Hindawi
International Journal of Mathematics and Mathematical Sciences
Volume 2023, Article ID 1505337, 18 pages
https://doi.org/10.1155/2023/1505337

Research Article

On Parametric and Matrix Solutions to the Diophantine Equation $x^2 + dy^2 - z^2 = 0$ Where d Is a Positive Square-Free Integer

James D. Shaw and James Guyker

Department of Mathematics, SUNY College at Buffalo, 1300 Elmwood Avenue, Buffalo, NY 14222-1095, USA

Correspondence should be addressed to James Guyker; guykerj@buffalostate.edu

Received 24 August 2021; Revised 28 February 2022; Accepted 2 March 2022; Published 25 September 2023

Academic Editor: Sergejs Solovjovs

The well-known matrix-generated tree structure for Pythagorean triplets 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. The proof is based on a parametrization of these solutions as well as on a dual version of the Fermat's method of descent.

1. Introduction

Let d be a positive square-free integer. In this paper, the structure of the solutions to the Diophantine equation

$$x^2 + dy^2 - z^2 = 0, \tag{1}$$

is determined (Cf. [1–9]). Since (1) is homogeneous, we may assume that (x, y, z) is primitive, i.e., $\gcd(x, y, z) = 1$. It is well-known ([10–14]) that in the classical case $d = 1$, all such Pythagorean triplets (or nodes) form an infinite tree that is generated by the action of three explicit matrices at each node beginning with the root $(3, 4, 5)$. All nodes descend to $(3, 4, 5)$, and each node appears exactly once.

For each fixed $d > 1$, we construct finite sets of matrices and finite sets of roots that generate all solutions to (1). Given a primitive solution (x, y, z) of equation (1), an algorithm describes a path (or descent) from (x, y, z) to some element in the finite set of roots. The main differences in the classical case are that the descent path may not be unique and that the action of the matrices may result in a nonprimitive solution. These anomalies may, respectively, be remedied by removing improper branches and by dividing nodes by their gcds. Moreover, if d is 2, 6, or any odd square-free integer, the only root is $(1, 0, 1)$. In addition, for any other square-free d, nodes may descend to other roots defined as follows in terms of generating sets.

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 d be a positive square-free integer and let $M(d)$ be a set of nonsingular matrices. A primitive solution (x, y, z) of (1) satisfies the Fermat's method of descent with respect to $M(d)$, if there exists an element g of $M(d)$ with inverse $\mathrm{Inv}[g]$ such that the inner product $\mathrm{Inv}[g]$. (x, y, z) is a positive integer multiple of a primitive solution (x', y', z') where one of the following holds:

(a) $z - x > z' - x'$

(b) $z - x = z' - x'$ and $z > z'$

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

By Lemma 13, it will follow that for any positive square-free integer d, there exists a set $M(d)$ of nonsingular matrices such that every primitive solution of (1) satisfies the Fermat's method with respect to $M(d)$. Given a primitive solution (x, y, z) of (1), we generate the sequence of descents as follows: $(x_0, y_0, z_0) = (x, y, z)$, and for $n \geq 1$, $(x_n, y_n, z_n) = (x_{n-1}', y_{n-1}', z_{n-1}')/\gcd[(x_{n-1}', y_{n-1}', z_{n-1}')]$ and subsequently show that after a finite number of steps, 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 12 and prove that in the sequence of descents, (x',y',z') intertwines (x,y,z) indefinitely as follows: (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:

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

(b) if w is a primitive solution to (1), then there exists a positive integer k and a primitive root r that is either binary or $(1,0,1)$ such that $k \times w =$ (finite product of matrices from G).r.

The origin of the generating sets $G = G(d)$ is Shaw's observation which shows that if (x,y,z) satisfies (7), then so does $(x' = x - ut, y' = y - vt, z' = z - wt)$ where (u,v,w) is *not* a solution to (1) and

$$t = \frac{2(ux + \mathrm{d}v\,y - wz)}{\left(u^2 + \mathrm{d}v^2 - w^2\right)}, \tag{2}$$

or equivalently, $M(u,v,w,d)$ (x,y,z) satisfies (1) where $u^2 + \mathrm{d}v^2 \neq w^2$ and

$$\left(u^2 + \mathrm{d}v^2 - w^2\right) \times M(u,v,w,d) = \begin{pmatrix} -uu + \mathrm{d}v\,v - ww & -2\mathrm{d}u\,v & 2uw \\ -2uv & uu - dv\,v - ww & 2vw \\ -2uw & -2\mathrm{d}v\,w & uu + dv\,v + ww \end{pmatrix}. \tag{3}$$

The sets $G(d)$ result from judicious choices of the triplets (u,v,w) as follows:

Definition 3. Let d be a square-free positive integer and let $\delta(d)$ denote 1 if d is even and 2 otherwise. The kth seminal matrix $S(k,d)$ is defined by

$$\begin{aligned} \delta(d) \times S(k,d) &= (d - 2k + 1) \\ &\quad \times M(k-1,1,k,d) \text{ for } k = 1,2,\ldots,\mu(d) - 1, \\ S(\mu(d),d) &= M(d,1,d,d), \end{aligned} \tag{4}$$

where $2\mu(d) = d + \delta(d+1)$. Moreover, let $v(d) > 0$ and $p(d) > 0$ satisfy $v(d)^2 = \delta(d)$ and $p(d)^2 = d$.

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 matrices $e(j)$ $(j = 0,1,2,3)$, where $e(0)$ is the identity matrix, $e(j)$ $(j = 1,2)$ is $e(0)$ with the (j,j)-entry replaced by -1, and $e(3)$ is $e(0)$ with both (1, 1) and (2, 2) entries replaced by -1, 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 $S(k,d).\ e(j)$.

Our main result is

Theorem 4. *For any positive square-free integer d, the set*

$$G(d) = \{S(k,d).\ e(j):\ 1 \le k \le \mu(d), 0 \le j \le 3\}, \tag{5}$$

generates all primitive solutions to (1).

Minimal generating subsets of $G(d)$ are $G(d)^*$ and $G(d)^{**}$ defined as follows: if $d = 1$, then $G(d)^* = \{S(\mu(d),d).e(j):\ 1 \le j \le 3\}$.

If $d = 2, 3$ or 5, then

$$G(d)^* = \{S(1,d).e(2)\} \cup \{S(\mu(d),d).e(j):\ 0 \le j \le 3\}. \tag{6}$$

Finally, for $d \ge 6$,

$$q = \text{floor}\left[\frac{(p(d)+3)}{2}\right],$$

$$r = \text{floor}\left[\frac{(p(d)(p(d) - v(d)) - (2q - 1 + v(d)))}{2}\right],$$

$$\begin{aligned} G(d)^* &= \{S(q+s,d).\ e(1), S(q+s,d).\ e(3):\ 0 \le s \le r+1\} \cup \\ &\quad \{S(q+r+1,d).\ e(2)\} \cup \{S(\mu(d),d).\ e\ (j):\ 0 \le j \le 3\}. \end{aligned} \tag{7}$$

(a) If $2q - 1 - v\ (d) < p(d)$, then $G(d)^*$ is a generating set for all primitive solutions.

(b) On the other hand, if $p(d) < 2q - 1\text{-}v(d)$, then

$$G(d)^{**} = \{S(q-1,d).\ e(3)\} \cup G(d)^*. \tag{8}$$

is a generating set.

Remark 5. Since $x - 1 < \text{floor}(x) < x$ for irrational x, we have the following useful bounds:

$$q + r < \frac{(p(d)(p(d) - v(d)) + 1 - v(d))}{2} < q + r + 1. \tag{9}$$

Example 1. For $d = 5$, $q = 2$, $r = -2$, root (1, 0, 1), and generating set

$$G(d)^* = \{S(1,d).e(2)\} \cup \{S(\mu(d),d).e(j):\ 0 \le j \le 3\}, \tag{10}$$

we have

$$\begin{aligned} &S(1,d).\ e(2).\ (1,0,1) = (2,1,3), \\ &S(3,d).\ e(0).\ (1,0,1) = (1,0,1), \\ &S(3,d).\ e(1).\ (1,0,1) = (19,4,21), \\ &S(3,d).\ e(3).\ (1,0,1) = (19,4,21), \\ &S(3,d).e(2).\ (1,0,1) = (1,0,1), \end{aligned} \tag{11}$$

so the first level consists of the proper nodes (2, 1, 3) and (19, 4, 21). Continuing as above,

$$
\begin{aligned}
S(1,d).e(2).\ (2,1,3) &= (4,6,14),\\
S(3,d).e(0).\ (2,1,3) &= (2,1,3),\\
S(3,d).e(1).\ (2,1,3) &= (38,9,43),\\
S(3,d).e(3).\ (2,1,3) &= (58,11,63),\\
S(3,d).e(2).\ (2,1,3) &= (22,3,23),\\
S(1,d).e(2).\ (19,4,21) &= (38,33,83),\\
S(3,d).e(0).\ (19,4,21) &= (-1,0,1),\\
S(3,d).e(1).\ (19,4,21) &= (341,76,381),\\
S(3,d).e(3).\ (19,4,21) &= (421,84,461),\\
S(3,d).e(2).\ (19,4,21) &= (79,8,81).
\end{aligned}
\tag{12}
$$

Dropping the irrelevant outputs (2,1,3) and (−1,0, 1), the first two levels of the tree of all primitive solutions by the proof of Theorem 4 are given in Figure 1.

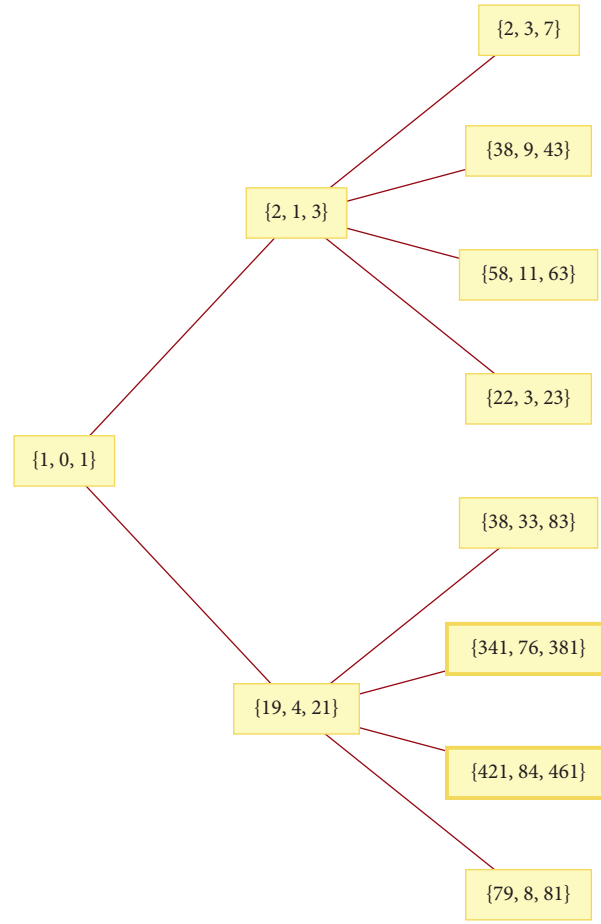

Figure 1: $x^2 + 5y^2 - z^2 = 0$.

2. Parametric Representation

Our descent method depends on the following generalization of the classical representation theorem ([15–17]) for primitive Pythagorean triplets.

Proposition 6. *Let d be an even square-free positive integer. The primitive solutions (x, y, z) of (1) are exactly of the form*

$$A(m,n,b,a) \equiv \left(x = nb^2 - ma^2,\ y = 2ab,\ z = nb^2 + ma^2\right), \tag{13}$$

for positive integers m, n, a and b such that $d = mn$, $bn > ap(d)$ and gcd $(bn, a\,m) = 1$.

On the other hand, if d is an odd square-free positive 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 of opposite parity; and when y is odd, $(x, y, z) = A(m, n, b, a)/2$ where a and b are odd.

Proof. Suppose that $(x.y, z)$ is a primitive solution of (1) so that the following holds:

If y is even, then $d(y/2)^2 = [(z - x)/2][(z + x)/2]$.

Otherwise,

$$dy^2 = (z - x)(z + x). \tag{14}$$

Assume first that d is even. Then, by (1), x and z have the same parities, $dy^2 = (z - x)\ (z + x)$ where z–x and $z + x$ are even, and since d is square-free, y^2 and y are even. It follows that x and z are odd since (x, y, z) is primitive. By (14), each prime factor (including 2) of d divides either $(z - x)/2$ or $(z + x)/2$, i.e., there exist square − free integers m and n such that $d = mn$ and $(y/2)^2 = [(z - x)/(2m)][(z + x)/(2n)]$. Moreover, any prime divisor of $(z - x)/(2m)$ and $(z + x)/(2n)$ must be 1 since it also divides $y/2$, $(z - x)/2$ and $(z + x)/2$ (i.e., x, y and z). Consequently, $(z - x)/(2m) = a^2$ and $(z - x)/(2n) = b^2$ for positive integers a and b by the prime factorization theorem (See [4]).

Solving for (x, y, z), we have $(x, y, z) = A(m, n, b, a)$ where $bn > ap(d)$. Furthermore, gcd $(bn,\ a\ m) = 1$ iff $\gcd(b^2n, a^2m) = 1$ iff $\gcd((z + x)/2, (z - x)/2) = 1$ iff $\gcd(x, z) = 1$. Let p be a prime divisor of x and z. Then, p^2 divides $d(y/2)^2$ by (14) where p may be at most one factor of d. It follows that p divides $y/2$ (and y) so that $p = 1$ since (x, y, z) is primitive.

Conversely, suppose that $(x, y, z) = A(m, n, b, a)$. Then, $x^2 + dy^2 - z^2 = (x - z)\quad(x + z) + dy^2 = -2a^2m(2b^2n) + d(2ab)^2 = 0$, and x, y, and z are positive. Finally, as above, $\gcd(x, z) = 1 = \gcd(bn,$ a m); and (x, y, z) is primitive since any prime divisor is a divisor of x and z.

Similar arguments may be made when d is odd and y is either even or odd. □

Remark 7. For a fixed factorization $d = mn \neq 1$ of square-free d 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 $(z - x)/(2m)$ is a square integer.

(b) $(x, y, z) = A(m, n, b, a)/2$ if and only if $(z - x)/(m)$ is a square integer.

These ensue directly from Proposition 6: For (a) $(z - x)/(2m) = a^2$ so we show that the condition $(z - x)/(2m)$ is

a square integer holds only in this case. The other possibilities are

(i) $(x, y, z) = A(n, m, b, a)$ where $\gcd(bm, an) = 1$. But in this case, $(z - x)/(2m) = (na^2)/m \neq$ square integer, since $\gcd(m, n) = 1 = \gcd(m, a)$.

(ii) $(x, y, z) = A(m, n, b, a)$ where $(z - x)/(2m) = a^2/2$ is not a square integer.

(iii) $(x, y, z) = A(n, m, b, a)/2$ where $\gcd(bm, an) = 1$. Again, in this case, $(z - x)/(2m) = (na^2)/(2m) \neq$ square integer, since $\gcd(m, n) = 1 = \gcd(m, a)$.

(b) is similar.

Remark 8. The proof of Proposition 6 shows the following concerning the parametric representations of primitive solutions (x, y, z) of (1) for square-free d:

If y is even, then $(x, y, z) = A(m, n, b, a)$ where m is the product of the common factors of d and $(z - x)/(2)$; and $n = d/m$.

Furthermore, $a^2 = (z - x)/(2m)$ and $b^2 = (z + x)/(2n)$. In this case, if d is odd, then a and b are of opposite parity.

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

Remark 9. Since $A(m, n, b, a) = nb^2(1, 0, 1) + 2ab(0, 1, 0) + ma^2(-1, 0, 1)$, expressions involving $S(k, d)$. $A(m, n, b, a)$ may be simplified accordingly: If $k < \mu(d)$, then $\delta(d)\, S(k, d).A(m, n, b, a) = nb^2 A(1, d, 1, 1) - 2ab(2d(k - 1), d + (2k - 1), 2dk) + ma^2 A(d, 1, 2k - 1, 1)$. Otherwise, $\delta(d)\, S(\mu(d), d).A(m, n, b, a) = nb^2(1, 0, 1) - 2ab(2d, 1, 2d) + ma^2 A(1, d, 2, 1)$.

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

Lemma 10. *The descent and ascent matrices are related by inverse formulas for all j, k, and d:* If $k = \mu(d)$, *then* $Inv[e(j).S(k, d)] = S(k, d).e(j)$.

Otherwise, $k < \mu(d)$ *and* $(d - 2k + 1)^2$ $\mathrm{Inv}[e(j).S(k, d)] = \delta(d)^2[S(k, d).e(j)]$.

Proof. Suppose that (x, y, z) is a solution to (1) and $u^2 + dv^2 \neq w^2$. By the definitions of M and t given in Section 1,

$$M(u, v, w, d).(x, y, z) = \left(x' = x - ut, y' = y - vt, z' = z - wt\right), \tag{15}$$

is a solution to (1) such that

$$M(u, v, w, d).\left(x', y', z'\right) = \left(x'' = x' - ut', y'' = y' - vt', z'' = z' - wt'\right), \tag{16}$$

where $t' = -t$. Consequently, $(x'', y'', z'') = (x, y, z)$ and

$$M(u, v, w, d)^2.(x, y, z) = (x, y, z), \tag{17}$$

for every solution (x, y, z) to (1). In particular, by Proposition 6, this identity holds for $(x, y, z) = A(1, d, d + 2n - 1, 1)$ $(n = 1, 2, 3)$. Since the determinant of the matrix with these solutions as rows is $-64d \neq 0$, we have that the solutions are linearly independent and, therefore, $M(u, v, w, d)^2$ is the identity matrix. Lemma 10 is now immediate since the vectors (u, v, w) in the definitions of the seminal matrices $S(k, d)$ satisfy $u^2 + dv^2 \neq w^2$. □

3. Theorem 4 When d Is Even

We now show that the only possibility of binary roots (x, y, z) defined by Definition 1 is when square-free $d = mn \geq 10$ is even and $(x, y, z) = A(m, n, b, a)$ where $bn = a(2k)$. In this case, the identity

$$nA(m, n, b, a) = 2a^2 A\left(\frac{d}{2}, 2, k, 1\right), \tag{18}$$

reduces $A(m, n, b, a)$ to "standard" binary roots of the form $A(d/2, 2, k, 1)$. Moreover, the copartner $A'(m, n, b, a)$ of (x, y, z) satisfies

$$nA'(m, n, b, a) = 2a^2 A'\left(\frac{d}{2}, 2, \frac{d}{2} - k, 1\right). \tag{19}$$

where $bn = a(2(d/2 - k))$. Note that the multiples n and $2a^2$ will usually be ignored in the descent process.

The next result is unexpected in view of the definitions of q and r. It will play a key role in determining the constant k.

Lemma 11. *Let $d \geq 6$ be a square-free even integer The following are equivalent:*

(a) $d = 4q + 2r - 2$

(b) $p(d) < 2(q - 1)$

(c) r is even.

Similarly, the following are equivalent:

(d) $d = 4q + 2r$

(e) $p(d) > 2(q - 1)$

(f) r is odd

Proof. Let $d \geq 6$ be even and square-free.

$(a) \Rightarrow (c)$. If $d = 4q + 2r - 2$, then $d/2 = (2q - 1) + r$ so r is even since $d/2$ and $2q - 1$ are odd.

$(d) \Rightarrow (f)$. It is similar to $(a) \Rightarrow (c)$.

$(b) \Rightarrow (a)$. Assume that $\rho(d) < 2(q - 1)$. Then, by the definitions of q and r,

$$4q + 2r - 2 < d + [p(d) - 2(q - 1)] + 2 < d + 2. \tag{20}$$

Since $4q + 2r - 2$ and $d + 2$ are even integers, we have that $4q + 2r - 2 \leq d$. Moreover, as in Remark 8,

$$4q + 2r - 2 > [(2(q - 1) - p(d)] + d - 2 > d - 2, \tag{21}$$

so $4q + 2r - 2 \geq d$ and (a) follows.

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

$$4q + 2r - 2 < d + [2(q-1) - \rho(d)] < d. \tag{22}$$

Since $4q + 2r - 2$ and d are even, $4q + 2r - 2 \le d$.

Similarly, by the assumption,

$$4q + 2r > d + p(d) - 2q > d - 2. \tag{23}$$

Since $4q + 2r$ and $d - 2$ are even, $4q + 2r \ge d$ and (d) follows.

$(a)\Longleftrightarrow(b)$. It remains to show $(a)\Rightarrow(b)$. Assume that $d = 4q + 2r - 2$. Then, either $p(d) < 2(q-1)$ or $p(d) > 2(q-1)$. However, if $\rho(d) > 2(q-1)$, then by $(e)\Rightarrow(d)$, $d = 4q + 2r$ which is false in this case, so $p(d) < 2(q-1)$.

$(d)\Longleftrightarrow(e)$. We only need to show $(d)\Rightarrow(e)$ which is similar to $(a)\Longrightarrow(b)$.

$(c)\Longleftrightarrow(a)$. It remains to show $(c)\Longrightarrow(a)$. Assume r is even. Either $p(d) < 2(q-1)$ or $p(d) > 2(q-1)$. By the equivalences $(a)\Longleftrightarrow(b)$ and $(d)\Longleftrightarrow(e)$, either $d = 4q + 2r - 2$ or $d = 4q + 2r$. But if $d = 4q + 2r$, then $d/2 = 2q + r$ so r must be odd (a contradiction) since d/2 is odd and 2q is even. It follows that $d = 4q + 2r - 2$ and (a) results.

$(f)\Longleftrightarrow(d)$. It is similar to $(c)\Longleftrightarrow(a)$.

By Lemma 11, we have the resulting characterizations of binary roots and their copartners: □

Theorem 12. *Let the square-free integer $d \ge 10$ be even. There are exactly $[r + \delta(r+1)]/2$ standard binary roots as follows: Let $k = q + i + 1\text{-}\delta(r+1)$ for some integer i in $[0, r/2]$. Then, $d/2 - k > k$ and we have the following cycle:*

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

$$\left(e(3).S\left(\frac{d}{2}-k,d\right)\right).A\left(\frac{d}{2},2,\frac{d}{2}-k,1\right) = A\left(\frac{d}{2},2,k,1\right). \tag{24}$$

It follows that $A(d/2,2,k,1)$ is a binary root with copartner $A(d/2, 2, d/2-k, 1)$ by Definition 1.

Moreover, if $g(k) = \gcd(k, d/2)$, then

$$A\left(\frac{d}{2},2,k,1\right) = g(k)A\left(\frac{(d/2)}{g(k)},2g(k),\frac{k}{g(k)},1\right), \tag{25}$$

where $A((d/2)/g(k), 2g(k), k/g(k), 1)$ is primitive and similarly,

$$A\left(\frac{d}{2},2,\frac{d}{2}-k,1\right) = g(k)\,A\left(\frac{d/2}{g(k)},2g(k),\frac{((d/2)-k)}{g(k)},1\right), \tag{26}$$

where $A((d/2)/g(k), 2g(k), ((d/2)-k)/g(k), 1)$ is primitive.

Proof. Let $d \ge 10$ be even and square-free. Then, $q \ge 3$ and $r \ge 0$.

Let us suppose first that r is even and $k = q - 1 + i$ where $0 \le i \le r/2$. By Lemma 11, $d = 4q + 2r - 2$ and $d/2 - k = q + r - i > k$. By Remark 9, since $k \le q - 1 + r/2 < \mu(d) = 2q + \mathrm{r}$,

$$\begin{aligned}(e(3).S(k,d)).A\left(\left(\frac{d}{2}\right),2,k,1\right) &= 2k^2\{1-d,-2,d+1\} - 2k\{2d(1-k),1-2k-d,2dk\} \\ &\quad + \left(\frac{d}{2}\right)\left\{d-(2k-1)^2,-2(2k-1),d+(2k-1)^2\right\}.\end{aligned} \tag{27}$$

Moreover, $A(d/2, 2, d/2-k, 1) = \{2(d/2-k)^2 - \mathrm{d}/2, 2(\mathrm{d}/2-\mathrm{k}), 2(d/2-k)^2 + d/2\}$.

By expanding and comparing each component, we have the proposed equation.

By Proposition 6, $A(d/2,2,k,1)$ is a solution to (1) since $d = 2(d/2)$ is even and $2k > p(d)$: r is even, so by the definition of k and part (b) of Lemma 11, $2k = 2(q-1+i) \ge 2(q-1) > p(d)$. Furthermore, $A(d/2, 2, d/2\text{-}k, 1)$ is also a solution since $d = 2(d/2)$ is even and $2(d/2-k) > \rho(d)$: $2(d/2-k) = 2(q+r-i) > 2k > \rho(d)$ by the first case.

By the proof of Proposition 6, $\mathrm{A}(d/2, 2, \mathrm{k}, 1)$ is primitive if and only if $\gcd(2k, d/2) = 1$ (or equivalently: $\gcd(k, d/2) = 1$, since d 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.

Moreover, $A(d/2,2,k,1)$ is a solution to (1) since $d = 2(d/2)$ is even and $2k > p(d)$: by the definitions of k and q, we have $2k = 2(q+i) \ge 2q > p(d) + 1 > p(d)$. Additionally, $A(d/2, 2, d/2-k, 1)$ is also a solution by the first case as in part (a).

For the corresponding relations, we simply replace k by $d/2 - k$ in the algebraic part of the previous proof.

Finally, by the proof of Proposition 6, $A(d/2, 2, d/2-k, 1)$ is primitive if and only if

$$\gcd\left(2\left(\frac{d}{2}-k\right),\frac{d}{2}\right) = 1\left(\text{or equivalently, as above: } \gcd\left(\frac{d}{2}-k,\frac{d}{2}\right) = 1\right). \tag{28}$$

Factoring $g(k) = \gcd(k, d/2)$ out of $A(d/2,2,k,1)$ and $A(d/2, 2, d/2-k, 1)$ are straightforward computations. The first result is primitive since $d/2$ is square-free and $\gcd(k, (d/2)/g(k)) = 1$. The second is similar since $g(k)$ is also $\gcd(d/2-k, d/2)$

For example, if $d = 30$, then $q = 4$ and $r = 8$. Let us suppose that $k = q - 1$. Then,

$$
\begin{aligned}
g(k) &= \gcd\left(k, \frac{d}{2}\right) \\
&= \gcd\left(\frac{d}{2} - k, \frac{d}{2}\right) \\
&= 3, \\
A\left(\frac{d}{2}, 2, k, 1\right) &= 3 \times (1, 2, 11) \\
&= g(k) A\left(\frac{(d/2)}{g(k)}, 2g(k), \frac{k}{g(k)}, 1\right) \\
&= 3A(5, 6, 1, 1) \text{and}, \\
A\left(\frac{d}{2}, 2, \frac{d}{2} - k, 1\right) &= 3 \times (91, 8, 101) \\
&= g(k) A\left(\frac{(d/2)}{g(k)}, 2g(k), \frac{(d/2 - k)}{g(k)}, 1\right) \\
&= 3A(5, 6, 4, 1).
\end{aligned} \tag{29}
$$

By (18) and (31), Theorem 12 holds for the more general forms $A(m, n, 2k/n, 1)$ and $A(m, n, 2(d/2 - k)/n, 1)$ of binary roots and their copartners whenever $d = mn$ is even.

In this case, they are primitive if and only if $\gcd(2k, m) = 1 = \gcd(2(d/2 - k), m)$ and if and only if m is odd and $\gcd(k, m) = 1 = \gcd(d/2 - k, m)$. □

4. A General Interval Decomposition

Let us consider the following sets of inverses for the set $M(d)$ from Definition 1:

$$
\begin{aligned}
M(d) &= \{\mathbf{Inv}[e(j).S(k,d)]:\ j \text{ and } k \text{ as in } G(d)\}, \\
M(d)^* &= \{\mathbf{Inv}[e(j)\,.\,S(k,d)]:\ j \text{ and } k \text{ as in } G(d)^*\}, \\
M(d)^{**} &= \{\mathbf{Inv}[e(j).S(k,d)]:\ j \text{ and } k \text{ as in } G(d)^{**}\}.
\end{aligned} \tag{30}
$$

By Lemma 10, these sets contain noninteger matrices, but in some sense $G(d)$, $G(d)^*$ and $G(d)^{**}$ from Theorem 4 will, respectively, be their generator completions.

Let (x, y, z) be a primitive solution of (1). By Proposition 6, there is a unique factorization $d = mn$ such that (x, y, z) is either $A(m, n, b, a)$ or $A(m, n, b, a)/2$ for certain positive integers a and b with $bn > a\rho(d)$ and $\gcd(bn, a\,m) = 1$. The interval $(a\ p(d),\ \infty)$ will now be expressed as a union of subintervals with the property that if bn is in the kth subinterval, then there is an element g_{jk} of $M(d)^*$ or $M(d)^{**}$ such that $\mathrm{Inv}[g_{jk}].\ (x, y, z)$ 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 and 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 6, for primitive solution (x, y, z) of (1), $(x + z)/y = (b \times n)/a$, and by the proof, $\gcd(bn, a\,m) = 1$ is equivalent to $\gcd(x, z) = 1$. (Actually, $\gcd(x, z) = 1$ follows directly from (x, y, z) being a primitive solution of (1)).

Lemma 13. *Let (x, y, z) be a primitive solution of (l) for some positive square-free integer d. Suppose that integer k satisfies $1 \le k < \mu(d)$ so that*

$$
p(d)\left[\frac{(2k - p(d) - 1)}{(p(d) - 1)}\right] < 2k - 1 < p(d)\left[\frac{(2k + p(d) - 1)}{(p(d) + 1)}\right] < d. \tag{31}
$$

Then, $p(d) < (x + z)/y \le d$ and $z - x > z_{jk} - x_{jk}$ where

$$
\mathrm{Inv}\left[g_{jk}\right].\ (x, y, z) = (e(j).\ S(k, d)).\ (x, y, z) = \left(x_{jk}, y_{jk}, z_{jk}\right), \tag{32}
$$

when $(x + z)/y$ is in any of the intervals in $(a) - (c)$ except for a specified case of $(b)(i)$:

(a) For $j = 1$ and $d \ge 6$,

$$
(2k - 1 - v(d), 2k - 1] \text{where } q \le k \le q + r + 1. \tag{33}
$$

Moreover, if $(x + z)/y = 2k - 1$, then $z_{1k} - x_{1k} = 0$.

(b) For $j = 3$ and $d \ge 6$, either

(i) $(2k - 1, 2k - 1 + v(d)]$ where $q \le k \le q + r$, and where $k = q - 1$ whenever $p(d) < 2q - 1\text{-}v(d)$.
or

(ii) $(2k - 1, p(d)[(2k + \rho(d) - 1)/(p(d) + 1)])$ where $k > q + r$.

However, if $d \ge 10$ is even and $(x + z)/y = 2k < d/2$ in $(b)(i)$, then (x, y, z) is a binary root. This is the only possibility for part (c) of Definition 1.

(c) For $j = 2$, either

(i) $p(d) < (x + z)/y < d$ where $k = 1$ and $2 \le d \le 5$.
or

(ii) $p(d)[(2k + p(d) - 1)/(p(d) + 1)] < (x + z)/y \le d$, where $d \ge 6$ and

$$
q + r < k < \frac{[((p(d) + 1)/p(d))((x + z)/y) + 1 - p(d)]}{2}. \tag{34}
$$

In this case, faster convergence may be obtained with the largest possible k.
Moreover, if $(x + z)/y = d$, then $z_{2k} - x_{2k} = 0$.
Note that the case $d = 1$ is a consequence of parts (e), (f), and (g).
On the other hand, let $k = \mu(d)$ and $(x + z)/y > d$. Then, (x_{jk}, y_{jk}, z_{jk}) satisfies Definition 1 if

(d) $(j = 0)$

$$d < \frac{(x+z)}{y} < p(d)(2\rho(d) - 1). \tag{35}$$

In this case, $z - x = z_{0k} - x_{0k}$ and $z > z_{0k}$.

(e) $(j = 1)$

$$p(d)(2p(d) - 1) < \frac{(x+z)}{y} \leq 2d. \tag{36}$$

In this case, $z - x > z_{1k} - x_{1k}$ and $z > z_{1k}$.

Moreover, if $(x + z)/y = 2d$, then $z_{1k} - x_{1k} = 0$.

(f) $(j = 3)$

$$2d < \frac{(x+z)}{y} < p(d)(2p(d) + 1). \tag{37}$$

In this case, $z - x > z_{3k} - x_{3k}$ and $z > z_{3k}$.

(g) $(j = 2)$

$$\frac{(x+z)}{y} > p(d)(2p(d) + 1). \tag{38}$$

In this case, $z - x = z_{2k} - x_{2k}$ and $z > z_{2k}$.

Proof. Let $1 \leq k < \mu(d)$ so that (31) is straightforward. Remark 9 may be helpful with the following computations since:

$$(e(j).S(k,d)).A(m,n,b,a) = e(j).(S(k,d).A(m,n,b,a)). \tag{39}$$

(a) Let $j = 1$, and for (x_{1k}, y_{1k}, z_{1k}): $x_{1k} > 0 \Longleftrightarrow z_{1k} + x_{1k} > z_{1k} - x_{1k} \Longleftrightarrow n \quad (am - b)^2 - m(bn - a(2k - 1))^2 > 0 \Longleftrightarrow$

$$\{n(m - b/a) - p(d)[(bn)/a - 2k + 1]\}$$

$$\times\{p(d)(d - (bn)/a) + d[(bn)/a - (2k - 1)]\}$$

$$> 0 \Longleftrightarrow \{-(bn)/a + [d + p(d)(2k - 1)]/[1 + p(d)]\}$$

$$\times\{-(bn)/a + d[p(d) - 2k + 1]/[p(d)(1 - p(d))]\} < 0 \Longleftrightarrow p(d)\left[\frac{(2k - p(d) - 1)}{(p(d) - 1)}\right] < \frac{(x+z)}{y} < p(d)\left[\frac{(2k + p(d) - 1))}{(p(d) + 1)}\right]. \tag{40}$$

Similarly,

$$\begin{aligned} y_{1k} > 0 &\Longleftrightarrow z_{1k} + y_{1k} > z_{1k} - y_{ik} \\ &\Longleftrightarrow (bn - a(2k - 1))(bn - ad) > 0 \\ &\Longleftrightarrow \frac{(x+z)}{y} < 2k - 1 \text{ or } \frac{(x+z)}{y} > d. \end{aligned} \tag{41}$$

Moreover, $2z_{1k} = n(d + 1)b^2 - (4\text{akd})b + a^2m\ (d + (2k - 1)^2) = 0$ is a quadratic equation in b with discriminant $-4a^2d(d - 2k + 1)^2 < 0$. Evaluating $2z_{1k}$ at $b = 4\text{akd}$, we find that $2z_{1k} = 16a^2k^2d^2(n(d + 1) - 1) + a^2m \times (d + (2k - 1)^2) > 0$, so z_{1k} is always positive.

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

$$p(d)\left[\frac{(2k - p(d) - 1)}{(p(d) - 1)}\right] < \frac{(x+z)}{y} < 2k - 1. \tag{42}$$

Next,

$$\begin{aligned} &n[(z - x) - (z_{1k} - x_{1k})] \\ &\quad = n\left[2a^2m - \delta(d + 1)m(a(2k - 1) - bn)^2\right] \\ &\quad = -\delta(d + 1)d[bn - a(2k - 1 - v(d))] \\ &\qquad \times [bn - a(2k - 1 + v(d))], \end{aligned} \tag{43}$$

and $z - x > z_{1k} - x_{1k}$ if and only if $2k - 1 - v(d) < (x + z)/y < 2k - 1 + v(d)$.

Note that it is straightforward to show $p(d)[(2k - p(d) - 1)/(p(d) - 1)] < 2k - 1 - v(d) < \Rightarrow k < [p(d)(p(d) - v(d)) + 1 + v(d)]/2$ By hypothesis, assume that $2k - 1 - v(d) < (x + z)/y \leq 2k - 1$ where $q \leq k \leq q + r + 1$.

By the previous part, the components of (x_{1k}, y_{1k}, z_{1k}) are positive and z-x $> z_{1k} - x_{1k}$.

Since $k \leq q + r + 1$, it follows by Remark 5 that

$$k \leq (q + r) + v(d) < \frac{[p(d)(p(d) - v(d)) + 1 + v(d)]}{2}. \tag{44}$$

Therefore, by the second equivalence given above, we have that

$$p(d)\left[\frac{(2k-p(d)-1)}{(p(d)-1)}\right] < 2k-1-v(d) < \frac{(x+z)}{y} < 2k-1 < 2k-1 + v(d), \text{ and thus } z-x > z_{1k}-x_{1k}. \tag{45}$$

Note that since $p(d) < (x+z)/y < 2k-1$, it follows that

$$k > \frac{(p(d)+1)}{2} = \frac{(p(d)+3)}{2} - 1 > \text{floor}\left[\frac{(p(d)+3)}{2}\right] - 1. \tag{46}$$

So, the hypothesis that $k \geq q$ is necessary.

Finally, if $(x+z)/y = 2k-1$, then $a(z_{1k}-x_{1k}) = m((x+z)/y - (2k-1))^2 = 0$.

(b) Let $j = 3$.

$$x_{3k} > 0 < \Rightarrow p(d)\left[\frac{(2k-p(d)-1)}{(p(d)-1)}\right] < \frac{(x+z)}{y} < p(d)\left[\frac{(2k+p(d)-1)}{(p(d)+1)}\right] \text{as with } x_{1k} > 0. \tag{47}$$

As in (a)

$$\begin{aligned} y_{3k} > 0 &\Leftrightarrow z_{3k} + y_{3k} \\ &> z_{3k} - y_{3k} \\ &\Leftrightarrow (bn - a(2k-1))(bn - ad) < 0 \\ &\Leftrightarrow 2k-1 < \frac{(x+z)}{y} < d. \end{aligned} \tag{48}$$

The proof of $z_{3k} > 0$ is identical to that of $z_{1k} > 0$.

Subsequently, by (31), all components are positive if and only if

$$2k-1 < \frac{(x+z)}{y} < p(d)\left[\frac{(2k+\rho(d)-1)}{(\rho(d)+1)}\right]. \tag{49}$$

Next, $z-x > z_{3k}-x_{3k}$ is equivalent to

$$2k-1-v(d) < \frac{(x+z)}{y} < 2k-1+v(d), \tag{50}$$

as in (a).

Special Case. Moreover, $z-x = z_{3k}-x_{3k}$ if and only if $(x+z)/y = 2k-1 \pm v(d)$. If $d \geq 10$ is even and $2k-1 < (x+z)/y = 2k < d/2$, then (x, y, z) is a binary root by a shortened version of the proof of Theorem 12.

By a direct calculation,

$$2k-1+v(d) < p(d)\left[\frac{(2k+p(d)-1)}{(p(d)+1)}\right] \Leftrightarrow k < \frac{[p(d)(p(d)-v(d))+1-v(d)]}{2}. \tag{51}$$

Since

$$2k-1-v(d) < 2k-1 < p(d)\left[\frac{(2k+p(d)-1)}{(p(d)+1)}\right], \tag{52}$$

by (31), we have the previous intervals on $(x+z)/y$ 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

$b(i)$ $2k-1 < (x+z)/y < 2k-1+v(d)$ when $k < [p(d)(p(d)-v(d))+1-\text{v(d)}]/2$

and

$b(ii)$ $2k-1 < (x+z)/y < p(d)[(2k+p(d)-1)/(p(d)+1)]$ otherwise.

Let $d \geq 6$ and assume that $k < [p(d)(p(d)-v(d))+1-v(d)]/2$. By Remark 5, $k \leq q+r$. Then, $2k-1 < (x+z)/y < 2k-1+v(d)$ holds where $(x+z)/y > p(d)$ by (31), so $2k > p(d)-v(d)+1$. In particular, $2q > p(d)+1 > p(d)-v(d)+1$ and thus $q \leq k \leq q+r$. Moreover, if $p(d) < 2q-1-v(d)$, then $k = q-1$ is also possible since $2q-1-v(d) \leq 2q-3+v(d)$ and it follows that $p(d) < 2q-3+v(d)$ or $2(q-1) > p(d)-v(d)+1$.

On the other hand, if $k > [p(d)(p(d)-v(d))+1-\text{v(d)}]/2$, then by Remark 5, $k > q+r$ for interval (ii) as follows: $2k-1 < (x+z)/y < p(d)[(2k+p(d)-1)/(p(d)+1)]$.

(c) Let $j = 2$. Then, as in (a),

$$x_{2k} > 0 \Leftrightarrow z_{2k} + x_{2k} > z_{2k} - x_{2k}$$
$$\Leftrightarrow \frac{(x+z)}{y} < [p(d)(2k - p(d) - 1)/(p(d) - 1)] \text{or} \frac{(x+z)}{y} > p(d)\left[\frac{(2k + p(d) - 1)}{(p(d)+1)}\right]. \tag{53}$$
$$y_{2k} > 0 < \Rightarrow 2k - 1 < \frac{(x+z)}{y} < d,$$

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

$$p(d)\left[\frac{(2k + p(d) - 1)}{(p(d)+1)}\right] < \frac{(x+z)}{y} < d. \tag{54}$$

Next,

$$n[(z - x) - (z_{2k} - x_{2k})] = n\left[2a^2 m - \delta(d+1)(am - b)^2 n\right]$$
$$= -\delta(d+1)[bn - a\,p(d)(p(d) - v(d))][bn - a\,p(d)(p(d) + v(d))]. \tag{55}$$

Consequently, $z - x > z_{2k} - x_{2k}$ if and only if

$$p(d)(p(d) - v(d)) < \frac{(x+z)}{y} < p(d)(p(d) + v(d)). \tag{56}$$

It is easy to check that

$$p(d)\left[\frac{(2k + p(d) - 1)}{(p(d)+1)}\right] < p(d)(p(d) - v(d)), \tag{57}$$

if and only if $k < [p(d)(\rho(d) - v(d)) + 1 - v(d)]/2$. Therefore, by (31) and the previous results, (x_{2k}, y_{2k}, z_{2k}) fulfills part (a) of Definition 1 if and only if

$$p(d)(p(d) - v(d)) < \frac{(x+z)}{y} < d \text{ when } k < \frac{[p(d)(p(d) - v(d)) + 1 - v(d)]}{2},$$
$$p(d)\left[\frac{(2k + p(d) - 1)}{(\rho(d)+1)}\right] < \frac{(x+z)}{y} < d \text{ otherwise.} \tag{58}$$

$c(i)$ Note that for $d \neq 1$,

$$2 < p(d)(p(d) - v(d)) + 1 - v(d) = d + 1 - v(d)(p(d) + 1)$$
$$\Leftrightarrow v(d)(p(d)+1) < (p(d) - 1)(p(d)+1) \Leftrightarrow p(d) > 1 + v(d) \Leftrightarrow d \geq 6. \tag{59}$$

It follows that if $2 \leq d \leq 5$, then the second possibility given above holds with $k = 1$ and

$$p(d) < \frac{(x+z)}{y} < d. \tag{60}$$

$c(ii)$ Let $d \geq 6$. By Remark 5 as in the proof of (b), the condition

$$k < \frac{[p(d)(p(d) - v(d)) + 1 - v(d)]}{2}, \tag{61}$$

is equivalent to $1 \leq k \leq q + r$. Therefore, the second possibility given above holds whenever $k > q + r$. However, in this case, k can always be maximized at this step to ensure faster convergence since $2k + p(d) - 1 < [(p(d) + 1)/p(d)] \times (x+z)/y$ so we can choose k = Floor of $[[(p(d)+1)/p(d)] \times [(x+z)/y] + 1 - p(d)]/2$.

Finally, if $(x+z)/y = d$, then $n(z_{2k} - x_{2k}) = (bn - ad)^2 = 0$.

On the other hand, suppose that $k = \mu(d)$ and $(x+z)/y > d$ where $d = mn$ is square-free.

$(d)\,(j=0)$

$$\begin{aligned} x_{0k} > 0 &\Leftrightarrow n(z_{0k} + x_{0k}) - n(z_{0k} - x_{0k}) > 0 \\ &<\Rightarrow (bn - 2ad)^2 - (a\,p(d))^2 > 0 \\ &\Leftrightarrow ((x+z)/y - p(d)(2p(d)-1))((x+z)/y - p(d)(2p(d)+1)) > 0. \\ &\Leftrightarrow \text{Either } \frac{(x+z)}{y} < p(d)(2p(d)-1) \text{ or } \frac{(x+z)}{y} > p(d)(2p(d)+1). \end{aligned} \tag{62}$$

Similarly,

$$\begin{aligned} y_{0k} > 0 &\Leftrightarrow \text{bn} < 2ad \\ &<\Rightarrow \frac{(x+z)}{y} < 2d. \end{aligned} \tag{63}$$

Finally, $z_{0k} = nb^2 - (4\text{amn})b + a^2m(4mn+1) = 0$ is a quadratic equation in b with negative discriminant $-4a^2d$. Since $z_{0k} > 0$ when $b^2 = 4a^2md$, we have that z_{0k} is always positive.

It follows that the components are positive if and only if $(x+z)/y < p(d)(2p(d)-1)$.

Next, $z - x = 2a^2m = z_{0k} - x_{0k}$.

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

$(e)\ (j=1)$

$$\begin{aligned} x_{1k} > 0 &<\Rightarrow (bn - a\,p(d)(2p(d)-1)\ (bn - a\,p(d)(2p(d)+1)) < 0 \\ \Leftrightarrow p(d)(2p(d)-1) &< \frac{(x+z)}{y} < p(d)(2p(d)+1), \end{aligned} \tag{64}$$

as in (d).

Similarly, $y_{1k} > 0 \Leftrightarrow (x+z)/y < 2d$, and z_{1k} is always positive.

Moreover,

$$\begin{aligned} z - x > z_{1k} - x_{1k} &\Leftrightarrow p(d)(2p(d)-1) < \frac{(x+z)}{y} \\ &< p(d)(2p(d)+1). \end{aligned} \tag{65}$$

We conclude that (x_{1k}, y_{1k}, z_{1k}) has positive components such that $z - x > z_{1k} - x_{1k}$ if and only if $p(d)(2p(d)-1) < (x+z)/y \le 2d$.

In this case, $n(z - z_{1k}) = 4a^2d((x+z)/y - d) > 0$ since $x_{1k} > 0$ and thus,

$$\frac{(x+z)}{y} > 2d - p(d) = d + p(d)(p(d)-1) \ge d. \tag{66}$$

Finally, if $(x+z)/y = 2d$, then $n(z_{1k} - x_{1k}) = 2a^2[(x+z)/y - 2d]^2 = 0$.

$(f)\ (j=3)$

As in (e),

$$x_{3k} > 0 <\Rightarrow p(d)(2p(d)-1) < \frac{(x+z)}{y} < p(d)(2p(d)+1). \tag{67}$$

As in (d),

$$y_{3k} > 0 \Leftrightarrow \frac{(x+z)}{y} > 2d \tag{68}$$

and z_{3k} is always positive.

Next, as in (e), $z - x > z_{3k} - x_{3k} \Leftrightarrow p(d)(2p(d)-1) < (x+z)/y < p(d)(2p(d)+1)$.

We have that (x_{3k}, y_{3k}, z_{3k}) has positive components that satisfy

$z - x > z_{3k} - x_{3k}$ if and only if $2d < (x+z)/y < p(d)(2p(d)+1)$.

In this case, $n^2(z - z_{3k}) = 4a^2d((x+z)/y - d) > 0$ since $(x+z)/y > 2d > d$.

$(g)\ (j=2)$

As in (d),

$$x_{2k} > 0 \Leftrightarrow \left(\frac{(x+z)}{y} - 2d\right)^2 - d > 0$$
$$< \Rightarrow \text{Either } \frac{(x+z)}{y} < p(d)(2\rho(d)-1) \text{ or } \frac{(x+z)}{y} > \rho(d)(2\rho(d)+1). \tag{69}$$

As in (f),

$$y_{2k} > 0 \Leftrightarrow \frac{(x+z)}{y} > 2d, \tag{70}$$

and z_{2k} is always positive.

Ergo, (x_{2k}, y_{2k}, z_{2k}) has positive components if and only if $(x+z)/y > p(d)(2p(d)+1)$. Next,

$$n(z-x) = 2a^2 d = n\left(z_{2k} - x_{2k}\right) \text{ and } z - x = z_{2k} - x_{2k}. \tag{71}$$

In this case, $z > z_{2k}$:

$$n\left(z - z_{2k}\right) = 4a^2 d\left(\frac{(x+z)}{y} - d\right) > 0 \text{ since } y_{2k} \tag{72}$$
$$> 0 \text{ so } \frac{(x+z)}{y} > 2d > d.$$

□

Remark 15. Let (x, y, z) be $A(m, n, b, a)$ or $A(m, n, b, a)/2$ as in Proposition 6. In view of $(a) - (c)$ of Definition 1, we proved by Lemma 13 that $\text{Inv}[g]$. $(x, y, z) = i'(x', y', z')$ for some g in $M(d)^*$ or $M(\text{d})^{**}$, positive integer i', and primitive solution (x', y', z') such that one of the following holds:

(a') $\text{z} - \text{x} > i'(z' - x')$

(b') $\text{z} - \text{x} = i'(z' - x')$ and $z > i'z'$

(c') $\text{z} - \text{x} = i'(z' - x')$ and $z < i'z'$.

However, if $i' > 1$, then $(a') - (c')$ all reduce to (a), and if $i' = 1$, then $(a') - (c')$ imply $(a) - (c)$, respectively. In both cases, (x, y, z) satisfies Definition 1.

Lemma 13 provides an algorithm for determining matrices $e(j)$. $S(k, d)$ for the descent of any primitive solution (x, y, z) of (1). Rephrasing parts $(a) - (c)$ of Lemma 13, we have the following simplifications:

Corollary 16. *Suppose first that integer k satisfies $1 \le k < \mu(d)$ so that (31) holds and $p(d) < (x+z)/y \le d$.*

(a) $(j = 1 \text{ and } \text{d} \ge 6)$

For any positive square-free integer d, let $k \equiv (\text{Ceiling}[(x+z)/y] + 1)/2$.

Moreover, if d is odd, then a second possible choice for k is $((x+z)/y + 2)/2$. If either choice of k is an integer such that $q \le k \le q + r + 1$, then we have the descent matrix $e(1)$. $S(k, d)$. Note that in this case, if $(x+z)/y = 2k - 1$, then $z_{1k} - x_{1k} = 0$ (and STOP).

If both choices of k fail, then we proceed to (b).

(b) $(j = 3 \text{ and } d \ge 6)$

Either (i) or (ii):

(i) For any positive square-free integer d, let $k \equiv \text{Ceiling}[(x+z)/y]/2$.
If k is an integer such that $q \le k \le q + r$, then we have $e(3)$. $S(k, d)$.
Moreover, if $k = q - 1$ and $p(d) < 2q - 1\text{-}v(d)$, then $e(3)$. $S(q-1, d)$ is also a descent matrix.
If (i) fails, then we go to (ii).
Note that if $d \ge 10$ is even and (i) succeeds where $(x+z)/y = 2k < d/2$, then there exists a positive integer multiple of (x, y, z) that is a binary root.

(ii) Let $k \equiv \text{Ceiling}[((p(d)+1)/p(d)) \times ((x+z)/y) + 1 - p(d)]/2$. Then, $(x+z)/y < p(d)[(2k + p(d) - 1)/(p(d)+1)]$.
Therefore, if $2k - 1 < (x+z)/y$ and $k > q + r$, then we have $e(3)$. $S(k, d)$.
Otherwise, (ii) fails so proceed to (c).

(c) $(j = 2)$

Either

(i) $k = 1$ when $2 \le d \le 5$ and $p(d) < (x+z)/y < d$.
or

(ii) Let $k \equiv$ Floor $[((p(d)+1)/p(d)) \times ((x+z)/y) + 1 - p(d)]/2$. Then, $p(d)[(2k + p(d) - 1)/(p(d) + 1)] < ((x+z)/y) \le d$.
Thus, if $k > q + r$, then we have the descent matrix $e(2)$. $S(k, d)$.
In this case, if $(x+z)/y = d$, then $z_{1k} - x_{1k} = 0$ (and STOP)
Note that the case $d = 1$ is a consequence of parts (e), (f), and (g) below.
Let's suppose finally that $k = \mu(d)$ and $(x+z)/y > d$.

(d) $(j = 0)$

$$d < \frac{(x+z)}{y} < p(d)(2\rho(d) - 1). \tag{73}$$

In this case, $z - x = z_{0k} - x_{0k}$ and $z > z_{0k}$.

(e) $(j = 1)$

$$p(d)(2p(d) - 1) < \frac{(x+z)}{y} < 2d. \tag{74}$$

In this case, $z - x > z_{1k} - x_{1k}$ and $z > z_{1k}$.

Moreover, if $(x+z)/y = 2d$, then $z_{1k} - x_{1k} = 0$.

(f) $(j = 3)$

$$2d < \frac{(x+z)}{y} < \rho(d)(2p(d)+1). \tag{75}$$

In this case, $z - x > z_{3k} - x_{3k}$ *and* $z > z_{3k}$.

$(g)(j=2)$

$$\frac{(x+z)}{y} > p(d)(2p(d)+1). \tag{76}$$

In this case, $z - x = z_{2k} - x_{2k}$ *and* $z > z_{2k}$.

Example 2. Let $d = 3 \times 5 \times 7 \times 11 \times 13 \times 17$ and $(x, y, z) = A(385, 663, 34, 19) = (627443,1292,905413)$ Then, $q = 254$, $r = 127016$, and $p(d) < 2q - 1\text{-}v(d)$. By Theorem 1, $G(d)^{**}$ is a generating set for all primitive solutions, and by Corollary 16, we have the following descent:

Since $(x+z)/y \le d$, we start with (a) $k = 594$ that checks out, but $(x+z)/y \neq 2k-1$. Our first descent matrix is

$$\begin{aligned} e(1).\, S(q+340, d).\, (x, y, z) &= (17573773279, 80091, 17573819864) \\ &= \frac{A(385, 663, 7281, 11)}{2} \\ &= \left(x', y', z'\right). \text{ Note that } z - x \\ &= 277970 > z' - x' = 46585. \end{aligned} \tag{77}$$

Replacing (x, y, z) with (x', y', z'), we return to (a) where now $(x+z)/y > d$. Thus, with $k = (d+1)/2 = q + r + 358$, we check $(d) - (g)$ and find that (d) holds. Our next descent is

$$\begin{aligned} e(0).\, S(q+r+358, d).\, (x, y, z) &= (468625219, 13079, 468671804) \\ &= \frac{A(385,663,1189,11)}{2} \\ &= \left(x', y', z'\right). \text{ Then } z - x \\ &= 46585 = z' - x'. \end{aligned} \tag{78}$$

Replacing (x, y, z) with (x', y', z'), since $(x+z)/y < d$, we are back to

(a) $k = 35833 = q + 35579$ that checks out, but $(x+z)/y \neq 2k-1$. Our next descent matrix is

$$\begin{aligned} e(1).\, S(q+35579, d).\, (x, y, z) &= (1537\,841567, 12184, 1537853\,887) \\ &= A(385,663,1523,4) = \left(x', y', z'\right). \text{ Note that } z - x = 46585 > z' - x' = 12320. \end{aligned} \tag{79}$$

Replacing (x, y, z) with (x', y', z'), since $(x+z)/y < d$, we return to

(a) Both possibilities for k fail, so we go to
(b) (i) Here, $k = 126219 = q + 125965$ so the next descent matrix is $e(3).\, S(q+125965, d).\, (x, y, z) = (95611, 17, 95996) = A(385, 663, 17, 1)/\, 2 = (x', y', z')$, and z-x = 12320 > $z' - x' = 385$.
Replacing (x, y, z) with (x', y', z'), since (x + z)/y < d, we are back to

(a) k = 5636 = q + 5382 checks out, and (x + z)/y = 2k − 1 so we are done with $z_{1k} - x_{1k} = 0$. Our final descent matrix is

$$e(1).S(q+5382, d).\, (x, y, z) = (22446528, 0, 22446528). \tag{80}$$

Summary of Corollary 16 is as follows:

$$\begin{aligned} &(e(1).S(q+5382, \mathrm{d})).\, (e(3).\, S(q+125965, d)).\, (e(1).S(q+35579, d)). \\ &(e(0).S(q+\mathrm{r}+358, \mathrm{d})).\, (e(1).S(q+340, d)).A(385, 663, 34, 19) = 22446528\,(1, 0, 1). \end{aligned} \tag{81}$$

By Lemma 10, according to Definition 2 of a generating set, we have the following ascent:

$$((S(q+340,d).e(1)).\ (S(q+r+358,d).e(0)).\ (S(q+35579,d).e(1)).\ (S(q+125965,d).e(3)).((S(q+5382,d).e(1))).$$
$$(1,0,1) = 2^2 \times 5^2 \times 11^2 \times 19^2 \times 1409^2 \times 1669^2 \times 3343^2 \times (3 \times 13 \times 17)A(385,663,34,19). \tag{82}$$

Example 3. Let $d = 7 \times 11 \times 19 \times 31 \times 47$ and $(x, y, z) = A(7 \times 19 \times 47, 11 \times 31, 197, 16) =$ (11633613, 6304, 14834125). Then, $q = 731$, $r = 1064031$ and $p(d) > 2q - 1\text{-}v(d)$.

By Theorem 4, $G(d)^{**}$ is a generating set for all primitive solutions, and by Corollary 16, we have the following descent:

Summary is as follows:

$$(e(1).\ S(q+515373,d)).\ (e(1).\ S(q+548962,d)).\ (e(2).\ S(q+r+1034,d)).$$
$$(e(3).\ S(q+298984,d)).\ (e(2).\ S(q+r+1034,d)).\ (e(1).\ S(2100,d)).\ (x,y,z) = 886103504(1,0,1). \tag{83}$$

By Lemma 10 and the definition of a generating set, we have the following ascent:

$$((S(2100,d).\ e(1)).\ (S(q+r+1034,d).\ e(2)).\ (S(q+298984,d).\ e(3)).$$
$$(S(q+r+1034,d).\ e(2)).\ (S(q+548962,d).\ e(1)).\ (S(q+515373,d).\ e(1)).\ (1,0,1) \tag{84}$$
$$= 2^8 \times 7^2 \times 17^2 \times 19^2 \times 283^2 \times 2707^2 \times 3499^2 \times 4337^2 \times (11 \times 31)(x,y,z).$$

Example 4. Let $d = 2 \times 3 \times 5 \times 11 \times 17 \times 19$ and $(x, y, z) = A(190, 561, 1329, 7) = (990851891, 18606, 990870511)$. Then, $q = 164$, $r = 52967$, and $p(d) < 2(q-1)$.

By Theorem 4, $G(d)^{**}$ is a generating set for all primitive solutions; and by Corollary 16, for even d, we have the following descent to primitive binary root $(x', y', z') = A(187, 570, 2, 1)$.

Summary is as follows:

$$(e(2).\ S(q+r+124,d)).\ (x,y,z) = 3\left(x', y', z'\right). \tag{85}$$

By Lemma 10 and the definition of a generating set, we have the expansion

$$\left((S(q+r+124,d).\ e(2)).\left(x', y', z'\right) = 3^7(x,y,z).\right. \tag{86}$$

Example 5. Let $d = 2 \times 13 \times 23 \times 29 \times 37$ and $(x, y, z) = A(2 \times 37, 13 \times 23 \times 29, 31, 17) =$(8311445, 1054, 8354217). Then $q = 402$, $r = 320024$ and $p(d) < 2q - 1\text{-}v(d)$.

By Theorem 4, $G(d)^{**}$ is a generating set for all primitive solutions, and by Corollary 16, we have the following descent to $(1,0,1)$ for even d.

Summary is as follows:

$$(e(1).\ S(q+133999,d)).\ (e(0).\ S(q+r+402,d)).\ (e(1).\ S(q+66799,d)).\ (e(3).\ S(q+275625,d)).$$
$$(e(1).\ S(q+261277,d)).\ (e(0).\ S(q+r+402,d)).\ (e(3).\ S(q+7504,d)).\ (x,y,z) = 16032679(1,0,1). \tag{87}$$

By Lemma 10, according to the definition of a generating set, we have the expansion

$$((S(q+7504,d).\ e(3)).\ (S(q+r+402,d).\ e(0)).\ (S(q+261277,d).\ e(1)).\ (S(q+275625,d).$$
$$e(3)).\ (S(q+66799,d).\ e(1)).\ (S(q+r+402,d).\ e(0)).\ (S(q+133999,d).\ e(1)).\ (1,0,1) \tag{88}$$
$$= 3^2 \times 31^2 \times 107^2 \times 5849^2 \times 16363^2 \times 29867^2 \times 118297^2 \times (13 \times 23 \times 29)(x,y,z).$$

5. Proof of Theorem 4

We first show by Lemma 13 that any primitive solution (x, y, z) of (1) satisfies the Fermat's method of descent with respect to $M(d)^*$ (when 2q-1-ν $(d) < p(d)$) and with respect to $M(d)^{**}$ (when $p(d) < 2q - 1\text{-}\nu(d)$). The interval $(ap(d), \infty)$ will now be expressed as a union of subintervals with the property that if bn is in the kth subinterval, then there is an element g_{jk} of $M(d)^*$ or $M(\mathrm{d})^{**}$ such that Inv$[g_{jk}]$. (x, y, z) is a positive integer multiple of a primitive solution (x', y', z') as in Definition 1. Since $(x + z)/y = (bn)/a$, the subintervals follow directly from those derived in Lemma 13.

Let $d = 1$. Since

$$(ap(d), \infty) = [ap(d), 2ad] \cup [2ad, 3ad] \cup (3ad, \infty), \tag{89}$$

the following descent matrices of Lemma 13 satisfy Definition 1

(e) $e(1).S(\mu(d), d)$ when bn is in $(\mathrm{a}\, p(d), 2ad]$

(f) $e(3).S(\mu(d), d)$ when bn is in $(2ad, 3ad]$

(g) $e(2).S(\mu(d), d)$ when bn is in $(3ad, \infty)$.

Let $d = 2, 3$ or 5. Since

$$(ap(d), \infty) = (ap(d), ad] \cup (ad, ap(d)(2p(d) - 1)] \cup . \tag{90}$$

$(ap(d)(2p(d) - 1),\ 2ad] \cup [(2ad, ap(d)(2p(d) + 1)] \cup (ap(d)(2p(d) + 1), \infty)$, the following descent matrices of Lemma 13 satisfy Definition 1:

(c) (i) $e(2).S(1, d)$ when bn is in $(\mathrm{a}p(d), \mathrm{a}d]$

(d) $e(0).\ S(\mu(d), d)$ when bn is in $(\mathrm{a}d, \mathrm{a}\rho(d)(2p(d) - 1)]$

(e) $e(1).\ S(\mu(d), d)$ when bn is in $(ap(d)(2p(d) - 1), 2ad]$

(f) $e(3).\ S(\mu(d), d)$ when bn is in $(2ad,\ ap(d)(2p(d) + 1)]$

(g) $e(2).\ S(\mu(d), d)$ when bn is in $(ap(d)(2\rho(d) + 1), \infty)$.

Let $d \geq 6$ and define for $s = 0, 1, \ldots, r$: Int $(q + s) \equiv (a(2(q + s) - 1), a(2(q + s) - 1 + \nu(d))]$ and Int $(\mathrm{q} + \mathrm{s})^* \equiv (a(2(q + s) - 1 + \nu(d)), a(2(q + s + 1) - 1)]$.

Then,

$$\begin{aligned}(a\,p(d), \infty) = {} & (a\,p(d), a(2q - 1)] \cup_{0 \leq s \leq r} (\mathrm{Int}(q + s) \cup \mathrm{Int}(q + s)^*) \cup \\ & (a(2(q + r + 1) - 1), a\,p(d)\frac{[2(q + r + 1) + p(d) - 1]}{(p(d) + 1)} \cup \\ & \left(a\,p(d)\frac{[2(q + r + 1) + p(d) - 1]}{(p(d) + 1)}, a\,d\right] \cup \\ & (ad, a\,p(d)(2p(d) - 1)] \cup (a\,p(d)(2p(d) - 1), 2\mathrm{ad}] \cup \\ & (2ad, a\,p(d)(2p(d) + 1)] \cup (a\,p(d)(2p(d) + 1), \infty),\end{aligned} \tag{91}$$

where the following descent matrices of Lemma 13 satisfy Definition 1:

(a) $e(1).\ S(q, d)$ when $2\mathrm{q} - 1 - \nu(d) < p(d)$ and bn is in $(\mathrm{a}p(d), a\ (2\mathrm{q} - 1)]$

In this case, q- floor $[(p(d) + 3)/2] > (p(d) + 1)/2$, so (a) applies to $e(1).S(q, d)$ over the interval $a\ (2\ q\text{-}1\text{-}\nu(d)) < ap(d) < bn \leq a\ (2q\text{-}1)$.

(b) (i) $e(3).S(q - 1, d)$ when $p(d) < 2q - 1\text{-}\nu(d)$ and bn is in $(ap(d),\ a(2q - 1 - \nu(d))]$

Since $q < (p(d) + 3)/2$, we apply (b)(i) to $e(3).\ S(q - 1, d)$ over the larger interval $a\ (2q\text{-}3) < ap\ (d) < bn < a(2q - 1 - \nu(d)) \leq a\ (2\ q\text{-}\ 3 + \nu(d))$.

(a) $e(1).S(q, d)$ when $p(d) < 2q - 1\text{-}\nu(d)$ and bn is in $(a\ (2q - 1 - \nu\ (d)),\ a\ (2q - 1)]$

For $s = 0, 1, \ldots, r$ is in the next two lines:

(b) (i) $e(3).\ S(q + s, d)$ when bn is in lnt (q + s).

(a) $e(1).\ S(q + s + 1, d)$ when bn is in the interval $(a\ (2\,(q + s + 1) - 1\text{-}\ \nu(d)), a\,(2\,(q + s + 1) - 1)]$ that also contains $\mathrm{lnt}(q\ +\ s)^*$ (with equality holding when d is even).

(b) (ii) $e(3).\ S(q + r + 1, d)$ when bn is in $(a\,(2\,(q + r + 1) - 1),\ ap(d)[2\,(q + r + 1) + \rho(d) - 1]/(p(d) + 1)]$

(c) (ii) $e(2).\ S(q + r + 1, d))$ when bn is in $(ap(d)[2\,(q + r + 1) + p(d) - 1]/(\rho(d) + 1)],\ ad]$

(d) $e(0).\ S(\mu(d), d)$ when bn is in $(a\,d, a\,p(d)\ (2p(d) - 1)]$

(e) $e(1).\ S(\mu(d), d)$ when bn is in $(a\ p(d)(2p(d) - 1),\ 2ad]$

(f) $e(3).\ S(\mu(d), d)$ when bn is in $(2ad,\ a\ p(d)(2p(d) + 1)]$

(g) $e(2).\ S(\mu(d), d)$ when bn is in $(a\ p(d)(2p(d) + 1),\ \infty)$.

By Proposition 6 and the interval decomposition of $(ap(d), \infty)$ with corresponding descent matrices, arbitrary primitive solutions (x, y, z) of (1) satisfy Fermat's method of descent with respect to $M(d)^*$ or $M(d)^{**}$. Finally, we show that Theorem 4 is a consequence of this result and Theorem 12.

Let d be any positive square-free integer and let (x_1, y_1, z_1) be a primitive solution of (1). By the argument mentioned above, there is g in $M(d)^*$ or $M(d)^{**}$ such that lnv$[g]$. $(x_1, y_1, z_1) = i_2(x_2, y_2, z_2)$ satisfies Definition 1. By Lemma 13, if d is 2 or 6, then only parts (a) and (b) of Definition 1 are used in the descent. Moreover, by $b(i)$ of Lemma 13 and Theorem 12, the only situation where part (c) of Definition 1 occurs is when $d \geq 10$ is even and (x_1, y_1, z_1) is a binary root or a copartner of a binary root. In this case, (x_1, y_1, z_1) and (x_2, y_2, z_2) intertwine indefinitely so the descent is to a binary root. We assume henceforth that part (c) of Definition 1 does not occur.

Replacing (x_1, y_1, z_1) with (x_2, y_2, z_2) and continuing by induction, we construct a sequence $(x_{\mathfrak{n}}, y_n, z_{\mathfrak{n}})$ of primitive solutions of (1). In view of our assumption on part (c) of Definition 1, we wish to show that there exists $N > 0$ such that $z_N - x_N = 0$ (i.e., $y_N = 0$). Suppose by way of contradiction, that $y_n > 0$ for all n. We first show that $z_1 - x_1 > z_k - x_k$ for some k.

Since Lemma 13 holds for any positive square-free integer d, we may assume without loss of generality that $(x_1, y_1, z_1) = A(m_1, \mathrm{n}_1, \mathrm{b}_1, \mathrm{a}_1)$ and consider two cases on $b_1 \times n_1$:

Case 16. Suppose that $b_1 \times n_1$ is not in

$$(a_1 d, a_1 p(d)(2p(d) - 1] \cup (a_1 p(d)(2p(d) + 1), \infty), \tag{92}$$

(i.e., (d) and (g) of Lemma 13). Then, by Lemma 13, there exists an element g of $M(\mathrm{d})^*$ or $M(\mathrm{d})^{**}$ and a primitive solution (x_2, y_2, z_2) such that $\mathrm{Inv}[g]$. $(x_1, y_1, z_1) = i_2(x_2, y_2, z_2)$ for some positive integer i_2; and moreover, $z_1 - x_1 > z_2 - x_2$ (so that $k = 2$).

Case 18. Let's assume on the other hand that $b_1 \times n_1$ is in (92). By Lemma 13, there exists g in $M(d)^*$ or $M(d)^{**}$ such that $\mathrm{Inv}[g]$. $(x_1, y_1, z_1) = i_2(x_2, y_2, z_2)$ satisfies Definition 1 with $z_1 - x_1 = z_2 - x_2$ and $z_1 > z_2$ (since $y_2 \neq 0$). By Remark 7, the parametric representation of (x_2, y_2, z_2) is of the same type as that of (x_1, y_1, z_1). Furthermore, by Remark 8, if $(x_2, y_2, z_2) = A(m_2, n_2, b_2, a_2)$, then $\mathrm{m}_2 = \mathrm{m}_1$, $n_2 = n_1$, $a_2 = a_1$ and therefore,

$$z_1 = n_1 b_1^2 + m_1 a_1^2 > z_2 = n_2 b_2^2 + m_2 a_2^2 = n_1 b_2^2 + m_1 a_1^2. \tag{93}$$

It follows that

$$(x_2, y_2, z_2) = A[m_2 (= m_1), n_2 (= n_1), b_2 (< b_1), a_2 (= a_1)]. \tag{94}$$

If $b_2 \times n_2$ is also in (92), then for $i = 1$ and 2, we replace (x_i, y_i, z_i) with $(\mathrm{x}_{\mathrm{i}+1}, \mathrm{y}_{\mathrm{i}+1}, \mathrm{z}_{\mathrm{i}+1})$ as mentioned above.

In this case, $z_1 - x_1 = z_2 - x_2 = z_3 - x_3$. $z_1 > z_2 > z_3$ and

$$(x_3, y_3, z_3) = A[m_3 (= m_2 = m_1), n_3 (= n_2 = n_1), b_3 (< b_2 < b_1), a_3 (= a_2 = a_1)]. \tag{95}$$

Continuing in this way, since the $b_i \times n_i$ are positive integers, there exists p such that $b_j \times n_j$ is in (92) for $j = 1, \ldots,$ p-2, but $b_{p-1} \times n_{p-1}$ is not in (92), and by Case 16, $z_1 - x_1 = z_{p-1} - x_{p-1} > z_p - x_p$. It follows that $k = p$ and the conjecture on $z_1 - x_1$ in general is established.

Repeating the previous argument with (x_k, y_k, z_k) in place of (x_1, y_1, z_1), we have that $z_1 - x_1 > z_k - x_k > z_m - x_m$ for some $m > k$. Continuing in this manner, we construct a strictly decreasing sequence of positive integers which is impossible; so $y_N = 0$ for some N.

We deduce that either (x_t, y_t, z_t) is a binary root (or a copartner of a binary root) for some t or the sequence (x_n, y_n, z_n) descends to $(1,0,1)$.

Conclusion to the proof of Theorem 4 is given as follows: 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 mentioned above to determine integers k_i in $[1, \mu(d)]$, j_i in $[0, 3]$ and positive integer n such that $S(k_i, d).e(j_i)\,(1 \leq i \leq n)$ is in G for the descent

$$(e(j_1).S(k_1, d))\ldots(e(j_{\mathrm{n}}).S(k_n, d)).(x, y, z) = \mathbf{Kr}, \tag{96}$$

where $\mathbf{r}$ is either $(1, 0, 1)$ or a primitive binary root, and $\mathbf{K} = \gcd[(e(j_1).S(k_1, d))\ldots(e(j_n).S(k_n, d)).(x, y, z)]$. Taking inverses by Lemma 10, we then have

$$(S(k_n, d).e(j_n))\ldots(S(k_1, d).e(j_1)).\mathbf{r} = \mathbf{P} \times \frac{(x, y, z)}{\mathbf{K}}, \tag{97}$$

where $\mathbf{P}$ is the square of the product of the terms (d-2 k_i + 1)/$\delta(d)$ over all k_i defined above that are strictly less than $\mu(d)$. 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 left side is an integer triplet, the coefficient of (x, y, z) must be a positive integer and hence G is a generating set.

6. 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 4, 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 $\mathrm{lnv}[g]$. (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 notation of Definition 1, assume that (x', y', z') is a primitive solution of (1), $g(x', y', z') = (x, y, z)$ and, as in the proof of Theorem 4, e(j). $S(k, d)$. $(x, y, z) = \mathrm{i}'(\mathrm{x}', \mathrm{y}', \mathrm{z}')$ satisfies the 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.

Example 6. Let $d = 10$. Then, $q = 3$ and $r = 0$ so by Theorem 12, $w = (\mathrm{x}', \mathrm{y}', \mathrm{z}') = A(5, 2, 2, 1) = (3, 4, 13)$ is a primitive

binary root. Moreover, since $2(q-1) > p(d)$, by Theorem 4, $G(10)^*$ is a generating set for the primitive solution to (1) and the first level of its corresponding tree of solutions (x, y, z) is

$$\begin{aligned}(S(q-1,d).e(1)).\mathrm{w} &= (-43,6,47),\ (S(q,d).e(1)).w = 5(1,6,19),\ (S(q,d).e(3)).w = 25(13,6,23),\ (S(q+1,d).e(1)).w \\ &= 9(13,6,23),\ (S(q+1,d).\,e(3)).\,w = (597,190,847),\ (S(q+1,d).\,e(2)).w \\ &= (507,154,703),\ (S(\mu(d),d).\,e(0)).w = (123,16,133),\ (S(\mu(d),d).e(1)).w \\ &= (237,28,253),\ (S(\mu(d),d).\,e(3)).\,w = (397,36,413),\ (S(\mu(d),d).e(2)).\,w = (283,24,293).\end{aligned} \tag{98}$$

The first node satisfies $(a1)$ and must be pruned. The second, third, and fourth nodes satisfy $(a2)$ so their common divisors 5, 25, and 9 must be dropped. Consequently, there are two paths to (13, 6, 23) which we show in (a4)(ii) below always corresponds to $j = 1$ and $j = 3$ when they exist. Thus, by convention, we keep the node with $j = 1$ and eliminate the other one.

The next situation does not occur with the predetermined generators of parametric interval descent but may arise when taking all possible products in the ascending development of a tree. In $(a3)$, we must again prune (x, y, z). In practice, one simply checks each new node for the adverse conditions.

$(a3)$ For some odd square-free d, there may exist g in G such that the binary root conditions $\mathrm{z}' - \mathrm{x}' = \mathrm{z} - \mathrm{x}$ and $\mathrm{z}' > \mathrm{z}$ in part (c) of Definition 1 hold:

Example 7. Let $d \geq 7$ be odd, $(x', y', z') = A(d, 1, 1 + 2(d-q), 1)/2$, and $g = S(\mu(d), d).\ e(0)$. Then $(x, y, z) = g.\ (x', y', z') = A(d, 1, 2q-1, 1)/2$, $z' - x' = d = z - x$ and $2z' = [2d - (2q-1)]^2 + d > 2z = (2q-1)^2 + d$ since by the definition of q, z'-z = 2d [d- (2q-1] >0.

$(a4)$ There are duplicate nodes in the first level of the derived tree that must be pruned. They arise from the subsets

$$\{S(q+\mathrm{s},d).\,e(3).w, S(q+s+1,d).\,e(1).w\}\,(0 \leq s \leq r) \tag{99}$$

for some primitive root w defined as follows:

(i) For odd square-free $d \geq 13$, the nearest nodes in the abutting sets agree when $w = (1, 0, 1)$:

$$S(q+s+1,d).\,e(1).w = S(q+s+1,\mathrm{d}).\,e(3).\,w\ (0 \leq s < r), \tag{100}$$

since $e(1).\mathrm{w} = e(3).w$.

(ii) For even square-free $d \geq 10$ and standard binary root $\mathrm{w} = A(d/2, 2, k, 1)$ as defined in Theorem 12, there exists a unique s in $[0, r]$ such that

$$\frac{S(q+\mathrm{s},d).e(3).w}{\gcd\,[S(q+s,d).e(3).w]} \text{ coincides with } \frac{S(q+s+1,d).e(1).w}{\gcd\,[S(q+s+1,d).e(1).w]}. \tag{101}$$

Proof. Since $q + s = d/2 - k$ in Theorem 12, uniqueness of s will follow from the definition of w. For the proof of (ii), we will need an analog of the statement

$$\left(e(3).\,S\left(\frac{d}{2}-k,d\right)\right).A\left(\frac{d}{2},2,\frac{d}{2}-k,1\right) = A\left(\frac{d}{2},2,k,1\right), \tag{102}$$

given in Theorem 12. Taking inverses by Lemma 10, it follows that

$$\mathrm{A}\left(\frac{d}{2},2,\frac{d}{2}-k,1\right) = (2k+1)^{-2}\mathrm{S}\left(\frac{d}{2}-k,d\right).\,e(3).A\left(\frac{d}{2},2,k,1\right). \tag{103}$$

By an argument similar to the proof of the statement given above from Theorem 12,

$$\left(e(1).\,S\left(\frac{d}{2}-k+1,d\right)\right).A\left(\frac{d}{2},2,\frac{d}{2}-k,1\right) = A\left(\frac{d}{2},2,k,1\right). \tag{104}$$

Moreover, by Lemma 10 again,

$$A\left(\frac{d}{2},2,\frac{d}{2}-k,1\right) = (2k-1)^{-2}S\left(\frac{d}{2}-k+1,d\right).\ e(1).A\left(\frac{d}{2},2,k,1\right). \tag{105}$$

Finally, by (103) and (105), we have the integer equations

$$(2k+1)^{-2}S\left(\frac{d}{2}-k,d\right).e(3).A\left(\frac{d}{2},2,k,1\right)$$
$$=(2k-1)^{-2}S\left(\frac{d}{2}-k+1,d\right).e(1).A\left(\frac{d}{2},2,k,1\right)$$
$$=A\left(\frac{d}{2},2,\frac{d}{2}-k,1\right). \tag{106}$$

Dividing both sides by their gcds, (ii) follows.

When d is odd, duplicate nodes may also be a consequence of distinct paths from $(1,0,1)$ to a common node, that are initiated by the generators given above:

(iii) The interval decomposition in the proof of Theorem 4 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 $(x,y,z)=A(m,n,b,a)$ is a primitive solution to (1) such that bn is in the intersection $(a(2(q+s)+1)+1\text{-}v(d),\ a(2(q+s)-1+v(d))]$, of these intervals, then there exist two distinct paths from $(1,0,1)$ to (x,y,z). □

Example 8. Example 6 provides a one-step illustration of $(a4)$(ii).

For $(a4)$(iii), let $d=11$ and $s=-1$. Then, $q=3$ and $p(d)<2q-1\text{-}v(d)$. If $a=10$, $b=39$ and $n=1$, the previous intersection is approximately $(35.858,44.142)$ and we obtain the following distinct paths from $(1,0,1)$ to $(x,y,z)=A(11,1,39,10)$:

$$\begin{aligned}
&16^2\times 9^7(x,y,z)=(S(3,11).e(1)).(S(3,11).e(2)).(S(2,11).e(3)).(S(6,11).e(0)).(S(3,11).e(2)).\\
&\quad(S(3,11).e(2)).(S(6,11).e(0)).(S(3,11).e(2)).(S(2,11).e(3)).(S(3,11).e(2)).(S(3,11).e(3)).\\
&\quad(S(3,11).e(2)).(1,0,1)\\
&16\times 9^4(x,y,z)=(S(2,11).e(3)).(S(3,11).e(2)).(S(3,11).e(2)).(S(6,11).e(2)).(S(6,11).e(2)).\\
&\quad(S(6,11).e(2)).(S(3,11).e(2)).\\
&(S(3,11).e(3)).(S(3,11).e(2)).(1,0,1).
\end{aligned} \tag{107}$$

We then select the first path with last ascent matrix having $j=1$ by convention and prune the branch including and emanating from (x,y,z) on the second path.

7. Conclusion

By the bxn-interval decomposition of $(ap(d),\infty)$ in the proof of Theorem 4, the only way that distinct paths may arise from $(1,0,1)$ to (x,y,z) is by $(a4)$. Moreover, the only nontrivial anomalies when d is even are $(a1)$, $(a2)$, and $(a4)$(ii). By the parametric interval 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 $G(d)^{**}$

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Supplementary Materials

A supplementary file contains a Mathematica program $SqFr[d,(x,y,z)]$ for any square-free positive integer d and primitive solution (x,y,z) of the Diophantine equation $x^2+dy^2=z^2$ that computes directly from Theorem 4: a decomposition of a positive multiple of (x,y,z) into a product of generators acting on either $(1,0,1)$ or a primitive binary root. As an alternative to the algorithm of Corollary 16, SqFr is executed with Examples 2–5 and the results are then checked with the definition of a generating set and compared with Corollary 16. Moreover, SqFr determines the decomposition of Example 8 (a4)(iii). (*Supplementary Materials*)

References

[1] T. Andreescu and D. Andrica, "Quadratic diophantine equations. With a foreword by preda mihailescu," *Developments in Mathematics*, vol. 40, 2015.

[2] T. Cochrane and P. Mitchell, "Small solutions of the Legendre equation," *Journal of Number Theory*, vol. 70, no. 1, pp. 62–66, 1998.

[3] A. Hari Ganesh, K. Prabhakaran, and G. Sivakumar, "Solutions of ternary quadratic Diophantine equations $x^2+y^2\pm\lambda y=z^2$," *Malaya Journal of Matematik*, vol. 8, no. 2, pp. 427–432, 2020.

[4] L. Holzer, "Minimal solutions of Diophantine equations," *Canadian Journal of Mathematics*, vol. 2, pp. 238–244, 1950.

[5] M. Legendre, "Théorème sur la possibilité des équations indeterminées du second degré," *Histoire De Academie Royale Des Sciences*, vol. 4, pp. 507–513, 1785.

[6] M. Murata, "Primitive solutions of nonscalar quadratic Diophantine equations," *Journal of Number Theory*, vol. 201, pp. 398–435, 2019.

[7] M. Murata and T. Yoshinaga, "On the solutions of quadratic Diophantine equations II," *Journal of The Mathematicle Socity of Japan*, vol. 70, no. 3, pp. 895–919, 2018.
[8] L. J. Mordell, "On the magnitude of the integer solutions of the equation a x^2 + b y^2 + c z^2 = 0," *Journal of Number Theory*, vol. 1, pp. 1–3, 1969.
[9] L. J. Mordell, *Diophantine Equations*, Academic Press, London, UK, 1969.
[10] R. C. Alperin, "The modular tree of Pythagoras," *The American Mathematical Monthly*, vol. 112, no. 9, pp. 807–816, 2005.
[11] B. Berggren, "Pytagoreiska trianglar (in Swedish), Elementa: tidskrift för elementär matematik," *Fysik Och Kemi*, vol. 17, pp. 129–139, 1934.
[12] A. Hall, "232. Genealogy of pt," *The Mathematical Gazette*, vol. 54, no. 390, pp. 377–379, 1970.
[13] A. R. Kanga, "The family tree of Pythagorean triples," *Bull. Inst. Math. Appl.*vol. 26, no. 1-2, pp. 15–17, 1990.
[14] R. A. Saunders and T. Randall, "78.12 the family tree of the Pythagorean triplets revisited," *The Mathematical Gazette*, vol. 78, no. 482, pp. 190–193, 1994.
[15] M. Burton, *Elementary Number Theory*, Wm. C. Brown Publishers, Dubuque, LA, USA, 3rd edition, 1994.
[16] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Wiley, New York, NY, USA, 3rd edition, 1972.
[17] M. H. Stark, *An Introduction to Number Theory*, Markham Publishing Co, Chicago, IL, USA, 1970.