

Triples of Sums of Two Squares

Titu Andreescu

Marian Tetiva

How can one get parameterizations for integers n such that each of n , $n + a$, and $n + b$ is a sum of two squares?

The problem that asks to show that there are infinitely many triples of consecutive integers, each of which can be expressed as a sum of two squares is well-known to the readers who are interested in mathematical contests and, generally, in beautiful mathematics. (Throughout this paper, as usual, by a sum of two squares we will understand a number that can be written in the form $x^2 + y^2$, with x and y being integers, possibly 0.) There exist many parameterizations that give infinitely many n such that n , $n + 1$, and $n + 2$ are all sums of two squares (and hence they solve the problem). To name only two of the most widely known such parameterizations, we can take $n = 4k^4 + 4k^2 = (2k^2)^2 + (2k)^2$ (for which $n + 1 = (2k^2 + 1)^2 + 0^2$, and $n + 2 = (2k^2 + 1)^2 + 1^2$), or we can consider $n = (2k^2 + 2k)^2$ (for which $n + 1 = (2k^2 + 2k)^2 + 1^2$, and $n + 2 = (2k^2 + 2k - 1)^2 + (2k + 1)^2$). Not to mention that an inductive proof is also available, via the simple observation that if n , $n + 1$, and $n + 2$ are all sums of squares, then each of $n(n + 2)$, $n(n + 2) + 1$, and $n(n + 2) + 2$ is a sum of two squares, too. (For proving that $n(n + 2)$ is a sum of two squares, remember the Brahmagupta-Fibonacci identity: $(x^2 + y^2)(z^2 + t^2) = (xz + yt)^2 + (xt - yz)^2$, which, in particular, shows that the product of two sums of two squares is also a sum of two squares.) Note that we cannot ask for four consecutive integers to be all sums of two squares, as long as among any four consecutive integers there is one congruent to 3 modulo 4—which, definitely, is not a sum of two squares.

Now, a harder problem can be posed: given two integers a and b , can we find infinitely many integers n such that each of n , $n + a$, and $n + b$ is a sum of two squares? And, indeed, the problem has been formulated by Littlewood at the beginning of the 20th century (see [1], or [3] for a more detailed history of such problems). It was only in 1973 that C. Hooley solved this problem in his paper [2]. Nevertheless, his solution used quadratic forms and offered no concrete construction for such n . Not knowing about this at that time, the second author proposed a particular case to *The American Mathematical Monthly*, and the editors decided to accept it—and published it in the general form. Consequently, a very simple solution (by J. P. Robertson) appeared in the *Monthly*'s issue from November 2018 (p. 852). Our purpose with this note is to show how some parameterizations for infinitely many n with the property that (given integers a and b) all of n , $n + a$, and $n + b$ are sums of two squares can be obtained, without too much effort (we would say, although it was not quite so in practice). The interested reader can see more complicated such calculations in the paper [1].

1. One (more empirical) way to solve the problem. We basically try to find (infinitely many) n of the form

$$n = u^2 + v^2,$$

for which we also have

$$n + a = x^2 + y^2 \quad \text{and} \quad n + b = z^2 + t^2$$

for integers u, v, x, y, z, t (thus $a = x^2 + y^2 - u^2 - v^2$ and $b = z^2 + t^2 - u^2 - v^2$). After some trial and error process, one realizes that, in order to find such n , one has to consider cases about a and b being odd or even. Let us try first to solve the case when both a and b are odd, say $a = 2c + 1$ and $b = 2d + 1$ for some integers c and d .

We start with the (probably simplest) observation that

$$2d + 1 = (d + 1)^2 - d^2 = m^2 + (d + 1)^2 - d^2 - m^2$$

for any integer m . So, it now seems natural to look for an expression of $2c + 1$ such as

$$2c + 1 = (p + d)^2 + (q + c + 1)^2 - d^2 - (q + c)^2 = p^2 + 2pd + 2q + 2c + 1$$

(where we wrote m^2 in the form $(q + c)^2$). This equality requires $2q = -p^2 - 2pd$ thus, with $p = 2k$, we need have $q = -2k^2 - 2kd$, and the identity

$$\begin{aligned} 2c + 1 &= (2k + d)^2 + (-2k^2 - 2kd + c + 1)^2 - d^2 - (-2k^2 - 2kd + c)^2 = \\ &= (2k + d)^2 + (2k^2 + 2kd - c - 1)^2 - d^2 - (2k^2 + 2kd - c)^2 \end{aligned}$$

follows. (We changed the signs in the second and fourth parentheses only from aesthetical reasons.)

Now we choose $m = 2k^2 + 2kd - c$ in the identity for $2d + 1$, and we find the identities:

$$2c + 1 = (2k + d)^2 + (2k^2 + 2kd - c - 1)^2 - d^2 - (2k^2 + 2kd - c)^2$$

and

$$2d + 1 = (2k^2 + 2kd - c)^2 + (d + 1)^2 - d^2 - (2k^2 + 2kd - c)^2.$$

Thus the numbers

$$n_k = d^2 + (2k^2 + 2kd - c)^2$$

have the property that each of n_k ,

$$n_k + 2c + 1 = (2k + d)^2 + (2k^2 + 2kd - c - 1)^2,$$

and

$$n_k + 2d + 1 = (2k^2 + 2kd - c)^2 + (d + 1)^2$$

is a sum of two squares. So, the above identities solve the problem when $a = 2c + 1$ and $b = 2d + 1$ are both odd.

Proceeding analogously (in the case of $a = 2c$ and $b = 2d + 1$), we get the identities

$$2c = (2k + d + 1)^2 + (2k^2 + 2k - c + (2k + 1)d)^2 - d^2 - (2k^2 + 2k - c + (2k + 1)d + 1)^2,$$

and

$$2d + 1 = (2k^2 + 2k - c + (2k + 1)d + 1)^2 + (d + 1)^2 - d^2 - (2k^2 + 2k - c + (2k + 1)d + 1)^2$$

that solve the problem when a is even and b is odd (or vice versa).

Finally, we remain with the case when a and b are both even. In this situation, let α and β be the exponents of 2 in the factorizations of a and b respectively, and let $\gamma = \min\{\alpha, \beta\}$. We then have $a = 2^\gamma a_1$, and $b = 2^\gamma b_1$, where at least one of a_1 and b_1 is odd. Thus the statement of the problem holds true for a_1 and b_1 , as shown above: there exist infinitely many positive integers n such that all numbers n , $n + a_1$, and $n + b_1$ are sums of two squares. Then, for any such n , the numbers $2^\gamma n$, $2^\gamma n + a = 2^\gamma(n + a_1)$, and $2^\gamma n + b = 2^\gamma(n + b_1)$, are also sums of two squares, which solves this case, too (and completes the solution of the problem). We used the simple and well-known fact that if m is a sum of two squares and γ is a positive integer, then $2^\gamma m$ is also a sum of two squares. For even γ this is obvious, while for odd γ one can use the identity $2(x^2 + y^2) = (x + y)^2 + (x - y)^2$ in order to prove this result.

2. One second (more analytical) approach. Again we try to find n of the form

$$n = u^2 + v^2,$$

for which we also have

$$n + a = x^2 + y^2 \quad \text{and} \quad n + b = z^2 + t^2$$

for integers u, v, x, y, z, t . Clearly, we need have $a = x^2 + y^2 - u^2 - v^2$, which can be read

$$(x - u)(x + u) = v^2 - y^2 + a,$$

hence it would be satisfied if $x - u = 1$ and $x + u = v^2 - y^2 + a$, that is, for

$$x = \frac{v^2 - y^2 + a + 1}{2} \quad \text{and} \quad u = \frac{v^2 - y^2 + a - 1}{2}.$$

Similarly, we must have $b = z^2 + t^2 - u^2 - v^2$, or

$$(z - u)(z + u) = v^2 - t^2 + b,$$

and this would hold if we chose

$$z = \frac{v^2 - t^2 + b + 1}{2} \quad \text{and} \quad u = \frac{v^2 - t^2 + b - 1}{2}.$$

The two expressions of u require the equality $v^2 - y^2 + a - 1 = v^2 - t^2 + b - 1$, that is,

$$(t - y)(t + y) = b - a.$$

This is satisfied by

$$t = \frac{b - a + 1}{2} \quad \text{and} \quad y = \frac{b - a - 1}{2}$$

if a and b have different parities, and by

$$t = \frac{b - a + 4}{4} \quad \text{and} \quad y = \frac{b - a - 4}{4}$$

if (a and b have the same parity and) $b - a$ is a multiple of 4.

So (in these two cases for a and b), we can find solutions in the following way: we first choose t and y such that $t^2 - y^2 = b - a$. This implies that $-y^2 + a - 1 = -t^2 + b - 1$, so we can pick v (in infinitely many ways) to be any integer having the same parity as $-t^2 + b - 1$ (and as $-y^2 + a - 1$), and then we have

$$u = \frac{v^2 - y^2 + a - 1}{2} = \frac{v^2 - t^2 + b - 1}{2}$$

an integer. Finally,

$$x = \frac{v^2 - y^2 + a + 1}{2} = u + 1 \quad \text{and} \quad z = \frac{v^2 - t^2 + b + 1}{2} = u + 1$$

will be integers, too.

For example, applying the above described procedure in the case $a = 2c$, and $b = 2d + 1$, we first get

$$t = d - c + 1 \quad \text{and} \quad y = d - c,$$

which gives

$$-y^2 + a - 1 = -t^2 + b - 1 = -(d - c)^2 + 2c - 1.$$

Thus we must choose

$$u = \frac{v^2 - (d - c)^2 + 2c - 1}{2},$$

with v an arbitrary integer having opposite parity with respect to $d - c$. Finally, we must have

$$x = z = u + 1 = \frac{v^2 - (d - c)^2 + 2c + 1}{2},$$

and the desired numbers (such that n , $n + a$, and $n + b$ are sums of squares) will have the form

$$n_v = u^2 + v^2 = \left(\frac{v^2 - (d - c)^2 + 2c - 1}{2} \right)^2 + v^2$$

for some integer v such that v and $d - c$ have opposite parities.

Indeed, we have

$$\begin{aligned} x^2 + y^2 - (u^2 + v^2) &= (u + 1)^2 - u^2 + y^2 - v^2 = 2u + 1 + (d - c)^2 - v^2 = \\ &= v^2 - (d - c)^2 + 2c + (d - c)^2 - v^2 = 2c = a, \end{aligned}$$

and

$$\begin{aligned} z^2 + t^2 - (u^2 + v^2) &= (u + 1)^2 - u^2 + t^2 - v^2 = 2u + 1 + (d - c + 1)^2 - v^2 = \\ &= v^2 - (d - c)^2 + 2c + (d - c + 1)^2 - v^2 = 2c = 2d + 1 = b. \end{aligned}$$

That is, for the above

$$n_v = u^2 + v^2 = \left(\frac{v^2 - (d - c)^2 + 2c - 1}{2} \right)^2 + v^2$$

we have

$$n_v + a = x^2 + y^2 = \left(\frac{v^2 - (d - c)^2 + 2c + 1}{2} \right)^2 + (d - c)^2,$$

and

$$n_v + b = z^2 + t^2 = \left(\frac{v^2 - (d - c)^2 + 2c + 1}{2} \right)^2 + (d - c + 1)^2,$$

as claimed.

Note that we cannot use this method when a and b have the same parity, but $b - a$ is not a multiple of 4; that is, in the case of $a = 4e$ together with $b = 4f + 2$ (or viceversa), or in the case of $a = 4e + 1$ and $b = 4f + 3$ (or vice versa). Nevertheless, in the first of these situations, we can find (as we previously shown) infinitely many n for which n , $n + 2e$, and $n + 2f + 1$ are all sums of two squares, therefore we will have (for such n) that $2n$, $2n + a = 2(n + 2e)$, and $2n + b = 2(n + 2f + 1)$ are all sums of two squares. In what concerns the second case (when $a = 4e + 1$ and $b = 4f + 3$), we have that $-a$ and $-a + b$ have different parities, so there exist infinitely many m such that m , $m - a$, and $m - a + b$ are all sums of two squares, meaning that n , $n + a$, and $n + b$ are all sums of two squares whenever $n = m - a$ for such an m .

Finally, a more complicated problem naturally arises. Namely, given integers $a_1, \dots, a_k$, one could ask whether there are (or not) infinitely many integers n such that each of $n + a_1, \dots, n + a_k$ is a sum of two squares. Clearly, a necessary condition is that the remainders of $a_1, \dots, a_k$ when divided by 4 do not cover all the possible remainders 0, 1, 2, 3. However, this is not at all a sufficient condition: for instance, there is no n such that all of n , $n + 2$, $n + 4$, and $n + 6$ are sums of two squares (see [3]). Clearly, conditions about congruences modulo other numbers can be imposed, too, depending on each specific k -tuple $(a_1, \dots, a_k)$. The paper [1] provides examples of parameterizations for a few cases of this general problem.

References

- [1] A. Choudhry, B. Maji: *Finite Sequences of Integers Expressible as Sums of Two Squares*, arXiv:2310.13317v2 [math.NT] 9 Apr 2024
- [2] C. Hooley: *On Intervals between Numbers that Are Sums of Two Squares, II*, *J. Number Theory*, 5(1973), 215-217
- [3] <https://mathoverflow.net/questions/38211/tuples-of-sums-of-two-squares>