

# Pythagorean Triples

Jonathan L.F. King

University of Florida, Gainesville FL 32611-2082, USA  
squash@ufl.edu

Webpage <http://squash.1gainesville.com/>

7 August, 2018 (at 11:54)

**Entrance.** Let “ $n \equiv_4 k$ ” mean<sup>♥1</sup>  $4 \bullet \mid [n - k]$ .

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

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

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

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

$$P2: \quad \text{GCD}(a, b, c) = 1. \quad \left[ \begin{array}{l} \text{Necessarily, each pair} \\ \text{of } a, b, c \text{ is coprime,} \\ \text{courtesy (P0).} \end{array} \right]$$

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:

$$1a: \quad \begin{array}{l} c = \frac{1}{2}[y^2 + x^2]. \\ b = \frac{1}{2}[y^2 - x^2]. \\ a = yx. \end{array} \quad \begin{array}{l} \sqrt{c+b} = y. \\ \sqrt{c-b} = x. \end{array}$$

A reworking gives this corr., and its inverse:

$$1b: \quad \begin{array}{l} c = r^2 + q^2. \\ b = 2rq. \\ a = r^2 - q^2. \end{array} \quad \begin{array}{l} \sqrt{\frac{1}{2}[c+a]} = r. \\ \sqrt{\frac{1}{2}[c-a]} = q. \end{array}$$

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

**D1:**  $x, y \in \mathbb{Z}_+$ . Additionally,  $1 \leq x < y$ .

**D2:**  $x \perp y$ .

**D3:** Both  $x$  and  $y$  are odd.

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

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

**M1:**  $r, q \in \mathbb{Z}_+$ . Furthermore,  $r > q \geq 1$ .

**M2:**  $r \perp q$ .

**M3:** Integers  $q$  and  $r$  have opposite parities.

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

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

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

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

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

*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  $1 \leq x < y$ . Since  $x^2$  and  $y^2$  are each odd, and ODD  $\pm$  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  $p \bullet \mid x$ . Were  $p$  to divide  $b$ , forcing  $p \bullet \mid [y^2 - x^2]$ , then  $p \bullet \mid y^2$  and consequently  $p \bullet \mid y$ . But that contradicts that  $(x, y)$  is an 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

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

This is a contradiction. ♦

**T(·) 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

$$Y := c + b, \quad X := c - b. \quad \text{Thus,}$$

$$Y \cdot X = [c + b] \cdot [c - b] \stackrel{\text{note}}{=} c^2 - b^2 = a^2.$$

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

$$\exists: \quad x := \sqrt{X} \quad \text{and} \quad y := \sqrt{Y},$$

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, ISTEestablish that

$p$  does *not* divide  $Y$ .

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

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

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  $(\exists)$  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  $y > x \geq 1$ . Lastly,  $y$  &  $x$  are each odd, since each divides  $a$ , which is odd.  $\blacklozenge$

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

$$\text{Mixed-Pairs} \xrightarrow{\mathbf{U}} \text{Primitive Triples}. \quad \blacklozenge$$

**Pf.** Define  $f((y, x)) := (r, q)$ , where  $r := \frac{1}{2}[y + x]$  and  $q := \frac{1}{2}[y - x]$ . Reversing,  $g((r, q)) := (y, x)$ , 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 you show (exercise) that  $f(\text{odd-pair}) \in \text{Mixed-pair}$  and  $g(\text{mixed-pair}) \in \text{Odd-pair}$ .  $\blacklozenge$

**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:*

$$\begin{aligned} \dagger: & \quad a^4 + b^4 = c^4 ; \\ \ddagger: & \quad D^4 + E^4 = U^2 . \end{aligned} \quad \blacklozenge$$

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

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

**Proof.** FTSOC, suppose we have a  $(\ddagger)$  which has minimum  $U$ , over all  $(\ddagger)$ . Were there a prime with  $p \bullet D$  and  $p \bullet E$ , then  $p^2 \bullet U$ , so  $(\frac{D}{p}, \frac{E}{p}, \frac{U}{p^2})$  is a smaller  $(\ddagger)$ ;  $\otimes$ . 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  $R \perp Q$  such that

$$\begin{aligned} *1: & \quad U = R^2 + Q^2 ; \\ *2: & \quad E^2 = 2RQ ; \\ & \quad D^2 = R^2 - Q^2 . \end{aligned}$$

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

$$\pounds: \quad R \in \square \quad \text{and} \quad 2Q \in \square .$$

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

$$\begin{aligned} *3: & \quad R = r^2 + q^2 ; \\ *4: & \quad Q = 2rq ; \\ & \quad D = r^2 - q^2 . \end{aligned}$$

Our  $(\pounds)$  implies  $\exists$  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  $(\pounds)$ , 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

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

This has form  $(\ddagger)$ . Moreover,  $u \leq u^2 = R < U$  courtesy  $(*1)$ . We see to our relief that  $(**3)$  contradicts the minimality of  $U$ .  $\blacklozenge$

## Pell's Equation

What are all the Pythagorean triples

$$5: \quad a^2 + [a + 1]^2 = c^2,$$

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

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

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  $\begin{bmatrix} a_1 \\ c_1 \end{bmatrix} \odot \begin{bmatrix} a_2 \\ c_2 \end{bmatrix}$  described by this formula:

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

The group-inverse of an elt:  $\begin{bmatrix} a' \\ c' \end{bmatrix} := \begin{bmatrix} a \\ c \end{bmatrix}^{\odot -1}$  where

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

E.g.,  $\begin{bmatrix} 3 \\ 5 \end{bmatrix}^{\odot -1} = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$ .

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

$$8: \quad d^2 - 2c^2 = -1.$$

This is special case of what the “*generalized Pell's eqn* with *Pell coefficient*  $\mu$ ”:

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

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

Just “Pell's eqn” shall mean the  $\tau=1$  case:

$$\varepsilon_{\mu}: \quad d^2 - \mu c^2 = 1.$$

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

We will find all *consecutive pythag-triples* by solving (8), which we will get from the soln set of  $(\varepsilon_2)$ .

### Group structure

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

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

$$\mathbf{M} := \mathbf{M}_{d,c} := d\mathbf{I} + c\mathbf{J} = \begin{bmatrix} d & \mu c \\ c & d \end{bmatrix} \quad \text{(always with letters “d” and “c”).}$$

The set

$$\mathcal{L} := \left\{ \mathbf{M}_{d,c} \mid d, c \in \mathbb{Z} \right\}$$

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

9:  $(\mathcal{L}, \cdot, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix})$  is a commutative semi-group.

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

$$\mathcal{G} := \left\{ \mathbf{M} \in \mathcal{L} \mid \text{Det}(\mathbf{M}) \in \{1, -1\} \right\},$$

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

$$10: \quad \begin{aligned} \mathbf{M}^{-1} &= \frac{1}{\text{Det}(\mathbf{M})} \begin{bmatrix} d & -\mu c \\ -c & d \end{bmatrix} \stackrel{\text{note}}{=} \widehat{d}\mathbf{I} + \widehat{c}\mathbf{J}, \text{ where} \\ \widehat{d} &:= \frac{d}{\text{Det}(\mathbf{M})} \quad \text{and} \quad \widehat{c} := \frac{-c}{\text{Det}(\mathbf{M})}. \end{aligned}$$

Note  $\hat{d}$  and  $\hat{c}$  are integers, since  $\text{Det}(\mathbf{M}) = \pm 1$ .

Define two sets by the condition above them

$$\mathcal{G} = \begin{matrix} \text{Det}(\mathbf{M})=+1 \\ \mathcal{P} \end{matrix} \sqcup \begin{matrix} \text{Det}(\mathbf{M})=-1 \\ \mathcal{N} \end{matrix}.$$

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

$$\mathcal{P} := \text{Det}^{-1}(\{1\}).$$

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

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

*Proof.* Fix a matrix  $\mathbf{N}_\mu \in \mathcal{N}_\mu$ . For each  $\mathbf{M} \in \mathcal{N}_\mu$ , note that  $\mathbf{M} \cdot \mathbf{N}_\mu \stackrel{\text{Det}}{=} [-1]^2 = 1$ . I.e,  $\mathbf{MN}_\mu \in \mathcal{P}$ .  $\blacklozenge$

*Remark.* When  $\mu = 2$ : Matrix  $\mathbf{N}_2 := \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$  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  $\mu$  have  $\mathcal{N}_\mu = \emptyset$ ; see the **Appendix**.  $\square$

### Henceforth $\mu$ is a posint

**Upper-lefthand entry.** Define two sets

$$\mathcal{U} = \begin{matrix} d > 0 \\ \mathcal{U} \end{matrix} \sqcup \begin{matrix} d < 0 \\ \mathcal{U}^- \end{matrix};$$

this  $\mathcal{U}$  is the set of  $\begin{bmatrix} d & \mu c \\ c & d \end{bmatrix}$  with  $d > 0$ .

**12: Lem.**  $[\mu \in \mathbb{Z}_+]$   $(\mathcal{U}, \cdot, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix})$  is a group.  $\diamond$

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

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

$$\begin{bmatrix} \alpha & \mu\beta \\ \beta & \alpha \end{bmatrix} \cdot \begin{bmatrix} d & \mu c \\ c & d \end{bmatrix} = \begin{bmatrix} \alpha d + \mu\beta c & ? \\ \alpha c + \beta d & ? \end{bmatrix};$$

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

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

Now  $\mu \geq 0$ , so the RhSes are non-negative; hence

$$*2: \quad |\alpha d|^2 > |\mu\beta c|^2.$$

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

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

$$\mathbf{S} = \mathbf{S}_\mu := \begin{bmatrix} \Delta & \mu\Upsilon \\ \Upsilon & \Delta \end{bmatrix}$$

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

As an example,  $\mathbf{S}_2 = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}$ .

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

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

is strictly increasing.  $\diamond$

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

$$\begin{aligned} \begin{bmatrix} d' & \mu c' \\ c' & d' \end{bmatrix} &:= \mathbf{S}^{-1} \cdot \mathbf{M} = \begin{bmatrix} \Delta & -\mu\Upsilon \\ -\Upsilon & \Delta \end{bmatrix} \cdot \begin{bmatrix} d & \mu c \\ c & d \end{bmatrix} \\ &= \begin{bmatrix} \Delta c - \mu\Upsilon d & ? \\ \Delta c - \Upsilon d & ? \end{bmatrix}. \end{aligned}$$

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  $\Delta - 1 \geq 0$ ), and so our goal becomes  $\frac{\Delta - 1}{\Upsilon} < \frac{d}{c}$ . Its LhS  $\geq 0$ , so establishing

$$*: \quad \left[ \frac{\Delta - 1}{\Upsilon} \right]^2 < \left[ \frac{d}{c} \right]^2$$

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

**14: Prop'n.** Imagine an  $\mathbf{M} := \begin{bmatrix} d & \mu c \\ c & d \end{bmatrix} \in \mathcal{U}$ . Suppose

$$15: \quad c \geq 0 > c',$$

where  $\begin{bmatrix} d' & \mu c' \\ c' & d' \end{bmatrix} := \mathbf{S}^{-1} \cdot \mathbf{M}$ . Then  $\mathbf{M} = \mathbf{I}$ .  $\diamond$

*Proof.* Whoa! 03Nov2009: This proof was empty.  $\blacklozenge$

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

## Appendix

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

Consider our eqn  $d^2 - \mu c^2 = -1$ , but modulo a prime  $p \nmid \mu$ . This gives

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

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

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

$$19: \quad d^2 \equiv_\mu -1$$

*has a soln IFF our  $\mu$  is a product of powers of **4POS**-primes and, possibly, one copy of the prime 2.  $\diamond$*

**Proof.** A **4POS** prime  $p$  admits a soln to (17). Now Hensel's lemma applies<sup>♥2</sup> 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,  $\blacklozenge$

Filename: Problems/NumberTheory/pythag-triples.tex  
As of: Tuesday 21Feb2006. Typeset: 7Aug2018 at 11:54.

---

<sup>♥2</sup>It is the easy non-singular case, since  $p$  is odd.