PYTHAGORAS AND ALL THAT

Man seems to have known of Pythagoras' Theorem since the early days of civilisation, although the Greek geometers were the first to provide a logical proof. Indeed the 3,4,5 triangle is still widely used in building to ensure that two brick walls are laid perpendicular to one another.

Sets of three integers which satisfy $a^2 + b^2 = c^2$ are called Pythagorean triples. It would be useful to know if there's a formula for these triples; let's look.

First, if $\{a,b,c\}$ is such a set, so is $\{ka,kb,kc\}$, where k is any non-zero integer, as $a^2 + b^2 = c^2$ implies $(ka)^2 + (kb)^2 = (kc)^2$. We therefore look only for "primitive" sets: sets with no common factors. However, if $a = hx$ and $b = hy$, then $c^2 = h^2(x^2+y^2)$ so h^2 must divide c^2 which, in turn, means h must divide c. We find, similarly, that if d divides both a and c then it must divide b and so on. If we write the greatest common divisor of r and s as (r,s), this means that in a primitive Pythagorean triple we have $(a,b) = (b,c) = (c,a) = 1$. Consequently only one of $\{a,b,c\}$ can be even.

We now show that one <u>must</u> be even and it can't be c. The square of an even number $(2n)^2 = \overline{4n^2} \equiv 0 (\text{mod } 4)$ and the square of an odd number $= (2n+1)^2 = 4n + 4n+1 \equiv 1 (\text{mod } 4)$. We cannot have each of $\{a,b,c\}$ odd as $1 + 1 \equiv 2 (\text{mod } 4)$ not 1, while we cannot have less than two odd. On the other hand, $c^2 \equiv 2 (\text{mod } 4)$ is impossible so we can't have both a and b odd. We therefore must finish up with one of $\{a,b\}$ even and the rest of $\{a,b,c\}$ odd.

Suppose it's b that's even. As we are to have $b^2 = c^2 - a^2 = (c-a)(c+a)$ with a and c odd, then each of $(c-a)$ and $(c+a)$ will be even. But, if d divides $(c-a)$ and $(c+a)$ then it divides $2c = (c-a) + (c+a)$ and $2a = (c+a) - (c-a)$. As $(a,c) = 1$, this means that 2 is their only common factor. Indeed, as an odd number is congruent to 1 or $3 (\text{mod } 4)$ it is easy to work out that one of $(c-a)$, $(c+a)$ must be congruent to $2 (\text{mod } 4)$ and the other must be divisible by 4.

So both $\frac{1}{2}(c+a)$ and $\frac{1}{2}(c-a)$ are integers, one odd, one even, and having no common factors except 1. But $\frac{1}{2}b$ is also an integer as b is even and $(\frac{1}{2}b)^2 = \frac{1}{2}(c+a).\frac{1}{2}(c-a)$. Now if x, y, z are whole numbers and $z^2 = xy$ where $(x,y) = 1$ each of x and y must be perfect squares. We put $\frac{1}{2}(c+a) = m^2$, $\frac{1}{2}(c-a) = n^2$, remembering that $m \not\equiv n (\text{mod } 2)$ and $(m,n) = 1$. Then $c = \frac{1}{2}(c+a) + \frac{1}{2}(c-a) = m^2+n^2$, $a = \frac{1}{2}(c+a) - \frac{1}{2}(c-a) = m^2-n^2$ and $(\frac{1}{2}b)^2 = m^2n^2$ giving $\frac{1}{2}b = mn$ or $b = 2mn$.

What we have done is to show that all primitive Pythagorean triples must follow these formulae. It is easy to check that

$(m^2-n^2)^2 + (2mn)^2 = (m^2+n^2)^2$ so that, in mathematical language, the conditions are both necessary and sufficient. Thus $m = 2$, $n = 1$ gives $\{3,4,5\}$; $m = 3$, $n = 2$ gives $\{5,12,13\}$; $m = 4$, $n = 3$ gives $\{7,24,25\}$ and so on.

Naturally, having solved the problem of $a^2+b^2 = c^2$, it seems sensible to look at the more general problem $a^n + b^n = c^n$ for $n > 2$. Unfortunately Fermat's Last Theorem states that there are no solutions to this equation, whatever the value of n. Mathematicians believe in the truth of this theorem - BUT no general proof has yet been found. The French mathematician Pierre de Fermat, 1601-1605, after whom the theorem is named, wrote on the margin of a book on numbers by Diophantus that he had found "a truly marvellous proof" but "it was too long for the margin". There has been argument ever since whether he was right in his claim or not; his proof has never been found. Quite large money prizes were offered in the 19th Century for a proof; none was ever won, though the endeavour to produce a proof led to many valuable mathematical investigations being undertaken by Kummer and others. On the other hand, the prizes offered led to a vast number of incorrect proofs being produced by amateur mathematicians; so much so, that the mathematician Landau kept a supply of printed letters containing the sentence: "On page .., lines .. to .. you will find there is a mistake".

However, the theorem has been proved true for $n \leq 253,747,889$ (which is a prime number). We only need to consider prime numbers for n because $a^{kp} + b^{kp} = c^{kp}$ automatically gives the solution $(a^k)^p + (b^k)^p = (c^k)^p$ for $n = p$. If there are no solutions for $n = p$, there can't be any for $n = kp$.

Those readers interested in learning more about the theorem may like to read the fuller article on it in Vol 5 No 1 of Parabola. Incidentally, the proof for $n = 4$ is given there.

There are other directions in which we can go. We can ask for any numbers, not just squares, which are the sums of two squares: thus $8 = 2^2+2^2$, $34 = 3^2+5^2$, $17 = 4^2+1^2$. It can be proved that for all prime numbers p of the form $4n+1$, there is a unique pair of numbers a, b such that $a^2+b^2 = p$. Thus $13 = 3^2+2^2$ only, although $65 = 7^2+4^2$ and $65 = 8^2+1^2$.

Again, given n, we can ask what the smallest number, m, is so that every integer can be written as the sum of m, or fewer, n'th powers. Thus, for $n = 2$, $m = 4$: every integer can be written as the sum of 4, or fewer, squares e.g. $6 = 2^2+1^2+1^2$, $7 = 2^2+1^2+1^2+1^2$, $8 = 2^2+2^2$, $9 = 3^2$, etc. We can go on to ask which numbers <u>cannot</u> be written as the sum of less than four squares. The answer to these and many other such questions are known, but there is always the possibility that shorter or more elegant proofs may be found.

* * *

Follow-up problems

1. Prove that numbers of the form $4n+3$ cannot be represented as a^2+b^2.

2. Show that if $c = a^2+b^2$ and $f = d^2+e^2$ then $cf = p^2+q^2$ for some integers p, q.

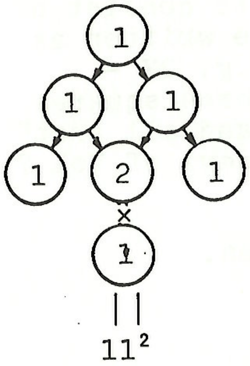
3. Show that if $m = a^2+b^2+c^2+d^2$ and $n = e^2+f^2+g^2+h^2$ then $mn = p^2+q^2+r^2+s^2$ for some integers p, q, r, s. (Some considerable algebraic manipulation is required, or else a knowledge of quaternions.)

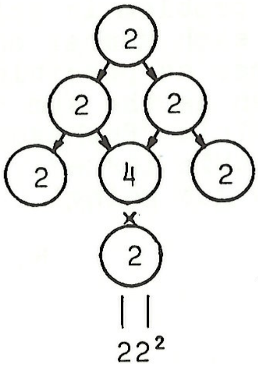
4. Prove that numbers of the form $4^k(8h+7)$ cannot be written as the sum of less than four squares.

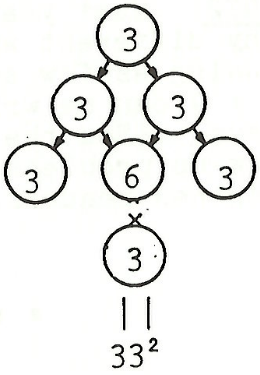
5. Prove that if c is the sum of two squares then so is $2c$. Also prove the converse: that if $2c$ is the sum of two squares, then so is c.

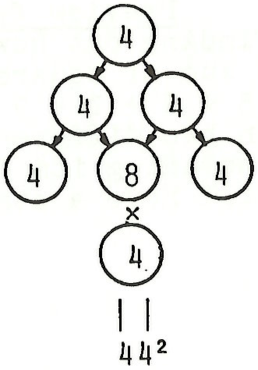
M.G. Greening.

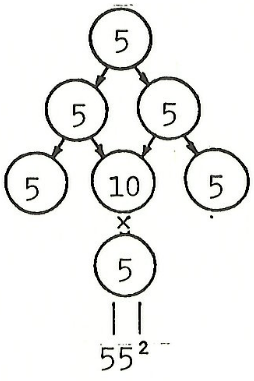
* * *



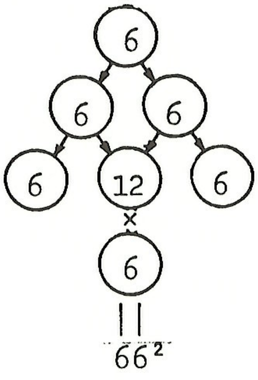








This group of X-mas trees was contributed by Helen Pollack (11 years old) 6th Class of Woollahra Demonstration School. It illustrates some interesting patterns arising from finding multiples of 11 and their squares. To retain the symmetry, she did not "carry" in cases of 5 and 6. It can be extended for numbers greater than 10. Can you do this?


6
6 6
6 12 6
×
6
||
66^2