Sums of Two Squares and Four Squares

Jonathan L.F. King, squash@ufl.edu

9 August, 2018 (at *11:23*)

A lemma from LBolt

To compute $G{:=}\mathrm{GCD}(73,27)$ and Bézout multipliers S,T st. $G = S{\cdot}73 + T{\cdot}27$, a particular tabular way of laying out the Euclidean Algorithm I call the ***lightning bolt*** or ***LBolt*** table, because the update rule can be drawn so as to resemble a lightning bolt.

n	r_n	q_n	s_n	t_n
0	73	**—**	**1**	**0**
1	27		**0**	**1**
2				

Stage 1 is shown above. At stage n, we compute remainder r_{n+1} and quotient q_n so that

1.1: $$r_{n+1} \;=\; r_{n-1} - \mathsf{q}_n r_n$$

In (1.1), replace "r" by "s" to compute s_{n+1}. Then replace "r" by "t" to compute t_{n+1}. Inductively,

1.2: $$r_n \;=\; 73 s_n + 27 t_n$$

for each n. Continue until some $r_{L+1} = 0$; then r_L is G. Hence $S := s_L$ and $T := t_L$ are particular ***Bézout multipliers***, satisfying $G = 73S + 27T$, a linear combination. Below, L equals 6.

1.3:

n	r_n	q_n	s_n	t_n
0	73	**—**	1	0
1	27	2	0	1
2	19	1	1	−2
3	8	2	−1	3
4	3	2	3	−8
5	2	1	−7	19
6	*1*	*2*	*10*	*−27*
7	0	∞	−27	73

Now this particular example has a further property: Value 27 is a 73-rono.

Summing squares. Fix a posint modulus $\mathcal{T}$ and an $\mathcal{T}$-rono $\mathcal{R}$. Let $\equiv$ mean $\equiv_{\mathcal{T}}$. Construct the LBolt

1.4:

n	r_n	q_n	s_n	t_n
0	$\mathcal{T}$	**—**	**1**	**0**
1	$\mathcal{R}$		**0**	**1**

Ignoring the $\vec{\mathbf{s}}$ column for the time being, note, for $n = 0,1$, that $[r_n]^2 + [t_n]^2$ is divisible by $\mathcal{T}$.

1.5: LBolt-SOTs Lemma. *Complete the* $(\mathcal{T},\mathcal{R})$*-LBolt started in (1.4), where* $\mathcal{R}$ *is a* $\mathcal{T}$*-rono. Define row vector* $\mathsf{A}_n := \begin{bmatrix} r_n & t_n \end{bmatrix}$*. Then for* $n = 0,1,2,\ldots$

$$\dagger_n\textbf{:} \qquad [r_n]^2 + [t_n]^2 \;\equiv\; 0 \quad \textit{and}$$
$$\ddagger_n\textbf{:} \qquad r_n r_{n+1} + t_n t_{n+1} \;\equiv\; 0\,.$$

[Moreover, the $\vec{\mathbf{t}}$*-column is, up to sign, the* $\vec{\mathbf{r}}$*-column upside down, as illustrated in the (1.3) table.]* ◊

Pf. Easily, $(\dagger_0, \ddagger_0, \dagger_1)$.

Since $r_{n+1} = r_{n-1} - \mathsf{q}_n r_n$ ditto t_{n+1}. Squaring,

$$\begin{aligned}[r_{n+1}]^2 + [t_{n+1}]^2 \;=\;& \Big[r_{n-1}^2 + t_{n-1}^2\Big] \\ &- 2\Big[r_{n-1}r_n + t_{n-1}t_n\Big]\mathsf{q}_n \\ &+ \Big[r_n^2 + t_n^2\Big]\mathsf{q}_n^2\,.\end{aligned}$$

And RhS $\equiv 0$, as each bracketed-sum is $\equiv 0$, courtesy $(\dagger_{n-1}, \ddagger_{n-1}, \dagger_n)$. Hence $(\dagger_{n+1})$.

Note $r_n r_{n+1} = r_n\big[r_{n-1} - \mathsf{q}_n r_n\big] = r_{n-1}r_n - r_n^2{\cdot}\mathsf{q}_n$. Thus $r_n r_{n+1} + t_n t_{n+1}$ equals

$$\mathrm{LhS}(\ddagger_{n-1}) - \mathrm{LhS}(\dagger_n){\cdot}\mathsf{q}_n\,,$$

which is $\equiv 0$. Hence $(\ddagger_n)$. ♦

Whoa! Need to type the argument that [using symmetric remainders in LBolt] when first $|r_n| < \sqrt{\mathcal{T}}$, then (r_n, t_n) is a SOTS decomp of $\mathcal{T}$.

RONO: Root-Of-Negative-One

W.r.t a posint $\mathcal{T}$, an integer $\mathcal{R}$ is an ***$\mathcal{T}$-rono***, a "(square) Root Of Negative One", if

$$\mathcal{R}^2 \;\equiv_{\mathcal{T}}\; {-1}\,.$$

Say that $\mathcal{T}$ is ***rono-ish*** if $\mathcal{T}$ is a posint that has a rono. I.e, 13 is rono-ish since $5^2 = 25 \equiv_{13} -1$.

2: Prop'n. *A posint* $\mathcal{T}$ *has a rono IFF* $\mathcal{T}$ *has form* B *or* $2B$*, where* B *is a product of* 4Pos *primes.* ◊

Pf of $(\Rightarrow)$. A $\mathcal{T}$-rono $\mathcal{R}$ is a rono w.r.t each factor of $\mathcal{T}$. But 4 has no rono, so can't be a factor of $\mathcal{T}$. And each 4NEG prime has no rono, courtesy LSThm.[♡1] ♦

Pf of $(\Leftarrow)$. If $J_1 \perp J_2$ are each rono-ish, then the product $J_1 \cdot J_2$ has a rono, thanks to CRThm. Since 2 is rono-ish, we only need prove:

2a: *Suppose* P *is a* 4POS *prime. For each natnum* $\mathbf{k}$, *then,* $M := \mathsf{P}^{\mathbf{k}}$ *has a rono.*

WLOG, $\mathbf{k} \geqslant 1$. Courtesy the Primitive-root Theorem,[♡2] the group $(\Phi(M), \cdot, 1)$ is *cyclic*. It has order

$$\varphi(M) \;=\; \mathsf{P}^{\mathbf{k}-1} \cdot [\mathsf{P}-1] \;=:\; \mathcal{T}.$$

Letting g be an M-primroot, we have that $g^{\mathcal{T}/2}$ equals -1. And $\mathcal{T}$ is divisible by 4 (since $\mathsf{P}-1$ is) so negative 1 has sqroots; namely, $g^{\pm\mathcal{T}/4}$. ♦

Sums of Two Squares

A posint T is a ***SOTS*** if there exist $x, y \in \mathbb{Z}$ with

$$*: \qquad x^2 + y^2 \;=\; T.$$

Write $(x,y) \rightsquigarrow T$ to indicate $(*)$ <u>and</u> that T is a posint. To indicate this *and* that $x \perp y$, write

$$(x,y) \overset{\perp}{\rightsquigarrow} T.$$

Some pair in (T, x, y) is coprime IFF *every* pair is. Call T ***coprime-SOTS*** or just ***cop-SOTS*** if <u>*there exists*</u> a pair $(x,y) \overset{\perp}{\rightsquigarrow} T$. Finally, T is ***strictly cop-SOTS*** if T is SOTS and *every* SOTS decomposition $T = x^2 + y^2$ has $x \perp y$.

Note that 8 is SOTS $[8 = 4+4]$, but not cop-SOTS. In contrast, 25 is cop-SOTS $[25 = 9+16]$ but *not* **strictly** cop-SOTS, since $25 = 0^2 + 5^2$. Finally, $13 = 4 + 9$ is *strictly* cop-SOTS, since that is its only SOTS decomposition.

[♡1] The Legendre-Symbol Thm. Use CRT for the Chinese Remainder Thm. An integer N is ***4Pos*** if $N \equiv_4 +1$. And N is ***4Neg*** if $N \equiv_4 -1$.

[♡2] Alternatively, thm (10‡) shows the existence of an M-rono.

3: Fermat SOTS-prime Thm. *Prime* P *is SOTS IFF* $\mathsf{P} = 2$ *or* $\mathsf{P} \equiv_4 1$. *Then,* P *has but one SOTS decomposition; further, it is a coprime-SOTS decomp.* ◊

Set up. Below we fix a 4POS prime P and give two proofs that it is SOTS. Each uses a P-rono $\mathcal{R}$, and

$$\mathsf{S} \;<\; \sqrt{\mathsf{P}} \;<\; \mathsf{S}+1$$

where $\mathsf{S} := \lfloor \sqrt{\mathsf{P}} \rfloor$. Let $\equiv$ mean $\equiv_{\mathsf{P}}$. □

First Proof. We will show that the integer M in (3a), below, is 1, by establishing that $0 < M < 2$.

The number of pairs in $[0 \,..\, \mathsf{S}]^{\times 2}$ is $[\mathsf{S}+1]^2$. This exceeds P, so there exist (Pigeon-hole principle) two distinct pairs $(a,b) \neq (\alpha, \beta)$ such that

$$a + \mathcal{R}b \;\equiv_{\mathsf{P}}\; \alpha + \mathcal{R}\beta.$$

So $\boxed{x \equiv \mathcal{R}y}$, where $x := a - \alpha$ and $y := \beta - b$. Hence

$$x^2 + y^2 \;\equiv\; [-1 + 1] \cdot y^2 \;\equiv\; 0.$$

So there is a "multiplier" $M \in \mathbb{Z}$ with

$$3a: \qquad x^2 + y^2 \;=\; M \cdot \mathsf{P}.$$

Not both x and y are zero (since the pairs were distinct), so $M \geqslant 1$. And $x^2 + y^2 \leqslant 2 \cdot \mathsf{S}^2 < 2\mathsf{P}$, so $M < 2$. ♦

3b: *Question.* Where did the above proof use that P is prime? □

Second Proof. We can view $(\mathbb{Z}_{\mathsf{P}}, +, 1)$ as a discrete circle. On it, define "circular distance"

$$\mathsf{d}(b,c) \;:=\; \left|\langle b - c \rangle\right|, \qquad \text{where } \langle\cdot\rangle \text{ means } \textbf{symmetric} \text{ residue.}$$

Since $\mathcal{R} \perp \mathsf{P}$, the $\mathsf{S}+1$ points $t\mathcal{R} \in \mathbb{Z}_{\mathsf{P}}$, for $t \in [0 \,..\, \mathsf{S}]$, are distinct. Measuring from each point "clockwise" around the circle to the next, the average distance to the (spatially) next point is

$$\frac{\mathsf{P}}{\mathsf{S}+1} \;\overset{\text{note}}{<}\; \sqrt{\mathsf{P}}.$$

Thus there are distinct points whose distance (Why?) is $\leqslant \mathsf{S}$. I.e, there are indices $0 \leqslant i < j \leqslant \mathsf{S}$, with

$$\mathsf{S} \geqslant \mathsf{d}(j\mathcal{R}, i\mathcal{R}) = \langle k\mathcal{R}\rangle =: x\,, \quad \text{where } k := j-i, \text{ and therefore } k \in [1 \,..\, \mathsf{S}].$$

Consequently, $0 < x^2 + k^2 \leqslant 2{\cdot}\mathsf{S}^2 < 2\mathsf{P}$. And, as above, $x^2 + k^2 \equiv -k^2 + k^2 = 0$. ♦

Melding. Is SOTS sealed under multiplication? If

4a: $$[\alpha^2 + \beta^2] \cdot [x^2 + y^2] = \mu^2 + \nu^2\,,$$

where we have integer-valued formulas for μ and ν, then *"Yes!"*. And indeed, these definitions work:

4b: $$\mu := \alpha x - \beta y \quad \text{and} \\ \nu := \beta x + \alpha y\,.$$

We have ***melded*** (α, β) with (x, y), getting new pair (μ, ν). That is,

$$\mathrm{Meld}\big((\alpha,\beta),(x,y)\big) =: (\mu,\nu)\,, \quad \textit{defined in } (4b).$$

Motivation?: Multiplying scaled rotation-matrices,

4c: $$\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \begin{bmatrix} x & -y \\ y & x \end{bmatrix} = \begin{bmatrix} \mu & -\nu \\ \nu & \mu \end{bmatrix},$$

certainly gives another scaled rotation-matrix. Using (4c) to *define* μ and ν, gives (4b). And taking determinants in (4c), hands us (4a). [Equivalently, view (α, β) as complex number $\alpha + \beta\boldsymbol{i}$, then multiply.]

Melding is sometimes conveniently written as an infix operator:

$$(\alpha,\beta)\,\mathcal{M}\,(x,y) := \mathrm{Meld}\big((\alpha,\beta),(x,y)\big)\,.$$

Easily, operator $\mathcal{M}$ is commutative and associative.

Full meld. To ***normalize*** an intpair (α, β) means:

> *Replace α by $|\alpha|$ and β by $|\beta|$. Then, if need be, exchange α, β so that now $\alpha \leqslant \beta$.*

For example, the normalized version of $(-6, 5)$ and of $(-5, -6)$, is $(5, 6)$.

Define the ***full meld*** of pairs to be

4d: $$(\alpha,\beta)\,\mathcal{F}\,(x,y) := \mathrm{Nrmlize}\Big((\alpha,\beta)\,\mathcal{M}\,(x,y)\Big).$$

E.g, $$(2,1)\,\mathcal{M}\,(-3,4) = (-10,\,5)\,, \quad \textit{but} \\ (2,1)\,\mathcal{F}\,(-3,4) = (5,\;10)\,.$$

Easily, $\mathcal{F}$ is commutative. Exer 4d: Prove or CEX: *Operatorname $\mathcal{F}$ is associative.*

Pf of Uniqueness of prime-SOTS. [Use $\equiv$ for $\equiv_{\mathsf{P}}$, and $\langle\cdot\rangle$ for $\langle\cdot\rangle_{\mathsf{P}}$.] WLOG P is odd. Consider two decompositions

$$**: \qquad \alpha^2+\beta^2 \;=\; \mathsf{P} \;=\; x^2+y^2\,,$$
$$*: \qquad \textit{with}\;\; \alpha,\beta,x,y \in [1\,..\sqrt{\mathsf{P}}\,)\,.$$

Taking $(**)$ mod-P implies $\langle\alpha/\beta\rangle^2 \equiv$ -1. In particular, $\langle\alpha/\beta\rangle$ does not equal its own reciprocal, so $\langle\beta/\alpha\rangle$ is the *other* [P is prime] sqroot of -1. Also $\langle x/y\rangle$ and $\langle y/x\rangle$ are the two sqroots of -1. So WLOG, $\langle x/y\rangle = \langle\beta/\alpha\rangle$. I.e,

$$\mu \;:=\; \alpha x - \beta y \;\equiv\; 0\,.$$

Our $(*)$ implies $0 < \alpha x < \mathsf{P}$. Thus $-\mathsf{P}<\mu<\mathsf{P}$, so $\mu = 0$. Thus $\alpha x = \beta y$.

Melding the two SOTS decompositions $(**)$, by letting $\nu := \beta x + \alpha y$, says that

$$\mathsf{P}^2 \;=\; \mu^2+\nu^2 \stackrel{\text{note}}{=\!=} \nu^2\,,$$

so $\nu = \mathsf{P}$, since they're both positive. Thus

$$\dagger: \qquad \alpha x \;=\; \beta y \quad \textit{and}$$
$$\ddagger: \qquad \mathsf{P} \;=\; \beta x + \alpha y\,.$$

Consider a prime $q \bullet| \alpha$, and write $q^n \bullet\| \alpha$. If q^n *fails* to divide y, then $q \bullet| \beta$, so $q \bullet| \mathsf{P}$, hence $q = \mathsf{P}$. But $x,y \geqslant 1$ forces ※, since $\text{RhS}(\ddagger) \geqslant 2\mathsf{P}$. Hence $q^n \bullet| y$.

This applies to *every* prime dividing α; thus $\alpha \bullet| y$. This argument applies in reverse, hence $\alpha \,|\!\bullet\, y$. Thus $\alpha = y$, since both are positive. Consequently, the two decompositions are the same. ♦

5: Fermat SOTS Thm. *A posint T is SOTS IFF: Every* 4NEG *prime $\mathsf{P} \bullet| T$ occurs to an even power in T.* ◊

Pf of ($\Leftarrow$).

Pf of ($\Rightarrow$).

The Setting for coprime-SOTS

We prove several lemmas with a common setting. We have posints Ω and T as well as integers

$$\text{S1:} \qquad \begin{aligned} \alpha^2+\beta^2 \;&=\; \Omega\,; \\ x^2+y^2 \;&=\; T\,; \\ (\mu,\nu) \;&:=\; \text{Meld}((\alpha,\beta),(x,y))\,; \\ (m,n) \;&:=\; \text{Meld}((\beta,\alpha),(x,y))\,. \end{aligned}$$

6: Lemma. *Consider (S1), and a prime P which divides $\text{GCD}(\mu,\nu)$. Then*

$$\dagger: \quad \mathsf{P} \bullet| \quad [\quad \Omega \quad \textit{or}\; \text{GCD}(x,y)]\,, \qquad \textbf{\textit{and}}$$
$$\ddagger: \quad \mathsf{P} \bullet| \quad [\text{GCD}(\alpha,\beta)\;\textit{or}\quad T \quad]\,. \qquad \Diamond$$

Proof. Well, P divides $\mu\alpha+\nu\beta$, which by (S1) equals

$$\alpha x\alpha + \beta x\beta \;=\; [\alpha^2+\beta^2]\cdot x\,.$$

I.e, $\mathsf{P} \bullet| \Omega x$. By symmetry, $\mathsf{P} \bullet| \Omega y$. So if $\mathsf{P} \nmid \Omega$, then P divides **both** x and y.

We have established (6†). Symmetry gives (6‡). ♦

7: Corollary. *Suppose $(\alpha,\beta) \stackrel{\perp}{\rightsquigarrow} \Omega$ and $(x,y) \stackrel{\perp}{\rightsquigarrow} T$. If $\Omega \perp T$, then*

$$\text{Meld}((\alpha,\beta),(x,y)) \;\stackrel{\perp}{\rightsquigarrow}\; \Omega T\,. \qquad \Diamond$$

8: Both-melds Lemma. *Assume (S1), and that some oddprime P divides each of μ,ν,m,n. Then:*

$$9: \quad \textit{Either}\;\; \mathsf{P} \bullet| \text{GCD}(\alpha,\beta) \;\; \underline{\textit{or}} \;\; \mathsf{P} \bullet| \text{GCD}(x,y)\,. \qquad \Diamond$$

Pf. By hyp., $\mathsf{P} \bullet| [\mu^2+\nu^2] \stackrel{\text{note}}{=\!=} \Omega T$. I.e, $\mathsf{P} \bullet| \Omega T$. Note

$$4b': \qquad \begin{aligned} m \;&=\; \beta x - \alpha y \quad \text{and} \\ n \;&=\; \alpha x + \beta y\,. \end{aligned}$$

And P divides $\nu^2+n^2 \stackrel{\text{note}}{=\!=} [\Omega T] + 4\alpha\beta xy$. But $\mathsf{P} \neq 2$, so $\mathsf{P} \bullet| \alpha\beta xy$. Courtesy $(*)$, then, WLOG

$$\mathsf{P} \bullet| \alpha\,.$$

So to establish (9), WLOG $\mathsf{P} \nmid \beta$. Now (6‡) gives us

$$\mathsf{P} \bullet| T\,.$$

And $T = x^2 + y^2$. So **if** we can prove that

Goal: $$\mathsf{P} \bullet\!\!| \; x,$$

then necessarily $\mathsf{P} \bullet\!\!| \; y$. Now (9) will follow.

By hypothesis, P divides ν and m. Consequently, P divides $\nu^2 + m^2 \overset{\text{note}}{=\!=} 2[\beta^2 x^2 + \alpha^2 y^2]$. Therefore,

$$\mathsf{P} \bullet\!\!| \; [\beta^2 x^2 + \alpha^2 y^2].$$

This, together with $\mathsf{P} \bullet\!\!| \; \alpha$, produces $\boxed{\mathsf{P} \bullet\!\!| \; \beta x}$. But $\mathsf{P} \nmid \beta$. Thus (*Goal*). ♦

Application. For an oddprime P, we like to know that each power, $\mathsf{P}^{\mathbf{k}}$, is coprime-SOTS. We get this by inducting[♡3] on $\mathbf{k}$, using the next theorem. It says, given a couple of coprime-SOTS decomps, that at least *one* of their two melds will be a coprime-SOTS decomposition. □

10: Good-meld Thm. *Suppose*

$*$: $$(\alpha,\beta) \overset{\perp}{\rightsquigarrow} \Omega \quad \text{and} \quad (x,y) \overset{\perp}{\rightsquigarrow} T,$$

where Ω and T are powers of an oddprime P. Then

10†: *At least one of* $\mathrm{Meld}((\alpha,\beta),(x,y))$ *and* $\mathrm{Meld}((\beta,\alpha),(x,y))$ *is a coprime-SOTS decomposition of ΩT.*

Consequently, by inducting on the below $\mathbf{k}$*,*

10‡: *For each prime $\mathsf{P} \equiv_4 1$ and each natnum $\mathbf{k}$, the power $\mathsf{P}^{\mathbf{k}}$ is coprime-SOTS.* ◊

Proof. Since Ω and T are powers-of-P, the only way both melds could fail is if P divides each of μ, ν, m, n. But (9) contradicts ($*$).

As for (10‡), use (3) for the $\mathbf{k}$=1 case. And use (10†) for the induction on $\mathbf{k}$. ♦

[♡3] Indeed, given a SOTS-decomposition of P, we can use the repeated-squaring technique to produce a coprime SOTS-decomp of $\mathsf{P}^{\text{Large}}$. However, since we are not reducing mod-something, this only changes a cubic-alg into a quadratic-algorithm.

Sums of FOUR squares

4Square Notation. Below, a ***tuple*** $\mathbf{x}$ means the 4-tuple (x_1, x_2, x_3, x_4) of *integers*. Use $[\![\mathbf{x}]\!]^2$ for the sum $\sum_{j=1}^{4} [x_j]^2$. □

11: Prop'n. *For oddprime* P*, there exists tuple* $\mathbf{x}$ *and "multiplier"* $M \in [1 .. \mathsf{P})$ *st.* $[\![\mathbf{x}]\!]^2 = M\mathsf{P}$. ◇

Prelim. Let NQR and QR mean mod-P, use $\equiv$ for $\equiv_{\mathsf{P}}$, and let $H := \frac{\mathsf{P}-1}{2}$. □

Pf. Since each 4Pos P is SOTS, WLOGenerality $\mathsf{P} \in$ 4Neg. Take $\beta \in \mathbb{Z}_+$ **smallest** st. $\beta \in$ NQR; thus $\beta \geqslant 2$. Since $-1 \in$ NQR, it follows that $-\beta \in$ QR; so there exists $x \in [1 .. H]$ with $x^2 \equiv -\beta$.

Recall $\beta - 1 \geqslant 1$; thus $\beta - 1 \in$ QR, since β was the *smallest* non-QR. So $\exists y \in [1 .. H]$ with $y^2 \equiv \beta - 1$. Summing,

$$0 < 1 + x^2 + y^2 < 1 + [\tfrac{\mathsf{P}}{2}]^2 + [\tfrac{\mathsf{P}}{2}]^2 < 1 + [\mathsf{P}^2/2] < \mathsf{P}^2 .$$

OTOHand, $1 + x^2 + y^2 \equiv 1 + -\beta + [\beta - 1] = 0$. Consequently, $1 + x^2 + y^2$ equals $M\mathsf{P}$ for some *posint* $M < \mathsf{P}$. And $1 + x^2 + y^2$ is a sum of three [hence four] squares. ♦

12: Euler's four-square identity. *Suppose* $\boldsymbol{\beta}$ *and* $\mathbf{x}$ *are tuples. Then this* $\mathbf{y}$

$$\text{12a:}\quad \begin{aligned} y_1 &:= \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 \\ y_2 &:= -\beta_1 x_2 + \beta_2 x_1 - \beta_3 x_4 + \beta_4 x_3 \\ y_3 &:= -\beta_1 x_3 + \beta_3 x_1 + \beta_2 x_4 - \beta_4 x_2 \\ y_4 &:= -\beta_1 x_4 + \beta_4 x_1 - \beta_2 x_3 + \beta_3 x_2 \end{aligned}$$

is a tuple for which $[\![\mathbf{y}]\!]^2 = [\![\boldsymbol{\beta}]\!]^2 \cdot [\![\mathbf{x}]\!]^2$.

Now suppose M *is a posint st.* $\beta_j \equiv_M x_j$ *for* <u>*all*</u> j. *Then each of* y_2, y_3, y_4 *is* $\equiv_M 0$. ◇

Proof. Verifying $[\![\mathbf{y}]\!]^2 = [\![\boldsymbol{\beta}]\!]^2 \cdot [\![\mathbf{x}]\!]^2$ can be done tediously, or by using the norm on the Quaternions.

As for looking mod M, note that the sum of the first two terms of y_2 is mod-M congruent to

$$-x_1 x_2 + x_2 x_1 \equiv_M 0 ;$$

ditto the last two terms. And ditto for y_3 and y_4. ♦

Defn. Write the $\mathbf{y}$ from (12a) as $\mathbf{y} = \text{BigMeld}(\boldsymbol{\beta}, \mathbf{x})$. □

13: 4Square Thm (Lagrange). *Each natnum* $\mathcal{T}$ *is a sum of 4 squares.* ◇

Reduction. By factoring $\mathcal{T}$ into primes, write each prime as a 4Sqr, then BigMeld the decompositions. So WLOG $\mathcal{T}$ is prime. Since 2 and 4Pos are SOTS –and SOTS is 4Sqr– WLOG $\mathcal{T}$ is a 4Neg prime. □

Proof: 4Neg prime P *is 4Sqr.* From (11), take $\mathbf{x}$ and M with $[\![\mathbf{x}]\!]^2 = M\mathsf{P}$. WLOG $M \geqslant 2$. An Infinite Descent argument will give us our thm, <u>*if*</u> we can produce a new tuple $\mathbf{z}$ and multiplier $K \in [1 .. M)$ such that $[\![\mathbf{z}]\!]^2 = K\mathsf{P}$.

$\boxed{\text{Case: } M \text{ is even}}$ Since $M\mathsf{P}$ is even, the number of odd entries in $\mathbf{x}$ must be even. So WLOG $x_1 \equiv_2 x_2$ and $x_3 \equiv_2 x_4$. Thus these are integers:

$$\begin{aligned} z_1 &:= \tfrac{1}{2}[x_1 + x_2] , & z_3 &:= \tfrac{1}{2}[x_3 + x_4] , \\ z_2 &:= \tfrac{1}{2}[x_1 - x_2] , & z_4 &:= \tfrac{1}{2}[x_3 - x_4] . \end{aligned}$$

Due to cancelling of cross-terms, $[\![\mathbf{z}]\!]^2 = \frac{1}{2}[\![\mathbf{x}]\!]^2 = \frac{M}{2}\mathsf{P}$.

$\boxed{\text{Case: } M \text{ is odd}}$ Thus $M \geqslant 3$. Taking **symmetric**-residues mod-M, let $\beta_j := \langle x_j \rangle_M$ and thus define a tuple $\boldsymbol{\beta}$. Evidently

$$[\![\boldsymbol{\beta}]\!]^2 \equiv_M [\![\mathbf{x}]\!]^2 \equiv_M 0 ,$$

so there is a natnum K with $[\![\boldsymbol{\beta}]\!]^2 = KM$.

Could each β_j be zero? Well, if M divided each x_j, then $M^2 \bullet\!| \, [\![\mathbf{x}]\!]^2 = M\mathsf{P}$. So $M \bullet\!| \, \mathsf{P}$, contradicting that $M \in [2 .. \mathsf{P})$. Thus $\boxed{K \geqslant 1}$. To show that $\boxed{K < M}$, note we have *strict* inequality $|\beta_j| < \frac{M}{2}$, since M is odd. Thus

$$[\![\boldsymbol{\beta}]\!]^2 < 4 \cdot \tfrac{M^2}{4} = M \cdot M .$$

So our task is to produce a tuple $\mathbf{z}$ st. $[\![\mathbf{z}]\!]^2 = K\mathsf{P}$.

BigMelding. Define $\mathbf{y}$ by (12a). Courtesy (12), each of y_2, y_3, y_4 is $\equiv_M 0$. And

$$y_1 \equiv_M [\![\mathbf{x}]\!]^2 = M\mathsf{P} \equiv_M 0 .$$

Thus $\mathbf{z} := \frac{1}{M}\mathbf{y}$ is an integer-tuple. Moreover

$$\begin{aligned} [\![\mathbf{z}]\!]^2 &= \tfrac{1}{M^2} \cdot [\![\boldsymbol{\beta}]\!]^2 \cdot [\![\mathbf{x}]\!]^2 \\ &= \tfrac{1}{M^2} \cdot KM \cdot M\mathsf{P} = K\mathsf{P} . \end{aligned}$$

Now ain't that Nifty! ♦

SOTS to Dirichlet

Krishna Alladi and George Andrews sketched to me (over coffee) a proof of a special case of Dirichlet's theorem on Arithmetic Progressions. It shows that $\mathcal{P} := 4\mathbb{Z} + 1$ has ∞ly many primes. (They don't know the author of the proof.) The tool we need is

14: *Fix a SOTS N, and let q be the product of all the 4*NEG *primes (with multiplicity) that divide N. Then q is a perfect square.*

I.e, each 4NEG prime dividing a SOTS must divide it to an even power.

Producing a new 4POS prime. Given a finite multiset S of 4POS primes, we will produce a new 4POS prime. Define

$$\begin{aligned} \sigma &:= \prod(S) \quad \text{and} \\ N &:= 1^2 + [2\sigma]^2 \;=\; 1 + 4\sigma^2 \,. \end{aligned}$$

Every divisor of σ is coprime to N, so ISTShow that N *has* a 4POS prime-divisor. FTSOC, suppose every prime-divisor of N is 4NEG. By (14), then, N is a perfect square. Hence N and $4\sigma^2$ are squares differing by 1. But the the only such pair is $(1, 0)$. Yet $4\sigma^2$ is not zero, since $\sigma \geqslant \prod(\varnothing) = 1$, so $4\sigma^2 \geqslant 4$. ♦