SUMS AND DIFFERENCES OF VALUES OF A QUADRATIC POLYNOMIAL

Alan F. Beardon

Centre for Mathematical Sciences, Cambridge CB3 0WB, England

(Submitted May 2001-Final Revision January 2002)

1. INTRODUCTION

Let P be a quadratic polynomial with integer coefficients. Motivated by a series of results on polygonal numbers (which we describe below) we consider the existence of integers a, b, c, d and n such that

$$P(n) = P(a) + P(b) = P(c) - P(d), \qquad P(a)P(b)P(c)P(d) \neq 0. \tag{1}$$

The simplest example of a polynomial P for which (1) has infinitely many solutions is $P(x) = x^2$, for $(3m)^2 + (4m)^2 = (5m)^2 = (13m)^2 - (12m)^2$ for every m. Now $x^2 = P_4(x)$ where, for each integer N with $N \geq 3$, $P_N(n)$ is the *polygonal number* $(N-2)n^2/2 - (N-4)n/2$. In 1968 Sierpinski [5] showed that there are infinitely many solutions to (1) when $P = P_3$, and this was subsequently extended to include the cases P_5, P_6 and P_7 (see [2], [4] and [3], respectively). In 1981 S. Ando [1] showed that there are infinitely many solutions to (1) when $P(x) = Ax^2 + Bx$, where A and B are integers with $A - B$ even, and this implies that, for each N, (1) has infinitely many solutions when $P = P_N$.

It is easy to find polynomials P for which (1) has no solutions (for example, if $P(n)$ is odd for every n), and this leads to the problem of characterizing those P for which (1) has infinitely many solutions. This problem has nothing to do with polygonal numbers, and here we prove the following result.

Theorem 1: *Suppose that $P(x) = Ax^2 + Bx + C$, where A, B and C are integers, and $A \neq 0$.*

(i) *If $8A^2$ divides $P(k)$ for some integer k, then there are infinitely many n such that* (1) *holds for some integers a, b, c and d.*

(ii) *If $\gcd(A, B)$ does not divide C then there are no integer solutions to* (1).

Theorem 1(i) is applicable when $P(0) = 0$, and this special case implies Ando's result. As illustrations of Theorem 1 we note that (1) has infinitely many solutions when $P(x) = x^2+2x+5$ (because $P(1) = 8$), but no solutions when $P(x) = 6x^2+3x+5$. Not every quadratic polynomial is covered by Theorem 1; for example, $x^2 + 2x + 4$ is not (to check that 8 does not divide $P(k)$ for any k it suffices to consider $k = 0, 1, \ldots, 7$). In fact, if $P(x) = x^2 + 2x + 4$, then $P(u+1) - P(u) = 2u + 3$, and it follows from this that for all k,

$$\begin{aligned} P(2k^2) + P(2k-1) &= P(2k^2+1) \\ &= P(2k^4 + 4k^2 + 3) - P(2k^4 + 4k^2 + 2). \end{aligned}$$

The existence of solutions of (1) may have something to do with Diophantine equations; for example, if $P(x) = x^2 - 4x + 3$, then $P(x+2) = P(y+1) + P(y+3)$ is equivalent to Pell's equation $x^2 - 2y^2 = 1$. This link with Diophantine equations suggests perhaps that there may be no simple criterion for (1) to have infinitely many solutions.

2. THE PROOF

The proof of (i) is based on the following observation.

Lemma 2: *Let p be any polynomial with integer coefficients. Suppose that there are non-constant polynomials t, u, v and w with integer coefficients such that $u(w(x)) = v(t(x)) + 1$ and $P(v(x)+1) - P(v(x)) = P(u(x))$. Then there exist infinitely many n such that* (1) *holds for some integers a, b, c and d.*

Proof: It is easy to see that if, for any integer x, we put $n = u(w(x))$, $a = v(t(x))$, $b = u(t(x))$, $c = v(w(x)) + 1$ and $d = v(w(x))$ then (1) holds.

The Proof of (i): First, we show that the conclusion of (i) holds if $8A^2$ divides $P(0)(= C)$. Let $u(x) = 1 + 4Ax$ and $v(x) = 8A^2x^2 + (4A + 2B)x + C/2A$. Then u and v have integer coefficients and as is easily checked, $P(v(x)+1) - P(v(x)) = P(u(x))$. Next define $t(x) = 4Ax$ and $w(x) = v(4Ax)/4A$. The assumption that $8A^2$ divides C implies that w has integer coefficients, and by construction, $u(w(x)) = 1 + 4Aw(x) = v(t(x)) + 1$. The conclusion of (i) now follows from Lemma 2.

Now suppose that $8A^2$ divides $P(k)$, and let $Q(x) = P(x+k)$. Then Q has leading coefficient A, and $8A^2$ divides $Q(0)$; thus there are infinitely many n such that (1), with P replaced by Q, holds for some a, b, c and d. The conclusion of (i) follows immediately from this.

The Proof of (ii): If there are integers n, a and b such that $P(n) = P(b) - P(a)$, then there are integers u and v such that $Au + Bv = C$, and this implies that $\gcd(A, B)$ divides C, contrary to our assumption.

REFERENCES

[1] S. Ando. "A Note on Polygonal Numbers." *The Fibonacci Quarterly* **19.2** (1981): 180-183.

[2] R.T. Hansen. "Arithmetic of Pentagonal Numbers." *The Fibonacci Quarterly* **8.1** (1970): 83-87.

[3] H.J. Hindin. "A Theorem Concerning Heptagonal Numbers." *The Fibonacci Quarterly* **18.3** (1980): 258-259.

[4] W.J. O'Donnell. "Two Theorems Concerning Hexagonal Numbers." *The Fibonacci Quarterly* **17.1** (1979): 77-79.

[5] W. Sierpinski. "Sur les Nombres Triangulaires Qui Sont Sommes De Deux Nombres Triangulaires." *Elem. Math.* **17** (1962): 63-65.

AMS Classification Numbers: 11D09

✠✠✠