Sums of Two Squares theorem - Visual Proof

> "Another famous and beautiful theorem is Fermats 'two square' theorem... All the primes of the first class" [i.e. 1 mod 4] ... "can be expressed as the sum of two integral squares... This is Fermat 's theorem, which is ranked, very justly, as one of the finest of arithmetic. Unfortunately, there is no proof within the comprehension of anybody but a fairly expert mathematician."
>
> H. Hardy

Proofs were later developed that were more elementary. In 2007 a Russian school teacher, Alexander Spivak, gave a simple visual proof that you could explain to a high school student.

Theorem: *(Fermat's two squares theorem) An odd prime p can be expressed as the sum of two squares:*

$$p = x^2 + y^2$$

with x and y integers if and only if p is of the form $4k + 1$ where k is a positive integer.

Note: As p is odd, one the integrs is odd and the other is even.

Proof:

Consider the problem of solving

$$p = x^2 + 4yz \tag{1}$$

where p is a prime number, x is a positive odd integer and y, z are non-zero positive integers. If we find a solution where $y \neq z$, then swapping the values of y and z around gives a second solution. As such, if there were an odd number of solutions then there must be at least one solution where $y = z$. In other words, there must be a soluton such that

$$p = x^2 + (2y)^2. \tag{2}$$

That is, p could be expressed as the sum of two squares. We will show that (1) has on odd number of solutions if and only if p is of the form $4k + 1$, and thus demonstrate Fermat's theorem on the sum of two squares.

The right hand side of (1) can be thought of as the area of a square of side length x and four rectangles of dimensions $y \times z$ arranged in a windmill configuration. In fig (1) we list the four allowable types of skewed windmill diagrams, two types of skewed windmillws that are excluded, and a straight cross type diagram. With a type 1 windmill $2y < x$ and with a type 2 windmill $2x > 2y > x$. The case where $x = 2y$ is excluded because x is an odd integer, see fig (1). The case where the skewed windmill forms a square, see fig (1), corresponds to the case where the area is the square of an integer, and so cannot be equal to a prime number. The definition of type 3 and 4 are are obvious from the diagrams. A straight cross diagram corresonds to the case where $x = y$. The reason for this classification will become apparant in a moment.

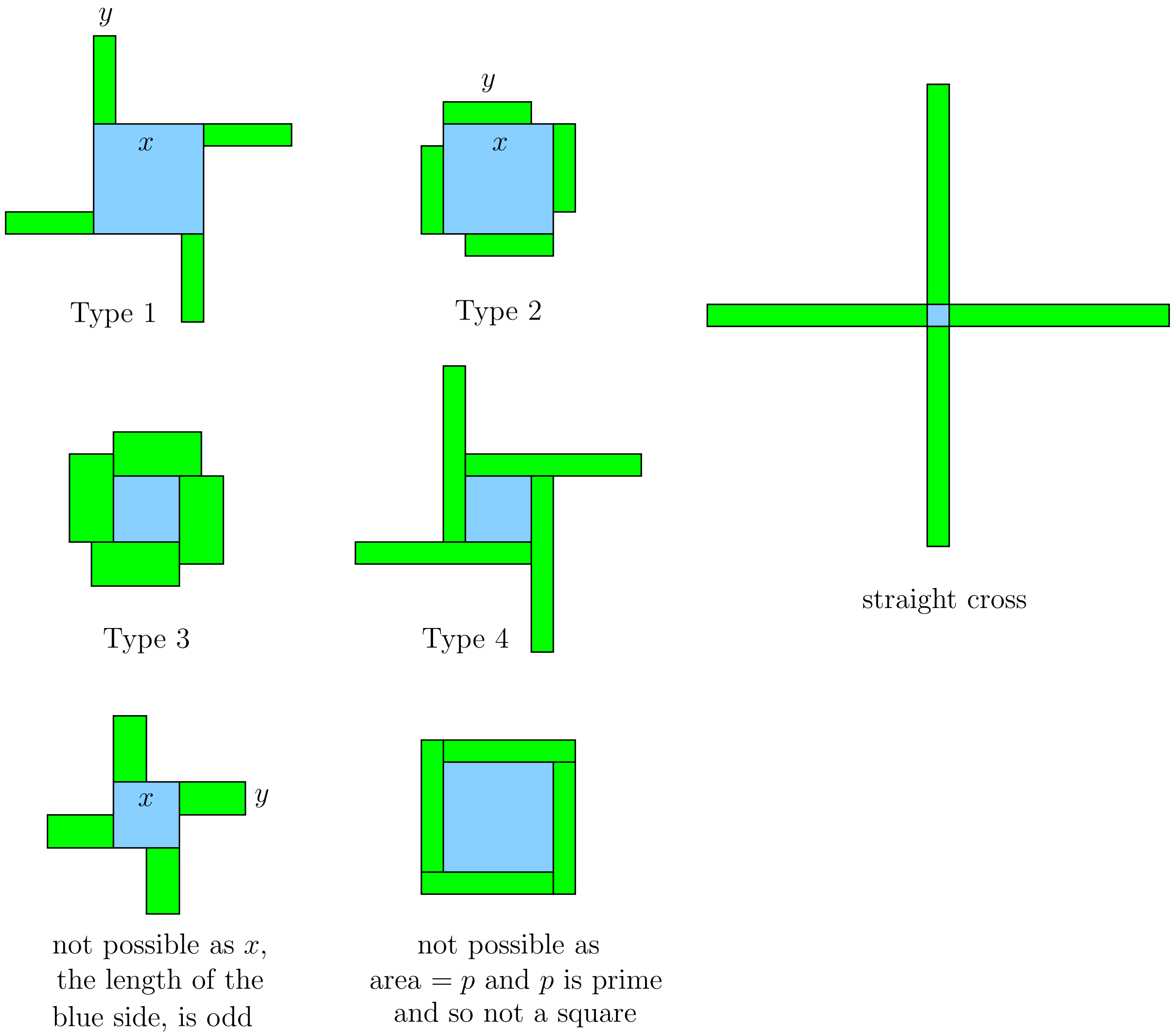

Figure 1: .

A windmill is a solution of (1) if its area is equal to p. A cruical observation is that given a type 1 windmill we obtain a type 4 windmill by simultaneously drawing vertical and horizontal (red) lines into the interior of the square as displayed in fig (2). Likewise, given a type 2 windmill solution we obtain a type 3 windmill solution (reflected) by a similar method as displayed in fig (2). If the first skewed windmill is a solution, then so is the second skewed windmill as it obviously has the same area. The first solution and the second solution are related by having the same underlying footprint (see fig (3)). We see from fig (2) that every type 4 windmill is associated with a type 1 windmill, and that every type 3 windmill is associated with a type 2 windmill.

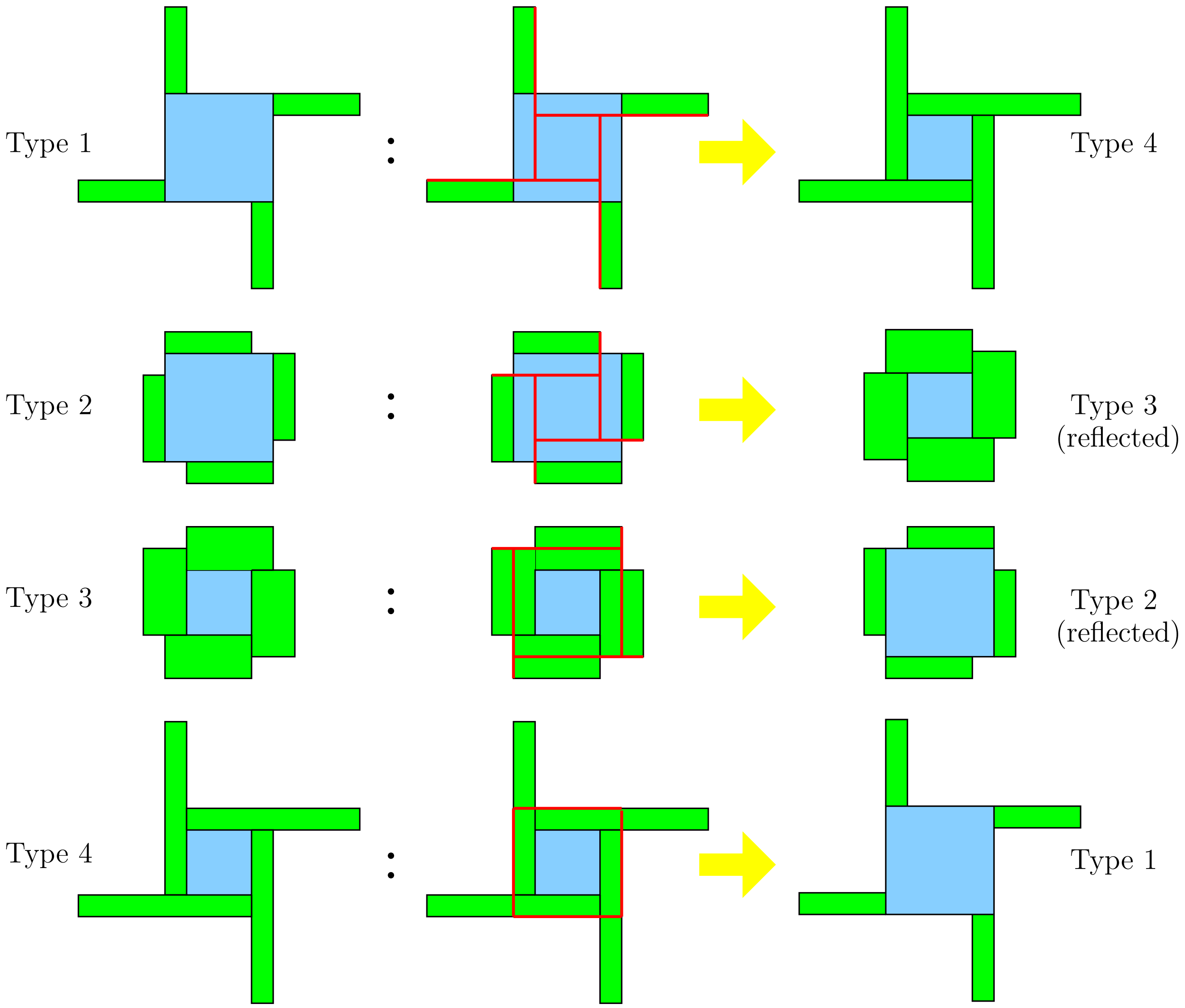

Figure 2: .

We can arrange solutions by underlying footprints.

Take the underlying footprint of a type 1 skewed windmill (see fig (3)). It corresponds to a single type 1 windmill and a single type 4 windmill, but it cannot correspond to a type 2 or type 3 windmill. Obviously, there are no type 4 windmills that are not associated with a type 1 windmill.

Take the underlying footprint of a type 2 windmill (see fig (3)). It corresponds to a single type 2 windmill and a single type 3 windmill (reflected), but it cannot correspond to a type 1 or type 4 windmill with it. Obviously, there are no type 3 windmills (reflected) that are not associated with a type 2 windmill.

From these observations it is clear that there are an even number of skewed windmill solutions.

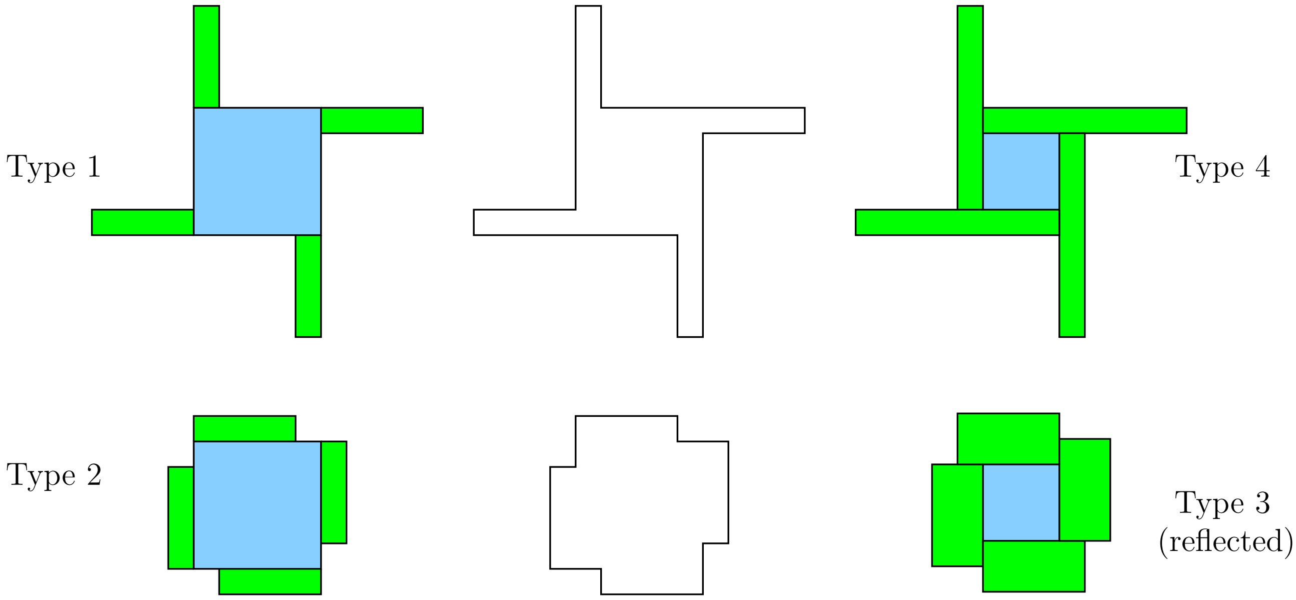

Figure 3: A typle 1 and type 4 windmill and their common underlying footprint. A typle 2 and type 3 (reflected) windmill and their common underlying footprint.

A straight cross solution is drawn in fig. (4). It corresponds to the case where $x = y$. In this case we would have that p is the product of two integers,

$$p = x(x + 4z) \tag{3}$$

As p is a prime we must have $x = 1$, in which case

$$p = 1 + 4z. \tag{4}$$

We immediately see that there is at most one straight cross solution, and that there is a straight cross solution if and only if p is of the form $p = 4k + 1$ (note that all other odd primes are of the form $4l + 3$, where l is some integer, and these primes don't have a straight cross solution). Therefore, we have that there are an odd number of solutions if and only if p is of the form $p = 4k + 1$. Therefore, p can be written as the sum of two squares if and only if p is of the form $p = 4k + 1$.

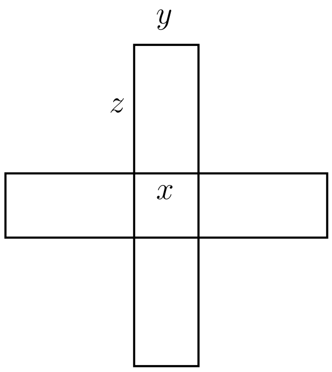

Figure 4: A straight cross.

$\square$