REPRESENTATIONS OF EVERY INTEGER AS THE DIFFERENCE OF POWERFUL NUMBERS

WAYNE L. McDANIEL
University of Missouri, St. Louis, MO 63121

(Submitted May 1981)

1. INTRODUCTION

A powerful number has been defined by Golomb [3] to be a positive integer with the property that whenever the prime p divides r, p^2 divides r. In this paper, we show that every nonzero integer can be written as the difference of two relatively prime powerful numbers in infinitely many ways.

Let $P(m_1, m_2) = m_1 - m_2$, where m_1 and m_2 are powerful numbers. $k = m_1 - m_2$ is said to be a proper representation of k by P if $(m_1, m_2) = 1$, and an improper representation if $(m_1, m_2) > 1$.

It has been shown that there exist infinitely many proper representations of k by P if $k = 1$ or 4 [3], if $k = 2$ [6], or if k is a prime congruent to 1 modulo 8 [4]. It is also known [3] that there is at least one proper representation of each odd integer and each multiple of 8 by P. Golomb has conjectured that there are infinitely many integers that cannot be written as the difference of two powerful numbers. Our principal result in this paper disproves this conjecture, showing that, in fact, every integer $\neq 0$ has infinitely many representations as the difference of relatively prime powerful numbers.

2. THE DIOPHANTINE EQUATION $x^2 - Dy^2 = n$

Our approach involves showing that corresponding to a given positive integer $n \not\equiv 2 \pmod 4$ there exists an integer D such that

$$x^2 - Dy^2 = n \tag{1}$$

has an infinitude of solutions x, y for which $D|y$.

(1) has been extensively studied (see [5] or [7]), and it is well known that if p, q is a solution of (1), where D is not a square, and u, v is a solution of the Pell equation $x^2 - Dy^2 = 1$, then $pu + Dqv$, $pv + qu$ is also a solution of (1). It follows that (1) has an infinitude of solutions when one solution exists, since the Pell equation has infinitely many solutions: if u, v is a solution of $x^2 - Dy^2 = 1$, then so is x_j, y_j, where

$$x_j + y_j\sqrt{D} = (u + v\sqrt{D})^j,\ j = 1, 2, 3, \ldots,$$

that is, where

$$x_j = u^j + \sum_{k=2}^{j} \binom{j}{k} u^{j-k}v^kD^{k/2}, \tag{2}$$

and

$$y_j = ju^{j-1}v + \sum_{k=3}^{j} \binom{j}{k} u^{j-k}v^kD^{(k-1)/2}. \tag{3}$$

[The index ranges over even values of k in (2) and odd values in (3).]

We will find it convenient to make the following definition.

DEFINITION: If p, q is a solution of (1) and u, v is a solution of $x^2 - Dy^2 = 1$, $pu + Dqv$, $pv + qu$ is a Type A solution of (1) if u is odd, v is even, and $D|pv + qu$.

THEOREM 1: Let p, q be a solution of (1) and x_0, y_0 be a solution of $x^2 - Dy^2 = \pm 1$. Then (1) has infinitely many Type A solutions if $d = (2py_0, D)$ implies $d|q$.

PROOF: Let $x_1 = x_0^2 + Dy_0^2$ and $y_1 = 2x_0y_0$. Then $x_1^2 - Dy_1^2 = 1$, y_1 is even, and x_1 is odd. Replacing u by x_1 and v by y_1 in (2) and (3) yields solutions

$$X_j = px_j + Dqy_j,\ Y_j = py_j + qx_j$$

of (1) with x_j odd and y_j even for $j = 1, 2, 3, \ldots$. Now, $D|Y_j$ if

$$0 \equiv Y_j \equiv py_j + qx_j \equiv pjx_1^{j-1}y_1 + qx_1^j \equiv x_1^{j-1}(py_1j + qx_1) \pmod{D}.$$

Since $x_1^2 - Dy_1^2 = 1$, $(x_1, D) = 1$, so $D|Y_j$ if

$$0 \equiv (py_1)j + qx_1 \equiv (2x_0y_0p)j + q(x_0^2 + Dy_0^2) \equiv (2x_0y_0p)j + qx_0^2 \pmod{D}.$$

Solutions of this linear congruence exist if and only if $(2x_0y_0p, D)$ divides qx_0^2. Since $x_0^2 - Dy_0^2 = \pm 1$ implies $(x_0, D) = 1$, it follows that if $(2y_0p, D)$ divides q, $j \equiv b \pmod{D}$ for some integer b and X_{b+tD}, Y_{b+tD} is a Type A solution of (1) for $t = 1, 2, 3, \ldots$.

We observe at this point that if u, v is a solution of $x^2 - Dy^2 = 1$, and p and q are relatively prime integers, then $pu + Dqv$ and $pv + qu$ are relatively prime integers, for if $d = (pu + Dqv, pv + qu)$, then d divides $u(pv + qu) - v(pu + Dqv) = q$ and d divides $u(pu + Dqv) - vD(pv + qu) = p$, which implies that $d = 1$.

THEOREM 2: If $n \equiv -1$, 0, or 1 (mod 4), there exists an odd integer D such that $x^2 - Dy^2 = n$ has infinitely many relatively prime Type A solutions.

PROOF: The proof involves making a judicious choice for D in each of the three cases. In each case, we identify a solution p, q of (1) and a solution x_0, y_0 of $x^2 - Dy^2 = \pm 1$. D is odd in each of the three cases and is clearly not a square; it is then shown that $(py_0, D) = 1$, assuring, by Theorem 1, that (1) has infinitely many Type A solutions, and that $(p, q) = 1$, making the solutions relatively prime.

Case 1. $n = 4k - 1$, $k = 1, 2, 3, \ldots$. We choose $D = 16k^2 - 8k + 5$. If p, q, x_0, and y_0 are chosen, respectively, to be $8k^2 - 6k + 2$, $2k - 1$, $32k^3 - 24k^2 + 12k - 2$, and $8k^2 - 4k + 1$, then $p^2 - Dq^2 = 4k - 1$, and $x_0^2 - Dy_0^2 = -1$. Let $d_0 = (p, D)$. We find that d_0 divides $4(D - 2p) - [(D - 2p)^2 - D] = 8$, so $d_0 = 1$. Let $d_1 = (y_0, D)$. Since d_1 divides $D - 2y_0 = 3$, and $D \not\equiv 0 \pmod{3}$ for any k, $d_1 = 1$. Let $d_2 = (p, q)$. Since d_2 divides $(4k - 1)q - p = -1$, $d_2 = 1$.

Case 2. $n = 4k + 1$, $k = 2, 3, 4, \ldots$. We choose $D = 4k^2 - 4k - 1$. If p, q, x_0, and y_0 are chosen, respectively, to be $2k$, 1, $4k^2 - 4k$, and $2k - 1$, then $p^2 - Dq^2 = 4k + 1$ and $x_0^2 - Dy_0^2 = 1$. Let $d_0 = (p, D)$. Since d_0 divides $p^2 - 2p - D = 1$, $d_0 - 1$. (y_0, D) and (p, q) are obviously equal to 1.

Because $D = 4k^2 - 4k - 1$ is negative when $k = 0$ or 1, we treat $n = 1$ and $n = 5$ separately, by considering $x^2 - 3y^2 = 1$ and $x^2 - 11y^2 = 5$. $x^2 - 3y^2 = 1$ is satisfied by p,q and x_0,y_0 if $p = x_0 = 2$ and $q = y_0 = 1$. If $p = 4$, $q = 1$, $x_0 = 10$, and $y_0 = 3$, then $p^2 - 11q^2 = 5$ and $x_0^2 - 11y_0^2 = 1$. Clearly, in both cases, (py_0, D) and (p, q) equal 1.

Case 3. $n = 4k$, $k = 1, 2, 3, \ldots$. We choose $D = 4k^2 + 1$. If p, q, x_0, and y_0 are chosen, respectively, to be $2k + 1$, 1, $2k$, and 1, then $p^2 - Dq^2 = 4k$ and $x_0^2 - Dy_0^2 = -1$. Let $d = (py_0, D)$. Since d divides $D - (2k - 1)py_0 = 2$, $d = 1$. Obviously, $(p, q) = 1$.

Since the proof gives no clue as to how the polynomials D were found, it might be helpful to mention that they were discovered, essentially, as a result of a process which began in an examination of the continued fraction expansion of $\sqrt{m}$, where m is a polynomial whose continued fraction has a relatively small period (≤ 10). The interested reader might consult Chrystal's *Algebra* [2] and the paper by Boutin [1].

3. APPLICATION TO POWERFUL NUMBERS

THEOREM 3: If n is any integer $\neq 0$, there exist infinitely many relatively prime pairs m_1 and m_2 of powerful numbers such that $n = m_1 - m_2$.

PROOF: If X_j, Y_j is a Type A solution of $x^2 - Dy^2 = n$, $n \neq 2 \pmod 4$, then $m_1 = X_j^2$ and $m_2 = DY_j^2$ are powerful numbers whose difference is n. Since in each of the three cases of Theorem 2 p and q were shown to be relatively prime, X_j and Y_j and, hence, m_1 and m_2 are relatively prime.

If $n \equiv 2 \pmod 4$, we let $n = 2 + 4t$ and consider the equation of Case 2 of Theorem 2: $x^2 - Dy^2 = 4k + 1$. Since $n^2/4 = 4(t^2 + t) + 1$, there exist infinitely many relatively prime Type A solutions X_j, Y_j of $x^2 - Dy^2 = n^2/4$, where $D = 3$, if $t = 0$, and

$$D = 4(t^2 + t)^2 - 4(t^2 + t) - 1, \text{ if } t \geq 1.$$

Let $m_1 = X_j + n/2$ and $m_2 = X_j - n/2$. We observe that since, for all k in Case 2, p is even and q is odd, and since X_j, Y_j is a Type A solution, X_j is even and Y_j is odd. Thus m_1 and m_2 are odd. It follows immediately that $(m_1, m_2) = 1$: any common divisor of m_1 and m_2 must be odd and must divide $m_1 + m_2 = 2X_j$ and $m_1 - m_2 = n$, but $(X_j, Y_j) = 1$ and $X_j^2 - DY_j^2 = n^2/4$ imply that $(X_j, n) = 1$. Since $m_1m_2 = DY_j^2$ is a powerful number, so is each of m_1 and m_2. Hence $n = m_1 - m_2$ is the difference of two relatively prime powerful numbers.

The theorem is obviously true when n is negative, since $n = m_1 - m_2$ implies $-n = m_2 - m_1$.

COROLLARY: Let S denote the set of all squarefree integers and n be any integer. n has infinitely many improper representations by P if $n \notin S$. If $n \in S$, n has no improper representations by P.

PROOF: Assume $n \notin S$. If $n = 0$, the result is obvious. If $n \neq 0$, there exists a prime p and an integer $m \neq 0$ such that $n = mp^2$. By Theorem 3, there exist infinitely many pairs of powerful numbers m_1 and m_2 such that $m = m_1 - m_2$. Then, $n = m_1p^2 - m_2p^2$, the difference of two powerful numbers. Conversely, if n has an improper representation by P, then n is divisible by the square of an integer and is not in S.

Example 1. $9 = m_1 - m_2$. The equation $x^2 - 7y^2 = 9$ has Type A solutions

$$X_{2+7t},\ Y_{2+7t}.$$

For $t = 0$, we obtain

$$m_1 = X_2^2 = (214372)^2 = 2^4 \cdot 53593^2 \quad\text{and}\quad m_2 = 7Y_2^2 = 7(81025)^2 = 5^4 \cdot 7^3 \cdot 463^2.$$

Example 2. $6 = m_1 - m_2$. Since $6 \equiv 2 \pmod 4$ and $6^2/4 = 9$, we again use $x^2 - 7y^2 = 9$. Letting $m_1 = X_2 + 3 = 214375 = 5^4 \cdot 7^3$ and $m_2 = X_2 - 3 = 214369 = 463^2$, we have

$$5^4 \cdot 7^3 - 463^2 = 6.$$

REFERENCES

1. M. A. Boutin. "Développement de $\sqrt{n}$ en fraction continue et résolution de équations de Fermat." *Assoc. Franc. pour l'Adv. des Sci.* 37 (1908):18-26.
2. G. Chrystal. *Textbook of Algebra.* Pt. II. New York: Chelsea, 1964.
3. S. W. Golomb. "Powerful Numbers." *Amer. Math. Monthly* 77 (1970):848-52.
4. A. Makowski. "On a Problem of Golomb on Powerful Numbers." *Amer. Math. Monthly* 79 (1972):761.
5. T. Nagel. *Introduction to Number Theory.* New York: Wiley, 1951.
6. W. A. Sentance. "Occurrences of Consecutive Odd Powerful Numbers." *Amer. Math. Monthly* 88 (1981):272-74.
7. H. N. Wright. *First Course in Number Theory.* New York: Wiley, 1939.

*****