Pythagorean Triples

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
23 September, 2017 (at *15:52*)

Entrance. Let "$n \equiv_4 k$" mean[♡1] $4 \bullet\!\!| [n-k]$.

A ***Pythagorean triple*** $\langle a,b,c\rangle$ of integers satisfies

P0: $$a^2 + b^2 = c^2 .$$

It is a ***PPT***, a ***primitive Pythagorean triple***, if, in addition,

P1: $a,b,c \in \mathbb{Z}_+$.

P2: $\text{Gcd}(a,b,c) = 1$. [Necessarily, each pair of a,b,c is coprime, courtesy (P0).]

P3: a is odd. [We'll see that b is even, and c is odd.]

By (P2), a and b can't *both* be even; so there is no loss of generality in the (P3) normalization. Could also b be odd? If yes, then $a^2 + b^2 \equiv_4 1 + 1 = 2$. But c is even, so $c^2 \equiv_4 0$. ⋙.

Here is one correspondence, and its inverse:

1a: $$\begin{aligned} c &= \tfrac{1}{2}\left[y^2 + x^2\right] . \\ b &= \tfrac{1}{2}\left[y^2 - x^2\right] . \\ a &= yx . \end{aligned} \qquad \begin{aligned} \sqrt{c+b} &= y . \\ \sqrt{c-b} &= x . \end{aligned}$$

A reworking gives this corr., and its inverse:

1b: $$\begin{aligned} c &= r^2 + q^2 . \\ b &= 2rq . \\ a &= r^2 - q^2 . \end{aligned} \qquad \begin{aligned} \sqrt{\tfrac{1}{2}[c+a]} &= r . \\ \sqrt{\tfrac{1}{2}[c-a]} &= q . \end{aligned}$$

To make this precise, say that a pair (y,x) is an ***odd-pair*** if:

D1: $y,x \in \mathbb{Z}_+$. *Additionally,* $y > x \geqslant 1$.
D2: $x \perp y$.
D3: *Both* x *and* y *are odd.*

A pair (r,q) is a ***mixed-pair*** if:

M1: $r,q \in \mathbb{Z}_+$. *Furthermore,* $r > q \geqslant 1$.
M2: $r \perp q$.
M3: *Integers* q *and* r *have opposite parities.*

Given x,$y \in \mathbb{Z}$, define

2a: $$\mathbf{T}(x,y) := \langle a,b,c\rangle , \quad \text{where } \begin{aligned} a &:= yx ; \\ b &:= \tfrac{1}{2}\cdot[y^2 - x^2] ; \\ c &:= \tfrac{1}{2}\cdot[y^2 + x^2] . \end{aligned}$$

2b: $$\mathbf{U}(r,q) := \langle a,b,c\rangle , \quad \text{where } \begin{aligned} a &:= r^2 - q^2 ; \\ b &:= 2rq ; \\ c &:= r^2 + q^2 . \end{aligned}$$

3a: Odd-pair Thm. *There is a 1-to-1 correspondence between odd-pairs and primitive triples: The map*

$$\textit{Odd-Pairs} \xrightarrow{\mathbf{T}} \textit{Primitive Triples}$$

is a bijection. ♢

Our $\mathbf{T}$ *is well-defined.* Necessarily, $a \stackrel{\text{def}}{=} yx$ is odd and a, b and c are positive since $1 \leqslant x < y$. Since x^2 and y^2 are each odd, and ODD ± ODD is even, we have that b and c are indeed integers.

To establish that $\langle a,b,c\rangle$ is primitive, what remains is to prove that $\text{Gcd}(a,b,c) = 1$. So suppose that p is a prime dividing a. Necessarily, p divides x or y; WLOGenerality $p \bullet\!\!| x$. Were p to divide b, forcing $p \bullet\!\!| [y^2 - x^2]$, then $p \bullet\!\!| y^2$ and consequently $p \bullet\!\!| y$. But that contradicts that (x,y) is a odd-pair. Thus $a \perp b$. ♦

$\mathbf{T}(\cdot)$ *is injective.* Suppose another odd-pair (w,z) also gives rise to the same triple

$$\mathbf{T}(w,z) = \langle a,b,c\rangle = \mathbf{T}(x,y) .$$

Since $wz = a = xy$, without loss of generality $w < x$ and $z > y$. But then

$$b = \tfrac{1}{2}\left[z^2 - w^2\right] > \tfrac{1}{2}\left[y^2 - x^2\right] = b .$$

This is a contradiction. ♦

[♡1] Use $\equiv_N$ to mean "congruent mod N". Let $n \perp k$ mean that n and k are co-prime. Use $k \bullet\!\!| n$ for "k divides n". Its negation $k \not\bullet\!\!| n$ means "k does not divide n." Use $n \not\bullet\!\!| k$ and $n \not\bullet\!\!| k$ for "n is/is-not a multiple of k." Finally, for p a prime and E a natnum: Use double-verticals, $p^E \bullet\!\!\!|\, n$, to mean that E is the ***highest*** power of p which divides n. Or write $n \not\bullet\!\!\!|\, p^E$ to emphasize that this is an assertion about n. Use ***PoT*** for Power of Two and ***PoP*** for Power of (a) Prime.

T$(\cdot)$ *is surjective.* Fix a primitive triple $\langle a,b,c\rangle$. My first goal is to produce integers x & y so that $\mathbf{T}(x,y)=\langle a,b,c\rangle$. To this end, define X & Y by

$$Y \;:=\; c+b, \quad X \;:=\; c-b\,. \quad \text{Thus,}$$
$$Y\cdot X \;=\; [c+b]\cdot[c-b] \overset{\text{note}}{=\!=} c^2-b^2 \;=\; a^2\,.$$

Necessarily, Y,$X\in\mathbb{Z}_+$. I want to let

¥: $\qquad x:=\sqrt{X}$ and $y:=\sqrt{Y}$,

so I need to show that X & Y are squares. Since product YX is a square, ISTShow that $X\perp Y$. Fixing a prime $p\,|\!\bullet\, X$, then, ISTEstablish that

$$p \text{ does } \textit{not} \text{ divide } Y.$$

Were p to divide Y then it would divide the two linear combinations

$$Y+X \overset{\text{note}}{=\!=} 2c \quad \text{and} \quad Y-X \overset{\text{note}}{=\!=} 2b\,.$$

But $p\,|\!\bullet\, X\,|\!\bullet\, a^2$, so p is odd. Thus $p\,|\!\bullet\, c$ and $p\,|\!\bullet\, b$, contradicting (P1).

Final step. I've shown that $y\,\&\,x$ from (¥) are posints. Since the argument also showed that $Y\perp X$, we now have $y\perp x$. And (P1,P0,P3) show that $c>b>0$; so $Y>X$ and thus $y>x\geqslant 1$. Lastly, y & x are each odd, since each divides a, which is odd. ♦

3b**:** Mixed-pair Thm. *This map is a bijection:*

$$\textit{Mixed-Pairs} \xrightarrow{\mathbf{U}} \textit{Primitive Triples}\,. \qquad \Diamond$$

Pf. Define $f\Big(\big(y,x\big)\Big):=\big(r,q\big)$, where $r:=\frac{1}{2}[y+x]$ and $q:=\frac{1}{2}[y-x]$. Reversing, $g\Big(\big(r,q\big)\Big):=\big(y,x\big)$, where $y:=r+q$ and $x:=r-q$. Easily, f and g are well-defined on the rationals, and are inverses of each other. So the proof will be finished when <u>you</u> show (exercise) that $f(\text{odd-pair})\in\text{Mixed-pair}$ and $g(\text{mixed-pair})\in\text{Odd-pair}$. ♦

Special case of Fermat's Last Theorem

Fermat proved the following theorem.

4: FLT for $N = 4$. *There is no posint soln to either of these:*

$$\dagger: \qquad a^4 + b^4 = c^4 \ ;$$
$$\ddagger: \qquad D^4 + E^4 = U^2 \ . \qquad \lozenge$$

Prelim. A (†)-triple yields (‡)-triple $a^4 + b^4 = [c^2]^2$, hence ISTShow: $\nexists$ *soln to* (‡). Below, define $\perp\!\!\!\bullet$ so that $x \perp\!\!\!\bullet\, y$ means: $x \perp y$ *and* $x \not\equiv_2 y$.

Let expression "$\alpha \in \square$" mean that there exists a posint β with $\alpha = \beta^2$. ♦

Proof. FTSOC, suppose we have a (‡) which has minimum U, over all (‡). Were there a prime with $p \bullet\!\!| D$ and $p \bullet\!\!| E$, then $p^2 \bullet\!\!| U$, so $\left(\frac{D}{p}, \frac{E}{p}, \frac{U}{p^2}\right)$ is a smaller (‡); ≪. Thus $D \perp E$, so (D^2, E^2, U) is a PPT (prim. Pythag. triple), since $[D^2]^2 + [E^2]^2 = U^2$; WLOG D is odd and E even.

Our PPT parametrization (1b) yields posints $R > Q$ with $R \perp\!\!\!\bullet\, Q$ such that

$$*1: \qquad U = R^2 + Q^2 \ ;$$
$$*2: \qquad E^2 = 2RQ \ ;$$
$$D^2 = R^2 - Q^2 \ .$$

The latter is $D^2 + Q^2 = R^2$. As $R \perp Q$, this last is a PPT. Since D odd, nec. Q is even and R is odd. Hence $R \perp 2Q$, so (∗2) implies that

$$£: \qquad R \in \square \quad \text{and} \quad 2Q \in \square \, .$$

PPT $D^2 + Q^2 = R^2$ engenders posints $r > q$ with $r \perp\!\!\!\bullet\, q$, such that

$$*3: \qquad R = r^2 + q^2 \ ;$$
$$*4: \qquad Q = 2rq \ ;$$
$$D = r^2 - q^2 \ .$$

Our (£) implies ∃ posint c with $2Q = [2c]^2$, i.e $2c^2 = Q = 2rq$, by (∗4). Thus $c^2 = rq$. But $r \perp q$, so $r,q \in \square$. This, together with (£), tells us that there exist posints u, d, e such that

$$R = u^2, \quad r = d^2 \quad \text{and} \quad q = e^2 \, .$$

Consequently, we can restate (∗3) as

$$**3: \qquad d^4 + e^4 = u^2 \ .$$

This has form (‡). Moreover, $u \leqslant u^2 = R < U$ courtesy (∗1). We see to our relief that (∗∗3) contradicts the minimality of U. ♦

Pell's Equation

What are all the Pythagorean triples

$$5\text{:} \qquad a^2 + [a+1]^2 \;=\; c^2\,,$$

i.e, where the legs of the triangle are consecutive integers? I'll show, that if $\mathbf{(}a,c\mathbf{)}$ is a soln, then so is

$$6\text{:} \qquad \begin{aligned} a' &:= 3a + 2c + 1 \quad \text{and} \\ c' &:= 4a + 3c + 2\,. \end{aligned}$$

The first nine values are

a	c	a	c	a	c
0	1	119	169	23660	33461
3	5	696	985	137903	195025
20	29	4059	5741	803760	1136689

The set of soln-pairs has a group structure, with multiplication $\left[\begin{smallmatrix} a_1 \\ c_1 \end{smallmatrix}\right] \odot \left[\begin{smallmatrix} a_2 \\ c_2 \end{smallmatrix}\right]$ described by this formula:

$$7\text{:} \qquad \begin{aligned} a' &:= -a_2 + c_2 - a_1 - 2a_1a_2 + 2a_1c_2 \\ &\quad + c_1 + 2c_1a_2 - c_1c_2 - 1\,; \\ c' &:= -c_1 - 2c_1a_2 + 2c_1c_2 \\ &\quad + 2a_2 - c_2 + 2a_1 + 4a_1a_2 - 2a_1c_2 + 1. \end{aligned}$$

The group-inverse of an elt: $\left[\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right] := \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]^{\odot -1}$ where

$$7_{\text{inv}}\text{:} \qquad \begin{aligned} a' &:= -3a + 2c - 2\,; \\ c' &:= -4a + 3c - 2\,. \end{aligned}$$

E.g, $\left[\begin{smallmatrix} 3 \\ 5 \end{smallmatrix}\right]^{\odot -1} = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right]$.

Eqn (5) is equivalent to $[2a]^2 + [2a+2]^2 = [2c]^2$. We can write this in form $f(a,c) = 0$, but the f polynomial is not homogeneous. We can get a homogeneous eqn: Setting

$$d \;:=\; 2a + 1$$

makes the eqn $[d-1]^2 + [d+1]^2 = [2c]^2$. Dividing by 2 and rewriting gives

$$8\text{:} \qquad d^2 \;-\; 2c^2 \quad = \quad -1\,.$$

This is special case of what the "***generalized Pell's eqn*** with ***Pell coefficient*** $\boldsymbol{\mu}$":

$$\varepsilon_{\boldsymbol{\mu}}^{\boldsymbol{\tau}}\text{:} \qquad d^2 \;-\; \boldsymbol{\mu} c^2 \quad = \quad \boldsymbol{\tau}\,, \qquad \text{where } \boldsymbol{\mu} \in \mathbb{Z}_+.$$

We'll ask: *What* ***targets*** $\boldsymbol{\tau} \in \mathbb{Z}$ *admit a soln pair* $\mathbf{(}d,c\mathbf{)}$ *in integers? And: When* $\boldsymbol{\tau}$ *admits a soln, what is the complete set of soln-pairs?*

Just "Pell's eqn" shall mean the $\boldsymbol{\tau}$=1 case:

$$\varepsilon_{\boldsymbol{\mu}}\text{:} \qquad d^2 \;-\; \boldsymbol{\mu} c^2 \quad = \quad 1\,.$$

This always has the two ***trivial solns*** $\mathbf{(}\pm 1, 0\mathbf{)}$.

We will find all ***consecutive pythag-triples*** by solving (8), which we will get from the soln set of (ε_2).

Group structure

Below, the objects $\mathcal{G}, \mathcal{P}, \mathsf{M}, \ldots$ all depend on $\boldsymbol{\mu}$. When needed, I'll indicate the dependence as $\mathcal{G}_{\boldsymbol{\mu}}$, with a subscript.

Use $\mathbf{I} := \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $\mathsf{J} := \left[\begin{smallmatrix} 0 & \boldsymbol{\mu} \\ 1 & 0 \end{smallmatrix}\right]$. For the generic ***lin-comb*** (linear combination) of matrices, use

$$\mathsf{M} \;:=\; \mathsf{M}_{d,c} \;:=\; d\mathbf{I} + c\mathsf{J} \;=\; \left[\begin{smallmatrix} d & \boldsymbol{\mu} c \\ c & d \end{smallmatrix}\right] \quad \begin{array}{l}\text{(always with let-}\\ \text{ters "}d\text{" and "}c\text{").}\end{array}$$

The set

$$\mathcal{L} \;:=\; \Big\{ \mathsf{M}_{d,c} \;\Big|\; d, c \in \mathbb{Z} \Big\}$$

of lin-combs is sealed under multiplication, since $\mathbb{Z}$ is a ring and $\mathsf{J}^2 = \boldsymbol{\mu}\mathbf{I} \in \mathcal{L}$. Thus

$$9\text{:} \quad \mathbf{(}\mathcal{L}, \cdot, \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]\mathbf{)} \;\; \textit{is a commutative semi-group.}$$

Note $\text{Det}(\mathsf{M}) = d^2 - \boldsymbol{\mu} c^2$. The following set is a *group*

$$\mathcal{G} \;:=\; \Big\{ \mathsf{M} \in \mathcal{L} \;\Big|\; \text{Det}(\mathsf{M}) \in \{1, -1\} \Big\}\,,$$

because $\mathcal{G}$ is sealed under mult., since $\{1,-1\}$ is. And $\mathcal{G}$ is sealed under inverse, since

$$10\text{:} \qquad \begin{aligned} \mathsf{M}^{-1} \;&=\; \tfrac{1}{\text{Det}(\mathsf{M})} \left[\begin{smallmatrix} d & -\boldsymbol{\mu} c \\ -c & d \end{smallmatrix}\right] \overset{\text{note}}{=\!=} \widehat{d}\,\mathbf{I} + \widehat{c}\,\mathsf{J}, \text{ where} \\ \widehat{d} \;&:=\; \tfrac{d}{\text{Det}(\mathsf{M})} \quad \text{and} \quad \widehat{c} \;:=\; \tfrac{-c}{\text{Det}(\mathsf{M})}\,. \end{aligned}$$

Note $\widehat{d}$ and $\widehat{c}$ are integers, since $\mathrm{Det}(\mathsf{M}) = \pm 1$.

Define two sets by the condition above them

$$\mathcal{G} \;=\; \overset{\mathrm{Det}(\mathsf{M})=+1}{\mathcal{P}} \;\sqcup\; \overset{\mathrm{Det}(\mathsf{M})=-1}{\mathcal{N}} \;.$$

The map $\mathrm{Det}:\mathcal{G}\to\{+1,-1\}$ is a gp-homomorphism, so

$$\mathcal{P} \;:=\; \mathrm{Det}^{-1}\big(\{1\}\big)\,.$$

is a subgroup of $\mathcal{G}$.

11: Lemma. *For those values of $\boldsymbol{\mu}$ with $\mathcal{N}_{\boldsymbol{\mu}}$ not empty, then $\mathcal{N}_{\boldsymbol{\mu}}$ is a $\mathcal{G}$-coset of $\mathcal{P}_{\boldsymbol{\mu}}$.* ♢

Proof. Fix a matrix $\mathsf{N}_{\boldsymbol{\mu}} \in \mathcal{N}_{\boldsymbol{\mu}}$. For each $\mathsf{M} \in \mathcal{N}_{\boldsymbol{\mu}}$, note that $\mathsf{M}\cdot\mathsf{N}_{\boldsymbol{\mu}} \overset{\mathrm{Det}}{=} [-1]^2 = 1$. I.e, $\mathsf{MN}_{\boldsymbol{\mu}} \in \mathcal{P}$. ♦

Remark. When $\boldsymbol{\mu} = 2$: Matrix $\mathsf{N}_2 := \left[\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right]$ shows that $\mathcal{N}_2$ is not empty, hence is (the only other coset) of $\mathcal{P}_2$.

In contrast, $\mathcal{N}_3$ is empty. Indeed, *lots* of $\boldsymbol{\mu}$ have $\mathcal{N}_{\boldsymbol{\mu}} = \varnothing$; see the **Appendix**. □

Henceforth μ is a posint

Upper-lefthand entry. Define two sets

$$\mathcal{P} \;=\; \overset{d>0}{\mathcal{U}} \;\sqcup\; \overset{d<0}{\mathcal{U}^-}\,;$$

this $\mathcal{U}$ is the set of $\left[\begin{smallmatrix}d&\boldsymbol{\mu}c\\c&d\end{smallmatrix}\right]$ with $d>0$.

12: Lem. $[\boldsymbol{\mu}\in\mathbb{Z}_+]$ $\big(\mathcal{U},\cdot,\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]\big)$ *is a group.* ♢

Proof. When $\mathsf{M}\in\mathcal{U}$, necessarily $\mathsf{M}^{-1}\in\mathcal{U}$, by (10).

Now consider a product of two matrices in $\mathcal{U}$:

$$\left[\begin{smallmatrix}\alpha&\boldsymbol{\mu}\beta\\\beta&\alpha\end{smallmatrix}\right]\cdot\left[\begin{smallmatrix}d&\boldsymbol{\mu}c\\c&d\end{smallmatrix}\right] \;=\; \left[\begin{smallmatrix}\alpha d+\boldsymbol{\mu}\beta c&?\\ \alpha c+\beta d&?\end{smallmatrix}\right];$$

here $d,\alpha\in\mathbb{Z}_+$ and $c,\beta\in\mathbb{Z}$ and

$$*1: \qquad \begin{aligned}\alpha^2 \;&=\; 1+\boldsymbol{\mu}\beta^2 \;>\; \boldsymbol{\mu}\beta^2\,;\\ d^2 \;&=\; 1+\boldsymbol{\mu}c^2 \;>\; \boldsymbol{\mu}c^2\,.\end{aligned}$$

Now $\boldsymbol{\mu}\geqslant 0$, so the RhSes are non-negative; hence

$$*2: \qquad [\alpha d]^2 \;>\; [\boldsymbol{\mu}\beta c]^2\,.$$

To show $\mathcal{U}$ sealed under product we need to prove that $\alpha d+\boldsymbol{\mu}\beta c \overset{?}{>} 0$. I.e, that $\alpha d \overset{?}{>} -\boldsymbol{\mu}\beta c$. So $|\alpha d| \overset{?}{>} |\boldsymbol{\mu}\beta c|$ certainly suffices, since αd is positive. And this is implied by $(*2)$. ♦

When $\mathcal{U}$ non-trivial. Suppose that $\mathcal{U}_{\boldsymbol{\mu}}$ is <u>not</u> the trivial gp $\{\mathbf{I}\}$. So we can pick the *minimal* posint Υ for which there exists a $\Delta\in\mathbb{Z}_+$ with $\Delta^2-\boldsymbol{\mu}\Upsilon^2=1$. This Δ is unique. W.r.t Δ or Υ,

$$\mathsf{S} \;=\; \mathsf{S}_{\boldsymbol{\mu}} \;:=\; \left[\begin{smallmatrix}\Delta&\boldsymbol{\mu}\Upsilon\\\Upsilon&\Delta\end{smallmatrix}\right]$$

is the minimal positive elt of $\mathcal{U}$.

As an example, $\mathsf{S}_2 = \left[\begin{smallmatrix}3&4\\2&3\end{smallmatrix}\right]$.

13: Lem. *Fix an $\mathsf{M}\in\mathcal{U}$. Then the map $h_{\mathsf{M}}:\mathbb{Z}\to\mathbb{Z}$ by*

$$h_{\mathsf{M}}(n) \;:=\; c\text{-}coord(\mathsf{S}^n\cdot\mathsf{M})$$

is strictly increasing. ♢

Pf. Our goal is $c'<c$, where

$$\begin{aligned}\left[\begin{smallmatrix}d'&\boldsymbol{\mu}c'\\c'&d'\end{smallmatrix}\right] \;:=\; \mathsf{S}^{-1}\cdot\mathsf{M} \;&=\; \left[\begin{smallmatrix}\Delta&-\boldsymbol{\mu}\Upsilon\\-\Upsilon&\Delta\end{smallmatrix}\right]\cdot\left[\begin{smallmatrix}d&\boldsymbol{\mu}c\\c&d\end{smallmatrix}\right]\\ &=\; \left[\begin{smallmatrix}?&?\\ \Delta c-\Upsilon d&?\end{smallmatrix}\right].\end{aligned}$$

So our goal is i.e $\Delta c-\Upsilon d<c$, i.e $[\Delta-1]c<\Upsilon d$. WLOG $c>0$ (since $\Delta\in\mathbb{Z}_+$ so $\Delta-1\geqslant 0$), and so our goal becomes $\frac{\Delta-1}{\Upsilon} \;<\; \frac{d}{c}$. Its LhS $\geqslant 0$, so establishing

$$*: \qquad \left[\tfrac{\Delta-1}{\Upsilon}\right]^2 \;<\; \left[\tfrac{d}{c}\right]^2$$

suffices. But $d^2=\boldsymbol{\mu}c^2+1$, so $\mathrm{RhS}(*)>\boldsymbol{\mu}$. Hence showing $\left[\frac{\Delta-1}{\Upsilon}\right]^2\leqslant\boldsymbol{\mu}$ suffices, i.e $[\Delta-1]^2\leqslant\boldsymbol{\mu}\Upsilon^2$, i.e $\Delta^2-2\Delta+2\leqslant 1+\boldsymbol{\mu}\Upsilon^2$ suffices. But this is equivalent to $-2\Delta+2\leqslant 0$. This latter is true since $\Delta\in\mathbb{Z}_+$. ♦

14: Prop'n. *Imagine an $\mathsf{M}:=\left[\begin{smallmatrix}d&\boldsymbol{\mu}c\\c&d\end{smallmatrix}\right]\in\mathcal{U}$. Suppose*

15: $$c \;\geqslant\; 0 \;>\; c'\,,$$

where $\left[\begin{smallmatrix}d'&\boldsymbol{\mu}c'\\c'&d'\end{smallmatrix}\right] := \mathsf{S}^{-1}\cdot\mathsf{M}$. Then $\mathsf{M}=\mathbf{I}$. ♢

Proof. Whoa! 03Nov2009: This proof was empty. ♦

16: Theorem. $[\boldsymbol{\mu}\in\mathbb{Z}_+]$ *The map $f:\mathbb{Z}\to\mathcal{U}$ given by $f(n):=\mathsf{S}^n$, is a bijection.* ♢

Appendix

Which values of have $\mathcal{N}_{\boldsymbol{\mu}}$ non-empty? Although we won't give a complete answwer here, we will rule out many. Say that an integer D is 4**Neg** if $D \equiv_4 -1$; and it is 4**Pos** if $D \equiv_4 +1$.

Consider our eqn $d^2 - \boldsymbol{\mu} c^2 = -1$, but modulo a prime $p \bullet\!\!| \boldsymbol{\mu}$. This gives

17: $$d^2 \equiv_p -1\,.$$

The Legendre-symbol thm implies that (17) has a soln, d, IFF p is 4Pos or is 2.

18: Lemma. *Consider a posint $\boldsymbol{\mu}$. Then congruence*

19: $$d^2 \equiv_{\boldsymbol{\mu}} -1$$

has a soln IFF our $\boldsymbol{\mu}$ is a a product of powers of 4Pos-primes and, possibly, one copy of the prime 2. ♢

Proof. A 4Pos prime p admits a soln to (17). Now Hensel's lemma applies[♡2] to give us a solution modulo an arbitrary power, p^n.

Certainly $d^2 \equiv -1$ has a soln modulo 2 (but modulo 4, it certainly does *not*). Now the Chinese Remainder Thm allows us to stitch these congruence-solns together, ♦

Filename: `Problems/NumberTheory/pythag-triples.latex`
As of: *Tuesday 21Feb2006.* Typeset: *23Sep2017 at 15:52.*

[♡2] It is the easy non-singular case, since p is odd.