MATHEMATICS OF COMPUTATION
VOLUME 53, NUMBER 187
JULY 1989, PAGES 431-437

A New Lower Bound for Odd Perfect Numbers

By Richard P. Brent and Graeme L. Cohen*

Abstract. We describe an algorithm for proving that there is no odd perfect number less than a given bound K (or finding such a number if one exists). A program implementing the algorithm has been run successfully with $K = 10^{160}$, with an elliptic curve method used for the vast number of factorizations required.

1. Introduction. Let $\sigma(N)$ be the sum of the positive divisors of the natural number N. If $\sigma(N) = 2N$ then N is called perfect. Most elementary textbooks in number theory show that an even number is perfect if and only if it has the form $2^{a-1}(2^a - 1)$, where $2^a - 1$ is a (Mersenne) prime, so that the search for even perfect numbers is equivalent to the search for Mersenne primes. No odd perfect number has been found, but it has not been proved that none exists.

The search for odd perfect numbers has often proceeded by showing that there is none less than a given bound K. Kanold [10] did this for $K = 10^{20}$ in 1957, and improvements were given by Tuckerman [14] ($K = 10^{36}$) and Hagis [9] ($K = 10^{50}$). The last-mentioned result has been accepted (e.g., by Guy [8] and Wagon [15]) as the best to date, despite announced extensions [5], [6] up to $K = 10^{200}$. Details of these extensions have never been published; an alternative proof [13] of Hagis's result was not acceptable to a reviewer [12].

Being wary of the fate of these later "proofs", we have adopted a very straightforward, algorithmic approach to prove the

THEOREM. *There is no odd perfect number less than* 10^{160}.

The proof is almost entirely computer generated and has some similarity to Tuckerman's. In being a comprehensive case study, the proof is also similar to that of Beck and Najar [1], who showed that there are no odd triperfect numbers (odd numbers M for which $\sigma(M) = 3M$) less than 10^{50}. (This bound was improved to 10^{70} by Cohen and Hagis [7], and could no doubt be still further improved by the methods of the present paper.) For the many large factorizations required in our proof, an elliptic curve method [2] was used. The chosen bound 10^{160} is related to the state of the art in factorization methods, in which 80-digit numbers are accessible.

Some general background is given below, followed by a deeper analysis of the method.

Received January 13, 1988; revised August 16, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A25; Secondary 11Y05, 11Y70.

*The research was carried out while a Visiting Fellow at the Australian National University.

2. Overview of the Method. On the assumption that there is an odd perfect number N, Euler showed that necessarily $N = \prod_{i=0}^{t} p_i^{a_i}$ for distinct odd primes $p_0, \ldots, p_t$, with (say) $p_0 \equiv a_0 \equiv 1 \pmod 4$ and $a_i \equiv 0 \pmod 2$ for $i = 1, \ldots, t$. This will be our standard form for N. Each $p_i^{a_i}$ is called a component of N, and p_0 is called the special prime.

Since σ is multiplicative and $\sigma(N) = 2N$, the sets $\{q\colon q \text{ prime}, q > 2, q \mid \sigma(p_i^{a_i}) \text{ for some } i = 0, 1, \ldots, t\}$ and $\{p_0, \ldots, p_t\}$ are equal. This leads to the customary factor-chain method for problems involving odd perfect numbers. From any postulated component p^a of N, we may generate further prime factors of N, namely the odd prime factors of $\sigma(p^a)$. For such a prime q, we postulate an exponent b and then factorize $\sigma(q^b)$ to generate still more prime factors of N. The process is continued until a contradiction is reached (or an odd perfect number is found!). The set of contradictions resulting from an exhaustive choice of primes and exponents constitutes a proof of the relevant theorem.

For any prime p, $\sigma(p^a) \mid \sigma(p^b)$ if $a+1 \mid b+1$, so that for many purposes, including ours, it is sufficient in postulating an exponent a to require that $a + 1$ be prime. Thus, in particular, it may be assumed that $a_0 = 1$. The possible prime divisors of $\sigma(p^a)$, where p and $a + 1$ are prime and $a > 1$, are $a + 1$ (exactly) if and only if $p \equiv 1 \pmod{(a+1)}$, and primes $q \equiv 1 \pmod{(a+1)}$. (See Nagell [11, Theorems 94 and 95].)

For our theorem, we suppose that N is an odd perfect number and $N < 10^{160}$. If p^a, a even, is a postulated component of N, then we may assume $p^a < 10^{80}$, since otherwise $N \geq p^a\sigma(p^a) > p^{2a} > 10^{160}$. (The same is true, though not obvious, if $a = 1$; however this case does not arise.) This bounds the possible exponents to be considered.

To avoid repeating the same factorizations, some experimentation suggested that we postulate (and then eliminate) the following primes in turn as factors of N: $127, 19, 7, 11, 31, 13, 3, 5$. If none of these is a factor of N, then N must have at least 101 distinct prime factors, for if there were less, then

$$\frac{\sigma(N)}{N} = \prod_{i=0}^{t} \frac{p_i - p_i^{-a_i}}{p_i - 1} < \prod_{i=0}^{t} \frac{p_i}{p_i - 1} \leq \frac{17}{16}\frac{23}{22}\frac{29}{28}\prod_{P}\frac{p}{p-1} < 2,$$

where P is the set of primes p satisfying $37 \leq p \leq 599$, $p \neq 127$. This is a contradiction. (There are 100 factors altogether in the right-hand product.) We then have

$$N \geq \left(17 \cdot 23 \cdot 29 \cdot \prod_{P} p\right)^2 \cdot 601 > 10^{473},$$

so that the elimination of the eight mentioned primes as possible factors of N proves the theorem. (It was convenience, rather than necessity, and a striving for simplicity of exposition, that led us to consider these primes.) Once one of the eight primes was eliminated, its occurrence in a later factor chain terminated that chain.

Individual factor chains were continued, using the largest prime found in the previous factorization, until either there was a component exceeding 10^{80} or until the product of every prime generated in the chain, often with their exponents adjusted upwards in conformity with Euler's form, exceeded 10^{160}. Care was required in insisting the exponent be 1 on the largest prime generated which was congruent to 1 (mod 4), if no other prime in the chain had been postulated as the special prime (unless of course this largest prime was generated more than once—but it never was).

Some chains could be terminated early because of the occurrence of previously eliminated primes, as mentioned above. In other cases, several small primes were generated whose product, with exponents adjusted in accordance with Euler's form, was a number m satisfying $S = \sigma(m)/m > 2$. Any divisor l of N must satisfy $\sigma(l)/l \leq 2$, so this "S-test" provided another means of terminating chains early.

Many composite numbers or probable primes arose for which factorization or primality testing was not required. These numbers were checked for common factors with other numbers in the chain and then entered into the product with those numbers, with exponent 1. Testing for common factors by the Euclidean algorithm is, in general, must faster than factorization.

3. A Closer Look. Figure 1 is an extract from the program's output, illustrating the points made above. It shows the end of the elimination of 19 as a factor of N, and the beginning of the elimination of 7. The various symbols are described in the following discussion of some of the lines.

```
940:  19^42 => 189176725481496888955557513.p29,  B1 132
941:    28461948730641665973894996037^1 => 7.223.n,  B1 164
942:    28461948730641665973894996037^2 => 3.67.97.397.433.n,  B1 202;  q^4, B2 227
944:  19^46 => p59,  B1 117
945:    p59^1 => 3.37.113.n,  B1 180;  q^2, B2 235
947:  19^52 => 107.3239308216871 53.2551089855701675251204783.p26,  B1 173
948:  19^58 => p75,  B1 148
949:    p75^1 => 3.n,  B1 222;  q^2, B2 296
951:  19^60 => p77,  B1 153
952:    p77^1 => 109.n,  B1 231;  q^2, B2 306
954:  19^66,  B2 168

955:  7^2 => 19...,  D
956:  7^4 => 2801,  B1 6
957:    2801^1 => 3.467,  B1 13
958:      467^2 => 19...,  D
959:      467^4 => 11.31.41.3409261,  B1 39
960:        3409261^2 => 3.7.31.43...,  S 3^2.7^4.11^2.31^2.41^2.43^2
961:        3409261^4 => 5...,  S 3^2.5^2.7^4
962:        3409261^6 => 1009.44129.387199.p26,  B1 144
963:          91077720102741705253194653^2 => 43...,  S 3^2.7^4.11^2.31^2.41^2.43^2
964:          91077720102741705253194653^4,  B2 207
965:        3409261^10 => 74449.16180057477.138855190541.P40,  B1 222
966:        3409261^12 => 53...,  S 3^2.7^4.11^2.31^2.41^2.53^2.467^4
967:        3409261^16,  B2 209
968:      467^6 => 449.104707.221110919,  B1 55
969:        221110919^2 => 13.p16,  B1 89
970:          3760772209395037^2 => 3.7.2371.164173.741859.P16,  B1 148
971:            2332276869007711^2 => 19...,  D
972:            2332276869007711^4,  B3 179
973:          3760772209395037^4 => 41.n,  B1 184;  q^6, B2 186
975:        221110919^4 => 41.3994171.66010998331.p15,  B1 139
976:          221112832862321^2 => 31.151.n,  B1 171;  q^4, B3 167
```

FIGURE 1

Extract from the computer output.

955: If $7^2 \parallel N$ then $\sigma(7^2) = 3 \cdot 19 \mid N$. We use D to indicate a divisor previously eliminated and ... to indicate that the other factors are irrelevant.

956: If $7^4 \parallel N$ then $\sigma(7^4) = 2801 \mid N$.

957: 2801 is the special prime. Later cases will consider the exponents $2, 4, 6, 10, \ldots$ on 2801. We use B1 as a "running" bound; it is $\lfloor \log_{10} B \rfloor$, where B is the least common multiple of the primes appearing to that point (possibly with exponents adjusted in accordance with Euler's form). Here B1 = 13 since so far $N \geq 3^2 \cdot 7^4 \cdot 467^2 \cdot 2801 > 10^{13}$.

960: The factor $m = 3^2 \cdot 7^4 \cdot 11^2 \cdot 31^2 \cdot 41^2 \cdot 43^2$ of N may be identified; but $\sigma(m)/m > 2$. Such an occurrence is indicated by S followed by the worst-case possible exponents on the primes that have occurred.

962: p# means a prime of # decimal digits, congruent to 1 (mod 4), defined by division or the same as on the previous line. Here, p26 = $\sigma(3409261^6)/(1009 \cdot 44129 \cdot 387199)$. This prime is printed in full on the following line.

964: B2 is $\lfloor \log_{10} B \rfloor$, where B is the square of the indicated component. Here, $N > (\mathrm{p26})^8 > 10^{207}$.

970: P# is a prime with # decimal digits, like p# but congruent to 3 (mod 4). Such primes are always squared in the product. The prime on the left is p16 from line 969.

972: B3 is $\lfloor \log_{10} B \rfloor$, similar to B1 but where, in calculating B, account is not taken of $\sigma(p^a)$ for the current component p^a. Thus this bound applies when $p^a \mid N$, not merely when $p^a \parallel N$. The present subcase is concluded because we must have

$$N \geq 2801 \cdot (3 \cdot 13 \cdot 449 \cdot 2371 \cdot 104707 \cdot 164173 \cdot 741859 \cdot 221110919 \cdot 3760772209395037)^2 \\ \cdot (7 \cdot 2332276869007711)^4 \cdot 467^6 > 10^{179}.$$

973: n means a number (prime or composite—it was not necessary to determine which in order to exceed our bound) which is entered into the least common multiple with the other primes in the chain. The use of the least common multiple effectively clears n of any earlier primes in the chain. As usual, those other primes may have their exponents adjusted.

q refers to the prime at the beginning of the line. This is a space-saving device only. Note the implicit line number 974.

The complete output has 3133 lines and appears in the Supplements section of this issue.

4. Comments on the Program. Our program is written almost entirely in Pascal and runs on a VAX computer. A few inner loops of the multiple-precision arithmetic routines are coded in VAX assembler to speed up their execution.

The program accepts as input a bound K, a set of prime "forbidden divisors", i.e., primes which may be assumed to have already been ruled out as divisors of N, and one or more further primes to be considered as potential divisors of N.

The program implements the procedure outlined in Section 2. Suppose that at some point we are considering powers of p as divisors of N and we can assume $p^a | N$, where $a + 1$ is prime. At this point we know that $B \mid N$, where B is a certain product of prime powers considered already.

The program computes two bounds, $\beta_2 = p^{2a}$ and $\beta_3 = \mathrm{LCM}(p^a, B)$, and their maximum $\beta = \max(\beta_2, \beta_3)$. Clearly, $N \geq \beta$, so the program can stop consideration of powers of p if $\beta > K$. This is indicated in the output by B2 or B3, followed by $\lfloor \log_{10} \beta \rfloor$. For example, at line 954 of Figure 1, the program stops consideration of powers of 19 because $\lfloor \log_{10} 19^{132} \rfloor = 168$ is sufficiently large.

If β is not sufficiently large, the program assumes that $p^a \| N$ and attempts to factorize $\sigma(p^a)$, using first trial division and then Lenstra's single-phase elliptic curve algorithm [2] (except if $p \in \{3, 5, 7, 11\}$, in which case we used Brillhart et al. [4]). The program gives up the attempt if it does not succeed in a specified number of iterations. At this point it generally has

$$\sigma(p^a) = c \cdot \prod_{i=1}^{j} p_i^{a_i},$$

where c is either 1 or a composite number, and the $p_i^{a_i}$ are powers of distinct primes p_i. (We can assume that the p_i are not primes which have been considered already and ruled out as possible divisors of N.)

At this point, the known divisor B of N can be updated. We know that $p_i^{b_i} \mid N$, where

$$b_i = \begin{cases} a_i + 1, & \text{if } a_i \text{ is odd and } p_i \text{ could not be the special prime,} \\ a_i, & \text{otherwise,} \end{cases}$$

so we can set $B \leftarrow \mathrm{LCM}(B, c, \prod_{i=1}^{j} p_i^{b_i})$. In the output, the program gives B1, followed by $\lfloor \log_{10} B \rfloor$ to indicate the size of B.

The program performs the S-test using exact (rational) arithmetic and the known factorization of B. Here, if one of several primes appearing to the first power in B could be the special prime, then we must assume that the *smallest* of them is special and square the others. For other bounds, such as B1, we must assume that the *largest* such prime is special and square the others.

If p^a has been ruled out as an exact divisor of N, we increase a and repeat the procedure outlined above. As noted in Section 2, it is enough to consider exponents a such that $a + 1$ is prime.

If p^a has not been ruled out, we choose one of the p_i which divide $\sigma(p^a)$ and consider powers of p_i as divisors of N. Generally, the program chooses the largest known p_i, but it will avoid certain primes if instructed to do so (usually as a result of some experimentation). For example, we avoid 128341 and 567661 because this shortens the proof by 58 lines.

If the choice of p_i would cause the program to loop forever in a finite cycle of primes, the next largest candidate p_i is chosen, etc. If no choice of p_i is satisfactory (possibly because $\sigma(p^a)$ has no known prime factors), the program "backtracks" by ruling out the choice of p at an earlier stage. Eventually, either the program succeeds by constructing a proof, or fails by backtracking to one of the primes which were input as divisors to be considered.

The program prints a "trace" of its progress, and in particular it prints those p^a at which it has to backtrack. We may then attempt to factorize $\sigma(p^a)$ by other means (e.g., use of a two-phase elliptic curve algorithm [2]) and add any new factors to a file of "hints". When attempting a factorization, the program looks in this file of hints before attempting the elliptic curve algorithm. The program also adds factors which it finds by the elliptic curve algorithm to the hints file. Our hints file now contains several thousand factors of $\sigma(p^a)$ and is indexed by p and a for fast access.

Our first proof to 10^{160} had many incomplete factorizations and several examples of backtracking. However, we have now eliminated the backtracking and completed all factorizations which are relevant to the proof. An element of luck entered into this as our elliptic curve algorithm cannot be relied on to find factors greater than 10^{20} in a reasonable time (i.e., a few days on a VAX 11/750). The largest factor required for the proof to 10^{160} is the 31-digit factor $p_{31} = 5956707000538571084106691363703$ of $\sigma(61^{42})$. Finding p_{31} by the elliptic curve algorithm required a total of about 1.5×10^9 multiplications mod $\sigma(61^{42})$ on several SUN workstations.

Our program uses a probabilistic primality test, so it is possible (although most unlikely) that it might mistake a composite number for a prime. However, all probable primes required for the proof were written on a file and rigorously proved prime by another program. In all cases, the latter program was able to prove primality using a recursive application of the "$p-1$" or "$p+1$" primality tests [4].

5. Extensions. Our bound of 10^{160} could certainly be improved if a few difficult factorizations were completed. For example, to go beyond 10^{160}, we need to factorize the 81-digit composite number $\sigma(13^{72})$. Of course, special arguments can be used if we know that $13^{72} \parallel N$, but in order to keep the proof simple, we wish to avoid the need for a multiplicity of special cases.

In an unpublished paper [3], we have extended the bound of 10^{160} given here to 10^{200}. This uses an improvement of the B2 bound to handle composite numbers such as $\sigma(13^{72})$. Further computations are still being carried out, and our lower bound is likely to be still further improved. We hope to publish a second paper on this subject, containing the improved technique, at a later date.

Acknowledgment. We thank Dr. H. J. J. te Riele and R. Silverman for their kind assistance with some factorizations which, although not essential to the proof, enabled us to avoid backtracking and to eliminate the last remaining composite numbers whose appearance in the proof was aesthetically displeasing.

Added in Proof. The lower bound has been improved now to 10^{300}. The details will be published later. Many of the factorizations required were supplied by Dr. te Riele, including: $\sigma(13^{72}) = 1450095861024908292185525482233366637 \cdot p46$.

Computer Sciences Laboratory
Research School of Physical Sciences
The Australian National University
GPO Box 4
Canberra, ACT 2601, Australia
E-mail: rpb@phys4.anu.oz

School of Mathematical Sciences
University of Technology, Sydney
PO Box 123
Broadway, NSW 2007, Australia
E-mail: glcohen@utscsd.oz

1. W. BECK & R. NAJAR, "A lower bound for odd triperfects," *Math. Comp.*, v. 38, 1982, pp. 249–251.

2. R. P. BRENT, "Some integer factorization algorithms using elliptic curves," *Australian Computer Science Communications*, v. 8, 1986, pp. 149–163.

3. R. P. BRENT, G. L. COHEN & H. J. J. TE RIELE, *An Improved Technique for Lower Bounds for Odd Perfect Numbers*, Report TR-CS-88-08, Computer Sciences Laboratory, Australian National University, August 1988.

4. J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN & S. S. WAGSTAFF, JR., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High Powers*, Contemp. Math., vol. 22, Amer. Math. Soc., Providence, R.I., 1983.

5. M. BUXTON & S. ELMORE, "An extension of lower bounds for odd perfect numbers," *Notices Amer. Math. Soc.*, v. 23, 1976, p. A-55.

6. M. BUXTON & B. STUBBLEFIELD, "On odd perfect numbers, " *Notices Amer. Math. Soc.*, v. 22, 1975, p. A-543.

7. G. L. COHEN & P. HAGIS, JR., "Results concerning odd multiperfect numbers," *Bull. Malaysian Math. Soc.*, v. 8, 1985, pp. 23–26.

8. R. K. GUY, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1981.

9. P. HAGIS, JR., "A lower bound for the set of odd perfect numbers," *Math. Comp.*, v. 27, 1973, pp. 951–953.

10. H.-J. KANOLD, "Über mehrfach vollkommene Zahlen. II," *J. Reine Angew. Math.*, v. 197, 1957, pp. 82–96.

11. T. NAGELL, *Introduction to Number Theory*, Chelsea, New York, 1981.

12. B. M. STEWART, *Math. Rev.*, **81m**:10011.

13. B. STUBBLEFIELD, "Lower bounds for odd perfect numbers (beyond the googol)" in *Black Mathematicians and Their Works*, Dorrance, Ardmore, PA, 1980, pp. 211–222.

14. B. TUCKERMAN, "A search procedure and lower bound for odd perfect numbers," *Math. Comp.*, v. 27, 1973, pp. 943–949.

15. S. WAGON, "Perfect numbers," *Math. Intelligencer*, v. 7, 1985, pp. 66–68.