Tree Structure for Primitive Solutions of the Diophantine Equation $px^2 + y^2 - z^2 = 0$, p 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 **- In this paper focused to study the well-known matrix-generated tree structure for Pythagorean triples is extended to he primitive solutions of the Diophantine equation $Px^2 + y^2 - z^2 = 0$ …….[1] where P is a positive square-free integer. Also, focused to study the basic structure of the solutions to the Diophantine equations $px^2 + y^2 - z^2 = 0$ is determined. Since above equation is homogeneous, we may assume that (x, y, z) is primitive. Hence for p =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 P>1, we construct finite sets of matrices and finite sets of roots that generate all the solutions to $Px^2 + y^2 - z^2 = 0$. Given a primitive solution (x, y, z) of $Px^2 + y^2 - z^2 = 0$, an algorithm to describes a path (or descent) from (x, y, z) to some element in the finite set of roots.**

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 $Px^2 + y^2 - z^2 = 0$, where P is a positive square free integer.

The essential idea of a generating set for solutions of (1) is a variation of Fermat's method of descent that requires the following to be true for special related sets of nonsingular matrices:

Definition 1: Let p be a positive square-free integer and let *M*(P) be a set of nonsingular 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*(P) 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:

a) $z - y > z' - y'$
b) $z - y = z' - y'$ and $z > z'$
c) $P \geq 10$ is even and (x, y, z) is a binary root, i.e., $z - y = z' - y'$ and $z < z'$. In thiscase, (x', y', z') is called the co-partner 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*(P) 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
a) if w is a primitive solution to (1), then there exist a positive integer k and a primitive root 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*(P) 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

$t = \frac{2(PUx + vy - wz)}{pu^2 + v^2 - w^2}$ or equivalently M(u, v, w, P) . (x, y, z) satisfies (1) where $Pu^2 + v^2 \neq w^2$ and

M(u, v, w, P) =

$$\frac{1}{pu^2+v^2-w^2}\begin{pmatrix} -pu^2+v^2-w^2 & -2puv & 2puw \\ -2puv & pu^2-v^2-w^2 & 2vw \\ -2puw & -2vw & u^2+v^2+w^2 \end{pmatrix}$$

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

S(k ,P) = $\frac{p-(2k-1)}{\text{floor}(p)}$ M(k-1,1,k,p) for k = 0,1,2,3,….. $\frac{P+\text{floor}(p+1)}{2}$-1. and S ($\frac{P+\text{floor}(p+1)}{2}, p$) = $M(p,1,p,p)$. Then for all k and d, S(k, p) is an integer matrix such that if (x, y, z) is a primitive solution to (1), then S(k, P) . (x, y, z) is an integer solution to (1). Multiplication by the elementary matrices

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

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

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, p), whereas paths back to (x, y, z) will be with products of ascent matrices S(k, P) . e(j). Our main result is

Main Result:

Theorem 1: For any positive square-free integer P,

the set G(P) = $\left\{S(k,P).e(j): 1 \le k \le \frac{p+\text{floor}(P+1)}{2}, 0 \le j \le 3\right\}$ generates all primitive solutions to (1).

Proof : Minimal generating subsets of G(P) are G (P) * and G (P) ** defined as follows: If P = 1, then G (P) * = $\{S(\frac{p+1}{2}, P).e(j) : 1 \le j \le 3\}$ and If P = 2, 3, or 5, then

G (P) * = $\{ S(1,P).e(2) \} \cup S(\frac{p+\text{floor}(P+1)}{2}, P).e(j) : 1 \le j \le 3\}$

Finally for p ≥ 6, let q = floor$\left(\frac{\sqrt{p}+3}{2}\right)$,

r = floor $\left\{\frac{1}{2}\sqrt{p}\left(\sqrt{p} - \sqrt{\text{floor}(P)}\right) - \left(2q - 1 + \sqrt{\text{floor}(p)}\right)\right\}$.

And G (P) * = {S(q + s, P) . e(1), S(q + s, P) . e(3) : 0 ≤ s ≤ r + 1 } ∪

{ S(q + r + 1, P) . e(2) } ∪ { S($\frac{p+\text{floor}(P+1)}{2}$,p) . e(j) : 0 ≤ j ≤ 3 },which is clearly represents as follows

a) $2q - 1 + \sqrt{\text{floor}(P)} < \sqrt{p}$, then G (P) * is a generating set for all primitive solutions.

b) On the other hand, if $2q - 1 + \sqrt{\text{floor}(P)} > \sqrt{p}$ then

G (P) ** = {S (q - 1, P). e (3) } ∪ G (P) * is a generating set.

Remark 1: Since x - 1 < floor(x) < x for irrational x, we have the following useful bounds: q + r < $\frac{1}{2}\sqrt{p}\left(\sqrt{p} - \sqrt{\text{floor}(P)}\right) - \left(-1 + \sqrt{\text{floor}(p)}\right)$ < q + r + 1.

Parametric Representation:

From References [1],[2],[3] we can go to define following Propositions:

Proposition 1: Let P be an even square-free positive integer. The primitive solutions (x , y, z) of (1) are exactly of the form
A(m, n, b, a) ≡ $\{y = nb^2 - ma^2, x = 2ab, z = nb^2 + ma^2\}$ for positive integers m, n, a and b such that P = mn , bn>a$\sqrt{p}$ and gcd (b n , a m) =1. On the other hand, if p is an odd square-free integer, then the primitive solutions (x, y, z) of (1) are given exactly by the following: when y is even, (x , y , z) = A(m, n, b, a) as defined above where, in addition, a and b are opposite parity, And when y is odd

(x, y , z) = $\frac{1}{2}A(m,n,a,b)$ where a and b are odd.

Proof: Suppose that (x , y, z) is a primitive solution of (1) that may be written

$$\begin{cases} p\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right), when\ y\ is\ even \\ px^2 = (z-y)(z+y), otherwise \end{cases} \quad \text{.....(2)}$$

Assume first that P is even. Then by (1) , x and z have the same parties ,

$Px^2 = (z-y)(z+y)$ where z-y and z + y are even, and since P is square-free, x^2 and x are even. It follows that y and z are odd since (x, y, z) are primitive. And by (2), each prime factor (including 2) of P divides either $\left(\frac{z-y}{2}\right)$ or $\left(\frac{z+y}{2}\right)$, i.e., there exist square-free integers m and n such that P = mn and

$p\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2m}\right)\left(\frac{z+y}{2n}\right)$. Moreover, any prime divisor of $\left(\frac{z-y}{2m}\right)$ or $\left(\frac{z+y}{2n}\right)$ must be 1 since it also divides $\frac{x}{2}, \frac{z-y}{2}$ and $\frac{z+y}{2}$ (i.e., y, x and z). Consequently,

$\frac{z-y}{2m} = a^2$ and $\frac{z+y}{2n} = b^2$ for positive integers a and b by the prime factorization theorem.

Solving for (x , y , z) we have (x , y , z) = A (m , n , a, b) where b n > a $\sqrt{p}$. Moreover, gcd (b n, a m) =1 if and only if gcd ($b^2n, a^2m) = 1$ if and only if gcd ($\frac{z-y}{2}$, $\frac{z+y}{2}$)=1 if and only if gcd (y, z) = 1.

Let p be a prime divisor of x and z. Then p^2 divides $p\left(\frac{x}{2}\right)^2$ by (2) where p may be at most one factor of P. It follows that p divides $\frac{x}{2}$ (and y) so that p =1 since (x, y, z) is primitive. A similar argument may be made when p is odd.

Remark 2: For a fixed factorization P = m n ≠ 1 of square-free P and primitive solution (x, y, z) of (1), we have the following simple criteria for types: a) (x, y, z) = A (m n, b, a) if and only if $\frac{z-y}{2m}$ is a square integer.
b) (x, y, z) = $\frac{1}{2}$ A (m, n, b, a) if and only if $\frac{z-y}{m}$ is a square integer.

These ensue directly from Proposition 1: For (a), $\frac{z-y}{2m} = a^2$ so we show that the condition $\frac{z-y}{2m}$ is a square integer holds only in this case. The other possibilities are (x, y, z) = A (m, n ,b, a) where gcd(bm ,an) =1.

But in this case, $\frac{z-y}{2m} = \frac{na^2}{m}$ ≠ square integer, since gcd (m, n) =1= gcd (m, a).

(x, y, z) = $\frac{1}{2}$ A (m, n, b, a) where $\frac{z-y}{2m} = \frac{a^2}{2}$ is not a square integer.

(x, y, z) = $\frac{1}{2}$ A (m, n, b, a) where gcd (bm ,an) =1. And again, in this case,

$\frac{z-y}{2m} = \frac{na^2}{m}$ ≠ square integer, since gcd (m, n) =1= gcd (m, a). hence (b) is similar.

Remark 3: The proof of Proposition 1 shows the following concerning the parametric representations of primitive solutions (x , y ,z) of (1) for square-free d: If y is even , then (x , y ,z) = A(m ,n ,a, b) where m is the product of the common factors of d and $\frac{z-y}{2}$; and n = $\frac{p}{m}$, Moreover, a = $\sqrt{\frac{z-y}{2}}$ and b= $\sqrt{\frac{z+y}{2}}$. In this case, if p is odd, then a and b are of opposite parity.

On the other hand, if y is odd, then d is odd and (x, y, z) = $\frac{1}{2}$ A (m, n, b, a) where m is the product of the common factors of d and z-x; and n = $\frac{p}{m}$. In this case, a and b are odd such that a = $\sqrt{\frac{z-y}{2}}$ and b= $\sqrt{\frac{z+y}{2}}$.

Remark 4: Since A(m , n , b, a) = nb^2(1,0,1)+ 2ab(0,1,0)+ m$a^2(-1,0,1)$ expressions involving S(k, P) . A (m, n, b, a) may be simplified accordingly:

If k < $\frac{p+\square(P+1)}{2}$, then $\square$(P) S(k, P). A (m, n, b, a)

= n$b^2A(1, p, 1,1)$+2ab(2P(k-1), P+(2k-1),2Pk)+ m$a^2A(p, 1,2k-1,1)$

Otherwise,

$\square$(P) . S$\left(\frac{p+\square(P+1)}{2}, d\right)$. $A(m, n, b, a)$ = nb^2(1,0,1)+ 2ab (2P,1,2P)+ m$a^2A(1, p, 1,2)$.

The next result will be useful in expressing primitive solutions in terms of a generating set according to Definition 2.

Lemma 1: The descent and ascent matrices are related by inverse formulas for j, k and P:

$$e(j), S(k,p)^{-1} = \begin{cases} S(k,p).e(j) & if\ k = \frac{p+\square(p+1)}{2} \\ \left(\frac{p-(2k-1))}{\square(P)}\right)^{-2} S(k,p).e(j) & otherwise \end{cases}$$

Proof: Suppose that (x, y, z) is a solution to (1) and $pu^2 + v^2 \neq w^2$. By the definitions of M and t given in section 1, M(u, v, w, P) .(x , y, z) = (x′ = x - u t, y′ = y - v t, z′ = z - w t) is a solution to (1) such that M(u, v , w, P) .(x′ , y′, z′) = (x″ = x′ - u t′, y″ = y′ - v t′, z″ = z′ - w t′) where t′ = -t. Consequently, (x″ , y″, z″) = (x , y ,z) and M$(u, v, w, p)^2$. $(x, y, z) = (x, y, z)$. For every solution (x , y, z) to (1). In particular, By proposition 1, this identity holds for (x , y , z) = A (1,p , P+2n-1,1) where (n = 1,2,3). Since the determinant of the matrix with these solutions as rows is -64p ≠ 0 , we have that the solutions are linearly independent and therefore M$(u, v, w, p)^2$ is the identity matrix, Lemma 1 is now immediate since the vectors (u , v, w) in the definitions of the seminal matrices S(k , P) satisfy $pu^2 + v^2 \neq w^2$.

Theorem 2: We now show that the only possibility of binary roots (x , y , z) defined by Definition 1 is when square-free P = 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) = $2a^2A\left(\frac{p}{2}, 2, k, 1\right)$ reduces A(m ,n, a, b) to " standard' binary roots of the form $A\left(\frac{p}{2}, 2, k, 1\right)$.Moreover , the co-partner A′ (m ,n, a, b) of (x , y, z) satisfies n A(m ,n, a, b) = $2a^2A\left(\frac{p}{2}, 2, k, 1\right)$ where b X n = a $(2\left(\frac{p}{2} - k\right))$. 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.

Lemma 2: Let P≥ 6 be a square-free even integer, The following are equivalent.
a) P = 4q+2r -2
b) $\sqrt{p} < 2(q-1)$
c) r is even
Similarly the following are equivalent:
d) P = 4q +2r
e) $\sqrt{p} > 2(q-1)$
f) r is odd

Proof: Let P >6 be even and square-free,

(a) ⇒ (c) , If P = 4q +2r -2, then $\frac{p}{2} = (2q-1) + r$. so r is even since $\frac{p}{2}$ and 2q-1 are odd. (d) ⇒ (f), similar to (a) ⇒ (c). (b) ⇒ (a). Assume that $\sqrt{p} < 2(q-1)$. Then by the definitions of q and r,

4q +2r -2 < $4\left(\frac{1}{2}\left(\sqrt{p}+3\right)\right) + 2\left(\left(\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-1\right) - 2q\right]\right)\right) - 2$

= p+$\left[\sqrt{p} - 2(q-1)\right]$ + 2 < p+2

By the assumption. Since 4q +2r -2 and P+2 are even integers, we have that 4q +2r -2≤ P. Moreover, as in Remark 3,

4q +2r -2 > 4q +$2\left(\left(\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-1\right) - 2q\right]\right)\right) - 2$

= $\left[2(q-1) - \sqrt{p}\right] - 2$ < P-2

So 4q +2r -2≥ p and (a) follows.

(e) ⇒ (d). Assume that $\sqrt{p} > 2(q-1)$. Then in this case,

4q +2r -2 < $4\left(\frac{1}{2}\left(\sqrt{p}+3\right)\right) + 2\left(\left(\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-1\right) - 2q\right]\right)\right) - 2$

= p+$\left[\sqrt{p} - 2(q-1)\right]$ < p

By assumption, Since 4q +2r -2 and d are even , 4q +2r -2≤ p.

In addition, 4q +2r> $4\left(\frac{1}{2}\left(\sqrt{p}+3\right)\right) + 2\left(\left(\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-1\right) - 2q\right]\right)\right) - 1$ = p+$\left[\sqrt{d} - 2(q)\right]$ > p-2.

Since 4q+2r and p-2 are even, 4q +2r ≥ p and (d) follows.
(a) ⇔ (b) It remains to show that (a) ⇒ (b). Assume that d = 4q +2r-2. Then either $\sqrt{p} < 2(q-1)$ or $\sqrt{p} > 2(q-1)$.
However, if $\sqrt{p} > 2(q-1)$,then by (e) ⇒ (d), p = 4q+2r which is false in this case, so $\sqrt{p} < 2(q-1)$. (d) ⇔ (e). We only need to show (d) ⇒ (e) , which is similar to (a) ⇒ (b). (c) ⇔ (a). It remains to show (c) ⇒ (a). Assume that r is even. Either $\sqrt{p} < 2(q-1)$ or $\sqrt{p} > 2(q-1)$. By the equivalences (a) ⇒ (b) and (d) ⇔ (e) , either p= 4q+2r-2 or p= 4q+2r. But if p = 4q +2r, then $\frac{p}{2}$ = 2q +r so r must be odd (a Contradiction). Since $\frac{p}{2}$ is odd and 2q is even. It follows that p = 4q+2r -2 and (a) results.
(f) ⇔ (d). Similar to (c) ⇔ (a). By Lemma 2, we have the resulting characterizations of binary roots and their co-partners.

Conclusion to the Proof of Theorem 2:

Let d be a square-free positive integer , G = G(p)* or G(p)** 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

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

$(e(j_1).S(k_1,p)).....(e(j_n).S(k_n,p))$. (x , y ,z) = K_r

Where r is either (1, 0,1) or a primitive binary root, and

K = gcd

$((e(j_1).S(k_1,p)).....(e(j_n).S(k_n,p))$. (x , y ,z)) taking inverses by Lemma 1 , we then have

$\left[\frac{1}{K}\prod\left\{\left(\frac{p-(2k-1)}{\delta(p)}\right)^2 : k_i < \frac{p+\delta(p+1)}{2}\right\}\right]$. (x, y, z) =

$\langle S(k_n,p).e(j_n)\rangle \ldots\ldots \langle S(k_1,p).e(j_1)\rangle.r$

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.

Theorem 3: Let Square-free integer p≥ 10 be even, there are exactly $\frac{r+\delta(r+1)}{2}$ standard binary roots as follows.

Let k = q +i +1- $\delta(r+1)$ for some integer I in [0, $\frac{r}{2}$]. Then $\frac{p}{2}$ - k > k and we have the cycle:

$(e(3).S(k,p)).A\left(\frac{p}{2},2,k,1\right) = A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right)$

and

$$\left(e(3).S(\frac{p}{2}-k,p)\right).A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right) = A\left(\frac{p}{2},2,k,1\right)$$

It follows that $A\left(\frac{p}{2},2,k,1\right)$ is a binary root with co partner $A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right)$ by definition 1. Moreover, if g(k) = gcd (k, $\frac{p}{2}$), then

$$A\left(\frac{p}{2},2,k,1\right) = g(k)\,A\left(\frac{p}{2g(k)},2\,g(k),\frac{k}{g(K)},1\right)$$

Where $A\left(\frac{p}{2g(k)},2\,g(k),\frac{k}{g(K)},1\right)$ is primitive; and similarly

$$A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right) = g(k)\,A\left(\frac{p}{2g(k)},2\,g(k),\frac{\frac{p}{2}-k}{g(K)},1\right)$$

where $A\left(\frac{p}{2g(k)},2\,g(k),\frac{\frac{p}{2}-k}{g(K)},1\right)$ is primitive.

Proof: Let Square-free integer P≥ 10 be even. Then q≥ 3 and r≥ 0. Suppose first that r is even and k = q – 1 + i where $0\le i\le\frac{r}{2}$. By Lemma 2 , P = 4q+2r-2 and $\frac{p}{2}$ – k = q +r – I > k. By remark 4, Since k≤ $q-1+\frac{r}{2} < \frac{p+\delta(p+1)}{2} = 2q+r$,

$(e(3).S(k,p)).A\left(\frac{p}{2},2,k,1\right) = 2k^2\{1-p,-2,p+1\} - 2k\{2p(1-k),1-2k-p,2pk\} + \frac{p}{2}\{p-(2k-1)^2,-2(2k-1),p+(2k-1)^2\}$, Moreover,

$A\left(\frac{p}{2},2,k,1\right) = \left\{2\left(\frac{p}{2}-k\right)^2 - \frac{p}{2}, 2\left(\frac{p}{2}-k\right), 2\left(\frac{p}{2}-k\right)^2+\frac{p}{2}\right\}$. Expanding and comparing each component, we have proposed equation.

By Proposition 1 , $A\left(\frac{p}{2},2,k,1\right)$ is a solution to (1) since p = $\left(\frac{p}{2}\right)2$ is even and $2\left(\frac{p}{2}-k\right) > \sqrt{p}$: $2\left(\frac{p}{2}-k\right) = 2(q+r-i) > 2k > \sqrt{p}$ by the first case.

By the proof of Proposition 1, $A\left(\frac{p}{2},2,k,1\right)$ is primitive if and only in gcd (2k ,$\frac{p}{2}$) =1 (or equivalently: gcd (k , $\frac{p}{2}$) =1,since P is square free).

The proof of the equation when r is odd is the same as in (a) except for different values of the variables.

Furthermore, A ($\frac{p}{2}$,2, k, 1) is a solution to (1) since P = $\left(\frac{p}{2}\right)2$ is even and 2k > $\sqrt{p}$: by the definitions of k and q, we have 2k = 2 (q + i) ≥ $2q >$ $2\left(\frac{\sqrt{p}+3}{2}-1\right) > \sqrt{p}$. Additionally, $A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right)$ is also a solution by the first case as in part (a). For the corresponding relations, simply replace k by $\frac{p}{2}-k$ in the algebraic part of above proof. Finally, by the proof of Proposition 1, $A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right)$ is primitive if and only if gcd(2($\frac{p}{2}-k$), $\frac{p}{2}$) =1 (or equivalently as above : gcd ($\frac{p}{2}-k,\frac{p}{2}$) = 1). Factoring g(k) = gcd (k ,$\frac{p}{2}$) out of $A\left(\frac{p}{2},2,k,1\right)$ and $A\left(\frac{p}{2},2,\frac{p}{2}-k,1\right)$ are straight forward computations. The first result is primitive since $\frac{p}{2}$ is square-free and gcd (k ,$\frac{p}{2g(k)}$) =1. And the second is similar since g(k) is also gcd ($\frac{p}{2}-k,\frac{p}{2}$).

A general interval decomposition:

From References [1],[2],[3] , Consider the following possibilities for the set M(d) from definition 1.

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

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

M$(p)^{**}$= $\{e(j), S(k,p^{-1}): j\ and\ k\ as\ in\ G(p)^{**}\}$ of inverses of descent matrices. By Lemma 1, these sets contain non integer matrices, but in some sense $G(p)$, $G(p)^*$, $G(p)^{**}$ 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 P = 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 $\sqrt{p}$ and gcd (b n , a m) =1. The interval (a $\sqrt{p}$, ∞) 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$(p)^*$ or M$(p)^{**}$ 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), $\frac{y+z}{x} = \frac{bn}{a}$; 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 P. Suppose first that integer k satisfies $1 \leq k < \frac{p+\delta(p+1)}{2}$ so that

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

Then $\sqrt{p} < \frac{y+z}{x} \leq p;\ and\ z-y > z_{jk} - y_{jk}$ where g_{jk}^{-1}.(x,y,z) =$(e(j).S(k,p).(x,y,z)) = (x_{jk}, y_{jk}, z_{jk})$. Whenever $\frac{y+z}{x}$ is in any of the intervals in (a) –(c) except for a specified case of (b)(i): a) For j =1 and P≥ 6: (2k-1-$\sqrt{\delta(p)}$, $2k-1) where\ q \leq k \leq q+r+1$.
Moreover, if $\frac{x+z}{y}$ = 2k-1, then z_{1k}-x_{1k} =0. b) For j = 3 and P≥ 6 , either i) (2k-1 ,2k-1+$\sqrt{\delta(p)}$) $where\ q \leq k \leq q+r$; and also where k = q-1 when $\sqrt{p} < 2q-1-\sqrt{\delta(p)}$, or ii) (2k-1, $\sqrt{p}\,\frac{2k+\sqrt{p}-1}{\sqrt{p}+1}$) where k > q+r.

However, if P≥ 10 is even and $\frac{x+z}{y}$ = 2k < $\frac{p}{2}$ 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) $\sqrt{p} < \frac{y+z}{x}$ < p where k = 1 and $2 \leq p \leq 5$ or

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

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

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

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

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

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

e) (j=1), $\sqrt{p}\left(2\sqrt{p}-1\right) < \frac{x+z}{y} \leq 2d$.
In this case , z – y > z_{1k}-y_{1k} and z > z_{1k}.
Moreover, if $\frac{y+z}{x} = 2p$, then z_{1k}-$y_{1k} = 0$.

f) (j=2) $\frac{y+z}{x} > \sqrt{p}\left(2\sqrt{p}+1\right)$. In this case, z – y > z_{2k}-y_{2k} and z>z_{2k}.

g) (j=3) 2p< $\frac{y+z}{x} < \sqrt{p}\left(2\sqrt{p}+1\right)$ in this case , z – y > z_{3k}-y_{3k} and z>z_{3k}.

Proof. Let $1 \leq k < \frac{p+\delta(p+1)}{2}$ so that (4) is straightforward. Remark 4 may be helpful with the following computations since
$e(j).S(k,p).A(m,n,a,b) =$
$e(j).(S(k,p).A(m,n,a,b))$.

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

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

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

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

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

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

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

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

$Moreover,\ 2\ Z_{1k} = n(p+1)\,b^2 - (4akp)\,b + a^2 m(p+(2k-1)^2 = 0$ is a quadratic equation in b

with discriminant $-4a^2(p-2k+1)^2 < 0$. Evaluating 2 Z_{1k} at b = 4akp , we find that

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

It follows that the components are all positive if and only if $\sqrt{p}\frac{2k-\sqrt{p}-1}{\sqrt{p}-1} < \frac{y+z}{x} < \sqrt{d}\frac{2k+\sqrt{p}-1}{\sqrt{p}-1}$. Next,

$n[(z-y)-(Z_{1k}-y_{1k})]$ = n$[2a^2m-\delta(p)+1)m(a(2k-10)-bn^2]$

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

And z -y > $Z_{1k}-y_{1k}$ if and only if 2k-1 $-\sqrt{\delta(p)} < \frac{y+z}{x} < 2k-1+\sqrt{\delta(p)}$.

Note that it is straightforward to show

$\sqrt{p}\frac{2k-\sqrt{p}-1}{\sqrt{p}-1} < \frac{y+z}{x} < 2k-1-\sqrt{\delta(p)}$ if and only if

k < $\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-\sqrt{\delta(p)}\right)+1+\sqrt{\delta(p)}\right]$. By hypothesis, assume that

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

By the above, the components of (x_{jk}, y_{jk}, z_{jk}) are positive and z -y > $Z_{1k}-y$. Since

k≤ $(q+r)+\sqrt{\delta(p)} < \frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-\sqrt{\delta(p)}\right)+1+\sqrt{\delta(p)}\right]$. Therefore by the second equivalence above, we have that $\sqrt{p}\frac{2k-\sqrt{p}-1}{\sqrt{p}-1} < 2k-1-\sqrt{\delta(p)} < \frac{y+z}{x} \leq 2k-1 < 2k-1+\sqrt{\delta(p)}$; and thus z-y > $Z_{1k}-y_{1k}$. Note that $\sqrt{p} < \frac{y+z}{x} \leq 2k-1$, it follows that

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

(b) Let j =3.

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

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

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

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

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

k< $\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-\sqrt{\delta(p)}\right)+1-\sqrt{\delta(p)}\right]$ since 2k-1 - $\sqrt{\delta(p)} < 2k-1 < \sqrt{p}\frac{2k+\sqrt{p}-1}{\sqrt{p}+1}$ by (4) , and we have the above intervals on $\frac{y+z}{x}$ 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 < $\frac{y+z}{x}$ < 2k-1 + $\sqrt{\delta(p)}$ when k< $\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-\sqrt{\delta(p)}\right)+1-\sqrt{\delta(p)}\right]$ and ii) 2k-1 < $\frac{y+z}{x}$ < $\sqrt{P}\frac{2k+\sqrt{p}-1}{\sqrt{p}+1}$ otherwise. Let d ≥ 6 and assume that k< $\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-\sqrt{\delta(p)}\right)+1-\sqrt{\delta(p)}\right]$. By remark 1, k≤ $q+r$. Then 2k-1 < $\frac{y+z}{x}$ < 2k-1 + $\sqrt{\delta(p)}$ holds where $\frac{y+z}{x} > \sqrt{p}$, so k > $\frac{1}{2}\left[\sqrt{p}\left(\sqrt{p}-\sqrt{\delta(p)}\right)+1\right]$. It follows By theorem 2, a positive integer multiple of (x , y , z) will be binary root.

(c) Let j =2.

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

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

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

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

$Y_{2k} > 0 \Leftrightarrow$ 2k-1 < $\frac{y+z}{x} < p$ 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

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

And it is easy to check that

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

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

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

It follows that

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

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

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

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

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

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

(d) (j=0)

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

$\iff (bn-2ap)^2$-$\left(a\sqrt{p}\right)^2$>0

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

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

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

$\iff bn < 2ap \iff \frac{y+z}{x} < 2p.$

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 $\frac{y+z}{x} < \sqrt{p}\left(2\sqrt{p}-1\right)$.

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

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

Trees of Primitive Solutions:

A tree of the primitive solutions to (1) is an infinite network of nods 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 $M(P)^*$ or $M(p)^{**}$ exists such that g^{-1}.(x , y , z) produces a new node (x′, y′, z′) that satisfies Definition 1. In the classical case p =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 P > 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 $G(P)^*$ or $G(p)^{**}$, and let g = S(k , p).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, P). (x , y ,z) = i′ (x′, y′, z′) satisfies Fermat's Descent method for some positive integer i′. Unlike the case P = 1, it is necessary to consider the following anomalies.

a) The components of (x, y, z) may not all be positive.
b) The components of (x, y, z) may be positive but not relatively prime.
c) For some odd square-free P, there may exist g in G such that the binary root conditions z′- y′ = z -y in part (c) of Definition 1 hold:
d) There are duplicate nodes in the first level of the derived tree that must be pruned. They arise form the subsets

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

For some primitive root w as follows.
i) For odd square-free P≥ 13 , the nearest nodes in the abutting sets agree when w = (1,0 ,1): $\{S(q+s+1,p).e(1).w, S(q+s+1,p).e(3).w\}$ $(0 \le s \le r)$ Since e(1) . w = e(3) .w
ii) For even square-free P≥ 10 and standard binary root w = $A\left(\frac{p}{2}, 2, k, 1\right)$ as defined in Theorem 2, there exists a unique s in [0, r] such that

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

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, p) and e(1). S(q+s+1 ,p) when p 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

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 $G(P)^*$ or $G(p)^{**}$

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

[4] K.Sridevi and Thiruchinapalli Srinivas ,2020 "A New Approach To Define Two Types Of Binary Operations On Set Of Pythagorean Triples To Form As At Most Commutative Cyclic Semi Group " Journal of Critical Reviews .

[5] K.Sridevi and T. Srinivas ,2021,, A New Approach To Define Cryptographic coding on Binary Operations On Set Of Pythagorean Triples , Materials Today Proceedings, Elsevier (In press).

[6] K.Sridevi and T. Srinivas ,2021 , Transcendental Representation of Diophantine Equations And Some Of Its Inherent Properties , Materials Today Proceedings, Elsevier (In Press)

[7] K.Sridevi and T. Srinivas ,2021, Existence of Inner Addition and Inner Multiplication of Triangular Numbers and Some of Its Inherent Properties , Materials Today Proceedings , Elsevier (In Press).

[8] https://mathworld.wolfrom.com/pythagorean triples

[9] A new approach to generate all Pythagorean triples by Anthony Overmars ,AIMS Mathematics, 4(2):242-253.

[10] A text book " Introduction to Analytic Number Theory " by Tom M. Apostol, Springer.

[11] Pythagorean Triples- www.mathsisfun.com

[12] L.E.Dickson., 2005 History of the theory of numbers: Diophantine analysis, Dover publications,