Equally spaced squares and some impossible identities

G.J.O. JAMESON

Introduction

Consecutive squares are, of course, not equally spaced: the gap increases by 2 each time. However, it is quite possible to select three equally spaced squares, for example 1, 25, 49. Actually, such triples correspond to Pythagorean triples in a pleasantly simple way, which we will describe.

One of the many assertions stated, but not proved, by Fermat, is the fact that there is no instance of four equally spaced squares. This is known as "Fermat's four squares theorem". There is a fairly long history of attempted proofs; in particular, a rather sketchy one by Euler has not been accepted as conclusive. One of the earliest examples of a successful proof was given by Pocklington [1]. Here I will present a simplified version of an elegant method given much more recently in [2]. It seems that this article only appeared in arXiv, a favoured repository for pre-publication papers. (Van der Poorten may have intended to submit it to a journal, but regrettably he died in 2010.)

Van der Poorten's strategy is to equate the statement to a pair of Pythagorean-type identities, which is then shown to be "impossible" in the sense that it is not satisfied by any choice of positive integers. Having proved this result, we will then put it into its context by describing some further impossible identities of a similar type.

Here we summarise a few elementary facts that we will use repeatedly.

Lemma 1: If $x^2 + y^2$ is a multiple of 4, then x and y are even.

Proof: Clearly, x and y are both even or both odd. If x is odd, then $x^2 \equiv 1 \bmod 4$. So if x and y were odd, then $x^2 + y^2$ would be congruent to 2 mod 4.

Lemma 2: If $x^2 + y^2$ is a multiple of 3, then x and y are multiples of 3.

Proof: If a is congruent to 1 or 2 mod 3, then $a^2 \equiv 1 \bmod 3$. So the only way that $x^2 + y^2$ can be a multiple of 3 is for x^2 and y^2 to be both congruent to 0 mod 3, so that x and y are multiples of 3.

We willl also use the following fact, which is an obvious consequence of unique prime factorisation: *if m, n are coprime and $mn = c^2$, then m and n are squares*. Of course, this extends to a product of three pairwise coprime numbers.

We recall some basic facts about Pythagorean triples. These are triples (x, y, z) of positive integers, such as (3, 4, 5), satisfying $x^2 + y^2 = z^2$. We say that the triple is coprime (or primitive) if 1 is the greatest common divisor of x, y and z: it then follows that x, y and z are actually pairwise

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

coprime: any common divisor of two of them would divide the third one. Also, two of x, y and z must be odd. By Lemma 1, these are not x and y, so in fact z and one of x and y (say x) are odd. The well-known characterisation of coprime Pythagorean triples then states that there are coprime integers p, q (one even, one odd) such that

$$x = p^2 - q^2, \qquad y = 2pq, \qquad z = p^2 + q^2.$$

Further, if $z \equiv 1 \bmod 4$, then p must be odd and q even, while if $x \equiv 3 \bmod 4$, then p is even and q odd.

Equally spaced squares

Suppose that $a < b < c$ and $b^2 - a^2 = c^2 - b^2$, equivalently $a^2 + c^2 = 2b^2$. Then a and c are both even or both odd. If they are even, then $a^2 + c^2$ is a multiple of 4, so b is also even. If a and c are odd, then $a^2 + c^2 \equiv 2 \bmod 4$, so $b^2 \equiv 1 \bmod 4$, and b is also odd. So if the triple is coprime, then all three are odd.

Triples of equally spaced squares correspond to Pythagorean triples in the following way.

Theorem 1: The following statements are equivalent:

(i) $a^2 + c^2 = 2b^2$, with $0 < a < b < c$;

(ii) $a = x - y$, $b = z$ and $c = x + y$, where $x^2 + y^2 = z^2$ and $x > y > 0$.

Also, a, b, c are coprime if, and only if, x, y, z are coprime.

Proof: Given (ii), we have

$$a^2 + c^2 - (x - y)^2 + (x + y)^2 = 2\left(x^2 + y^2\right) = 2z^2 = 2b^2.$$

Given (i), we have seen already that $c + a$ and $c - a$ are even. Let $x = \frac{1}{2}(c + a)$, $y = \frac{1}{2}(c - a)$ and $z = b$. Then $a = x - z$, $c = x + y$ and $x^2 + y^2 = \frac{1}{2}\left(c^2 + a^2\right) = b^2 = z^2$.

If a prime p divides x, y and z, then it divides a, b and c. The converse applies if $p > 2$. For the case $p = 2$, suppose that a, b and c are even. Then z is even, so by Lemma 1, x and y are even.

Note that the common difference $b^2 - a^2$ equals $2xy$: we denote this by Δ.

By way of illustration, we list the first few cases.

x, y, z	a, b, c	a^2, b^2, c^2	Δ
4, 3, 5	1, 5, 7	1, 25, 49	24
12, 5, 13	7, 13, 17	49, 169, 289	120
15, 8, 17	7, 17, 23	49, 289, 529	240
24, 7, 25	17, 25, 31	289, 625, 961	336
21, 20, 29	1, 29, 41	1, 841, 1681	840
35, 12, 37	23, 37, 47	529, 1369, 2209	840
40, 9, 41	31, 41, 49	961, 1681, 2401	720

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

The reader can easily check that in each case the next number in the progression, obtained by adding Δ again, is not a square. As mentioned in the Introduction, Fermat stated the following result.

Theorem 2: There is no instance of four equally spaced squares.

We will prove this by a simplified version of van der Poorten's method. If there were four such squares, we could list them in the form $x - 3n$, $x - n, x + n, x + 3n$. So $x^2 - n^2$ and $x^2 - 9n^2$ would be squares. To prove Theorem 2, we now establish:

Theorem 3: For positive integers x, y, it is not possible for both $x^2 - y^2$ and $x^2 - 9y^2$ to be squares.

Proof: We use the "method of descent". Suppose that $x^2 - y^2 = z^2$ and $x^2 - 9y^2 = w^2$, and that among such pairs (x, y), this is the one with x minimal.

Then x and y are coprime: if a prime p divides both x and y, then it also divides z and w, and all four could be divided by p. Also, x is odd. If it were even, then x^2 would be a multiple of 4, and by Lemma 1, y and z would be even.

Next, y is even. If it were odd, then z and w would be even. Now $z^2 - w^2 = 8y^2$, so $\left(\frac{1}{2}z\right)^2 = \left(\frac{1}{2}w\right)^2 + 2y^2$. But $2y^2 \equiv 2 \bmod 4$ and $\left(\frac{1}{2}w\right)^2$ is congruent to 0 or 1 mod 4, so that $\left(\frac{1}{2}z\right)^2$ would be congruent to 2 or 3 mod 4, which is not possible for squares.

Since $x^2 = y^2 + z^2$, there exist coprime p, such that $y = 2pq$ and $x = p^2 + q^2$ (also $z = \pm\left(p^2 - q^2\right)$, but we won't use this). Exactly one of p, q is even: we can choose later which one.

Since $x^2 = (3y)^2 + w^2$, there exist coprime s_1, t_1 such that $3y = 2s_1t_1$ and $x = s_1^2 + t_1^2$. One (say t_1) is a multiple of 3: let $t_1 = 3t$ and $s_1 = s$. Then $y = 2st$ and $s = s^2 + 9t^2$. One of s, t is even (either is possible, and we are not free to interchange them!).

So $pq = st$: denote this number by N. Then pq and st represent two different disjoint partitions of the prime factorisation of N. By picking out common prime factors, we see that there exist pairwise coprime a, b, c, d such that

$$p = ab, \quad q = cd, \quad s = ac, \quad t = bd.$$

Since $p^2 + q^2 = s^2 - 9t^2$, we have

$$a^2\left(c^2 - b^2\right) = d^2\left(c^2 - 9b^2\right).$$

Since d^2 and a^2 are coprime and d^2 divides $a^2\left(c^2 - b^2\right)$, Euclid's lemma shows that there exists k such that $c^2 - b^2 = kd^2$, so that also $c^2 - 9b^2 = ka^2$. We will show that $k = 1$, so that in fact

$$c^2 - b^2 = d^2, \qquad c^2 - 9b^2 = a^2.$$

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

So (c, b) is another pair of the type required, with $c \leqslant s < x$, contradicting the minimality of x.

Now $8b^2 = k(d^2 - a^2)$ and $8c^2 = k(9d^2 - a^2)$, so k divides $8b^2$ and $8c^2$. We show next that k is odd: then k divides b^2 and c^2, so $k = \pm 1$. If t is even, choose the notation p, q so that p is even and q odd. Then b is even and c odd. If instead s is even, take q to be even: then c is even and b odd. In both cases, $c^2 - b^2$ is odd, hence k is odd.

So $k = \pm 1$. If $k = -1$, then $a^2 + c^2 = 9b^2$. By Lemma 2, this implies that a and c are multiples of 3 (so not coprime). Hence $k = 1$, as required.

We now describe a companion result to Theorem 3, also given in [2]. In fact, van der Poorten deduces Theorem 3 from Theorem 4 by deploying a further round of Pythagorean triples. Our simplification has been to prove Theorem 3 directly. Actually, neither of these theorems is stated explicitly in [2], only Theorem 2. The proof of Theorem 4 is along similar lines, but the details are quite different.

Theorem 4: For positive integers x, y, it is not possible for both $x^2 + y^2$ and $x^2 + 4y^2$ to be squares.

Proof: Suppose that $x^2 + y^2 = z^2$ and $x^2 + 4y^2 = w^2$, and that among such pairs (x, y), this is the one with z minimal. Then of course x and y are coprime.

We can dispose quickly of the case where x is even. Then w^2, hence w, is even, and we have $y^2 + (\frac{1}{2}x)^2 = (\frac{1}{2}w)^2$, while $y^2 + 4(\frac{1}{2}x)^2 = z^2$. So $(y, \frac{1}{2}x)$ is another pair of the required type, with $y^2 + (\frac{1}{2}x)^2 < z^2$, contradicting the minimality of z.

So suppose that x is odd. For the moment, suppose that $x \equiv 3 \bmod 4$. Then there exist coprime p, q, with p even and q odd, such that $x = p^2 - q^2$ and $y = 2pq$ (also $z = p^2 + q^2$). Also, there exist coprime s_1, t, with s_1 even and t odd, such that $x = s_1^2 - t^2$ and $2y = 2s_1t$. Let $s_1 = 2s$. Then $x = 4s^2 - t^2$ and $y = 2st$. If instead $x \approx 1 \bmod 4$, then the same identities hold with x replaced by −x. In either case, we have pq = st and p2 − q 2 = 4s2 − t2 , so that $p^2 + t^2 = q^2 + 4s^2$.

So there exist pairwise coprime a, b, c, d such that

$$p = ab, \qquad q = cd, \qquad s = ac, \qquad t = bd.$$

Then

$$b^2(d^2 + a^2) = c^2(d^2 + 4a^2).$$

By Euclid's lemma, there exists k such that $d^2 + a^2 = kc^2$, so that also $d^2 + 4a^2 = kb^2$. We show that $k = 1$, so that (d, a) is a pair of the required type with $d^2 + a^2 = c^2$, where $c < z$, since $c \leqslant s < y < z$.

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

If k is a multiple of 3, then $d^2 + a^2$ is a multiple of 3. By Lemma 2, this implies that d and a are multiples of 3, contradicting the fact that they are coprime. So k is not a multiple of 3. Now $k(b^2 - c^2) = 3a^2$ and $k(4c^2 - b^2) = 3d^2$. By Euclid's lemma again, k divides both a^2 and d^2: hence $k = 1$, as required.

Some further impossible identities

We now describe a number of other impossible identities of Pythagorean type, which will put Theorems 1, 3 and 4 into perspective. We will avoid tedious repetition of words like "for integers x, y, z": when we say that an identity or statement is not posssible, it is to be understood that we mean not possible for positive integer values of the variables.

We start with a very simple example. Theorem 1 identified (in different notation) numerous examples of triples satisfying $x^2 + y^2 = 2z^2$. By contrast, we have:

Theorem 5: The identity $x^2 + y^2 = 3z^2$ is not possible.

Proof: Supposing that such triples exist, let this be the one with z minimal. By Lemma2, x and y are multiples of 3. Hence $x^2 + y^2$ is a multiple of 9, so z^2, hence also z, is a multiple of 3. So $(\frac{1}{3}x, \frac{1}{3}y, \frac{1}{3}z)$ is another such triple, contradicting the minimality of z.

The same actually applies with 3 replaced by any prime p that is congruent to -1 mod 4. Lemma 2 generalises to such p, using the well-known fact [3, p. 126] that -1 is not congruent to a square mod p, so that if a is congruent to a square mod p, then $-a$ is not.

Meanwhile, given any positive integer a, there are plenty of triples satisfying $x^2 + ay^2 = z^2$. In fact, for any choice of p and q, such a triple is given by

$$a = |p^2 - aq^2|, \qquad y = 2pq, \qquad z = p^2 + aq^2.$$

The most famous example of an impossible identity is, of course, the one featured in Fermat's so-called last theorem: $x^n + y^n = z^n$ is impossible for all $n \geqslant 3$. As is well known, Fermat claimed to have a proof, but did not divulge it. However, he did prove the following pair of results, the first of which implies the case $n = 4$ of the "last theorem".

Theorem 6: The identity $x^4 + y^4 = z^2$ is not possible.

Theorem 7: The identity $x^4 - y^4 = z^2$ is not possible.

Here we just give the proof of Theorem 7, which is perhaps a little less well known. A proof of Theorem 6 along similar lines can be seen in many books, e.g. [3, p. 227].

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

Proof of Theorem 7: Again we use the method of descent. Supposing that such triples exist, let (x, y, z) be the one with x smallest. We show first that x and y are coprime. If some prime p divides both x and y, then p^4 divides z^2, so p^2 divides z. Let $x = px_1$, $y = py_1$ and $z = p^2z_1$. Then $x_1^4 - y_1^4 = z_1^2$, contradicting the minimality of x.

So (y^2, z, x^2) is a coprime Pythagorean triple. Either y or y is odd. We consider the cases separately.

If y is odd, then there exist u, y such that

$$y^2 = u^2 - v^2, \qquad z = 2uv, \qquad x^2 = u^2 + v^2.$$

Then $u^4 - v^4 = (u^2 + v^2)(u^2 - v^2) = (xy)^2$: this is another triple of the required type with $u < x$.

Now suppose that z is odd. Then there exist coprime u, v such that

$$y^2 = 2uv, \qquad z = u^2 - v^2, \qquad x^2 = u^2 + v^2.$$

There exist coprime p, q such that $x = p^2 + q^2$ and u, v are $p^2 - q^2$ and $2pq$ (one way round or the other). Then

$$\left(\frac{y}{2}\right)^2 = \tfrac{1}{2}uv = pq(p^2 - q^2).$$

Since p, q and $p^2 - q^2$ are pairwise coprime, they are all squares:

$$p = a^2, \qquad q = b^2, \qquad p^2 - q^2 = c^2.$$

Hence $a^4 - b^4 = c^2$: this is a triple of the required type with $a < x$.

These theorems (especially Theorem 7) deliver numerous further impossible identities. We list some of them as corollaries.

Corollary 1: It is not possible for both $x^2 + y^2$ and $x^2 - y^2$ to be squares.

Proof: This would imply that $x^4 - y^4 = (x^2 + y^2)(x^2 - y^2)$ is a square.

Corollary 2: It is not possible for both $x^2 + y^2$ and $x^2 + 2y^2$ to be squares. Similarly for $x^2 - y^2$ and $x^2 - 2y^2$.

Proof: Suppose that $x^2 + y^2 = z^2$ and $x^2 + 2y^2 = w^2$. Then $z^2 - y^2 = x^2$ and $z^2 + y^2 = w^2$, contradicting Corollary 1. The second statement is similar.

Corollary 3: If (x, y, z) is a Pythagorean triple, then at most one of x, y, z can be a square. Further, xy, xz and yz are not squares.

Proof: If $x = a^2$ and $y = b^2$, then $a^4 + b^4 = z^2$, contradicting Theorem 6. If $x = a^2$ and $z = b^2$ then $a^4 + y^2 = b^4$, contradicting Theorem 7. Similarly for the pair y, z. So at most one of the three can be a square. If x, y, z are coprime, it follows that xy, xz and yz are not squares. The same follows in the general case, since then we have $x = kx'$, $y = ky'$ and

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

$z = kz'$ for some k, where x, y, z are coprime.

Note that any one of the three can certainly be a square, as shown by the triples (3, 4, 5), (9, 40, 41) and (7, 24, 25).

Conversely, Corollary 3 obviously implies Theorems 6 and 7.

Next, we deduce a pair of results companion to Theorems 6 and 7.

Theorem 8: The identity $x^4 + 4y^4 = z^2$ is not possible.

Proof: Suppose that this is the example with z minimal. Then $(x^2, 2y^2, z)$ is a Pythagorean triple. We need to know that x^2 and $2y^2$ are coprime. For primes $p \neq 2$, this works exactly as in Theorem 7. We also require x to be odd. If it is even, then so is z. Let $x = 2x_1$ and $z = 2z_1$. Then $y^4 = 4x_1^4 = z_1^2$: a triple of the required type with $z_1 < z$.

So there exist coprime s, t such that $x^2 = s^2 - t^2$ and $2y^2 = 2st$, so $y^2 = st$. Hence there exist a, b such that $s = a^2$ and $t = b^2$, giving $a^4 - b^4 = x^2$, contrary to Theorem 7.

Theorem 9: The identity $x^4 - 4y^4 = z^2$ is not possible.

Proof: This is similar to the previous proof, but an extra trick is needed. We actually show at the same time that $4y^4 - x^4 = z^2$ is not possible. Supppose that $x^4 - 4y^4 = z^2$, and that this is the triple of either type with z minimal. Again we need to know that x is odd, so that x and $2y^2$ are coprime. If x is even, let $x = 2x_1$ and $z = 2z_1$. Then $4x_1^4 - y^4 = z_1^2$, a triple of the second type with $z_1 < z$. (If the minimal example is of the second type, similar reasoning applies.)

So $(z, 2y^2, x^2)$ is a coprime Pythagorean triple, and there exist coprime s, t such that $y^2 = st$ and $x^2 = s^2 + t^2$. This leads to $x^2 = a^4 + b^4$, contrary to Theorem 6.

These Theorems generate corollaries analogous to the previous ones.

Corollary 4: It is not possible for both $x^2 + 2y^2$ and $x^2 - 2y^2$ to be squares.

Corollary 5: It is not possible for both $x^2 + 2y^2$ and $x^2 + 4y^2$ to be squares.

Corollary 6: If (x, y, z) is a Pythagorean triple with y even, then at most one of $\frac{1}{2}y$, x and z is a square. Hence $\frac{1}{2}xy$ (the area of the triangle) is not a square.

Proof: If $x = a^2$ and $\frac{1}{2}y = b^2$, then $a^4 + 4b^4 = z^2$, contradicting Theorem 8. If $z = c^2$ and $\frac{1}{2}y = b^2$, then $c^2 - 4b^4 = x^2$, contradicting Theorem 9.

Conversely, Corollary 6 implies Theorems 8 and 9.

Stan Dolan has shown in [4] how one can prove Corollaries 3 and 6 (and hence Theorems 6, 7, 8 and 9) simultaneously, by an ingenious

https://doi.org/10.1017/mag.2024.58 Published online by Cambridge University Press

formulation, in terms of right-angled triangles, of the statement to be proved by descent,

One might be tempted to conjecture that these theorems are special cases of something much more general, perhaps that for any non-zero integer a, $x^2 + y^2$ and $x^2 + ay^2$ cannot both be squares. However, this idea is laid to rest by the following example:

$$15^2 + 8^2 = 17^2, \qquad 15^2 + 112^2 = 15^2 + 196 \times 8^2 = 113^2.$$

Could Theorems 3 and 4 have been deduced with less effort from Theorems 7 and 9? Not as far as I can see.

Finally, we remark that Pocklington's method for Theorem 2 is achieved by considering another quartic, $x^4 - x^2y^2 + y^4$.

References

1. H. C. Pocklington, Some diophantine impossibilities, *Proc. Cambridge Phil. Soc.* **17** (1914) pp. 110-118.
2. Alf van der Poorten, Fermat's four squares theorem, arXiv:0712.3850v1 (2007), available at arXiv.org.
3. G. A. Jones and J. M. Jones, *Elementary Number Theory*, Springer (1998).
4. Stan Dolan, Fermat's method of "descente infinie", *Math. Gaz.* **95** (July 2011) pp. 269-271.

10.1017/mag.2024.58
Published by Cambridge University Press
on behalf of The Mathematical Association

G.J.O. JAMESON
13 Sandown Road,
Lancaster LA1 4LN
e-mail: *pgjameson@talktalk.net*