4 The case for $k = 1$

We discuss the case by refering to the paper written by Zhang [9][10].

4.1 The tree structure of solutions

Lemma 4.1 *Every solution can be traced back to* $(3, 3, 3)$ *by repeatedly performing the following operation on solutions:*

$$(a, b, c) \longmapsto (a, b, c') := (a, b, ab - c), \tag{1}$$

where (a, b, c) *is arranged so that* $a \leq b \leq c$.

Proof. It is easy to see that c and c' are actually the roots of the quadratic equation $z^2 - abz + a^2 + b^2 = 0$ in z. It follows that $cc' = a^2 + b^2$. In particular, $c' > 0$. Thus, (a, b, c') is indeed a solution.

When the inward solution is nonsingular, the operation (1) can reduce the largest entry of the solution. Indeed, if $a < b < c$, then $(c-b)(c'-b) = cc'-(c+c')b+b^2 = a^2+2b^2-ab^2 < 0$; hence $c' < b$. Therefore, after finite number of steps of reduction, the process will stop at a singular solution which is in fact $(3, 3, 6)$. At last, $(3, 3, 6)$ can reduce to $(3, 3, 3)$. This completes the proof. □

Remark 4.2 *The following* (1) *and* (2) *are immediate results.*
(1) *By the Method of Infinite Descent, Lemma* 4.1 *implies that the equation has infinitely many positive integer solutions.*
(2) *By the proof of the Lemma* 4.1*, if* (a, b, c) *is an nonsingular solution, then we can obtain three other solutions* (a, b, c'), (a, b', c), (a', b, c), *where* $c' = ab - c$, $b' = ac - b$, $a' = bc - a$. *We say that the three solutions are the neighbors of the solution* (a, b, c). *See Figure* 1 *for the structure of a nonsingular solution and its neighbors. Thus, all the solutions can be arranged in a tree, as shown in Figure* 2.

4.2 Markoff Matrix

4.2.1 **Farey sum of rationals**. We need to introduce a method to generate all the fractions between 0 and 1. This is briefly sketched in the rest of this subsection.

The *standard reduced form* of a rational r is the unique fractional expression $r = a/b$, where a, b are coprime integers with $b \geq 1$. In particular, we call b the *Farey level* of r.

Two rationals r, s are said to be *Farey neighbors* if they have standard reduced forms $r = a/b$ and $s = c/d$ so that $ad - bc = \pm 1$.

The *Farey sequence* of level n is formed in the ascending order by arranging all rationals between 0 and 1 of Farey levels at most n. Any adjacent pair of rationals in a Farey sequence are Farey neighbors. It is a well known fact and can be found in any book on number theory.

A easy way to form the Farey sequence of level $n + 1$ from Farey sequence of level n is to make the Farey sums for appropriate Farey neighbors.

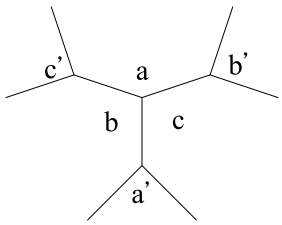

Figure 1: The structure of a nonsingular solution and its neighbors

Given two rationals r, s which are Farey neighbors and with standard reduced forms $r = a/b$ and $s = c/d$. Then their *Farey sum* is defined as

$$r \oplus s := \frac{a+c}{b+d}$$

which is automatically in standard reduced form. Note that $r \oplus s$ falls in between r and s and is a Farey neighbor of both r and s.

It follows from the Euclid algorithm that every rational between 0 and 1 can be split as the Farey sum of two rationals of smaller Farey levels. Thus, all rationals between 0 and 1 will appear in above process of making Farey sums.

We call (r, t, s) in $\mathbf{Q} \cap [0, 1]$ a Farey triple with $r < t < s$, where r, s are Farey neighbors and $t = r \oplus s$.

4.2.2 **Markoff matrices**. Following H.Cohn [3], we associate a matrix to each rational between 0 and 1. Initially, we set

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

and define

$$M_{\frac{0}{1}} = A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, M_{\frac{1}{1}} = AB = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$$

In general, for rationals $r, s \in [0, 1]$ which are Farey neighbors, where $r < s$, we set

$$M_{r \oplus s} = M_r M_s (\neq M_s M_r)$$

In this way, we have defined a Markoff matrix, $M_r \in SL(2, \mathbf{N})$, for every rational $r \in [0, 1]$. The following are a few examples.

$$M_{\frac{1}{3}} = \begin{pmatrix} 21 & 29 \\ 13 & 18 \end{pmatrix}, M_{\frac{1}{2}} = \begin{pmatrix} 8 & 11 \\ 5 & 7 \end{pmatrix}, M_{\frac{2}{3}} = \begin{pmatrix} 46 & 65 \\ 29 & 41 \end{pmatrix}$$

4.2.3**Characteristics of Markoff matrix**.

The following three lemmas tell us some characteristics of Markoff matrix.

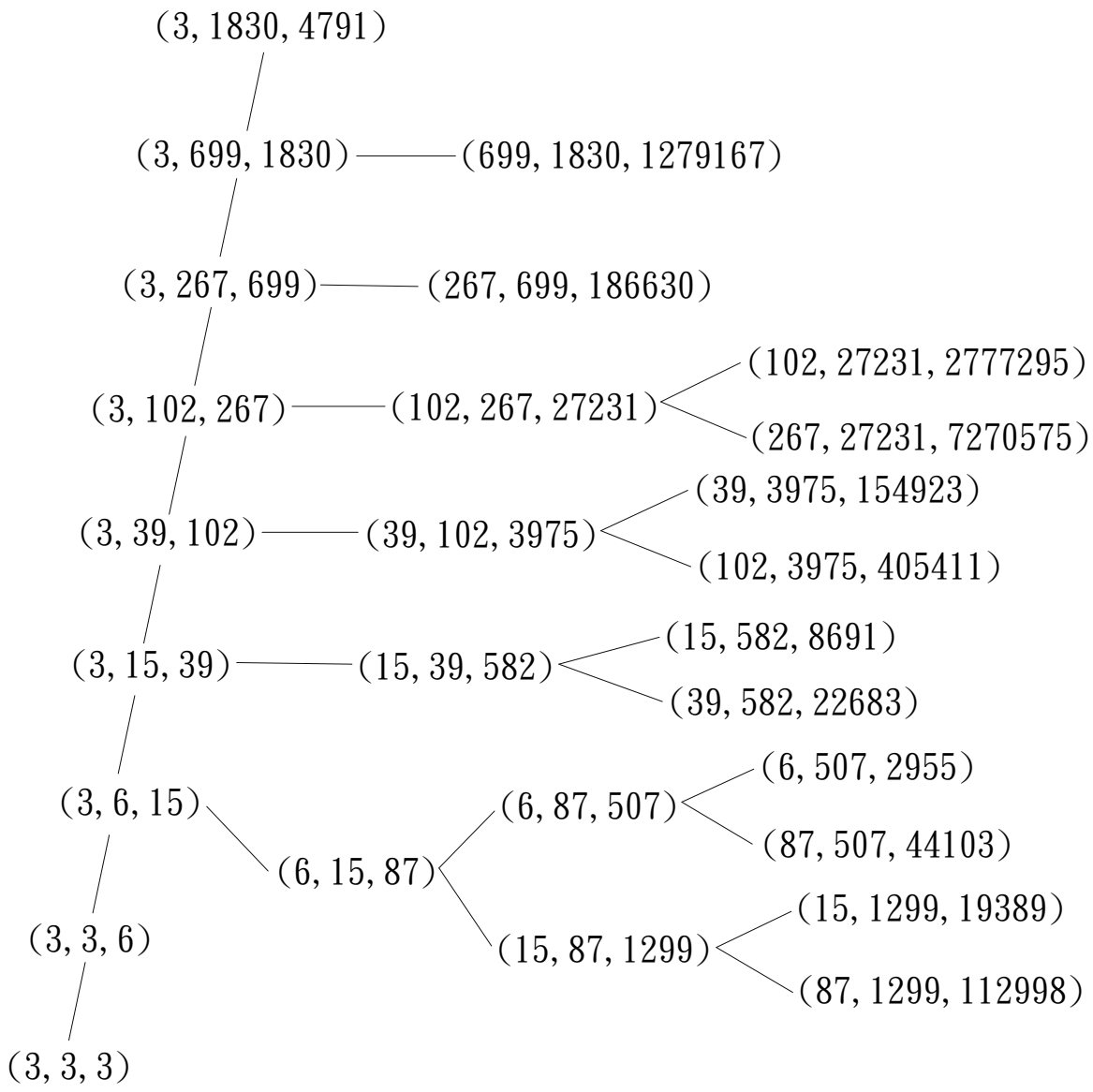

Figure 2: The solutions tree

Lemma 4.3 *For $t \in \mathbf{Q} \cap [0,1]$, let $M_t = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in SL(2,\mathbf{N})$ be the Markoff matrix defined above. Then (i) $g \leq h \leq e \leq f$; (ii) $3e \geq 2f$, $3g \geq 2h$; and (iii) $e+h = 3g$. Moreover, the inequalities in (i) and (ii) are all strict when $t \neq 0, 1$.*

Proof. We prove the lemma by induction on the Farey level of t. The conclusions are readily seen to be true for $t = \frac{0}{1}, \frac{1}{2}, \frac{1}{1}$. Now we suppose that $t \in \mathbf{Q} \cap [0,1]$ has Farey level at least 3. As pointed out in 4.2.1, there exists a unique Farey pair $r, s \in \mathbf{Q} \cap [0,1]$ with $r < s$, such that $t = r \oplus s$. In particular, r and s have smaller Farey levels. Let

$$M_r = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, M_s = \begin{pmatrix} x & y \\ z & w \end{pmatrix}. \tag{2}$$

Then, we get M_t by definition.

$$M_t = M_r M_s = \begin{pmatrix} ex+fz & ey+fw \\ gx+hz & gy+hw \end{pmatrix}. \tag{3}$$

We prove (ii) first. For the induction step, it suffices to observe the following:

$$\frac{y}{x} < \frac{ey+fw}{ex+fz} < \frac{gy+hw}{gx+hz} < \frac{w}{z} \leq \frac{3}{2}.$$

This completes the proof of (ii).
Next, we prove(iii). For the induction step, we only need to show the following:

$$(ex+fz) + (gy+hw) = 3(gx+hz). \tag{4}$$

By the induction hypothesis, we get the following:

$$e+h = 3g, \quad x+w = 3z. \tag{5}$$

Thus, (4) is equivalent to the following:

$$2hx = fz + gy. \tag{6}$$

There are two possibilities: the denominator of r is less or greater than that of s. Hence we have $s = r \oplus t'$ or $r = t' \oplus s$ and t' has Farey level lower than the maximum of r and s, where $t' \in \mathbf{Q} \cap [0,1]$. In the case where $s = r \oplus t'$, we have

$$M_{t'} = M_r^{-1} M_s = \begin{pmatrix} h & -f \\ -g & e \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} hx-fz & hy-fw \\ -gx+ez & -gy+ew \end{pmatrix}.$$

By the induction hypothesis on $M_{t'}$, we get the following:

$$(hx-fz) + (-gy+ew) = 3(-gx+ez). \tag{7}$$

(7) is equivalent to (6) by (5). The proof for the other case is entirely similar. This completes the proof of (iii).

Finally, we prove (i). By the induction hypothesis $x \leq y$ and $z \leq w$, and at least one of them is strict, we get the following inequalities:

$$ex + fz < ey + fw, \quad gx + hz < gy + hw.$$

It remains to prove the following:

$$ex + fz > gy + hw.$$

The above is equivalent to the following by (4)

$$3(gx + hz) > 2(gy + hw). \tag{8}$$

By the induction hypothesis $3x \geq 2y$and $3z \geq 2w$, and at least one of these two inequalities is strict, we know (8) is true.

This completes the Lemma 4.3. □

Remark 4.4 *It is easy to observe that* $tr(M_r) \in \mathbf{N}$ *equals* 3 *times the* $(2,1)$*-element.*

Thus we may write

$$m_r := tr(M_r)$$

It is convenient to introduce an index

$$\rho(M_r) := \frac{e}{g}$$

for every Markoff matrix $M_r = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, where $r \in \mathbf{Q} \cap [0,1]$.

Lemma 4.5 *Let* $t, t' \in \mathbf{Q} \cap [\mathbf{0}, \mathbf{1}]$*, where* $t < t'$*. Then* $\rho(M_t) > \rho(M_{t'})$*.*

Proof. We prove this lemma by induction on the maximum of the Farey level of t and t'. When t, t' both having Farey level 1, then $t = \frac{0}{1}$, $\rho(M_t) = \frac{2}{1}$ and $t' = \frac{1}{1}$, $\rho(M_{t'}) = \frac{3}{2}$, hence the conclusion is true. Now we suppose that $r, s \in \mathbf{Q} \cap [\mathbf{0}, \mathbf{1}]$ are Farey neighbors, where $r < s$, and let $t = r \oplus s$ be their Farey sum. We suppose that M_r and M_s are given by (2) ,then M_t is given by (3). By our induction hypothesis, we can get $\rho(M_r) > \rho(M_s)$. Hence $e/g > x/z$. Next, we need to prove the following inequalities

$$\frac{e}{g} > \frac{ex + fz}{gx + hz} > \frac{x}{z}. \tag{9}$$

The first inequality in (9) follows easily from the fact that $e/g > f/h$. The second inequality is equivalent to the following by Lemma 4.3 (iii)

$$\frac{gy + hw}{gx + hz} < \frac{w}{z},$$

This completes the proof. □

There is an immediate lemma as follows:

Lemma 4.6 *The Markoff matrices M_r, $r \in \mathbf{Q} \cap [\mathbf{0}, \mathbf{1}]$ are all distinct.*

4.2.4 **Fricke's Trace Identities**.

In order to associate the Markoff matrix with the solutions of $x^2 + y^2 + z^2 = xyz$, we introduce the Fricke's Trace Identities in Lemma 4.7.

Lemma 4.7 *If X and $Y \in SL(2, \mathbf{C})$ then*

$$tr(XY) + tr(XY^{-1}) = tr(X)tr(Y) \quad \textit{and} \tag{10}$$

$$tr^2(X) + tr^2(Y) + tr^2(XY) - tr(X)tr(Y)tr(XY) = 2 + tr(XYX^{-1}Y^{-1}). \tag{11}$$

In particular, if $X, Y \in SL(2, \mathbf{C})$ satisfy $tr(XYX^{-1}Y^{-1}) = -2$, then

$$tr^2(X) + tr^2(Y) + tr^2(XY) = tr(X)tr(Y)tr(XY). \tag{12}$$

Proof. First, note that if $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $Y^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Hence $tr(Y) = tr(Y^{-1})$ and $Y + Y^{-1} = tr(Y)I$, where I denotes the identity matrix. Then left-multiplying the latter equality by X gives

$$XY + XY^{-1} = Xtr(Y) \tag{13}$$

Taking traces on both sides of (13) , we obtain identity (10). As a specisl case, we take $X = Y$ in (10) to get

$$tr(Y^2) = tr^2(Y) - 2.$$

Finally, by making use of identity (10) repeatedly, we can calculate $tr(XYX^{-1}Y^{-1})$ and thus obtain (11) easily as follows:

$$\begin{aligned} tr(XYX^{-1}Y{-}1) &= tr(X)tr(YX^{-1})Y{-}1) \\ &= tr^2(X) - [tr(XY)tr(XY^{-1}) - tr(XYYX^{-1})] \\ &= tr^2(X) - tr(XY)[tr(X)tr(Y) - tr(XY)] + tr(Y^2) \\ &= tr^2(X) - tr(X)tr(Y)tr(XY) + tr^2(XY) + tr^2(Y) - 2 \end{aligned}$$

This completes the proof. □

By using Lemma 4.7, we can prove the following lemma easily.

Lemma 4.8 *For every Farey triple (r, t, s) in $\mathbf{Q} \cap [\mathbf{0}, \mathbf{1}]$, (m_r, m_s, m_t) is a solution.*

Proof. This follows from a simple application of identity (12) with $X = M_r$ and $Y = M_s$.

To apply (12), we need to verify that

$$tr(M_r M_s M_r^{-1} M_s^{-1}) = -2 \tag{14}$$

for every pair of Farey neighbor $r, s \in \mathbf{Q} \cap [\mathbf{0}, \mathbf{1}]$ with $r < s$. Indeed, since

$$tr(M_r M_t M_r^{-1} M_t^{-1}) = tr(M_r M_s M_r^{-1} M_s^{-1}) = tr(M_t M_s M_t^{-1} M_s^{-1}),$$

it suffices to check (14) for the initial pair $(r,s)=(\frac{0}{1},\frac{1}{1})$. This is true because

$$tr(M_{\frac{0}{1}}M_{\frac{1}{1}}M_{\frac{0}{1}}^{-1}M_{\frac{1}{1}}^{-1}) = tr\begin{pmatrix} -7 & 6 \\ -6 & 5 \end{pmatrix} = -2.$$

Since $tr(M_r)=m_r$ etc. , we can get the following result from (12):

$$m_r^2+m_s^2+m_t^2 = m_rm_sm_t.$$

This shows that (m_r,m_s,m_t) is a solution. □

By Lemma 4.8, we have the following conjecture:

Unicity Conjecture.(Matrix Form). The traces of the Markoff matrices M_r are all distinct, where $r\in\mathbf{Q}\cap[\mathbf{0},\mathbf{1}]$.

4.3 Proof of Theorem 1.1

In order to associate Theorem 1.1 to Markoff matrix we have the following lemma.

Lemma 4.9 *The Unicity Conjecture is equivalent to the Unicity Conjectue (Matrix Form).*

Proof. ($\Leftarrow$) It is clear. ($\Rightarrow$) Let M_t and $M_{t'}$ have the same trace (ie.$m_t=m_{t'}$). We want to claim that $M_t=M_{t'}$. First, we know that $\exists\ r,s\in\mathbf{Q}\cap[0,1]$, $r<s$, where r,s,t are Farey neighbors such that $t=r\oplus s$ and $\exists\ r',s'\in\mathbf{Q}\cap[0,1]$, $r'<s'$, where r',s',t' are Farey neighbors such that $t'=r'\oplus s'$. Thus, $M_t=M_rM_s$, $M_{t'}=M_{r'}M_{s'}$, and (m_r,m_s,m_t), $(m_{r'},m_{s'},m_{t'})$ are solutions. Since $m_t=m_{t'}$, by the Unicity Conjecture we obtain $m_r=m_{r'}$ and $m_s=m_{s'}$. We prove this by induction on the maximal Farey level of r,s,r',s'. By induction hypothesis, we obtain $M_r=M_{r'}$ and $M_s=M_{s'}$. This implies $M_t=M_{t'}$. This completes the proof. □

Lemma 4.10 *If the trace of a Markoff matrix M_r, where $r\in\mathbf{Q}\cap[\mathbf{0},\mathbf{1}]$, equals 3 times a prime power or 6 times a prime power, then no other Markoff matrix $M_{r'}$, where $r\neq r'\in\mathbf{Q}\cap[\mathbf{0},\mathbf{1}]$ has the same trace.*

Proof. **Case 1**. We suppose that the two Markoff matrices M_r and $M_{r'}$ have the same $(2,1)$-entry which is a prime power (since $e+h=3g$ and $e+h=3p^i$) , where $r,r'\in\mathbf{Q}\cap[\mathbf{0},\mathbf{1}]$ with $r<r'$.

By Lemma 4.5, we get $\rho(M_r)>\rho(M_{r'})$. Hence we have

$$M_r=\begin{pmatrix} e+k & f' \\ g & h-k \end{pmatrix}, M_{r'}=\begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

for some positive integer k. By assumption, $g=p^i$, where $i\geq 1$, for some prime p. Since $M_r,M_{r'}\in SL(2,\mathbf{N})$, we can get the following by comparing their determinants.

$$k(e+k-h)=(f-f')g$$

Note that $0 < k < g$ and $0 < e + k - h < g$ since $g < h < e$ and $g < e + k < 2g$ by Lemma 4.3. Thus, $p \mid k$ and $p \mid e + k - h$ (hence $i > 1$). This implies that $p \mid e - h$. Note that $p \mid e + h$ since $e + h = 3g$ by Lemma 4.3. If $p \neq 2$ then p divides each of e, f and g, contradicting to $eh - fg = 1$. Therefore $p = 2$. Then $g \equiv 0 (\mathrm{mod}\ 4)$. But now $e + h = 3g$ implies that $eh \equiv 3 (\mathrm{mod}\ 4)$ or $eh \equiv 0 (\mathrm{mod}\ 4)$, again contradicting to $eh - fg = 1$.
Case 2. The proof of the case 2 is similar to case 1. By assumption, $g = 2p^i$, where $i \geq 1$, for some prime p. Thus we can obtain three subcases.
subcase 2.1: $2 \mid k$ and $p^i \mid e + k - h$
Undoubtedly, $e+k-h = p^i$. Moreover $e+h = 6p^i$, this implies $2e+k = 7p^i$, a contradiction.
subcase 2.2: $p^i \mid k$ and $2 \mid e + k - h$
Undoubtedly, $k = p^i$. Moreover $e + h = 6p^i$ and let $e + k - h = 2m, m \in \mathbf{N}$, this implies $2e + p^i = 6p^i + 2m$, a contradiction.
subcase 2.3: $p \mid k$ and $p \mid e + k - h$.
It is the same as the proof of the case 1. Thus we can get a contradiction.
This completes the proof. □

Proof of Theorem 1.1.
Proof. It follows from Lemma 4.9 and Lemma 4.10 immediately. □

4.4 Properties of the solutions

In order to prove Theorem 1.2, we need to observe more precise properties about the solutions. Lemma 4.11, Lemma 4.13 and Lemma 4.14 are the properties of the solutions.

Lemma 4.11 *Let (a, b, c) be a solution of $x^2 + y^2 + z^2 = xyz$, then*
(i) $gcd(a, b) = gcd(b, c) = gcd(c, a) = 3$
(ii) Every odd entry $\equiv 3 (\mathrm{mod}\ 4)$
(iii) Every even entry $\equiv 6 (\mathrm{mod}\ 8)$

Proof. By the equation, we can get $gcd(a, b) = gcd(b, c) = gcd(c, a) = g(a, b, c)$. Then by Lemma 4.1, we get $gcd(a, b, c) = gcd(a, b, ab - c) = ... = gcd(3, 3, 3) = 3$. This proves (i). By (i), we can write the solution

$$(a, b, c) = (3l, 3m, 3n), \ \ gcd(l, m) = gcd(m, n) = gcd(n, l) = 1, \ l, \ m, \ n \in \mathbf{N}. \qquad (15)$$

Since $n(3lm - n) = l^2 + m^2$ and $gcd(l, m) = 1$, n is not a multiple of 4 and for each prime factor p, -1 is a quadratic residue modulo p. It is well known that -1 is not a quadratic residue modulo a prime which is $\equiv 3 (\mathrm{mod}\ 4)$ and each odd prime factor of n is $\equiv 1 (\mathrm{mod}\ 4)$. Hence, each odd prime factor of c is $\equiv 3 (\mathrm{mod}\ 4)$ and each even prime factor of c is $\equiv 6 (\mathrm{mod}\ 8)$.This proves (ii), (iii). □

Lemma 4.12 follows from Lemma 4.11 immediately.

Lemma 4.12 *If x and y are coprime integers then every odd factor of x^2+y^2 is $\equiv 1 (\mathrm{mod}\ 4)$.*

Lemma 4.13 *If c is an even entry of the solution, then $c \equiv 6 (\mathrm{mod}\ 32)$.*

Proof. We suppose that (a, b, c) is a solution with $a < b < c$ such that c is even. Let $a = 3l$ and $b = 3m$ and $c = 3n$, then by the proof of Lemma 4.11, $l \equiv m \equiv 1 (\mathrm{mod}\ 4)$ and $n \equiv 2 (\mathrm{mod}\ 8)$, hence $(m - l)/2$ is even and $n/2 \equiv 1 (\mathrm{mod}\ 4)$. Since $3n - 2 \equiv 4 (\mathrm{mod}\ 8)$, we know that $(3n - 2)/4$ is odd. Moreover, the original equation becomes to the following by (15).

$$((m - l)/2)^2 + (n/2)^2 = lm(3n - 2)/4.$$

Since $gcd(n/2, m) = gcd(n/2, l) = 1$ and $gcd(n/2, (3n - 2)/4) = 1$, we know that $n/2$ is coprime with $lm(3n - 2)/4$. Consequently, $(m - l)/2$ and $n/2$ are coprime. Then Lemma 4.12 implies $(3n - 2)/4 \equiv 1 (\mathrm{mod}\ 4)$, from which follows that $n \equiv 2 (\mathrm{mod}\ 16)$.
Then $3n + 2 \equiv 8 (\mathrm{mod}\ 16)$ and hence $(3n + 2)/8$ is odd. Moreover, the original equation becomes to the following by (15).

$$((l + m)/2)^2 + (n/2)^2 = 2lm(3n + 2)/8.$$

Since $gcd(n/2, l) = gcd(n/2, m) = 1$ and $gcd(n/2, (3n + 2)/4) = 1$, we know that $n/2$ is coprime with $lm(3n + 2)/4$. Consequently, $(l + m)/2$ and $n/2$ are coprime. Then Lemma 4.12 implies $(3n + 2)/8 \equiv 1 (\mathrm{mod}\ 4)$, from which follows that $n \equiv 2 (\mathrm{mod}\ 32)$.
Hence $c \equiv 6 (\mathrm{mod}\ 32)$. This completes the proof. □

Lemma 4.14 *Suppose that $(a, b, c) \neq (3, 6, 15)$ is a solution with $a < b < c$. Then*

$$c > 2ab/3 \quad \textit{and} \quad b > 2c'a/3, \tag{16}$$

where $c' = ab - c$; in particular, $c > 2b$ and $b > 2a$.

Proof. By Lemma 4.1, every solution $(a, b, c) \neq (3, 6, 15)$ can be obtained by repeatedly generating new neighbors starting from $(3, 6, 15)$. Hence we only need to show that if (16) holds for (a, b, c) then it also holds for the two new neighbors (a', b, c) and (a, b', c), where $a' = bc - a$ and $b' = ca - b$. For this we only need to check $a' > 2bc/3$ and $b' > 2ca/3$. These are very obvious. This completes the proof. □

Remark 4.15 *By Lemma 4.11 (i) and Lemma 4.14, we have an immediate conclusion as follows:*
If a solution $(a, b, c) = (3l, 3m, 3n) \neq (3, 6, 15)$ with $a < b < c$. Then

$$n > 2lm \quad \textit{and} \quad m > 2n'l,$$

where $n' = 3lm - n$; in particular, $n > 2m$ and $m > 2l$.

4.5 Proof of Theorem 1.2

In order to prove Theorem 1.2, we need to prove Lemma 4.16 first.

Lemma 4.16 *Suppose $k = p^i$ or $2p^i$ for an odd prime p and an integer $i \geq 1$. Then, for any integer r coprime to k, the binomial quadratic equation*

$$x^2 + r \equiv 0 \ (\mathrm{mod}\ k) \tag{17}$$

has at most one integer solution x with $0 < x < k/2$.

Proof. We only prove the lemma for $k = 2p^i$; the proof for the case where $k = p^i$ is similar and actually a bit simpler. We suppose that (17) has two integer solutions x and x' such that $0 < x < x' < k/2$. Then $2p^i \mid (x' + x)(x' - x)$. Note that $0 < x' + x < 2p^i$ and $0 < x' - x < p^i$. If $p \mid x' + x$ and $p \mid x' - x$ then $p \mid 2x$; hence $p \mid x$, and consequently $p \mid r$, a contradiction. Therefore, we must have $p^i \mid x' + x$ and $2 \mid x' - x$. But then $x' + x = p^i$ and $x' \equiv x (\text{mod } 2)$, which implies that p^i is even, again a contradiction. This completes the proof. □

Proof of Theorem 1.2

Proof. Let (a, b, c) and $(\tilde{a}, \tilde{b}, c)$ be solutions. By (15), we may let $(a, b, c) = (3l, 3m, 3n)$ and $(\tilde{a}, \tilde{b}, c) = (3\tilde{l}, 3\tilde{m}, 3n)$.

Case 1. c is odd.

subcase 1.1. We suppose that $c - 2 = p^i$. This implies $3n - 2 = p^i$. We write $k = 3n - 2$. Then the original equation becomes to the following by (15).

$$(m - l)^2 + n^2 = lmk \equiv 0(\text{mod } k) \tag{18}$$

Note that $gcd(n, k) = 1$ since $gcd(n, k) \mid 2$ and c is odd. By Lemma 4.16

$$0 < m - l < n/2 - 1 < (3n - 2)/2 = k/2 \tag{19}$$

Since (18) and (19) are also true for $(\tilde{l}, \tilde{m}, n)$, Lemma 4.16 implies $m - l = \tilde{m} - \tilde{l}$. Substituting this relation back into (18) for $(\tilde{l}, \tilde{m}, n)$, then we can obtain $lm = \tilde{l}\tilde{m}$. Hence, both $\{-l, m\}$ and $\{-\tilde{l}, \tilde{m}\}$ are the roots of the same quadratic equation. This implies $l = \tilde{l}$ and $m = \tilde{m}$. Hencs, $a = \tilde{a}$ and $b = \tilde{b}$.

subcase 1.2. We suppose that $c + 2 = p^i$. This implies $3n + 2 = p^i$. We write $k = 3n + 2$. The proof is similar to the subcase 1.1, by using

$$(l + m)^2 + n^2 = lmk \equiv 0(\text{mod } k)$$

and $0 < l + m < 3n/4 < (3n + 2)/2 = k/2$.

Case 2. c is even.

By Lemma 1.3, $c - 2$ is 4 times an odd and $c + 2$ is 8 times an odd. By (15), $3n - 2$ is 4 times an odd and $3n + 2$ is 8 times an odd. And by the proof of Lemma 4.11, $l \equiv m \equiv 1($ mod 4) and $\tilde{l} \equiv \tilde{m} \equiv 1(\text{mod } 4)$.

subcase 2.1. We suppose that $c - 2 = 4p^i$. This implies $3n - 2 = 4p^i$. We write $k = (3n - 2)/4 = p^i$. Then the original equation becomes to the following by (15).

$$((m - l)/2)^2 + (n/2)^2 = lmk \equiv 0(\text{mod } k) \tag{20}$$

Since $gcd(n, 3n - 2) = 2$, we have $gcd(n/2, k) = 1$. By Lemma 4.16

$$0 < (m - l/2) < n/4 < (3n - 2)/8 = k/2 \tag{21}$$

Since (20) and (21) are also true for $(\tilde{l}, \tilde{m}, n)$, Lemma 4.16 implies that $m - l = \tilde{m} - \tilde{l}$ Consequently, $lm = \tilde{l}\tilde{m}$. Therefore $l = \tilde{l}$ and $m = \tilde{m}$. This implies $a = \tilde{a}$ and $b = \tilde{b}$.

subcase 2.2. We suppose that $c + 2 = 8p^i$. This implies $3n + 2 = 8p^i$. We write $k = (3n + 2)/4 = 2p^i$. The proof is similar to the subcase2.1. By using

$$((l + m)/2)^2 + (n/2)^2 = lmk \equiv 0(\text{mod } k),$$

again $gcd(n/2, k) = 1$, and $0 < (l + m)/2 < 3n/8 < (3n + 2)/8 = k/2$.
This completes the proof . □