

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 $G := \text{GCD}(73, 27)$ 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

$$1.1: \quad r_{n+1} = r_{n-1} - q_n r_n$$

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

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

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.

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

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

Ignoring the \vec{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 $\mathbf{A}_n := [r_n \ t_n]$. Then for $n = 0, 1, 2, \dots$

$$\begin{aligned} \dagger_n: \quad & [r_n]^2 + [t_n]^2 \equiv 0 \quad \text{and} \\ \ddagger_n: \quad & r_n r_{n+1} + t_n t_{n+1} \equiv 0. \end{aligned}$$

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

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

Since $r_{n+1} = r_{n-1} - q_n r_n$ ditto t_{n+1} . Squaring,

$$\begin{aligned} [r_{n+1}]^2 + [t_{n+1}]^2 &= [r_{n-1}^2 + t_{n-1}^2] \\ &\quad - 2[r_{n-1}r_n + t_{n-1}t_n]q_n \\ &\quad + [r_n^2 + t_n^2]q_n^2. \end{aligned}$$

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 $r_n r_{n+1} = r_n [r_{n-1} - q_n r_n] = r_{n-1} r_n - r_n^2 q_n$. Thus $r_n r_{n+1} + t_n t_{n+1}$ equals

$$\text{LhS}(\ddagger_{n-1}) - \text{LhS}(\dagger_n) \cdot q_n,$$

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

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. \diamond

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 k , then, $M := P^k$ has a rono.

WLOG, $k \geq 1$. Courtesy the Primitive-root Theorem,^{♥2} the group $(\Phi(M), \cdot, 1)$ is *cyclic*. It has order

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

Letting g be an M -primroot, we have that $g^{\mathcal{T}/2}$ equals -1 . And \mathcal{T} is divisible by 4 (since $P-1$ 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

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

Write $(x, y) \rightsquigarrow T$ to indicate $(*)$ and 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 there exists 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 $P = 2$ or $P \equiv_4 1$. 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

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

where $S := \lfloor \sqrt{P} \rfloor$. Let \equiv mean \equiv_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 $[0..S]^{\times 2}$ is $[S+1]^2$. This exceeds P , so there exist (Pigeon-hole principle) two distinct pairs $(a, b) \neq (\alpha, \beta)$ such that

$$a + \mathcal{R}b \equiv_P \alpha + \mathcal{R}\beta.$$

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

$$3a: \quad x^2 + y^2 = M \cdot P.$$

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

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

Second Proof. We can view $(\mathbb{Z}_P, +, 1)$ as a discrete circle. On it, define “circular distance”

$$d(b, c) := |\langle b - c \rangle|, \quad \text{where } \langle \cdot \rangle \text{ means symmetric residue.}$$

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

$$\frac{P}{S+1} \stackrel{\text{note}}{<} \sqrt{P}.$$

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

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

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

Melding. Is SOTS sealed under multiplication? If

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

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

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

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

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

Motivation?: Multiplying scaled rotation-matrices,

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

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 $\alpha + \beta i$, then multiply.]

Melding is sometimes conveniently written as an infix operator:

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

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 $\alpha \leq \beta$.

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

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

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

$$\text{E.g.,} \quad \begin{aligned} (2, 1) \mathcal{M} (-3, 4) &= (-10, 5), \quad \text{but} \\ (2, 1) \mathcal{F} (-3, 4) &= (5, 10). \end{aligned}$$

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_P , and $\langle \cdot \rangle$ for $\langle \cdot \rangle_P$.] WLOG P is odd. Consider two decompositions

$$\begin{aligned} **: \quad & \alpha^2 + \beta^2 = P = x^2 + y^2, \\ *: \quad & \text{with } \alpha, \beta, x, y \in [1 \dots \sqrt{P}]. \end{aligned}$$

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 $0 < \alpha x < P$. Thus $-P < \mu < P$, so $\mu = 0$. Thus $\alpha x = \beta y$.

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

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

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

$$\begin{aligned} \dagger: \quad & \alpha x = \beta y \quad \text{and} \\ \ddagger: \quad & P = \beta x + \alpha y. \end{aligned}$$

Consider a prime $q \nmid \alpha$, and write $q^n \parallel \alpha$. If q^n fails to divide y , then $q \nmid \beta$, so $q \nmid P$, hence $q = P$. But $x, y \geq 1$ forces \times , since $\text{RhS}(\ddagger) \geq 2P$. Hence $q^n \nmid y$.

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

5: Fermat SOTS Thm. *A posint T is SOTS IFF: Every 4NEG prime $P \nmid T$ occurs to an even power in T .* \blacklozenge

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

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

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

$$\begin{aligned} \dagger: \quad & P \nmid [\Omega \text{ or } \text{GCD}(x, y)], \quad \text{and} \\ \ddagger: \quad & P \nmid [\text{GCD}(\alpha, \beta) \text{ or } T]. \quad \blacklozenge \end{aligned}$$

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, $P \nmid \Omega x$. By symmetry, $P \nmid \Omega y$. So if $P \nmid \Omega$, then P divides **both** x and y .

We have established $(6\dagger)$. Symmetry gives $(6\dagger)$. \blacklozenge

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

$$\text{Meld}((\alpha, \beta), (x, y)) \stackrel{\perp}{\rightsquigarrow} \Omega T. \quad \blacklozenge$$

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

$$9: \quad \text{Either } P \nmid \text{GCD}(\alpha, \beta) \text{ or } P \nmid \text{GCD}(x, y). \quad \blacklozenge$$

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

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

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

$$P \nmid \alpha.$$

So to establish (9), WLOG $P \nmid \beta$. Now $(6\dagger)$ gives us

$$P \nmid T.$$

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

Goal: $P \nmid x$,

then necessarily $P \nmid y$. Now (9) will follow.

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

$$P \mid [\beta^2 x^2 + \alpha^2 y^2].$$

This, together with $P \mid \alpha$, produces $\boxed{P \mid \beta x}$. But $P \nmid \beta$. Thus (*Goal*). \blacklozenge

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

10: Good-meld Thm. *Suppose*

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

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

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

Consequently, by inducting on the below k ,

10‡: For each prime $P \equiv_4 1$ and each natnum k ,
 the power P^k is coprime-SOTS. \blacklozenge

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 $k=1$ case. And use (10†) for the induction on k . \blacklozenge

^{♥3}Indeed, given a SOTS-decomposition of P , we can use the repeated-squaring technique to produce a coprime SOTS-decomp of P^{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 $\llbracket \mathbf{x} \rrbracket^2$ for the sum $\sum_{j=1}^4 [x_j]^2$. \square

11: Prop'n. For oddprime P , there exists tuple \mathbf{x} and “multiplier” $M \in [1..P)$ st. $\llbracket \mathbf{x} \rrbracket^2 = MP$. \diamond

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

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

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

$$\begin{aligned} 0 < 1 + x^2 + y^2 &< 1 + \left[\frac{P}{2}\right]^2 + \left[\frac{P}{2}\right]^2 \\ &< 1 + [P^2/2] < P^2. \end{aligned}$$

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

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

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

is a tuple for which $\llbracket \mathbf{y} \rrbracket^2 = \llbracket \beta \rrbracket^2 \cdot \llbracket \mathbf{x} \rrbracket^2$.

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

Proof. Verifying $\llbracket \mathbf{y} \rrbracket^2 = \llbracket \beta \rrbracket^2 \cdot \llbracket \mathbf{x} \rrbracket^2$ 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 . \diamond

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

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

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. \square

Proof: 4NEG prime P is 4Sqr. From (11), take \mathbf{x} and M with $\llbracket \mathbf{x} \rrbracket^2 = MP$. WLOG $M \geq 2$. An Infinite Descent argument will give us our thm, *if* we can produce a new tuple \mathbf{z} and multiplier $K \in [1..M)$ such that $\llbracket \mathbf{z} \rrbracket^2 = KP$.

CASE: M is even Since MP 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:

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

Due to cancelling of cross-terms, $\llbracket \mathbf{z} \rrbracket^2 = \frac{1}{2} \llbracket \mathbf{x} \rrbracket^2 = \frac{M}{2} P$.

CASE: M is odd Thus $M \geq 3$. Taking **symmetric**-residues mod- M , let $\beta_j := \langle x_j \rangle_M$ and thus define a tuple β . Evidently

$$\llbracket \beta \rrbracket^2 \equiv_M \llbracket \mathbf{x} \rrbracket^2 \equiv_M 0,$$

so there is a natnum K with $\llbracket \beta \rrbracket^2 = KM$.

Could each β_j be zero? Well, if M divided each x_j , then $M^2 \nmid \llbracket \mathbf{x} \rrbracket^2 = MP$. So $M \nmid P$, contradicting that $M \in [2..P)$. Thus $K \geq 1$. To show that $K < M$, note we have *strict* inequality $|\beta_j| < \frac{M}{2}$, since M is odd. Thus $\llbracket \beta \rrbracket^2 < 4 \cdot \frac{M^2}{4} = M \cdot M$.

So our task is to produce a tuple \mathbf{z} st. $\llbracket \mathbf{z} \rrbracket^2 = KP$.

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

$$y_1 \equiv_M \llbracket \mathbf{x} \rrbracket^2 = MP \equiv_M 0.$$

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

$$\begin{aligned} \llbracket \mathbf{z} \rrbracket^2 &= \frac{1}{M^2} \cdot \llbracket \beta \rrbracket^2 \cdot \llbracket \mathbf{x} \rrbracket^2 \\ &= \frac{1}{M^2} \cdot KM \cdot MP = KP. \end{aligned}$$

Now ain't that Nifty! \diamond

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

Fix a SOTS N , and let \mathfrak{q} be the product of
 14: all the 4NEG primes (with multiplicity) that divide N . Then \mathfrak{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 $\sigma \geq \prod(\emptyset) = 1$, so $4\sigma^2 \geq 4$. ♦