Internat. J. Math. & Math. Sci.
Vol. 9. No. 4 (1986) 801-806

ON POWERFUL NUMBERS

R.A. MOLLIN and P.G. WALSH

Department of Mathematics and Statistics
University of Calgary
2500 University Drive N.W.
Calgary, Alberta, Canada T2N 1N4

(Received December 10, 1985)

ABSTRACT. A powerful number is a positive integer n satisfying the property that p^2 divides n whenever the prime p divides n; i.e., in the canonical prime decomposition of n, no prime appears with exponent 1. In [1], S.W. Golomb introduced and studied such numbers. In particular, he asked whether (25, 27) is the only pair of consecutive odd powerful numbers. This question was settled in [2] by W.A. Sentance who gave necessary and sufficient conditions for the existence of such pairs. The first result of this paper is to provide a generalization of Sentance's result by giving necessary and sufficient conditions for the existence of pairs of powerful numbers spaced evenly apart. This result leads us naturally to consider integers which are representable as a proper difference of two powerful numbers, i.e. $n = p_1 - p_2$ where p_1 and p_2 are powerful numbers with g.c.d. $(p_1, p_2) = 1$. Golomb (op.cit.) conjectured that 6 is not a proper difference of two powerful numbers, and that there are infinitely many numbers which cannot be represented as a proper difference of two powerful numbers. The antithesis of this conjecture was proved by W.L. McDaniel [3] who verified that every non-zero integer is in fact a proper difference of two powerful numbers in infinitely many ways. McDaniel's proof is essentially an existence proof. The second result of this paper is a simpler proof of McDaniel's result as well as an effective algorithm (in the proof) for explicitly determining infinitely many such representations. However, in both our proof and McDaniel's proof one of the powerful numbers is almost always a perfect square (namely one is always a perfect square when $n \not\equiv 2 \pmod 4$). We provide in §2 a proof that all even integers are representable in infinitely many ways as a proper nonsquare difference; i.e., proper difference of two powerful numbers neither of which is a perfect square. This, in conjunction with the odd case in [4], shows that every integer is representable in infinitely many ways as a proper nonsquare difference. Moreover, in §2 we present some miscellaneous results and conclude with a discussion of some open questions.

KEY WORDS AND PHRASES. *Powerful number, integer.*
1980 MATHEMATICS SUBJECT CLASSIFICATION CODE. 10A99, 10B05, 10L99

1. PROPER DIFFERENCES OF POWERFUL NUMBERS

The first result is a natural generalization of Sentance [2, Theorem, p. 272].

Lemma 1.1.

(I) Suppose that x and n are relatively prime integers with different parity. Then x - n and x + n are powerful numbers if and only if $x^2 - n^2 = my^2$ has an integer solution $y \equiv 0 \pmod{m}$.

(II) Suppose that x and n are relatively prime odd integers. Then (x - n)/2 and (x + n)/2 are powerful numbers if and only if $x^2 - n^2 = my^2$ has an integer solution $y \equiv 0 \pmod{2m}$.

PROOF. (I) If x + n and x - n are powerful then $x^2 - n^2 = my^2$ where $m = \pm p_1 p_2 \ldots p_k$ with p_i for i = 1, 2, ..., k being all of the (distinct) primes dividing $x^2 - n^2$ which appear to an odd exponent in its prime decomposition.

Conversely, if $x^2 - n^2 = my^2$ with $y \equiv 0 \pmod{m}$ then it suffices to show that g = g.c.d.(x - n, x + n) = 1. If g > 1 then $2n \equiv 0 \pmod{p}$ for some prime p dividing g. However, if p = 2 then x and n have the same parity contradicting the hypothesis; and if p divides n then x and n are not relatively prime, again contradicting the hypothesis. This secures (I).

(II) If (x-n)/2 and (x + n)/2 are powerful then $(x^2 - n^2)/4 = mz^2$ with $z \equiv 0 \pmod{m}$ as in (I). Thus $x^2 - n^2 = my^2$ where $y = 2z \equiv 0 \pmod{2m}$.

Conversely, if $x^2 - n^2 = my^2$ where $y \equiv 0 \pmod{2m}$ then it suffices to show that g = g.c.d.((x - n)/2,(x + n)/2) = 1. If g > 1 then n is divisible by some prime p dividing g. This forces g.c.d. (x, n) > 1 contradicting the hypothesis, and thereby establishing the lemma. (Q.E.D.)

Lemma 1.1 effectively gives us a criterion for exhibiting even positive integers as a proper difference of two powerful numbers. There is a natural method of so doing by using fundamental units of quadratic fields.

The following example not only illustrates the process but also is a counterexample to Golomb's conjecture [1] that 6 is not a proper difference of two powerful numbers. Note that this example also appears in [3].

EXAMPLE 1.1. Since $9 = 4^2 - 7$ and the fundamental unit of $Q(7^{1/2})$ is $8 + 3(7)^{1/2}$ then we get that the norm of $(8 + 3(7)^{1/2})^4(4 + 7^{1/2})$ is $(214372)^2 - (81025)^2(7) = 9$. Thus the x of Lemma 1.1 (I) is 214372. Hence 214372 ± 3 are powerful. This yields the representation $6 = 214375 - 214369 = 5^4 7^3 - 463^2$.

The following is a simple proof of [3, Theorem 3, p. 87] containing an effective algorithm.

THEOREM 1.1. Every non-zero integer is a proper difference of two powerful numbers in infinitely many ways.

PROOF. Note that n is a proper difference of two powerful numbers if and only if -n is such a difference. Thus given n, it suffices to prove the result for either n or -n. We require the following notation. Let:

$$m = \begin{cases} -n & \text{if } n \equiv 3 \pmod 4 \\ n & \text{if } n \equiv 0 \text{ or } 1 \pmod 4 \\ (n/2)^2 & \text{if } n \equiv 2 \pmod 4 \end{cases};$$

$$A = |((m - \alpha)/2) + \beta|$$

and,

$$B = ((m - \gamma)/2)^2 + \delta$$

where:

$$(\alpha, \beta, \gamma, \delta) = \begin{cases} (-3, 0, -1, 2) & \text{if } n = 1, 2 \text{ or } 5 \\ (0, 1, 0, 1) & \text{if } n \equiv 0 \pmod 4 \\ (1, 0, 3, -2) & \text{in all other cases} \end{cases}$$

(Note that B cannot be a perfect square). Thus $A^2 - B = \pm m$ and g.c.d.(A, B) = 1 since g.c.d. (A, m) = 1. Now let:

$$T + U(B)^{1/2} = \begin{cases} 2 + (3)^{1/2} & \text{if } n = 1 \text{ or } 2 \\ 10 + 3(11)^{1/2} & \text{if } n = 5 \\ (n/2) + (B)^{1/2} & \text{if } n \equiv 0 \pmod 4 \\ [((m - 3)/2)^2 - 1] + |((m - 3)/2|(B)^{1/2} & \text{in all other cases} \end{cases}$$

Note that g.c.d.(B, U) = 1, and $T^2 - U^2B = \pm 1$. Furthermore, it is worth noting that if B is square-free then quadratic fields of type $Q(B^{1/2})$ are said to be of "Richaud-Degert type", and (by [5] and [6]) $T + U(B)^{1/2}$ is the fundamental unit of $Q(B^{1/2})$. Investigation of such fields was the inspiration for the idea of this proof.

Now let $(T + U(B)^{1/2})^i = T_i + U_i(B)^{1/2}$ for $i > 1$. Consider

$$(T_i + U_i(B)^{1/2})(A + B^{1/2}) = A_i + C_i(B)^{1/2}$$

where $A_i = T_iA + U_iB$ and $C_i = AU_i + T_i$. We now claim that

$$g = \text{g.c.d.}(A_i, C_i) = 1 \tag{1.1}$$

and

$$C_i \equiv 0 \pmod B. \tag{1.2}$$

If a prime p divides g then

$$A_i = ps \quad \text{where } s \in Z \tag{1.3}$$

and

$$C_i = pt \quad \text{where } t \in Z. \tag{1.4}$$

Multiplying (1.3) by U_i, (1.4) by T_i and subtracting we get:

$$\pm 1 = T_i^2 - U_i^2B = p(T_it - U_is)$$

a contradiction which establishes (1.1).

Since $T_i \equiv T^i \pmod B$ and $U_i \equiv iT^{i-1}U \pmod B$ then (1.2) becomes $T^i + AiT^{i-1}U \equiv 0 \pmod B$. Thus, to secure (1.2) it suffices to show that $T + AiU \equiv 0 \pmod B$. To do this we choose $i \equiv -T(AU)^{-1} \pmod B$ which is allowed since we have verified that g.c.d.(AU, B) = 1. Note that infinitely many such i exist.

Observe that if $n \not\equiv 2 \pmod 4$ then we have proved the theorem since we have $A_i^2 - C_i^2B = \pm n$ with $C_i \equiv 0 \pmod B$ and g.c.d. $(A_i, C_i) = 1$.

If $n \equiv 2 \pmod 4$ then we have $A_i^2 - C_i^2B = (n/2)^2$ with $C_i \equiv 0 \pmod B$ and g.c.d.$(A_i, n/2) = 1$. Thus by Lemma 1.1 (I), $A_i \pm (n/2)$ are powerful provided that A_i is even. The latter follows from the fact that A is even and U_i is also even provided we choose the even i's in the above congruence class modulo B. (Q.E.D.)

The following table illustrates the algorithm given in the above proof. The last column of the table provides the congruence class of i modulo B as indicated in the proof for achieving infinitely many representations of a given n as a proper difference of two powerful numbers.

Table 1.1

n	P_1	P_2	A	B	T	U	i ≡
1	$2^2 \cdot 13^2$	$3^3 \cdot 5^2$	2	3	2	1	2(mod 3)
2	3^3	5^2	2	3	2	1	2(mod 3)
3	$2^2 \cdot 7^3$	37^2	2	7	8	3	1(mod 7)
4	5^3	11^2	3	5	2	1	1(mod 5)
5	73^2	$2^2 \cdot 11^3$	4	11	10	3	1(mod 11)
6	$5^4 \cdot 7^3$	463^2	4	7	8	3	4(mod 7)
7			4	23	24	5	22(mod 23)
8	$5^4 \cdot 19^2 \cdot 31^2 \cdot 89^2$	$7^2 \cdot 17^3 \cdot 2671^2$	5	17	4	1	6(mod 17)
9	$2^4 \cdot 53593^2$	$5^4 \cdot 7^3 \cdot 463^2$	4	7	8	3	4(mod 7)
10			12	119	120	11	64(mod 119)

As a necessary result of the general nature of the algorithm given in the proof of Theorem 1.1 the representations given in Table 1.1 are not necessarily minimal. For example, if n = 7, then the power i of $T + U(B)^{1/2}$ given in table 1.1 is too large to explicitly state therein. However, we may choose A = 3, B = 2 and T = U = 1. Then $(T + U(B)^{1/2})^i (A + B^{1/2}) = -7$ for any $i \equiv 1 \pmod 2$. In particular for i = 1 we have $7 = 2^5 - 5^2$. Similarly for a specific n it is often possible to choose a smaller B than our more general algorithm allows.

§2. MISCELLANEOUS RESULTS AND OPEN QUESTIONS

In [1] Golomb mentions that no example of three consecutive powerful numbers is known, and that if they exist they must be of the form (4k - 1, 4k, 4k + 1). Moreover, he notes that no case of 4k - 1 and 4k + 1 both being powerful is known. Although the former remains open and appears to be quite difficult, we have obtained infinitely many examples of the latter.

Consider:

EXAMPLE 2.1. Let K = 32644082 then $4K + 1 = 130576329 = 3^2 \cdot 13^2 \cdot 293^2$ and $4K - 1 = 130576327 = 7^3 \cdot 617^2$. However $4K = 130576328 = 2^3 \cdot 29 \cdot 197 \cdot 2857$.

We obtained the above result by considering: $(3 + 7^{1/2})(8 + 3(7)^{1/2})^3 = 11427 - 4319(7)^{1/2}$. This gives us a method of generating infinitely many such K's. We merely choose $(3 + 7^{1/2})(8 + 3(7)^{1/2})^i$ where i is chosen as in the proof of Theorem 1.1 to give us $i \equiv 3 \pmod 7$.

Now suppose that u and v are powerful numbers such that v = u + 4k where k is odd then $(u + 2k)^2 - uv = 4k^2$. Consider:

EXAMPLE 2.2. $12 = 4 \cdot 3 = 47^2 - 13^3$. Hence $(13^3 + 2 \cdot 3)^2 - 47^2 \cdot 13^3 = 4 \cdot 3^2 = 36$. Thus $36 = 2203^2 - 47^2 \cdot 13^3$.

Note that from Table 1.1 we see that 1 is properly representable in infinitely many ways as a proper difference of two powerful numbers. This advances a question of Golomb [1] where he states that among the powerful numbers which are not perfect squares, the smallest difference known to occur infinitely often is 4. He also states that the only known instances where the difference between nonsquare powerful numbers is less than 4 are: $3 = 2^7 - 5^3$ and $1 = 2^3 \cdot 3^2 \cdot 13^2 - 23^3$. However,

consider the following representations for 2 which cannot be achieved via Theorem 1.1.

EXAMPLE 2.3. If we let $i \equiv 0 \pmod{15}$, i positive, then $(4 + (15)^{1/2})^i$ provides infinitely many representations of 2 as a proper difference of two powerful numbers neither of which is a perfect square. In particular, if $i = 15$ then $(4 + 15^{1/2})^i = 13837575261124 + 3572846569215(15)^{1/2}$. Thus, by Lemma 1.1 (II): 13837575261124 ± 1 must be powerful since 15 divides 357284659215. In fact, we find that: $2 = 13837575261125 - 13837575261123 = 5^3 \cdot 7^2 \cdot 11^2 \cdot 129^2 - 149^2 - 3^5 \cdot 71^2 \cdot 3361^2$.

Example 2.3 is no accident as the following result shows.

THEOREM 2.1. Every even integer is representable in infinitely many ways as a proper difference of two powerful numbers neither of which is a perfect square.

PROOF. As in Theorem 1.1, it suffices to prove the result for $n > 0$. Let $m > n$ be an odd integer relatively prime to n such that

$$B = m(m - n) \text{ is not a perfect square} \tag{2.3}$$

$$m \equiv 5 \pmod{8} \text{ if } n \equiv 2 \pmod{4} \tag{2.4}$$

and

$$m \equiv 3 \pmod{8} \text{ if } n \equiv 0 \pmod{4}. \tag{2.5}$$

Let (T, U) be the minimal positive integer solution of $T^2 - U^2B = 1$. By [7, Theorem, P. 57] there is at least one such B with g.c.d. (U, B) = 1.

Now let $A = m - (n/2)$ then $A^2 - B = (n/2)^2$ with g.c.d.(A, B) = 1. Let T_i, U_i, A_i and C_i be as in the proof of Theorem 1.1, then as in that proof $A_i^2 - C_i^2B = (n/2)^2$ with g.c.d.$(A_i, C_i) = 1$ and by choosing $i \equiv -T(AU)^{-1} \pmod{B}$ we guarantee that $C_i \equiv 0 \pmod{B}$. If we choose i to be even, then the hypothesis of Lemma 1.1 is satisfied and so $A_i \pm (n/2)$ are powerful. By (2.3) there are infinitely many such A_i. It remains to show that neither $A_i + (n/2)$ nor $A_i - (n/2)$ are perfect squares. Suppose $A_i \pm (n/2) = D_i^2$ then $A_i \equiv 1 \pm (n/2) \pmod{8}$. By further choosing $i \equiv 0 \pmod{4}$ (if necessary, i.e., if either $T \equiv 2 \pmod{4}$ or $U \equiv 2 \pmod{4}$) we get $U_i \equiv 0 \pmod{8}$ and $T_i \equiv 1 \pmod{8}$. Thus $A_i \equiv A \pmod{8}$. Now if $n \equiv 2 \pmod{4}$ then by (2.4) $1 \pm (n/2) \equiv A_i \equiv A \equiv 5 - (n/2) \pmod{8}$ which implies that $4 \equiv 0$ or $n \pmod{8}$ a contradiction. If $n \equiv 0 \pmod{4}$ then by (2.5) $1 \pm (n/2) \equiv A_i \equiv A \equiv 3 - (n/2) \pmod{8}$, which implies that $2 \equiv 0$ or $n \pmod{8}$ another contradiction which secures the theorem. (Q.E.D.)

To illustrate Theorem 2.1, we provide the following table containing the first 6 values of even n. Of course some of the powerful numbers are too astronomical to explicitly state therein.

n	P_1	P_2	A	B	T	U	i ≡
2	$5^3 \cdot 7^2 \cdot 11^2 \cdot 129^2 \cdot 149^2$	$3^5 \cdot 71^2 \cdot 3361^2$	4	15	4	1	14(mod 15)
4			9	77	351	40	128(mod 154)
6			10	91	1574	165	188(mod 364)
8	11^3	$3^3 \cdot 7^2$	7	33	23	4	-2(mod 33)
10	13^3	3^7	8	39	25	4	-2(mod 39)
12	$17^3 \cdot 241^2 \cdot 18245273^2$	$5^3 \cdot 1069^2 \cdot 25787431^2$	11	85	378	41	-8(mod 85)

Table 2.1

Now we turn to the question of the existence of r-tuples of powerful numbers spaced s units apart where r and s are positive integers.

The following result provides necessary and sufficient conditions for the existence of triples of odd powerful numbers spaced an even distance apart.

PROPOSITION 2.1. Let x and r be positive integers with $x > r$. Then $x - r$, $x + r$ and $x + 3r$ are powerful numbers provided:

(1) If x is even then $x^2 - my^2 = r^2$ and $(x + 2r)^2 - nz^2 = r^2$ where $m|y$ and $n|z$.

(2) If x is odd then $x^2 - my^2 = 4r$ and $(x + 2r)^2 - nz^2 = 4r^2$ where $m|y$ and $n|z$.

The proposition is immediate from Lemma 1.1. Consider the following application:

EXAMPLE 2.4. For $x = 169$ we have that $7^2 = 49$, $13^2 = 169$, and $17^2 = 289$ are powerful numbers spaced 120 apart. It is easy to show that the conditions of Proposition 2.1 (2) are satisfied.

It should be noted, however, that the authors have been unable to find a triple of powerful numbers spaced 2 apart. As noted earlier, it is a difficult problem to find a triple of powerfuls spaced an odd distance apart.

The next illustration shows how to build infinitely many powerful pairs which are 4 apart given a single such pair.

EXAMPLE 2.5. If u and v are odd powerful numbers such that $v = u + 4$ then $u' = u \cdot v = u(u + 4) = u^2 + 4u$ and $v' = (u + 2)^2 = u^2 + 4u + 4$ are odd powerfuls spaced 4 apart. For example if $(u, v) = (121, 125)$ then $(121 \cdot 125, 123^2)$, $(121 \cdot 125 \cdot 123^2)$, $(121 \cdot 125 + 2)^2)$ etc. are powerful pairs spaced 4 apart.

Finally we conclude the paper with a generalization of the concept of powerful numbers and new questions pertaining thereto. Define a positive integer n to be r-powerful, where r is a positive integer, provided p^r divides n whenever the prime p divides n. Hence, all positive integers are 1-powerful. The content of this paper has dealt with 2-powerful numbers. Do there exist consecutive pairs, triples, etc. of r-powerful numbers for $r > 2$? If so, are there infinitely many? In fact, many of the questions raised and/or settled for 2 powerful numbers in this paper may be applied to r-powerful numbers for $r > 2$.

Acknowledgement: The first author's research is supported by N.S.E.R.C. Canada. The author is an undergraduate mathematics student at the University of Calgary.

REFERENCES

1. GOLOMB, S.W. Powerful Numbers, Amer. Math. Monthly 77 (1970), 848-852.

2. SENTANCE, W.A. Occurences of Consecutive Odd Powerful Numbers, Amer. Math. Monthly 88 (1981), 272-274.

3. McDANIEL, W.L. Representations of Every Integer as the Difference of Powerful Numbers, Fib. Quar. 20 (1982), 85-87.

4. MOLLIN, R.A., and WALSH, P.G. On Nonsquare Powerful Numbers, (to appear: Fibonacci Quarterly).

5. DEGERT, G. Uber die Bestimmung der Grundeinbeit gewisser reellquadratischer Zahlkorper, Abh. Math. Sem. Univ. Hamburg 22 (1958), 92-97.

6. RICHAUD, C. Sur la resolution des equations $x^2 - Ay^2 = \pm 1$, Atti. Acad. pontif. Nuovi Lince (1866), 177-182.

7. SLAVUTSKY, I.S. On Mordell's Theorem, Acta Arith. 11 (1965), 57-66.