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 \( S, T \) s.t. \( G = S \cdot 73 + T \cdot 27 \), 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.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( r_n )</th>
<th>( q_n )</th>
<th>( s_n )</th>
<th>( t_n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>73</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>27</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1.1: \( r_{n+1} = r_{n-1} - q_n r_n \)

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 \( L \) is \( G \). Hence \( S := s_L \) and \( T := t_L \) are particular Bézout multipliers, satisfying \( G = 73 S + 27 T \), a linear combination. Below, \( L \) equals 6.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( r_n )</th>
<th>( q_n )</th>
<th>( s_n )</th>
<th>( t_n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>73</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>27</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>19</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>2</td>
<td>10</td>
<td>27</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1.3: \( t_n \land t_{n-1} \land r_{n+1} = r_{n+1} - q_n r_n \)

Note \( r_n t_{n+1} + t_n t_{n+1} = r_n - r_n^2 q_n \). Thus \( r_n t_{n+1} + t_n t_{n+1} \) equals

\[ \text{LHS} \left( t_{n+1} \right) - \text{LHS} \left( t_n \right) \cdot q_n, \]

which is \( 0 \). Hence \( t_{n+1} \).

Whoa! Need to type the argument that \( | r_n | < \sqrt{T} \), then \( (r_n, t_n) \) is a SOTS decomp of \( T \).

RONO: Root-Of-Negative-One
W.r.t a posint \( T \), an integer \( R \) is an \( T \)-rono, a “(square) Root Of Negative One”, if

\[ R^2 \equiv_T -1. \]

Say that \( T \) is rono-ish if \( T \) 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 \( T \) has a rono IFF \( T \) has form \( B \) or \( 2B \), where \( B \) is a product of 4Pos primes.
Pf of (⇒). 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 \( 4 \text{NEG} \) prime has no rono, courtesy \( \text{LSThm.}^{\dagger} \)

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

2a: Suppose \( \mathcal{P} \) is a \( 4 \text{POS} \) prime. For each natnum \( k \), then, \( M := \mathcal{P}^k \) has a rono.

WLOG, \( k \geq 1 \). Courtesy the \( \text{Primitive-root Theo-} \)rem,\(^\ddagger\) the group \( \langle \Phi(M), \cdot, 1 \rangle \) is cyclic. It has order

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

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

Sums of Two Squares

A posint \( T \) is a \( \text{SOTS} \) if there exist \( x, y \in \mathbb{Z} \) with

\[ x^2 + y^2 = T. \]

Write \( (x, y) \sim T \) to indicate (\#) and that \( T \) is a posint. To indicate this \( and \) that \( x \perp y \), write

\[ (x, y) \perp \sim T. \]

Some pair in \( (T, x, y) \) is coprime IFF every pair is. Call \( T \) \( \text{coprime-SOTS} \) or just \( \text{cop-SOTS} \) if there exists a pair \( (x, y) \perp \sim T \). Finally, \( T \) is \( \text{strictly cop-SOTS} \) 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 \( \text{not strictly} \) cop-SOTS, since \( 25 = 0^2 + 5^2 \). Finally, \( 13 = 4 + 9 \) is \( \text{strictly} \) cop-SOTS, since that is its only SOTS decomposition.

\(^\dagger\)The Legendre-Symbol Thm. Use CRT for the Chinese Remainder Thm. An integer \( N \) is \( 4 \text{POS} \) if \( N \equiv_4 1 \). And \( N \) is \( 4 \text{NEG} \) if \( N \equiv_4 -1 \).

\(^\ddagger\)Alternatively, thm (10†) shows the existence of an \( M \)-rono.
Thus there are distinct points whose distance (Why?) is \( \leq S \). I.e., there are indices \( 0 \leq i < j \leq S \), with

\[
S \geq d(j\mathcal{R},i\mathcal{R}) = \langle k\mathcal{R} \rangle =: x,
\]

where \( k := j - i \), and therefore \( k \in [1..S] \).

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

**Melding.** Is SOTS sealed under multiplication? If

\[ [\alpha^2 + \beta^2] \cdot [x^2 + y^2] = \mu^2 + \nu^2, \]

where we have integer-valued formulas for \( \mu \) and \( \nu \), then “Yes!” And indeed, these definitions work:

\[
\mu := \alpha x - \beta y \quad \text{and} \quad \nu := \beta x + \alpha y.
\]

We have melded \((\alpha,\beta)\) with \((x,y)\), getting new pair \((\mu,\nu)\). That is,

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

**Motivation?:** Multiplying scaled rotation-matrices,

\[
\begin{bmatrix}
\alpha & -\beta \\
\beta & \alpha
\end{bmatrix}
\begin{bmatrix}
x \\
y
\end{bmatrix}
= \begin{bmatrix}
\mu \\
\nu
\end{bmatrix},
\]

certainly gives another scaled rotation-matrix. Using (4c) to define \( \mu \) and \( \nu \), gives (4b). And taking determinants in (4c), hands us (4a). [Equivalently, view \((\alpha,\beta)\) as complex number \( \alpha + \beta i \), then multiply.]

Melding is sometimes conveniently written as an infix operator:

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

Easily, operator \( M \) is commutative and associative.

**Full meld.** To normalize an intpair \((\alpha,\beta)\) means:

Replace \( \alpha \) by \( |\alpha| \) and \( \beta \) by \( |\beta| \). Then, if need be, exchange \( \alpha,\beta \) 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

\[
(\alpha,\beta) \ F (x,y) := \text{Nrmlize}((\alpha,\beta) \ M (x,y)).
\]

E.g.,

\[
(2,1) \ M (-3,4) = (-10, 5), \quad \text{but} \quad (2,1) \ F (-3,4) = (5, 10).
\]

Easily, \( F \) is commutative. **Exer 4d:** Prove or CEX: Operatorname \( F \) 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

\[ \alpha^2 + \beta^2 = P = x^2 + y^2, \]

\[ \ast: \quad \text{with } \alpha, \beta, x, y \in [1..\sqrt{P}). \]

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 \( 0 < \alpha x < P \). 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

\[ P^2 = \mu^2 + \nu^2 \equiv \nu^2, \]

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

\[ \vdash: \quad \alpha x = \beta y \quad \text{and} \]

\[ \vdash: \quad P = \beta x + \alpha y. \]

Consider a prime \( q \vdash \alpha \), and write \( q^n \vdash \alpha \). If \( q^n \) fails to divide \( y \), then \( q \vdash \beta \), so \( q \vdash P \), hence \( q = P \). But \( x, y \geq 1 \) forces \( \nmid \), since RhS(\[ \vdash \]) \( \geq 2P \). Hence \( q^n \vdash y \).

This applies to every prime dividing \( \alpha \); thus \( \alpha \vdash y \). This argument applies in reverse, hence \( \alpha \vdash y \). 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 \( P \vdash T \) occurs to an even power in \( T \).

\[ \implies \]

**Pf of \((\Rightarrow)\).**

**Pf of \((\Leftarrow)\).**

---

**The Setting for coprime-SOTS**

We prove several lemmas with a common setting. We have posints \( \Omega \) and \( T \) as well as integers

\[ \alpha^2 + \beta^2 = \Omega; \]

\[ x^2 + y^2 = T; \]

S1:

\[ (\mu, \nu) := \text{Meld}((\alpha, \beta), (x, y)); \]

\[ (m, n) := \text{Meld}((\beta, \alpha), (x, y)). \]

6: Lemma. Consider (S1), and a prime \( P \) which divides \( \gcd(\mu, \nu) \). Then

\[ \vdash: \quad P \vdash [\Omega \text{ or } \gcd(x, y)], \quad \text{and} \]

\[ \vdash: \quad P \vdash [\gcd(\alpha, \beta) \text{ or } T]. \]

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

\[ \alpha x\alpha + \beta x\beta = [\alpha^2 + \beta^2]. x. \]

I.e, \( P \vdash \Omega \). By symmetry, \( P \vdash \Omega \). So if \( P \nmid \Omega \), then \( P \) divides both \( x \) and \( y \).

We have established (6\[ \vdash \]). Symmetry gives (6\[ \vdash \]).

7: Corollary. Suppose \( (\alpha, \beta) \nmid \Omega \) and \( (x, y) \nmid T \). If \( \Omega \perp T \), then

\[ \text{Meld}((\alpha, \beta), (x, y)) \nmid \Omega T. \]

8: Both-melds Lemma. Assume (S1), and that some oddprime \( P \) divides each of \( \mu, \nu, m, n \). Then:

9: Either \( P \vdash \gcd(\alpha, \beta) \) or \( P \vdash \gcd(x, y) \).

**Pf.** By hyp., \( P \vdash [\mu^2 + \nu^2] \equiv \Omega T \). I.e, \( P \vdash \Omega T \). Note

\[ 4b': \quad m = \beta x - \alpha y \quad \text{and} \]

\[ n = \alpha x + \beta y. \]

And \( P \) divides \( \nu^2 + n^2 \equiv \Omega T + 4\alpha \beta xy \). But \( P \neq 2 \), so \( P \vdash \alpha \beta xy \). Courtesy (\( \ast \)), then, WLOG

\[ P \vdash \alpha. \]

So to establish (9), WLOG \( P \vdash \beta \). Now (6\[ \vdash \]) gives us

\[ P \vdash T. \]
And $T = x^2 + y^2$. So if we can prove that 

\[ \text{Goal: } P \nmid x, \]

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

By hypothesis, $P$ divides $\nu$ and $m$. Consequently, $P$ divides $\nu^2 + m^2 \equiv 2[\beta^2 x^2 + \alpha^2 y^2]$. Therefore,

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

This, together with $P \mid \alpha$, produces $[P \mid \beta x]$. 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 $\heartsuit$ on $k$, 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 decompo-

\[ 10: \text{Good-meld Thm. } \] Suppose

\[ *= (\alpha, \beta) \dashv \Omega \quad \text{and} \quad (x, y) \dashv T, \]

where $\Omega$ and $T$ are powers of an oddprime $P$. Then

At least one of Meld\((\alpha, \beta), (x, y)\) and

\[ 10\dagger: \quad \text{Meld\(((\beta, \alpha), (x, y))\) is a coprime-SOTS de-
\]

composition of $\Omega T$.

Consequently, by inducting on the below $k$,

\[ 10\ddagger: \quad \text{For each prime } P \equiv 1 \text{ and each natnum } k, \]

the power $P^k$ is coprime-SOTS.

\[ \blacklozenge \]

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

As for (10$\ddagger$), use (3) for the $k=1$ case. And use (10$\dagger$) for the induction on $k$.

\[ \blacklozenge \]
Sums of FOUR squares

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

11: Propn. For oddprime $P$, there exists tuple $x$ and “multiplier” $M \in [1..P]$ s.t. $[x]^2 = MP$.

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

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

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

Summing,

\[
0 < 1 + x^2 + y^2 < 1 + \left(\frac{P^2}{2}\right) + \left(\frac{P^2}{2}\right) < 1 + \frac{P^2}{2} < P^2.
\]

OTOHand, $1 + x^2 + y^2 \equiv 1 - \beta + [\beta - 1] = 0$.

Consequently, $1 + x^2 + y^2$ equals MP for some positn $M < P$. And $1 + x^2 + y^2$ is a sum of three [hence four] squares.

12: Euler’s four-square identity. Suppose $\beta$ and $x$ are tuples. Then this $y$

\[
y_1 := \beta x_1 + \beta x_2 + \beta x_3 + \beta x_4
\]

\[
y_2 := -\beta x_1 + \beta x_2 - \beta x_3 + \beta x_4
\]

\[
y_3 := -\beta x_1 - \beta x_2 + \beta x_3 + \beta x_4
\]

\[
y_4 := -\beta x_1 - \beta x_2 - \beta x_3 + \beta x_4
\]

is a tuple for which $[y]^2 = [\beta]^2 \cdot [x]^2$.

Now suppose $M$ is a positn st. $\beta_j \equiv M x_j$ for all $j$. Then each of $y_2, y_3, y_4$ is $\equiv \beta M$.

Proof. Verifying $[y]^2 = [\beta]^2 \cdot [x]^2$ 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 $y_4$.

13: 4Square Thm (Lagrange). Each natnum $T$ is a sum of 4 squares.

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

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

Case: $M$ is even Since $M$ is even, the number of odd entries in $x$ must be even. So WLOG $x_1 \equiv x_2$ and $x_3 \equiv x_4$. Thus these are integers:

\[
z_1 := \frac{1}{2}[x_1 + x_2], \quad z_3 := \frac{1}{2}[x_3 + x_4],
\]

\[
z_2 := \frac{1}{2}[x_1 - x_2], \quad z_4 := \frac{1}{2}[x_3 - x_4].
\]

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

Case: $M$ is odd Thus $M \geq 3$. Taking symmetric-residues mod-$M$, let $\beta_j := (x_j)_M$ and thus define a tuple $\beta$.

Evidently

\[
[\beta]^2 \equiv_M [x]^2 \equiv_M 0,
\]

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

Could each $\beta_j$ be zero? Well, if $M$ divided each $x_j$, then $M^2 \cdot [x]^2 = MP$. So $M \mid P$, 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

\[
[\beta]^2 < 4 \cdot \frac{M^2}{4} = M \cdot M.
\]

So our task is to produce a tuple $z$ st. $[z]^2 = KP$.

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

\[
y_1 \equiv_M [x]^2 = MP \equiv_M 0.
\]

Thus $z := \frac{1}{M^2} y$ is an integer-tuple. Moreover

\[
[z]^2 = \frac{1}{M^2} \cdot [\beta]^2 \cdot [x]^2
\]

\[
= \frac{1}{M^2} \cdot KM \cdot MP = KP.
\]

Now ain’t that Nifty!

Filename: Problems/NumberTheory/sots-4sqr.latex
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 infinitely many primes. (They don’t know the author of the proof.) The tool we need is

Fix a SOTS $N$, and let $q$ be the product of all the 4NEG 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

$$\sigma := \prod(S) \quad \text{and} \quad N := 1^2 + [2\sigma]^2 = 1 + 4\sigma^2.$$

Every divisor of $\sigma$ 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 $4\sigma^2 \geq 4$. ♦