Internat. J. Math. & Math. Sci.
Vol. 10 No. 1 (1987) 125-130

THE POWER OF POWERFUL NUMBERS

R.A. MOLLIN

Mathematics Department, University of Calgary,
Calgary, Alberta, Canada, T2N 1N4

(Received May 14, 1986 and in revised form June 2, 1986)

ABSTRACT. In this note we discuss recent progress concerning powerful numbers, raise new questions and show that solutions to existing open questions concerning powerful numbers would yield advancement of solutions to deep, long-standing problems such as Fermat's Last Theorem. This is primarily a survey article containing no new, unpublished results.

KEY WORDS AND PHRASES. *Powerful Number, Fermat's Last Theorem, Quadratic Field, Diophantine Equation.*
AMS Subject Classification (1980): Primary: 10A05, 10B15, 10B35;
Secondary: 10J06, 10L10, 12A50, 12A25.

A powerful number is a positive integer n which is divisible by p^2 whenever n is divisible by the prime p; i.e., in the canonical prime factorization of n, no prime appears with exponent one. It is useful to note that all powerful numbers are expressible in the form x^2y^3 where x and y are positive integers. The term powerful was introduced by S.W. Golomb in [1], although P. Erdös and G. Szerkeres [2] investigated the more general case of positive integers n such that p^i divides n whenever p divides n where $i > 1$.

In [1] Golomb commented that there was no known case of a powerful pair $(4k - 1, 4k + 1)$. In [3] R.A. Mollin and P.G. Walsh gave an algorithm for finding infinitely many such pairs. However 4k was found not to be powerful. This naturally leads us to ask whether there exists three consecutive powerful numbers, (which as Golomb [1] noted must be of the form $(4k - 1, 4k, 4k + 1)$ if they exist). In [4] Mollin and Walsh conjectured that such triples do not exist, (it escaped the attention of both Mollin and Walsh [4] and Granville [5] that the conjecture asserting the non-existence of three consecutive powerful numbers was first made by

Erdos [7]. However Mollin and Walsh were the first to provide the data cited above (including the following Theorem 1) in support of the conjecture). They gave substantial numerical evidence for this conjecture and they proved in particular that:

Theorem 1. (R.A. Mollin and P.G. Walsh [4])

The following are equivalent:

(1) Three consecutive powerful numbers exist.

(2) There exist powerful numbers P and Q with P even and Q odd such that $P^2 - Q = 1$.

(3) There exists a square-free integer $m \equiv 7 \pmod 8$ with $T_1 + U_1\sqrt{m}$ being the fundamental unit of $Q(\sqrt{m})$ and, for some odd integer k, T_k is an even powerful number and $U_k \equiv 0 \pmod m$ is an odd number where $(T_1 + U_1\sqrt{m})^k = T_k + U_k\sqrt{m}$.

Mollin and Walsh showed that if these equivalent conditions hold then the minimal example of three consecutive powerful numbers for the least case, m = 7, arises from $(8 + 3\sqrt{7})^{114254287}$. Several avenues for proving that the conditions do not hold were given. Although the conjecture remains open, A. Granville has proved in [5] that the truth of the conjecture has rather strong implications. He proved using elementary techniques that:

Theorem 2. (A. Granville [5]).

If the conjecture of Mollin and Walsh is true then there exists an infinite sequence of primes p for which p^2 does not divide $2^p - 2$.

Corollary 1.

If the conjecture of Mollin and Walsh is true then there exists an infinite sequence of primes p for which the first case of Fermat's Last Theorem is true.

L. Adleman and D.R. Heath-Brown recently proved in [6] that there is in fact an infinite sequence of primes p for which the first case of Fermat's Last Theorem holds, although ostensibly a different sequence of primes than that of Granville. However their "sieve" techniques are relatively quite deep. Therefore given the elementary algebraic nature of Granville's proof, and Mollin and Walsh's Theorem 1, it would be highly valuable to find an elementary "algebraic" proof of the conjecture. The best route for achieving this task would be to find a general factorization result for the T_k's of Theorem 1. Such results are known for the U_k's via Lucas-Lehmer theory (see [8] and [9]), but such results for the T_k's seem to have been overlooked in the literature. The related problem for powers is solved; i.e., three consecutive integers cannot be proper powers (for example see P. Erdos [7] and P. Ribenboim [10, p.207]). In fact many questions pertaining to powerful numbers, when restricted to powers, are known. On the other hand some questions which have been answered for powerful numbers remain open for powers, as the following example shows. Note that in what follows n is a proper difference of two powerful numbers whenever $n = p_1 - p_2$ with p_1 and p_2 powerful and g.c.d.

$(p_1, p_2) = 1$. Although Golomb [1] conjectured that 6 is not a proper difference of two powerful numbers, and that there are infinitely many integers which cannot be represented as a proper difference of two powerful numbers, we have that $6 = 5^4 \cdot 7^3 - (463)^2$ a difference of powerful numbers, whereas it remains a conjecture that 6 is not a difference of powers.

The following fact is derived from an undated letter which Fermat wrote (probably to Mersenne) in 1643 (see [11, pp.110-111]). "An odd number can be written as a product of two factors in exactly as many ways as it can be expressed as a difference of two squares of non-negative numbers." Clearly not all even integers are representable as a difference of squares. In an attempt to find a more general representation of integers as a difference of integers involving prime powers larger than one it is natural to ask: which integers are a proper difference of two powerful numbers? The antithesis of the Golomb conjecture cited above was proved by W.L. McDaniel in [12] who gave an existence proof of the fact that every non-zero integer is a proper difference of two powerful numbers in infinitely many ways. In [3] Mollin and Walsh gave an elementary proof of McDaniel's result using Richaud-Degert quadratic fields (see [13] and [14]), and the theory of what is commonly (but erroneously) called Pell's equation ("Pell mathematically was a nonentity and humanly an egregious fraud", (see E.T. Bell [16]). Bell goes on to say that Pell never even saw the equation). Moreover an algorithm for determining such representations was given in [3]. However in both McDaniel's proof and in the Mollin-Walsh proof one of the powerful numbers in each representation of a given integer $n \neq 0$ is a square when $n \not\equiv 2 \pmod 4$ but not necessarily otherwise. This led Vanden Eynden in [15] to complete the task of showing:

Theorem 3. (McDaniel [12] and Vanden Eynden [15]).

Every non-zero integer is representable as a proper difference of a square and a non-square powerful number in infinitely many ways.

The result leads us to ask: Which integers are representable as a proper nonsquare difference of powerful numbers?, (i.e., a proper difference of two powerful numbers neither of which is a perfect square.) A solution is known:

Theorem 4. (Mollin and Walsh [3] and [17]).

Every non-zero integer is representable in infinitely many ways as a proper nonsquare difference of powerful numbers.

Furthermore in [3] and [17] Mollin and Walsh provided an algorithm for finding such representations. Until the Mollin-Walsh result, Theorem 4, the only known integer to have such a representation was the integer 1, (see D.T. Walker [18]).

Given the solution of the latter problem and the implications for Fermat's Last Theorem of the first cited problem, it is natural to ask for a similar setting in "higher" rings of integers. Let K be an algebraic number field and let $\mathcal{O}_K$ be the ring of integers of K. Call $\alpha \in \mathcal{O}_K$ a powerful algebraic integer if $N(\alpha)$ is powerful where N denotes the absolute norm from K to the rational number field Q. What are the consecutive powerful algebraic integers in $\mathcal{O}_K$? In particular for

$K = Q(\sqrt{d})$, d square-free, what are the consecutive r-tuples of powerful algebraic integers for a given rational integer $r > 1$, if any? Given the results which solved Fermat's Last Theorem in quadratic number fields by F.H. Hao and C.J. Parry [19]; does there exist a similar connection between consecutive powerful numbers and the solution of Fermat's Last Theorem in quadratic number fields as it does for Q?

Now we turn to open questions involving sums of powerful numbers. In a recent personal communication to the author, Professor Paul Erdös has indicated that over 10 years ago he conjectured that for sufficiently large N, every integer $n > N$ is representable as a sum of at most three powerful numbers. In [4] Mollin and Walsh conjectured more specifically that, with the exception of 7, 15, 23, 87, 111 and 119 every positive integer is the sum of at most three powerful numbers. Moreover evidence for the conjecture's validity as well as routes for attacking the problem were also given in [4].

It is well-known that an integer n is a sum of two integer squares if and only if n has no prime $p \equiv 3 \pmod 4$ appearing to an odd exponent in its canonical prime factorization. With this as a precursor, we ask which integers are a sum of two powerful numbers? In particular; which primes are a sum of two powerful numbers. As noted in Mollin-Walsh [4], Guass has given us a partial answer. If $p \equiv 1 \pmod 3$ and 2 is a cube modulo p then $p = x^2 + 27y^2$. When 2 is not a cube modulo $p \equiv 1 \pmod 3$ anything can happen. As noted earlier, for example, 7 is not a sum of less than four powerful numbers, yet $379 = 6^2 + 7^3$. This leads us to an intimate link between this problem and certain class number problems for quadratic number fields, (see Mollin [20] - [22]). For example $N(6 + 7\sqrt{-7}) = 379$. Which primes are obtainable as a norm from an imaginary quadratic field of class number one, in such a way as to be the sum of a square and a non-square powerful number? Which primes are so achievable from imaginary quadratic fields with class number larger than 1? For example, $N(2 + 3\sqrt{-15}) = 2^2 + 3^3 5^2$ but $78157 = 2^5 + 5^7$ is not the sum of a square plus a non-square powerful number. Certainly 78157 is the norm from some imaginary quadratic field, but not in such a way to be a sum of two powerful numbers. There are several avenues in this class number direction which deserve exploration.

Finally we refer the reader to the list of references for many other relevant works on powerful numbers not cited above. The first 22 items are referenced in the above text; while the remaining 12 items, although not referenced, are useful references and are listed alphabetically.

ACKNOWLEDGEMENT. The author's research is supported by N.S.E.R.C. Canada and is dedicated to Professor Shanks on the occasion of his 70th birthday.

References

1. S.W. Golomb, Powerful numbers, Amer. Math Monthly 77 (1970), 848-855.

2. P. Erdos and G. Szerkeres, Uber die Anzahl der Abelschen Gruppen gegehener Ordnung und uber ein verwandtes zahlentheoretisches Problem, Acta Litt. Sci. Szeged 7 (1934), 95-102.

3. R.A. Mollin and P.G. Walsh, On powerful numbers, 9 (1986), 801-806, Int. J. Math and Math. Sci.

4. R.A. Mollin and P.G. Walsh, A Note on Powerful Numbers, Quadratic Fields and the Pellian, C.R. Math. Rep. Acad. Sci. Canada 8 (1986), 109-114.

5. A. Granville, Powerful Numbers and Fermat's Last Theorem, (to appear: C.R. Math. Rep. Acad. Sci. Canada).

6. L.M. Adleman and D.R. Heath-Brown, The First Case of Fermat's Last Theorem, Invent. math., 79 (1985), 409-415.

7. P. Erdos, Consecutive Integers, Eureka, 38 (1975 - 76), 3 - 8.

8. D.H. Lehmer, An Extended Theory of Lucas' Functions, Annals Math. 2 (1930), 419-448.

9. E. Lucas, Theorie des fonctions numeriques simplement periodiques, American J. Math. 1 (1878), 184-240. (English translation available from the Fibonacci Association, San José University, San José, California (1969)).

10. P. Ribenboim, Consecutive Powers, Expositiones Math. 2 (1984), 193-221.

11. A. Beck, M.N. Bleicher and D.W. Crowe, Excursions Into Mathematics, Worth, New York, 1969.

12. W.L. McDaniel, Representations of every integer as the difference of powerful numbers, Fibonacci Quart. 20 (1982), 85-87.

13. G. Degert, Uber die Bestimmung der Grundeinheit gewisser reell-quadrastischer Zahlkorper, Abh. Math. Sem. Univ. Hamburg 22 (1958), 92-97.

14. C. Richaud, Sur la resolution des equations $x^2 - Ay^2 = 1$, Atti. Acad. pontif. Nuovi Lincei (1866), 177-182.

15. C. Vanden Eynden, Differences Between Squares and Powerful Numbers, (to appear: Fibonacci Quart.).

16. E.T. Bell, The Last Problem, Simon and Schuster, New York, 1961.

17. R.A. Mollin and P.G. Walsh, On non-square powerful numbers, (to appear: Fibonacci Quart.).

18. D.T. Walker, Consecutive integer pairs of powerful numbers and related Diophantine equations, Fibonacci Quad. 14 (1976), 111-116.

19. F.H. Hao and C.J. Parry, The Fermat Equation over Quadratic Fields, J. Number Theory 19 (1984), 115-130.

20. R.A. Mollin, Lower Bounds for Class Numbers of Real Quadratic Fields, Proc. Amer. Math. Soc. 96 (1986), 545-550.

21. R.A. Mollin, Class Numbers of Quadratic Fields Determined by Solvability of Diophantine Equations, (to appear: Math. Comp.).

22. R.A. Mollin, On Class Numbers of Quadratic Extensions of Algebraic Number Fields, Proc. Japan Acad. Sci. 62 Series A (1986), 33-36.

23. P. Erdos and J.L. Selfridge, The product of consecutive integers is never a power, Illinois J. Math. 19 (1975), 292-301.

24. P. Erdos, Problems and results on number theoretic properties of consecutive integers and related questions, Proceedings of the Fifth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man. 1975) pp.25-44. Congressus Numerantium, No. XVI, Utilitas Math. Publ., Winnipeg, Man., 1976.

25. A. Ivic and P. Shiu, The Distribution of Powerful integers, Illinois J. Math. 26 (1982), 576-590.

26. C.B. Lacompagne and J.L. Selfridge, Large highly powerful numbers are cubeful, Proc. Amer. Math. Soc. 91 (1984), 173-181.

27. E. Lehmer, Patterns of Power Residues, J. Number Theory 17 (1983), 37-46.

28. A. Makowski, On a problem of Golomb on powerful numbers, Amer. Math. Monthly 79 (1972), 761.

29. W.A. Sentance, Occurrences of consecutive odd powerful numbers, Amer. Math. Monthly 88 (1981), 272-274.

30. P. Shiu, On the number of square-full integers between successive squares, Mathematika 27 (1980), 171-178.

31. P. Shiu, On square-full integers in a short interval, Glasgow Math. J., 25 (1984), 127-134.

32. E.G. Straus and M.V. Subbarao, On exponential divisors, Duke Math. J. 41 (1974), 465-471.

33. D. Suryanarayana, The distribution of square-full integers, Ark. Math. 11 (1973), 195-201.

34. D. Suryanarayana, On the distribution of some generalized square-full integers, Pacific J. Math. 72 (1977), 547-555.