İstanbul Üniv. Fen Fak. Mat. Der. 49 (1990), 1-5

GENERALIZATION OF THE SET $\{1, 2, 5\}$

H. ALTINDİŞ

The set of numbers $\{1, 2, 5\}$ has the property that the product of any two numbers of the set decreased by 1 is a perfect square. The set which consists of such elements is said to have the property P_{-1}. The purpose of this work is to construct the sets with three elements which have the property P_{-1}. Moreover, the sets

$$\{1, n^2+1, n^2+2n+2\},\ \{2, 2n^2+2n+1, 2n^2+6n+5\},$$
$$\left\{a, n(an+s)+\frac{s^2+1}{a}, (n+1)[a(n+1)+2s]+\frac{s^2+1}{a}\right\}$$

are systematically obtained.

1. INTRODUCTION

Let $x_1, x_2, \ldots, x_n$ be positive integers. The set $\{x_1, x_2, \ldots, x_n\}$ is called a P_k set of size n if for $i \neq j$ $(i, j = 1, 2, \ldots, n)$ and k any integer, there exists an integer A such that $x_i x_j + k = A^2$ [1], [2].

Consider the set of positive integers $\{a, b, c\}$ with $a > 0$ and $a < b < c$. Suppose this set has the property P_{-1}. Then one gets

$$\begin{aligned} ab - 1 &= x^2 \\ ac - 1 &= y^2 \\ bc - 1 &= z^2 \end{aligned} \tag{1.1}$$

where x, y, z are integers.

2. MAIN RESULTS

Theorem 1. The system (1.1) has infinitely many solutions of the form $\{1, b, c\}$ for some integers x, y, z.

Proof. If $a = 1$ then (1.1) becomes

$$\begin{aligned} b - 1 &= x^2 \\ c - 1 &= y^2 \\ bc - 1 &= z^2 \end{aligned} \tag{1.2}$$

and it follows that $b = x^2+1$, $c = y^2+1$. We have $1 \leq x < y$ since $1 < b < c$ and consequently we get

$$(x^2+1)(y^2+1) - 1 = z^2. \tag{1.3}$$

Since the right hand side of (1.3) is a perfect square, the left hand side must also be a perfect square. (1.3) can be written as

$$(xy + 1)^2 + [(x - y)^2 - 1] = z^2 . \tag{1.4}$$

If $y - x = \pm 1$ for any integers x, y then the left hand side of (1.4) is a perfect square, therefore suitable triples (x, y, z) can be found as (1, 2, 3), (2, 3, 7), (3, 4, 13),... etc. Hence we obtain the sets P_{-1} ; $\{1, 2, 5\}$, $\{1, 5, 10\}$, $\{1, 10, 17\}$,... respectively. These sets can be generalized to the sets

$$\{1, n^2 + 1, n^2 + 2n + 2\} \tag{1.5}$$

where n is a positive integer. This gives infinitely many solutions of (1.1). If $n=1$ and $n = 2$, then we get the result of Ezra Brown [2] and S.P. Mohanty [3], respectively. Infinitely many solutions of (1.1) are called the fundamental solutions.

Now we would like to know whether there are any other solutions of (1.1) besides fundamental solutions. To do that, we return (1.3). (1.3) can be written as

$$z^2 - (x^2 + 1)\, y^2 = x^2 . \tag{1.6}$$

Let $x^2 + 1 = D$. If $x \geq 1$ and x integer, then D is never a perfect square. Hence the Diophantine equation (1.6)

$$z^2 - Dy^2 = D - 1 \tag{1.7}$$

is a Pell equation. It follows that for every D there are infinitely many solutions (z, y) of (1.7) [4].

If $x = x_j = 1$, then the equation (1.6) or (1.7) becomes

$$z^2 - 2y^2 = 1 \tag{1.8}$$

which is a Pell equation. The fundamental solution of this equation is $(z, y) =$ (3, 2). Consequently all solutions of (1.8) can be obtained from

$$z_n + \sqrt{2}\, y_n = (3 + 2\sqrt{2})^n ;$$

we have the following table:

n	z_n	y_n
0	1	0
1	3	2
2	17	12
3	99	70
4	577	408
5	3363	2378
6	19601	13860
7	114243	80782
8	665857	470832
.	.	.
.	.	.
.	.	.

Table 1

From table 1 the solutions of (1.6) which are in the form of $(1, y, z)$ can be found as (1, 2, 3), (1, 12, 17), (1, 70, 99), (1, 408, 577),... and the corresponding P_{-1} sets are $\{1, 2, 5\}$, $\{1, 2, 145\}$, $\{1, 2, 4901\}$, $\{1, 2, 166465\}$,... respectively. Let

$$A_{x_j} = \{\{1, 2, 5\}, \{1, 2, 145\}, \{1, 2, 4901\},\ldots\}$$

be the family of these sets.

If $x = x_k = 2$, then by the equation (1.7) we have

$$z^2 - 5y^2 = 4 \tag{1.9}$$

which is again a Pell equation and its all integer solutions can be found similarly. Let

$$A_{x_k} = \{\{1, 5, 10\}, \{1, 5, 442\}, \{1, 5, 3026\},\ldots\}$$

be the family of these sets. Clearly $A_{x_j} \cap A_{x_k} = \phi$ for $x_j \neq x_k$.

Continuing this procedure for $x = x_i = 3, \ldots$ etc. we get the following result:

Theorem 2. For every $x = x_j \geq 1$ where x_j is a positiv integer there is a family

$$A_{x_j} = \{\{1, b\,(x_j), c_i\}\} \quad (i \in I_0\,,\ I_0 \subset \mathrm{N})$$

with infinitely many elements having the property P_{-1}. Moreover, if $x_j \neq x_k$ then $A_{x_j} \cap A_{x_k} = \phi$.

Now let $a = 2$ then we have the following similar results to Theorem 1 and 2:

Theorem 3. The system (1.1) has infinitely many solutions of the form $\{2, b, c\}$ for some integers x, y, z and $a = 2$.

Proof. The proof is similar to the proof of the Theorem 1 and the solutions are in the form $\{2, 2n^2 + 2n + 1, 2n^2 + 6n + 5\}$ $(n \in \mathrm{N})$ [2].

Theorem 4. For every $x = x_j \geq 1$ where x_j is a positive integer there is a family

$$B_{x_j} = \{\{2, b\,(x_j), c_i\}\} \quad (i \in I_0\,, I_0 \subset \mathrm{N})$$

with infinitely many elements having the property P_{-1}, moreover if $x_j \neq x_k$, then $B_{x_j} \cap B_{x_k} = \phi$.

Proof. It is similar to the proof of Theorem 2.

So far we have shown that the system (1.1) has infinitely many solutions for $a = 1$, $a = 2$. The question is now is it possible for the system (1.1) to have infinitely many solutions for every positive integer a?

Showing this is the same as solving the quadratic congruence

$$x^2 \equiv -1 \pmod{a}.$$

If $a = 4k+3$, $k = 0, 1, 2, 3, \ldots$ is a prime, then this congruence has no solutions [5]. Hence if a is equal to 3, 7, 11,..., etc. and consequently one factor of a is a multiple of these prime numbers 3, 7, 11,... then the system (1.1) has no solutions.

If $a = 4k + 1$, $k = 1, 2, 3, \ldots$ is a prime then the congruence has solutions. Let

$$E_1 = \{a : a = 4k + 1, \text{ which is a prime number } (k = 1, 2, \ldots)\}.$$

If $a \in E_1$ then the congruence $x^2 \equiv -1 \pmod{a^\alpha}$, $\alpha \geqq 2$, $\alpha \in \mathbf{N}$ can also be solved [5].

Let

$$E_2 = \{a : a = (4k + 1)^\alpha, \; 4k + 1 \text{ is a prime}, \; \alpha \geqq 2, k = 1, 2, \ldots\},$$

$E_3 = \{a : a = 2 . (4k_1 + 1)^\alpha . (4k_2 + 1)^\beta$, α, β are integers and $4k_i + 1$ are primes for $i = 1, 2\}$.

If $a \in E_3$ then the congruence $x^2 \equiv -1 \pmod{a}$ can have solutions. Hence we have shown that a must be in the set

$$E = E_1 \cup E_2 \cup E_3 .$$

This characterizes the choice of a that we seek for.

Let us return to system (1.1). If we arrange the third equation in the system (1.1) as

$$(xy + 1)^2 + [(x - y)^2 - a^2)] = (az)^2$$

and set $y - x = \pm a$ then the left hand side becomes a perfect square. Let a be different from 1 and 2 with $a \in E$, and choose an element s so that $2 < s < a$ and $s^2 \equiv -1 \pmod{a}$.

If $x = an \pm s$, $y = x \pm a$, n is a positive integer, then we get

$$b = n(an \pm 2s) + \frac{s^2 + 1}{a}, \quad c = (n + 1) \; [a(n + 1) \pm 2s] + \frac{s^2 + 1}{a};$$

hence we have:

Theorem 5. Let $a \in E$ and

$$W = \left\{ a, n(an \pm 2s) + \frac{s^2 + 1}{a}, (n + 1) \; [a(n + 1) \pm 2s] + \frac{s^2 + 1}{a} \right\}.$$

Subtracting 1 from the product of any two elements in W is a perfect square, where $n \in \mathbf{N}$, and s is an integer satisfying $2 < s < a$ and $s^2 \equiv -1 \pmod{a}$.

We next give an example that how we can choose the number s in Theorem 5.

Example. Let $a = 2.5.13^2 = 1690 \in E$, note that $s^2 \equiv -1 \pmod{1690}$ has solutions which are $s \equiv 1113 \pmod{1690}$ and $s \equiv 1253 \pmod{1690}$. If $a = 1690, s = 1113, n = 1$ in Theorem 5 then the set $W = \{1690, 4649, 11945\}$ is a P_{-1} set. Similarly if $a = 1690, s = 1253, n = 1$ in Theorem 5 then we get $W = \{1690, 5125, 12701\}$ which is a P_{-1} set. Hence there are infinitely many P_{-1} sets which can be obtained from $n = 2, 3, \ldots$.

REFERENCES

[1] DICKSON, L.E. : History of the Theory of Numbers, Vol. 2, Carnegie Institute, Washington, 1920.

[2] BROWN, E. : *Sets in which $xy+k$ is always a square*, Mathematics of Computation, 45 (1985), N. 172, 613-620.

[3] MOHANTY, S.P. and RAMASAMY, M.S. : *The simultaneous diophantine equations $5y^2 - 20 = x^2$ and* $2y^2+1=z^2$, J. Number Theory, 18 (1984), 356-359.

[4] NAGELL, T. : Introduction to Number Theory, Wiley, New York, 1951.

[5] APOSTOL, T.M. : Introduction to Analytic Number Theory, Springer Verlag, 1984.

DEPARTMENT OF MATHEMATICS
FACULTY OF ARTS AND SCIENCES
ERCİYES UNIVERSITY
38039 KAYSERİ-TURKEY