ON THE NUMBERS OF THE FORM $an^2 + bn$

SHIRO ANDO
Hosei University, Koganei-shi, Tokyo 184, Japan
(Submitted December 1982)

It is clear that for any given positive integer N there are infinitely many square numbers which can be represented as the difference of square numbers in at least N different ways.

For instance, if $n = 4p_1p_2 \ldots p_r$, where $p_1, p_2, \ldots, p_r$ are the smallest r odd primes such that $r \geqslant \log_2 N$, then for each subset S of $\{1, 2, 3, \ldots, r\}$, n^2 has the expression

$$n^2 = (h^2 + k^2)^2 - (h^2 - k^2)^2,$$

where

$$h = 2\prod_{i \in S} p_i, \quad k = \prod_{i \in \overline{S}} p_i,$$

with the convention that an empty product means 1 and the notation $\overline{S}$ for the complement of S, giving $2^r \geqslant N$ distinct expressions.

Thus, we can choose n in such a way that

$$n = O(e^{c \log N \log\log N}) \tag{1}$$

for large values of N, where c is a constant.

In this paper we prove a similar theorem concerning the sequence of numbers $A_n = an^2 + bn$ for any integers a and b with $a > 0$, which includes the earlier result [1] as the special case of $N = 2$.

Theorem

For any given positive integer N, there exist an infinite number of A_n's which can be expressed as the difference of two numbers of the same type in at least N different ways. We can choose an n for each N in such a way that it satisfies (1) as N tends to infinity.

Proof: It is enough to prove that for any sufficiently large N, there is an A_n which has at least N such expressions. Since

$$A_n = A_h - A_k \tag{2}$$

is equivalent to

$$n(an + b) = (h - k)(ah + ak + b),$$

in order to get the expression (2) for given n, it is sufficient to find a decomposition of n into two factors s and t; $n = st$, for which

$$h - k = s, \; a(h + k) + b = t(an + b) \tag{3}$$

has positive integral solutions h and k.

Let $p_1, p_2, \ldots, p_r$ be the smallest r distinct prime numbers in the arithmetic progression consisting of positive integers congruent to 1 modulo $2a$, and let

$$n = 2p_1p_2 \ldots p_r.$$

For each proper subset S of $\{1, 2, \ldots, r\}$, there corresponds a distinct decomposition of n into two factors

$$s = 2\prod_{i \in S} p_i \quad \text{and} \quad t = \prod_{i \in \overline{S}} p_i,$$

where t can be expressed as $t = 1 + 2au$ for a positive integer u, and we have

$$h + k = st + 2u(an + b)$$

from the second equation of (3).

If n is sufficiently large so that it will satisfy $an + b > 0$, then Eq. (3) gives distinct pairs h, k for different decompositions $n = st$ of n.

In this case, however, two different h's may give the same A_h if b/a is a negative integer. Since at most four pairs of h, k give the same expression, we have at least N distinct expressions (2) of A_n if r satisfies

$$2^r - 1 \geqslant 4N,$$

and N is sufficiently large so that corresponding n will satisfy $an + b > 0$.

If we take r that satisfies

$$\log_2(4N + 1) \leqslant r < \log_2(4N + 1) + 1,$$

then for large values of N we have

$$\log n = \log 2 + \log p_1 + \cdots + \log p_r = O(p_r) = O(r \log r),$$

from which we obtain

$$n = O(e^{c \log N \log\log N})$$

for a constant c, completing the proof.

If we do not care about the size of n, we can take simpler forms for s and t in (3); if b/a is not a negative integer,

$$s = 2(1 + 2a)^i, \; t = (1 + 2a)^{N-i}, \; (i = 1, 2, \ldots, N - 1)$$

give N distinct expressions of the form (2) for h and k determined by (3), and if b/a is a negative integer, N will be substituted by $4N$.

These results apparently cover the case of polygonal numbers of any order.

Examples

For tiagonal numbers $t_n = \frac{1}{2}(n^2 + n)$, we have $t_n = t_h - t_k$, where

$$n = 2 \times 3^N, \; h = 3^i + 3^{2N-i} + \tfrac{1}{2}(3^{N-i} - 1), \; k = -3^i + 3^{2N-i} + \tfrac{1}{2}(3^{N-i} - 1)$$

for $i = 1, 2, \ldots, N - 1$.

For hexagonal numbers $h_n = 2n^2 - n$, we have $h_n = h_h - h_k$, where

$$n = 2 \times 5^N, \; h = 5^i + 5^{2N-i} - \tfrac{1}{4}(5^{N-i} - 1), \; k = -5^i + 5^{2N-i} - \tfrac{1}{4}(5^{N-i} - 1)$$

for $i = 1, 2, \ldots, N - 1$.

REFERENCE

1. S. Ando. "On a System of Diophantine Equations Concerning the Polygonal Numbers." *The Fibonacci Quarterly* 20, no. 4 (1982):349-53.

◆◇◆◇◆