A New Approach to Generate Trees of Primitive Solutions of Diophantine Equation $x^2 + dy^2 - z^2 = 0$ With Using A general interval decomposition where d is a positive square free integer

Divya Sree Reddy Choppa

Research Scholar, Dept. of Mathematics, Annamacharya University, Rajampet - 516126
Annamaiah Distract, Andhra Pradesh, India

***Abstract*—This paper focused to study to generate Trees of Primitive Solutions with using a general interval decomposition of the Diophantine equation $x^2+ dy^2-z^2 = 0$ …………….[1] where d is a positive square-free integer.**

***Keywords*—Diophantine equation, Square-free integer, Primitive Solution, Seminal Matrices.**

INTRODUCTION

The well-known Matrix generated tree structure for Pythagorean triples is extended to the primitive solutions of the Diophantine equation $x^2 +dy^2-z^2 = 0$, where d is a positive square free integer. This paper, focused to study the basic structure of the solutions to the Diophantine equations

$x^2 +d y^2- z^2 = 0$ is determined. Since above equation is homogeneous, we may assume that (x, y, z) is primitive. Hence for d =1, all such Pythagorean triples form an infinite tree with root (3, 4, 5). All nodes descend to (3, 4 ,5) and each node appears exactly Once. For each d>1, we construct finite sets of matrices and finite sets of roots that generate all the solutions to $x^2 +dy^2-z^2 = 0$. Given a primitive solution (x, y, z) of $x^2 +dy^2 - z^2 = 0$, an algorithm to describes a path (or descent) from (x, y, z) to some element in the finite set of roots.

Definition 1: Let d be a positive square-free integer and let *M*(d) be a set of non-singular matrices. A primitive solution (x, y, z) of (1) satisfies *Fermat's method of descent with respect to M*(d) if there exists an element *g* of *M*(d) such that g^{-1}. (x, y, z) is a positive integer multiple of a primitive solution (x', y', z') where one of the following holds:

$z - x > z' - x'$

$z - x = z' - x'$ and $z > z'$

$d \geq 10$ is even and (x, y, z) is a binary root, i.e., $z - x = z' - x'$ and $z < z'$. In thiscase, (x', y', z') is called the copartner of (x, y, z).

Suppose that primitive solution (x, y, z) of (1) satisfies Definition 1. If the scaled (by its gcd) output (x', y', z') successively satisfies Definition 1, we show for a specific set *M*(d) that after a finite number of steps (or descents) the result is a positive integer times either (1, 0, 1) or a primitive binary root. Moreover, we characterize all binary roots (x, y, z) and their copartners (x′, y′, z') in Theorem 2, and prove that (x', y', z') intertwines (x, y, z) indefinitely: (x, y, z), (x', y', z'), (x, y, z), (x', y', z'), etc.

Definition 2: A finite set *G* of matrices with integer entries is said to be a *generating set*

for solutions to (1) whenever the following conditions hold:

if *g* is in *G* and w = (x, y, z) is an integer solution to (1), then g.w also satisfies (1);and

if w is a primitive solution to (1), then there exist a positive integer k and a primitiveroot r that is either binary or (1, 0, 1) such that

k × w = (finite product of matrices from *G*). r.

The origin of the generating sets *G* = *G*(d) is in my observation that if (x, y, z) satisfies(1), then so does ($x' = x - u t$, $y' = y - v t$, $z' = z - w t$) where (u, v, w) is *not* a solution to (1) and

$t = \frac{2(ux + dvy - wz)}{u^2+dv^2-w^2}$ or equivalently M(u, v, w, d) . (x, y, z) satisfies (1) where $u^2+d v^2 \neq w^2$and

M(u, v, w, d) =

$$\frac{1}{u^2+dv^2-w^2}\begin{pmatrix} -u^2 + dv^2 - w^2 & -2duv & 2uw \\ -2uv & u^2 - dv^2 - w^2 & 2vw \\ -2uw & -2dvw & u^2 + v^2 + w^2 \end{pmatrix}$$

Definition 3: Let d be a square-free positive integer, and let □(d) denote 1 is d is even and 2 otherwise. The Kth seminal matrix S (k,d) is defined by:

S(k ,d) $=\frac{d-(2k-1)}{\square(\mathrm{d})}$ M(k-1,1,k,d) for k = 0,1,2,3,….. $\frac{d+\square(\mathrm{d+1})}{2}$ -1 ,..

and S $(\frac{d+\square(\mathrm{d+1})}{2}, d) = M(d, 1, d, d)$. Then for all k and d, S(k, d) is an integer matrix such that if (x, y, z) is a primitive solution to (1), then S(k, d) . (x, y, z) is an integer solution to (1). Multiplication by the elementary matrices

$$e(0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad e(1) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$e(2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad e(3) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

will be used to ensure that the components of solutions are nonnegative. In particular paths from (x, y, z) to a root will be in terms of products of descent matrices e(j) . S(k, d), whereas paths back to (x, y, z) will be with products of ascent matrices S(k, d) . e(j).

Theorem 1:

We now show that the only possibility of binary roots (x , y, z) defined by Definition 1 is when square-free d = m n ≥ 10 is even and

(x , y , z) = A(m, n, a, b) where b X n = a (2k) . In this case, the Identity n A(m ,n, a, b) = $2a^2 A\left(\frac{d}{2}, 2, k, 1\right)$ reduces A(m ,n, a, b) to " standard' binary roots of the form $A\left(\frac{d}{2}, 2, k, 1\right)$.Moreover , the co-partner A$'$ (m ,n, a, b) of

(x , y, z) satisfies n A(m ,n, a, b) = $2a^2 A\left(\frac{d}{2}, 2, k, 1\right)$ where b X n = a $(2\left(\frac{d}{2} - k\right))$. Note that the multiples n and 2a^2 will usually be ignored in the descent process.

The next result of Lemma 2, will play key role in determining the constant k.

Conclusion to the Proof of Theorem 1:

Let d be a square-free positive integer , G = G(d)* or G(d)** and suppose that (x , y ,z) is a primitive solution to (1), we will show that G satisfies Definition 2 of a generating set by using the proof to determine integers

$\left(k_i\left(1 \le k_i \le \frac{d+\delta(d+1)}{2}\right), j_i(0 \le j_i \le 3)\right)$ *and n* such that S(k_i , d). $e(j_i)$ $(1 \le i \le n)$ is in G for the descent

$(e(j_1).S(k_1, d))\ldots\ldots\ldots(e(j_n).S(k_n, d))$. (x , y ,z) = K$_r$ Where r is either (1, 0,1) or a primitive binary root, and

K=gcd ($(e(j_1).S(k_1, d))\ldots\ldots\ldots(e(j_n).S(k_n, d))$. (x , y ,z)) taking inverses by Lemma 1 , we then have

$$\left[\frac{1}{K}\prod\left\{\left(\frac{d-(2k-1)}{\delta(d)}\right)^2 : k_i < \frac{d+\delta(d+1)}{2}\right\}\right].$$

(x , y ,z) = $\langle S(k_n, d).e(j_n)\rangle\ldots\ldots\langle S(k_1, d).e(j_1)\rangle.r$

Where the coefficient of (x ,y ,z) is 1 whenever the product is over the empty set. Finally, since (x, y, z) is primitive and the right side is an integer triplet , the coefficient of (x ,y ,z) must be a positive integer and hence G is a generating Set.

A general interval decomposition

Consider the following possibilities for the set M(d) from definition 1.

M(d)=$\{e(j), S(k, d^{-1}) : j \text{ and } k \text{ as in } G(d)\}$,

M$(d)^*$= $\{e(j), S(k, d^{-1}) : j \text{ and } k \text{ as in } G(d)^*\}$,

M$(d)^{**}$= $\{e(j), S(k, d^{-1}) : j \text{ and } k \text{ as in } G(d)^{**}\}$ of inverses of descent matrices. By Lemma 1, these sets contain non integer matrices, but in some sense $G(d)$, $G(d)^*$, $G(d)^{**}$ form theorem 1 will respectively be their generator completions.

Let (x , y, z) be a primitive solution of (1) , By Proposition 1, there is a unique factorization d = mn such that (x , y, z) is either A(m, n, b, a) or $\frac{1}{2}$ A(m, n, b, a) for certain positive integers a and b with b n > a $\sqrt{d}$ and gcd (b n , a m) =1. The interval (a $\sqrt{d}$, ∞) will now be expressed as a union of subintervals with the property that if b n is in the kth subinterval, then there is an element g_{jk} of M$(d)^*$ or M$(d)^{**}$ such that ${g_{jk}}^{-1}$.$\{x, y, z\}$ is a positive integer multiple of a primitive solution $\{x', y', z'\}$ as in Definition 1. The following elementary result plays an essential role in identifying the generator g_{jk}. It is expressed in an equivalent form without the parameters m,n , a, b; and consequently may be used to determine j and k when dealing with large values of d that are not feasible to factoring.

By Proposition 1, for primitive solution (x , y , z) of (1), $\frac{x+z}{y}$ = $\frac{bn}{a}$; and by the proof, gcd (b n , a m) =1 is equivalent to gcd (x, z) = 1.(Actually , gcd (x, z) = 1 follows from (x , y, z) being a primitive solution of (1).)

Lemma 3: Let (x, y,z) be a primitive solution of (1) for some positive square-free integer d. Suppose first that integer k satisfies 1≤ $k < \frac{d+\delta(d+1)}{2}$ so that

$$\sqrt{d}\ \frac{2k-\sqrt{d}-1}{\sqrt{d}-1} < 2k-1 < \sqrt{d}\ \frac{2k+\sqrt{d}-1}{\sqrt{d}-1} < d.$$

Then $\sqrt{d}\ < \frac{x+y}{z} \le d;\ and\ z-x > z_{jk} - \ x_{jk}$ where g_{jk}^{-1}.(x,y,z) =$(e(j).S(k,d).(x,y,z))$ = (x_{jk}, y_{jk}, z_{jk}). Whenever $\frac{x+z}{y}$ is in any of the intervals in (a) –(c) except for a specified case of (b)(i):

a) For j =1 and d≥ 6: (2k-1-$\sqrt{\delta(d)}$, $2k-1)\ where\ q \le k \le q+r+1.$
Moreover, if $\frac{x+z}{y}$ = 2k-1, then z_{1k}-x_{1k} =0.

b) For j = 3 and d≥ 6 , either
   i) (2k-1 ,2k-1+$\sqrt{\delta(d)}$) $where\ q \le k \le q+r$; and also where k = q-1 when $\sqrt{d} < 2q-1-\sqrt{\delta(d)}$, or
   ii) (2k-1, $\sqrt{d}\ \frac{2k+\sqrt{d}-1}{\sqrt{d}+1}$) where k > q+r.

However, if d≥ 10 is even and $\frac{x+z}{y}$ = 2k < $\frac{d}{2}$ in (b)(i), then there exists a positive integer multiple of (x , y ,z) that is a binary root. This is the only possibility for part (c) of Definition 1.

c) For j =2, either

   i) $\sqrt{d} < \frac{x+z}{y}$ < d where k = 1 and 2≤ $d \le 5$ or

   ii) $\sqrt{d}\ \frac{2k+\sqrt{d}-1}{\sqrt{d}+1} < \frac{x+z}{y} \le d,$ where d≥ 6 and

   q + r < k < $\frac{1}{2}\left[\frac{\sqrt{d}+1}{\sqrt{d}}\left(\frac{x+z}{y}\right)+1-\ \sqrt{d}\right].$

In this case, faster convergence is obtained with the highest possible value of k. Moreover, if $\frac{x+z}{y}$ =d, then z_{2k}-x_{2k} =0.

(Note that the case d=1 is a consequence of parts (e), (f) , and (g) below.)

On the other hand, let k = $\frac{d+\delta 9d+1)}{2}$ and $\frac{x+z}{y} > d.$ Then (x_{jk}, y_{jk}, z_{jk}) satisfies Definition 1 if:

d) (j =0) d< $\frac{x+z}{y} < \sqrt{d}(2\sqrt{d}-1)$. In this case z -x = z_{0k}-x_{0k} and z>z_{0k}.

Proof. Let 1≤ $k < \frac{d+\delta(d+1)}{2}$ so that (4) is straightforward. Remark 4 may be helpful with the following computations since

$e(j).S(k,d).A(m,n,a,b) =$
$e(j).(S(k,d).A(m,n,a,b)).$

a) Let j=1 , and for (x_{1k}, y_{1k}, z_{1k}).:

$$X_{1k} > 0 \Leftrightarrow Z_{1k} + X_{1k} >\ Z_{1k}\ -\ X_{1k}$$

$$\Leftrightarrow\ n(am-b)^2 - m(bn-a(2k-1)^2 > 0$$

$$\Leftrightarrow \left(\frac{x+z}{y}\ - \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1}\right)\left(\frac{x+z}{y}\ - \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1}\right) < 0$$

$$\Leftrightarrow \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1} < \frac{x+z}{y} <\ \sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}-1}.$$

Similarly
$Y_{1k} > 0 \Leftrightarrow Z_{1k} + X_{1k} >\ Z_{1k}\ -\ X_{1k}$

$\Leftrightarrow\ (bn-a(2k-1))(bn-ad) > 0$

$\Leftrightarrow \frac{x+z}{y} <\ 2k-1$ or $\frac{x+z}{y} > d.$

$Moreover,\ 2\ \ Z_{1k}\ =\ n(d+1)\,b^2 - (4akd)\,b\ +$ $a^2m(d+(2k-1)^2$ = 0 is a quadratic equation in b with discriminant -4$a^2(d-2k+1)^2 < 0.$ Evaluating 2 Z_{1k} at b = 4akd , we find that

$2Z_{1k}\ =\ 16a^2k^2d^2(n(d+1)-1) + a^2m(d+(2k-1)^2)\ >\ 0$, so Z_{1k} is always positive.

It follows that the components are all positive if and only if

$\sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1} < \frac{x+z}{y} <\ \sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}-1}$. Next,

$n[(z-x)-(Z_{1k}-X_{1k})]$ = n$[2a^2m - \delta 9d + 1)m(a(2k-10)-bn^2]$

= -$\delta(d+1)d\left[bn-a(2k-1)-\sqrt{\delta(d)}\right]$

$\left[bn-a(2k-1)+\sqrt{\delta(d)}\right]$;

And z -x > $Z_{1k} - X_{1k}$ if and only if

2k-1 -$\sqrt{\delta(d)} < \frac{x+z}{y} < 2k-1+\sqrt{\delta(d)}.$

Note that it is straightforward to show

$\sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1} < \frac{x+z}{y} < 2k-1-\sqrt{\delta(d)}$

if and only if

k < $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1+\sqrt{\delta(d)}\right]$.

By hypothesis , assume that

2k -1 - $\sqrt{\delta(d)} < \frac{x+z}{y} \leq 2k-1$ where q≤ $k \leq q + r + 1$.

By the above, the components of $\left(x_{jk}, y_{jk}, z_{jk}\right)$ are positive and

z -x > $Z_{1k} - X_{1k}$. Since

k≤ $(q+r)+\sqrt{\delta(d)} < \frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1+\sqrt{\delta(d)}\right]$. There fore by the second equivalence above, we have that

$\sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1} < 2k-1-\sqrt{\delta(d) <} \quad \frac{x+z}{y} \leq 2k-1 < 2k-1+\sqrt{\delta(d)}$; and thus z-x > $Z_{1k} - X_{1k}$. Note that $\sqrt{d}$ < $\frac{x+z}{y} \leq 2k-1$,it follows that

k>$\frac{\sqrt{d}+1}{2} = \frac{\sqrt{d}+3}{2} - 1 = q-1$; so the hypothesis that k≥ q is necessary. Finally, if $\frac{x+z}{y} = 2k-1$, then a$(Z_{1k} - X_{1k}) = m\left(\frac{x+z}{y} - (2k-1)^2\right) = 0$

(b) Let j =3.

$X_{3k} \geq 0 \Leftrightarrow \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1} < \frac{x+z}{y} < \sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}+1}$ as with $X_{1k} > 0$, similary

$Y_{3k} > 0 \Leftrightarrow Z_{3k} + X_{3k} > Z_{3k} - X_{3k}$

$\Leftrightarrow (bn - a(2k-1)))(bn - ad) < 0$

$\Leftrightarrow 2k-1 < \frac{x+z}{y} < \sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}+1}$.

Next, z -x > $Z_{3k} - X_{3k}$ is equivalent to 2k-1 -$\sqrt{\delta(d)}$ < $\frac{x+z}{y} < 2k-1+\sqrt{\delta(d)}$ as in (a).

Moreover, z -x = $Z_{3k} - X_{3k}$ if and only if $\frac{x+z}{y} = 2k-1+\sqrt{\delta(d)}$. In this case , if d is even, then (x ,y,z) is a binary root by theorem 2.

By direct calculation , $2k-1+\sqrt{\delta(d)} < \sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}+1}$ if and only if

k< $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1-\sqrt{\delta(d)}\right]$ since 2k-1 - $\sqrt{\delta(d)} < 2k-1 < \sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}+1}$ by (4) , and we have the above intervals on $\frac{x+z}{y}$ for positivity and the inequality z -x > $Z_{3k} - X_{3k}$, it follows that part (a) of definition 1 holds for (x_{3k}, y_{3k}, z_{3k}) if and only if

i) 2k-1 < $\frac{x+z}{y}$ < 2k-1 + $\sqrt{\delta(d)}$ when k< $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1-\sqrt{\delta(d)}\right]$ and

ii) 2k-1 < $\frac{x+z}{y}$ < $\sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}+1}$ otherwise.

Let d≥ 6 and assume that k< $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1-\sqrt{\delta(d)}\right]$ .By remark 1, k≤ $q + r$. Then 2k-1 < $\frac{x+z}{y}$ < 2k-1 + $\sqrt{\delta(d)}$ holds where $\frac{x+z}{y} > \sqrt{d}$,so k> $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1\right]$. It follows By theorem 2, a positive integer multiple of (x , y , z) will be binary root.

(c) Let j =2.

$X_{2k} > 0 \Leftrightarrow Z_{2k} + X_{2k} > Z_{2k} - X_{2k}$

⇔m$(bn - a(2k-1)^2 - n(am-b)^2) > 0$

$\Leftrightarrow \left(\frac{x+z}{y} - \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1}\right)\left(\frac{x+z}{y} - \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}+1}\right)$>0

$\Leftrightarrow \ either\ \frac{x+z}{y} < \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}-1}$ or $\frac{x+z}{y} > \sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}+1}$

$Y_{2k} > 0 \Leftrightarrow$ 2k-1 < $\frac{x+z}{y} < d$ as with $Y_{3k} > 0$.

$Z_{2k} > 0$ is identical to that of $Z_{1k} > 0$.

It follows that all components are positive if and only if

$\sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}+1} < \frac{x+z}{y} < d.$

And it is easy to check that

$\sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}+1} < \sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)$ if and only if

k < $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1+\sqrt{\delta(d)}\right]$. Therefore by (4) and the above results , (x_{2k}, y_{2k}, z_{2k}) fulfils part (a) of Definition 1 if and only if

$\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right) < \frac{x+z}{y} < d$ when k < $\frac{1}{2}\left[\sqrt{d}\left(\sqrt{d}-\sqrt{\delta(d)}\right)+1+\sqrt{\delta(d)}\right]$, and $\sqrt{d}\frac{2k-\sqrt{d}-1}{\sqrt{d}+1} < \frac{x+z}{y} < d$ otherwise.

It follows that

i) $\sqrt{d} < \frac{x+z}{y}$ < d where k = 1 and 2≤ $d \leq 5$ or

ii) $\sqrt{d}\frac{2k+\sqrt{d}-1}{\sqrt{d}+1} < \frac{x+z}{y} \leq d$, where d≥ 6 and

$$q + r < k < \frac{1}{2}\left[\frac{\sqrt{d}+1}{\sqrt{d}}\left(\frac{x+z}{y}\right) + 1 - \sqrt{d}\right].$$

In this case, faster convergence is obtained with the highest possible value of k.

Finally , if $\frac{x+z}{y} = d$, then n$(Z_{2k} - X_{2k})$ = $(bn - ad)^2 = 0$.

On the other hand, suppose that k = $\frac{d+\delta(d+1)}{2}$ where d = m n is a square free.

(d) (j=0)

$$X_{0k} > 0 \Leftrightarrow n(Z_{0k} + X_{0k}) - n(Z_{0k} - X_{0k}) > 0$$

$$\Leftrightarrow (bn - 2ad)^2\text{-}\left(a\sqrt{d}\right)^2 > 0$$

$$\Leftrightarrow \left(\frac{x+z}{y} - \sqrt{d}\left(2\sqrt{d} - 1\right)\right)\left(\frac{x+z}{y} - \sqrt{d}\left(2\sqrt{d} + 1\right)\right) > 0$$

$\Leftrightarrow$ *either* $\frac{x+z}{y} < \sqrt{d}\left(2\sqrt{d} - 1\right)or\frac{x+z}{y} > \sqrt{d}\left(2\sqrt{d} + 1\right)$.

Similarly , $Y_{0k} > 0 \Leftrightarrow n(Z_{0k} + Y_{0k}) - n(Z_{0k} - Y_{0k}) > 0$

$\Leftrightarrow bn < 2ad \Leftrightarrow \frac{x+z}{y} < 2d.$

Finally, Z_{0k} = n $b^2 - (4amn)b + a^2m(4mn + 1) = 0$ is a quadratic In b with roots b= (2am$\sqrt{n} \pm a\sqrt{mi}$)/$\sqrt{n}$. Evaluating Z_{0k} at b = 2am$\sqrt{n}$, we have that

$Z_{0k} = a^2m\left(1 + 4mn\left(\sqrt{n} - 1\right)^2\right) > 0$, so Z_{0k} is always positive. It follows that the components are positive if and only if $\frac{x+z}{y} < \sqrt{d}\left(2\sqrt{d} - 1\right)$.

Next , z – x =2 a^2m = $Z_{0k} - X_{0k}$.

Moreover , n(z-Z_{0k}) = $4ad(bn - ad)$ = $4a^2d(\frac{x+z}{y} - d)$ and z > Z_{0k} since by assumption $\frac{x+z}{y} > d$;so (d) follows.

Example 1: Let d = (3*5*7*11*13*17 and (x , y ,z) = A(385,663,34,19) =(627443,1292,905413). Then q= 254, r= 127016 and

$\sqrt{d}$ < 2q-1-$\sqrt{2}$. By theorem 1, G(d)** .is a generating set for all primitive solutions; and by corollary 1, we have the following descent.

Since $\frac{x+z}{y} < d$, we start with

(a) K = 594 checks out, but $\frac{x+z}{y}$ ≠2k-1. Our first descent matrix is
e(1).S(q+340,d).(x,y,z)=(17573773279,80091, 17573819864)

= $\frac{1}{2}A(385,663,7281,11)$ = (x^1 ,y^1,z^1)

Note that z – x = 277790 > z^1-x^1 (=46585).

Replacing (x , y ,z) with (x^1 ,y^1,z^1),we return to (a) where now

$\frac{x+z}{y} > d$. Thus with k=$\frac{d+1}{2}$ = q+r+358 , we check (d) holds. Our next descent is e(0) .S(q+r+358,d).(x ,y ,z) =(468625219,13079,468671804) = $\frac{1}{2}A(385,663,1189,11)$= (x^1 ,y^1,z^1). Then z – x = 46585 = z^1-x^1.

Replacing (x , y, z) with (x^1 ,y^1,z^1),since $\frac{x+z}{y} < d$, we are back to (a) both possibilities for k fail. So we go to

(b) (i) Here k =126219 = q+125695 and the next descent matrix is
e(3). S(q+125965 ,d). (x ,y ,z) =(95611 ,17,95996)

= $\frac{1}{2}A(385,663,17,11)$ = (x^1 ,y^1,z^1) and

z-x =12320 > z^1-x^1 (=385). Replacing (x , y, z) with (x^1 ,y^1,z^1),since $\frac{x+z}{y} < d$, we are back to (a) k = 5636 =q+5382 checks out: and

$\frac{x+z}{y}$ = 2k-1 so we are done with $Z_{1k} - X_{1k}$= 0.
So our final descent matrix is
e(1) . S(q+5382,d). (x ,y ,z) = (22446528 ,0,22446528).

Trees of Primitive Solutions

A tree of the primitive solutions to (1) is an infinite network of nodes where each node branches (in our case via ascent matrix multiplications) to a number of subsequent nodes, with the totality giving all , and only , primitive solutions without duplication. By theorem 1, trees exist when d is 2 , 6, or any odd square-free positive integer. For any other even square-free d, the primitive solutions are attained from a finite forest of such trees.

Specifically, for any given node (x, y, z) there is a unique path via descent matrices back through the tree to either (1,0,1) or a primitive binary root; i.e., if (x , y ,z) is not a root , then exactly one of the matrices g in M(d)* or M(d)** exists such that g^{-1}.(x , y , z) produces a new node (x$'$, y', z') that satisfies Definition 1.

In the classical case d =1, the tree of primitive solutions is derived by simply taking all possible ascending products of three generators stemming from (1, 0 ,1). This is possible since products always produce distinct primitive solutions in this case.

For square-free d > 1 , families of generators are defined for the primitive solutions that satisfy the requirements for a tree structure with four exceptions that may easily be remedied by adjusting or removing improper branches.

Let G denote G(d)* or G(d)** , and let g = S(k , d).e(j) be in G. Reversing the descent notion of definition 1, Assume (x$'$, y', z') is a primitive solution of (1).

g. (x$'$, y', z') = (x , y, z) and , as in the proof of Theorem 1,

e(j). S(k, d). (x , y ,z) = i$'$ (x$'$, y', z') satisfies Fermat's Descent method for some positive integer i$'$. Unlike the case d = 1, it is necessary to consider the following anomalies.

A1) The components of (x, y, z) may not all be positive

A2) The components of (x, y, z) may be positive but not relatively prime.

A3) For some odd square-free d, there may exist g in G such that the binary root conditions z'- y' = z -y in part (c0 of Definition 1 hold:

A4) There are duplicate nodes in the first level of the derived tree that must be pruned. They arise form the subsets

$\{S(q+s,d).e(3).w, S(q+s+1,d).e(1).w\}$ $(0 \leq s \leq r)$

For some primitive root w as follows.

i) For odd square-free d≥ 13 , the nearest nodes in the abutting sets agree when w = (1,0 ,1): $\{S(q+s+1,d).e(1).w, S(q+s+1,d).e(3).w\}$ $(0 \leq s \leq r)$

Since e(1) . w = e(3) .w

ii) For even square-free d≥ 10 and standard binary root w = $A\left(\frac{d}{2},2,k,1\right)$ as defined in Theorem 2, there exists a unique s in [0, r] such that

$$\frac{S(q+s,d).e(3).w}{gcd[S(q+s,d),e(3).w]} = \frac{S(q+s+1,d).e(1).w}{gcd[S(q+s+1,d),e(1).w]}$$

iii) The interval decomposition in the proof of theorem 1 is disjoint except for the intervals corresponding to the descent matrices e(3). S(q + s, d) and

e(1). S(q+s+1 ,d) when d is odd. If (x , y, z) = A(m, n, a, b) is a primitive solution to (1) such that b x n is in the intersection

$\left[\left(a(2(q+s)+1)+1-\sqrt{2}\right),\left(a(2(q+s)+1)+1-\sqrt{2}\right)\right]$ of these intervals, then there exist two distinct paths form (1,0,1) to (x, y, z).

CONCLUSION

we proposed one of the method to generate A tree of the primitive solutions to (1) is an infinite network of nodes where each node branches (in our case via ascent matrix multiplications) to a number of subsequent nodes, with the totality giving all , and only , primitive solutions without duplication. By the b x n-interval decomposition of (a$\sqrt{d}$., ∞) in the proof of theorem 1, the only way that distinct paths may arise form (1 ,0,1) to (x ,y,z) is by A4. Moreover, the only nontrivial anomalies when d is even are A1 ,A2 , and A4. By the parametric intervals method of descent , after some modifications at each level, the primitive solutions of (1) satisfy requirements for one or more tree structures with generating sets G(d)* or G(d)** .

REFERENCES

[1] Roger C.Alpen , The modular tree of Pythagoras , Amer , Math, Monthly 112(2005),no.9 ,807-816.

[2] L.Holzer , Minimal solutions of Diophantine equations , Canad,J.Math.2((1950)238-244

[3] L.J.Mordell, Diophantine Equations, Academic Press ,London ,1969.