum of their factors, as shown earlier. Therefore, $p^{2a}|\sigma(v^2)$. Therefore,

$qp^{2a}|\sigma(p^{2a}v^2)$. Therefore $\sigma(p^{2a}v^2) > qp^{2a}$.

$$2x = \sigma(x) = (q+1)\sigma(p^{2a}v^2) > q^2p^{2a} > \frac{2q^2\sigma(p^{2a})}{3} > \frac{2q^2}{3}$$

using the $\sigma(y) < \frac{3}{2}y$ inequality we showed earlier, so we're done.

Now for our last case, let $p|\sigma(q)$. Let $u = \sigma(p^{2a})/q$. $\sigma(p^{2a}) \equiv 1$ (mod p) and $q = -1$ (mod p), therefore $u \equiv -1)$ (mod p). Furthermore, since $\sigma(p^{2a})$ is the sum of a series with an odd number of terms, and all the terms are odd, and q is also odd, u is odd. Therefore $u \neq p-1$. Therefore, $u \geq 2p-1$.

Let $p^b||\sigma(q)$, by assumption $b \geq 1$.

$$2qp^{2a-b}v^2 = \frac{\sigma(q)}{p^b}\sigma(p^{2a})\sigma(v^2)$$

Therefore $p^{2b-a}||\sigma(v^2)$. Therefore, $b \leq 2a$, and $\sigma(v^2) \geq p^{2a-b}$.

$$p^{2a+1}-1 = (p-1)\sigma(p^{2a}) = (p-1)uq = (p-1)u(\sigma(q)-1) = (p-1)u\sigma(q)-(p-1)u$$

Therefore, $p^{2a+1}-1 \equiv (p-1)u\sigma(q) - (p-1)u \pmod{p^b}$. $\sigma(q) \equiv p^{2a+1} \equiv 0 \pmod{p^b}$, so $-1 \equiv -(p-1)u \pmod{p^b}$. Therefore $1 \equiv (p-1)u \pmod{p^b}$. So,

$$(p-1)u > p^b$$

Together with $\sigma(v^2) \geq p^{2a-b}$, we get

$$u\sigma(v^2) > \frac{p^{2a}}{p-1}$$

$$2x = \sigma(x) = \sigma(q)\sigma(p^{2a})\sigma(v^2) = (q+1)uq\sigma(v^2).$$

$$2x > \frac{p^{2a}q^2}{p-1}$$

Then using the $\sigma(y) < \frac{3y}{2}$ inequality we get

$$2x > \frac{2\sigma(p^{2a})q^2}{3(p-1)} = \frac{2uq^3}{3(p-1)}$$

Then using $u \geq 2p - 1$ we get

$$2x > \frac{2(2p-1)q^3}{3(p-1)} > \frac{4q^3}{3}$$

so

$$(3x)^{1/3} > 2^{1/3}q > q$$

Finishing the proof. We also note that due to Euler's form of x, x has at most one prime factor $q \geq (2x)^{1/4}$, in addition to the restriction on all prime factors.

9 Citations

[1]: Acquaah, Peter ; Konyagin, Sergei. On Prime Factors of Odd Perfect Numbers. International Journal of Number Theory, September 2012, Vol.8(6), pp.1537-1540

[2]: Cohen, Graeme L. Even Perfect Numbers. The Mathematical Gazette Vol. 65, No. 431 (Mar., 1981), pp. 28-30

[3]: Ochem, Pascal, and Michaël Rao. "Odd Perfect Numbers Are Greater than 10^{1500}." Mathematics of Computation Math. Comp. 81.279 (2012): 1869-877.

[4]: Nielsen, Pace P. "Odd Perfect Numbers Have at Least Nine Distinct Prime Factors." Mathematics of Computation Math. Comp. 76.260 (2007): 2109-127.