Identifying Sums of Squares

Anuj Chordia

June 2023

1 Abstract

It is known that some whole numbers can be written as a sum of two squares, more whole numbers can be written as a sum of three squares, and every number that is an integer and non-negative, a sum of four squares. This paper will outline and prove a formula to identify which numbers can be stated as the above. In addition, this paper will outline how to calculate the sum of increasing squares up to a certain one to further discuss the topic.

2 Introduction

A square, or an integer that is the product of another integer and itself, is easy to identify when a lesser integer, but as the values grow larger ad larger, identifying one is far more difficult. When squares are added up, identifying the sums would appear to be even more difficult at first thought, but the truth is that sums of squares are more common and follow more rules than squares.

A sum of two squares, which will be referred to as a curtain for the context of this paper, can be identified by Fermat's Theorem, in a manner that is fairly convoluted, but a sum of three squares, which will be referred to as an armchair in terms of this paper, has a much easier identification with LeGendre's theorem. Unfortunately, it is also far more difficult to prove, and the full extent of it will not be proved in this paper. Following the trend, a sum of four squares will not have a special name for this paper, unless "non-negative integers" counts as one. That is because legitimately every non-negative integer is a sum of four squares, regardless of modular properties or value.

Furthermore, a special type of a sum of squares is one where all the squares in the sum are consecutive. They will not be referred to with a special identifier for this paper, though if necessary, one can view them as "pyramidal numbers". These integers, unlike any of the sorts discussed beforehand, rely on the next level of powers, cubes, for their formulation, and for them, calculation will be discussed rather than identification.

This paper will explain how to identify or calculate all the aforementioned kinds of sums of squares in many different theorems and lemmas, some more complicated than others.

3 Acknowledgements

Special thanks to Stanford Student, Alexander Perry, for guiding the processes of this paper. In addition, thanks to Dr. Simon Rubenstein-Salzedo.

4 Preliminaries

Important note: Anytime the character, i is seen on its own, it does NOT represent the imaginary number, the square-root of -1. It is meant to be a variable and simply that in the context of this paper.

4.1 Definitions

Definition 1. *Let a curtain be any non-negative integer, c where there exist two (not necessarily distinct) integers n and k, such that $n^2 + k^2 = c$. Furthermore, let C be the set where for any non-negative integer, p, $p \in C$ if and only if p is a curtain.*

Definition 2. *Let an armchair be any integer, a where there exist three (not necessarily distinct) integers, w, y, and z, such that $w^2+y^2+z^z = a$ In addition, let A be the set where any non-negative integer, s, is an element of A if and only if s is an armchair.*

Definition 3. *Let the nth triangular number denote $\sum_{k=1}^{n} k$ for all positive integers, n.*

4.2 Universal Lemma

Lemma 1. *For any integer, z, z^2 mod $8 \equiv 1$ if and only if z mod $2 \equiv 1$. If and only if z mod $4 \equiv 0$, z^2 mod $8 \equiv 0$, and if and only if z mod $4 \equiv 2$, z^2 mod $8 \equiv 4$*

Proof: If $z \mod 2 \equiv 1$, there exists an integer, k, where $2k + 1 = z$. In addition, $z + 2 = 2k + 1 + 2 = 2k + 3$. $z^2 = (2k + 1)^2 = (2k + 1)(2k + 1) = (2k)^2 + 2k + 2k + 1 = 4k^2 + 4k + 1$. $(z + 2)^2 = (2k + 3)^2 = (2k + 3)(2k + 3) = 4k^2+12k+9 = (4k^2+4k+1)+8k+8$. This is simply just $z^2+8(k+1)$, therefore, $(z+2)^2$ is always a multiple of 8 greater than z^2, and thus, $(z+2)^2 \equiv z^2 \mod 8$. If $z = 1$, $z^2 = 1$, and thus, $z^2 \mod 8 \equiv 1$. By induction, this can be generalized to all integers that are a multiple of 2 greater than 1, or all positive odd integers.

Otherwise, $z \equiv 0 \pmod 2$, which means that modulo 4, either $z \equiv 0 \pmod 4$ or $z \equiv 2 \pmod 4$

If $z \mod 4 \equiv 0$, $4|z$, and thus, there exists an integer, v, where $4v = z$. $z^2 = (4v)^2 = 4^2v^2 = 16v^2 = 8 * (2v^2)$.Therefore, $8|z^2$, thus, $z^2 \mod 8 \equiv 0$.

If $z \mod 4 \equiv 2$, there exists an integer, k, such that $4k+2 = z$. Furthermore, $z + 4 = 4k + 2 + 4 = 4k + 6$. Thus, $z^2 = (4k + 2)^2 = 16k^2 + 16k + 4)$ and $(z + 4)^2 = (4k + 6)^2 = 16k^2 + 48k + 36 = (16k^2 + 16k + 4) + 32k + 32$, or $z^2 + 32(k + 1) = z^2 + 8(4k + 4)$, so $(z + 4)^2$ is always a multiple of 8 more than

z^2, and thus, they are congruent modulo 8. If $z = 2$, $2^2 = 4 \equiv 4 \bmod 8$, and by induction, that can be similarly generalized to every integer that is a multiple of 4 greater than 2, or every non-negative integer that is congruent to 2 modulo 4.

Therefore, for any non-negative integer, z, z^2 is congruent to either 0, 1, or 4 modulo 8, and as $z^2 = (-z)^2$, this can be generalized to all integers.

5 Sums of two squares

To begin the meat of the paper, sums of two squares, or curtains, will be discussed. These integers are identifiable by Fermat's Theorem, of which, while most of the work was done by Pierre de Fermat, the completion was by Leonhard Euler, with Harold Edwards filling in some gaps. While many proofs of Fermat's Theorem exist, Euler's proof by infinite descent will be explained in this paper.

Lemma 2. *If a non-negative integer is congruent to either* 3 *modulo* 4 *or* 6 *modulo* 8*, it is not a curtain*

Proof: Suppose there exists a curtain, c that is congruent to 6 modulo 8. There exist two integers, n and k, such that $n^2 + k^2 = c$. By Lemma 1, n^2 can only be congruent to 0, 1, or 4 modulo 8. In the case where it is congruent to 0 modulo 8, k^2 is congruent to $6 - 0 = 6$ modulo 8, but this contradicts Lemma 1, so it is simply not. If n^2 is congruent to 1 modulo 8, k^z is $6 - 1 = 5$ modulo 8, which again, contradicts Lemma 1. In the last case, where n^2 is congruent to 4 modulo 8, k^2 has to be congruent to $6 - 4 = 2$ modulo 8, which, following in the footsteps of the previous 2 cases, contradicts Lemma 1. As every possibility is a contradiction, c cannot be congruent to 6 modulo 8.

Suppose there exists a curtain, u that is congruent to 3 modulo 4. There exist two integers, n and k, where $n^2 + k^2 = u$. By Lemma 1, n^2 is congruent to either 0, 1, or 4 modulo 8. If it is congruent to either 0 or 4 modulo 8, it is congruent to 0 modulo 4. This means that k^2 is congruent to $3 - 0 = 3$ modulo 4, which means that n^2 is either congruent to 3 or 7 modulo 8, both cases of which contradict Lemma 1.

If n^2 is congruent to 1 modulo 8, it is congruent to 1 modulo 4 as well. In addition, k^2 is congruent to $3 - 1 = 2$ modulo 4, meaning that modulo 8, it is congruent to either 2 or 6, both of which contradict Lemma 1. With this proposition, every possibility remains contradictory, so it is impossible as well.

Lemma 3. *Diophantus's identity: For any two curtains,* t *and* d*,* $t * d \in C$ *.*

Proof: As $t \in C$, there exist two integers, let them be f and v, where $f^2 + v^2 = t$. Similarly, as $d \in C$, there exist two integers, let them be l and m, where $l^2 + m^2 = d$. Thus, $t * d$ is simply $(f^2 + v^2)(l^2 + m^2) = f^2l^2 + f^2m^2 + v^2l^2 + v^2m^2$. A following expression equivalent to $0{,}2fmlv - 2fmlv$, can be added to rewrite it as $f^2l^2 + f^2m^2 + v^2l^2 + v^2m^2 = f^2l^2 + f^2m^2 + v^2l^2 + v^2m^2 + 2fmlv - 2fmlv$. The terms of the expression on the right can be rearranged

to be $f^2l^2 + 2fmlv + m^2v^2 + f^2m^2 - 2fmlv + l^2v^2$. The expression can be further rewritten to $(fl)^2 + 2(fl)(mv) + (mv)^2 + (fm)^2 - 2(fm)(lv) + (lv)^2$. For any two integers, u and s, $(u+s)^2 = uu + us + us + ss = u^2 + 2us + s^2$, and $(u-s)^2 = uu - us - us + ss = u^2 - 2us + s^2$. Therefore, the expression is equivalent to $(fl + mv)^2 + (fm - lv)^2$, and thus, $t * d \in C$.

Corollary 1. *Further application of Diophantus's identity: If for two curtains, c and q, c is prime and $c|q$, $\frac{q}{c} \in C$.*

Proof: As $c \in C$, there exist two integers, a and b, where $a^2 + b^2 = c$. Similarly, as $v \in C$, there exist two integers, d and f, where $d^2 + f^2 = v$. It can be noted that $a^2d^2 - f^2b^2 = a^2d^2 + b^2d^2 - b^2d^2 - f^2b^2 = d^2(a^2+b^2) - b^2(d^2+f^2) = d^2(q) + b^2(c)$. As $c|q$, $c|d^2(q)$, and thus, $c|d^2(q) + b^2(c) = a^2d^2 - f^2b^2$. The latter expression can be further simplified to $(ad)(ad) - (fb)(fb) = (ad)(ad) + (fb)(ad) - (fb)(ad) - (fb)(fb) = (ad+fb)(ad-fb)$, hence, $c|(ad+fb)(ad-fb)$. As c is prime, the only way for $(ad + fb)(ad - fb)$ to contain it in its prime factorization is if either $c|(ad + fb)$ or $c|(ad - fb)$.

On another note, $(af + bd)^2 + (ad - bf)^2 = cq = (ad + fb)^2 + (af - bd)^2$, following from the logic in the proof of the Lemma that this is a Corollary of.

Algebraically, $\frac{q}{c} = \frac{cq}{c^2} = \frac{(ad+fb)^2+(af-bd)^2}{c^2} = \frac{(ad+fb)^2}{c^2} + \frac{(af-bd)^2}{c^2} = (\frac{ad+fb}{c})^2 + (\frac{af-bd}{c})^2$. If $c|ad+fb$, $c|(ad+fb)^2$. Furthermore, $c|cq-(ad+fb)^2 = (af-bd)^2$. As c is prime, $af - bd$ must have it in its prime factorization for its square to have it, so $c|(af - bd)$. Therefore, $\frac{ad+fb}{c}$ and $\frac{af-bd}{c}$ are integers, so $\frac{q}{c} \in C$.

Otherwise, if $c|ad - fb$, it is also true that $\frac{q}{c} = \frac{cq}{c^2} = \frac{(af+bd)^2+(ad-bf)^2}{c^2} = \frac{(af+bd)^2}{c^2} + \frac{(ad-bf)^2}{c^2} = (\frac{af+bd}{c})^2 + (\frac{ad-bf}{c})^2$. In this case, $c|cq - (ad - fb)^2 = (af + bd)^2$. Similarly, c is prime, so $c|(af + bd)$. Thus, $\frac{ad-fb}{c}$ and $\frac{af+bd}{c}$ are both integers, so $\frac{q}{c} \in C$ in this case as well.

Theorem 1. *Wilson's theorem: For any prime number, v, $(v-1)! \equiv -1 \pmod{v}$.*

Proof: Let d be a positive integer where $d < v$. As v is a prime, d and v are relatively prime. Or in other words, the greatest common divisor between d and v is 1. Therefore, the least common multiple of d and v is simply $d * v$, as if it was $d * g$, where $g < v$, $v|d * g$, but as v is prime, it cannot be a factor of the multiple of two lesser positive integers, as neither of them would be able to have v in their prime factorization.

Let O be the set where for a positive integer, s, $s \in O$ if there exists an integer, l, where $0 < l < d + 1$, such that $(l-1)v + 1 = s$. As there are d possible values for l, and thus, for s, $|O| = d$. As $d * v$ is the least common multiple of d and v, the only way where for any two elements of O, o and p where $o < p$, $o \equiv p \pmod{d}$ is if $p = kdv + o$, where k is any positive integer. But as all elements of O are less than $d * v + 1$, and 1 is the element of the least value, the true conclusion is that no two elements of O can have the same remainder when divided by d. But there are d elements in O, and d possible remainders, therefore, there is a bijection of values of where the input is any

element in O, and the output, the remainder of the input when divided by d, and thus, only one element in O has a remainder of 0 when divided by d. In other words, there is only one element in O, q, where $d|q$.

Let r=q/d, Note that r is necessarily less than v, as $q \in O$, and thus, is $(d-1)v+1$ at most, or $dv-(v-1)$. v is a prime, 2 at the least, so $v-1>0$, meaning that $q<dv$. In addition, r is positive, as q and d are both positive. There is only 1 value of r for every value of d already, so the relation between d and r is a function, and as r and d have the exact same domains(positive integers less than v), the relation between them can further be said to be a bijection. In addition, $r|q$ meaning that if the input was r, the unique q would be the same, and the output would be $q/r=d$, meaning that the relation is also symmetric.

In addition, $d^2-1=(d+1)(d-1)$. If this value is positive, it cannot be divisible by v unless $v=d+1$, as $d<v$, meaning that $d-1$ is not a multiple of v, and $d+1$ cannot be a multiple of v greater than v, and v is a prime, meaning that if it is found in the prime factorization of a product, either of the multiples must contain it. However, if $d=1$, $(d^2-1)=0$, and so $v|(d^2-1)$. As $q \equiv 1 pmod v$ and is unique for all d, $q=(d^2-1)+1=d^2$ if and only if $v|(d^2-1)$, which is the case if and only if $d=1$ or $d=v-1$.

Therefore, if $1<d<v-1$, $r \neq d$. In addition, $r \neq 1$ and $r \neq v-1$, as r takes their value if $d=1$ or $d=v-1$ respectively, but the relation between them is bijective, meaning that no two values of d can yield the same value of r.

Thus, $1<r<v-1$, so for every integer greater than 1 but less than $v-1$, there is exactly one other integer greater than 1 but less than $v-1$ for which the product of the two $\equiv 1 \pmod v$. When $(v-1)! \pmod v$ is expanded, every pair where their product $\equiv 1 \pmod v$ can be simplified to 1. As this is for the entire domain from 2 to $v-2$, that entire block can be simplified to 1, therefore, $(v-1)! \equiv 1*1*v-1=v-1=-1 \pmod v$.

Lemma 4. *Lagrange's Lemma: For any prime number, u, where $u \equiv 1 \pmod 4$, there exists an integer, l, where $u|l^2+1$.*

Proof: As $u \equiv 1 \pmod 4$, there exists an integer, let it be r, where $4r+1=u$. Let L be a set for which, any integer, $m \in L$ if and only if m is a positive integer less than $2r+1$. Let G be a set for which any integer,h, $h \in G$ if and only if there exists an element, m, in the set, L, where $m+h=u$. Therefore, $h \equiv -m \pmod u$, and as $|L|=|G|=2r$, if l is the product of all elements in L, and g, the product of all elements in G, $g \equiv l(-1^2r)=l(1^r)=l \pmod u$, therefore, $gl \equiv l^2 \pmod u$

As L consists of all positive integers less than $2r+1$, $l=(2r)!$. G consists of all possible differences between u and any element of L, which range from $u-2r=2r+1$ to $u-1=4r$, so $g=(4r)!/l$, and $lg=(4r)!$. By Wilsons's theorem, $-1 \equiv (4r)! \pmod u$, therefore, $-1 \equiv (lg) \pmod u \equiv l^2 \pmod u$. This means that there exists an integer, k, such that $ku-1=l^2$, so $l^2+1=ku$, therefore, $u|l^2+1$.

Lemma 5. *Euler's second Proposition: For a curtain, q and its non-curtain factor, d, $\frac{q}{d}$ has a factor that is not a curtain.*

Assume that an integer, d, is not a curtain, but an integer, q, is, and $d|q$. Then, $\frac{q}{d}$ has to have at least one prime factor that is not a curtain, as if otherwise, the Corollary of Diophantus's Identity can be applied successively to each prime factor in relation to a variable, p that originally equals q, where for any prime factor, x, $\frac{p}{x} \in C$, and p can be reassigned to $\frac{p}{x}$, also a curtain, for the same procedure on the next prime factor. However, once all the prime factors are run through, d is what is left, but $d \notin C$, therefore, at least one of the prime factors is not a curtain such that d is not forced to be one.

Algorithm 1. *Euler's third proposition: Given a positive integer g, where $g > 1$ and a curtain, $v = l^2 + m^2$, such that l and m are relatively prime, return a curtain, $c_1 = a^2 + b^2$, such that a and b are relatively prime, $c_1 < \frac{g^2}{2}$, and $g|c_1$. Let this algorithm be defined as $El(g, v) = c_1$.*

Process: Note that $g \nmid l$ and $g \nmid m$. This is because if $g|l$, $g|l^2$, so $g|v - l^2$, as $g|v$. Thu, $g|m^2$, but that would mean that m^2 and l^2 have a common divisor of g when they should be relatively prime, having only 1 as a common divisor. The same logic can be applies if $g|m$, as then $g|m^2$, $g|v - m^2$, and thus, $g|l^2$.

As neither l nor m are divisible by g, there exist four integers, w, x, y, and z such that $wg + x = l$ and $yg + z = m$, where x and z are non-zero integers whose absolute value is less than $\frac{g}{2}$, and w and y are $\frac{l}{g}$ and $\frac{m}{g}$ rounded to the nearest integer. For example, if $l = 10$, $m = 7$, and $g = 4$, y is $\frac{7}{4}$ rounded to the nearest integer. 1.75 rounded to the nearest integer is $\lfloor 1.75 + 0.5 \rfloor = \lfloor 2.25 \rfloor = 2$. Similarly, $wis \lfloor \frac{10}{4} + 0.5 \rfloor = \lfloor 3 \rfloor = 3$. Thus, $x = l - wg = 10 - 3(4) = -2$ and $z = m - yg = 7 - 2(4) = -1$. Note that $-\frac{g}{2} \leq x, z \leq \frac{g}{2}$, as wg and yg are the nearest multiples of g to l and m respectively, meaning that the absolute value of the difference between them has to be less than or equal to half of g.

Thus, $v = l^2 + m^2 = (wg + x)^2 + (yg + z)^2 = w^2g^2 + 2wxg + x^2 + y^2g^2 + 2yzg + z^2 = (w^2g + 2wx + y^2g + 2yz)g + x^2 + z^2$. $g|v$, therefore $g|v - (w^2g + 2wx + y^2g + 2yz)g = x^2 + z^2$, so $g|x^2 + z^2$, but as $-\frac{g}{2} \leq x, z \leq \frac{g}{2}$, $x^2, z^2 \leq (\frac{g}{2})^2 = \frac{g^2}{4}$, so $x^2 + z^2 \leq 2(\frac{g^2}{4}) = \frac{g^2}{2}$, or to simplify, $x^2 + z^2 \leq \frac{g^2}{2}$.

As $g|x^2 + z^2$, $h := (x^2 + z^2)/g$. In addition, let s be the greatest common factor of c and d, and t, the greatest common factor of s and g. As x and z are divisible by s, and s, divisible by t, $t|x$ and $t|z$. $t|g$ by its assignment as well, therefore, $t|wg + x = l$ and $t|yg + z = m$. But l and m are relatively prime, therefore, $t = 1$, meaning that g and s are relatively prime.

Note that $s^2|x^2 + z^2$, as $s|x$ and $s|z$. In addition, as g is relatively prime to s, it is so to s^2, as relatively prime numbers have mutually exclusive sets of primes in their prime factorizations, and squaring a number does not add any new primes, keeping the factorizations disjoint. In addition, $g|\frac{x^2+z^2}{s^2}$, as on account of g's set of primes in its prime factorization being disjoint to s^2's, s^2's prime factorization can be removed from $x^2 + z^2$'s without encroaching on g's that is present in $x^2 + z^2$. In other words, $g|\frac{x^2+z^2}{s^2} = (\frac{x}{s})^2 + (\frac{z}{s})^2$.

For new assignments, $a := \frac{x}{s}$ and $b := \frac{z}{s}$. a and b are relatively prime, as if they were not, having a greatest common divisor greater than 1, the product of that and s would divide both x and z, contradicting s being their greatest common divisor. In addition, $c_1 := a^2+b^2$. $c_1 \leq x^2+z^2$, being a (not necessarily proper) factor of it, meaning that as $x^2 + z^2 \leq \frac{g^2}{2}$, $c_1 \leq \frac{g^2}{2}$, and as a and b are relatively prime, and as shown in the last paragraph, $g|c_1$, so c_1 is a valid output to this algorithm.

Theorem 2. *Fermat's theorem of two squares: For any non-negative integer, c, $c \in C$ if and only if there are either no primes that $\equiv 3 \pmod 4$ in its prime factorization or that the primes that are there are raised to an even power.*

Proof: For a curtain q, $p^2 + o^2 := q$, where $p^2 > 0$ and $o^2 > 0$, meaning that neither can be equivalent to q. For the greatest common divisor of p and o, let it be j, $\frac{q}{j^2} = \frac{p^2+o^2}{j^2} = (\frac{p}{j})^2 + (\frac{q}{j})^2$. It can be said that p/j and o/j are relatively prime, as if they were not, and had a greatest common divisor of some integer larger than 1, both p and q would be divisible by the product of j and that integer, which would be greater than j, contradicting j being the greatest common divisor.

Henceforth, $v := \frac{q}{j^2}$, $a := \frac{p}{j}$, and $b := \frac{o}{j}$, where a and b are relatively prime. In addition, a^2 and b^2 are relatively prime, as their prime factorizations would be mutually disjoint, and squaring a positive integer only doubles the exponents of the existing primes rather than adding new ones, so they cannot share prime factors, and thus, any factors larger than 1(composite numbers are just sets of prime factors multiples together).

If $v = 1$, all factors of v are curtains. If v is prime, it's a similar story, with v and 1 as the only factors, and both are prime.

Otherwise, let f be a proper factor of v such that $f > 1$ and $f \notin C$. Applying the algorithm, Euler's third proposition, such that $d = El(f, v)$, d is a curtain less than or equal to $\frac{f^2}{2}$ and $f|d$, so $h := \frac{d}{g}$,but $d \leq \frac{g^2}{2}$, so $h \leq \frac{g}{2}$. Assume that f, which as defined, can be any factor of v, is not a curtain. Thus, by Euler's second proposition, there exists a factor of h that also is not a curtain. Let this factor be denoted as f_1, and as $f_1|h$, $f_1 \leq h$, so $f_1 \leq \frac{f}{2}$. $f_1 \neq 1$, as $1 \in C$ so it can be used as the first input for the algorithm. $d_1 := El(f_1, d)$ follows a similar pattern, the quotient of it and f_1 having a factor that's a non-curtain, let this be f_2, where $f_2 \leq \frac{f_1}{2}$.

The outputs of each use of the algorithm can be repeatedly recycled with a non-curtain factor of the quotient between them and the first input, but each non-curtain factor is at most half of the previous one in the algorithm chain, so eventually, the non-curtain factor will be have to be the smallest non-curtain, 3, which is not a curtain on account of it having a remainder of 3 when divided by 8 according to the first Lemma of this section. Both 4 and 5, which are $2^2 + 0^2$ and $4^1 + 1^2$, are curtains, so 6, which has a remainder of 6 when divided by 8, is the second least curtain, and $3 \leq \frac{6}{2}$, so 3 can't be avoided by virtue of the non-curtain input being less than twice its value.

However, from 3, there simply is not a non-curtain value less than or equal to half of it, or less than it at all for that matter, as all three integers that are are curtains($0 = 0^2 + 0^2$,$1 = 1^2 + 0^2$, and $2 = 1^2 + 1^2$, meaning that the algorithm should not be able to continue. However, 3 satisfies the conditions of the first input, and the second input, is necessarily a multiple of 3 on account of 3 being a factor from a quotient of it, and necessarily a curtain where at least one case of the integers whose squares that add up to it are relatively prime on account of it being an output of the algorithm, meaning that the entire premise of f being a non-curtain is contradictory.

However, f, by its definition, can be any factor of v, which means that any factor of v is a curtain, and as demonstrated before the assignment of f, this would be still be the case, even if there was so such factor, f. v, per its assignment, is any curtain where it is $l^2 + m^2$ such that l and m are relatively prime. If $m := 1$, it will always be relatively prime to l, and in addition, by Lagrange's Lemma, for every prime, u, where $u \equiv 1 \pmod 4$, there exists an integer, k, such that $k^2 + 1 = u$. If $l := k$, $v = k^2 + 1^2$, so $u|v$. Therefore, for any value of u, there is a value of v such that $u|v$, but for all values of v, every factor of it is a curtain, so any value of u is a curtain, meaning that all primes that have a remainder of 1 when divided by 4 are curtains.

In addition, all factors of v are curtains, which means that v cannot have a factor that has a remainder of 3 when divided by 4, as that factor being a curtain would contradict Lemma 2. However, q(which, for a memory refresher, was the curtain defined at the beginning of this proof where the integers whose squares had a sum of it had a greatest common divisor of j), which is $v * j^2$, can have factors like that, as long as each one is raised to an even exponent such that j^2 can be set to equal the product of all the powers of primes where the primes have a remainder of 3 when divided by 4, allowing v's prime factorization to only encompass the primes that have a remainder of 1 when divided by 4. If any of the non-curtain primes are raised to an odd exponent, however, j^2 cannot represent them, so neither can q, meaning that no curtain can have that case.

By Diophantine's identity, every product of curtains is a curtain, meaning that every positive integer that only possesses prime curtains in its prime factorization(these prime curtains are either $2 = 1^2 + 1^2$ or have a remainder of 1 when divided by 4) is a curtain. All squares are curtains by defaults, as a square can said to be its square-root squared $+0^2$, so any product of (many) prime curtains can be further multiplied by any square of a prime non-curtain or any square of a product of many prime non-curtains, and the resulting product is necessarily a curtain. In addition, 1 and 0 are curtains because $1 = 1^2 + 0^2$ ND $0 = 0^2 + 0^2$.

Thus, a positive integer is a curtain if and only if the primes that $\equiv 3 \pmod 4$ in its prime factorization are raised to an even exponent or if there are none.

6 Sums of three squares

Sums of two squares are not that uncommon in the set of all non-negative integers. However, when another square is allowed to be added, they become even more of a regular occurrence. As stated in the preliminaries, these sums of three squares will be referred to as armchairs in this paper, denoted by the set, A, and the method of identifying integers that are armchairs was discovered by a French mathematician, Adrien-Marie Legendre, and Johann Peter Gustav Lejeune Dirichlet provided a simpler proof with ternary forms. However, either way, the complexities of it supercede this paper.

There are two parts to this, the "if" part and the "only if" part. The latter can be proved first on account of it simply being easier to do so:

Theorem 3. *For a non-negative integer, f, if and only if there do not exist two non-negative integers, r and x, where $f = 4^r(8x + 7)$, $f \in A$. In other words, an integer will be an armchair only if its largest factor not divisible by 4 does not have a remainder of 7 when divided by 8.*

Proof: Suppose that there exist two non-negative integers, r and x, where $f := 4^r(8x + 7) \in A$. If a variable, d, is assigned to represent $w^2 + y^2$, $d \in C$. By Lemma 1, z^2 is congruent to either 0, 1, or 4 modulo 8.

Suppose that $r = 0$, so $f = 8x + 7$, and thus, f is congruent to 7 modulo 8. Further suppose that z^2 is congruent to 0 modulo 8. In that case, $f - z^2 = w^2 + y^2 = d$ has to be congruent to $7 - 0 = 7$ modulo 8, but that would mean it is congruent to 3 modulo 4, which contradicts Lemma 2. Similarly, if z^2 is congruent to 4 modulo 8, d is congruent to $7 - 4 = 3$ modulo 8, which is also congruent to 3 modulo 4, once again contradicting Lemma 2. If z^2 is congruent to 1 modulo 8, following the same procedure as before, d is congruent to $7-1 = 6$ modulo 8, which goes against the other half of Lemma 2. As all cases are invalid, $r = 0$ similarly fails to be valid.

Otherwise, if $r > 0$, $4|f$, and thus, f is congruent to 0 modulo 4. If z^2 is congruent to 1 modulo 8, and thus, 1 modulo 4. Therefore, $f - z^2 = d$ is congruent to $0 - 1 = -1$ modulo 4, or to 3 modulo 4, but this is contradicted by Lemma 2, as $d \in C$. If d was assigned to represent $w^2 + z^2$ or $y^2 + z^2$, the same conclusions can be drawn about y^2 and w^2, them being $f - d$ in each respective case with d remaining a curtain. Therefore, y^2, z^2, and w^2 have to all be congruent to either 0 or 4 modulo 8. In either case, they are all divisible by 4. Thus, $f/4$ can be written as $w^2/4+y^2/4+z^2/4 = (w/2)^2+(y/2)^2+(z/2)^2$. If $r > 1$, this expression would also be divisible by 4, allowing the same conclusion to be reached. As f can be divided by 4 r times, each time dividing each variable by 2, $(w/2^r)^2 + (x/2^r)^2 + (z/2^r)^2 = f/(4^r) = 8x + 7$.

However, while the expression on the left fits the definition of an armchair, the expression on the right cannot be one, as it is f if $r = 0$, of which the possibility of it being an armchair was demonstrated to be invalid.

Therefore, the proposition that $r > 0$ also causes a contradiction, and as r is a non-negative integer, $r > 0$ and $r = 0$ both being impossibilities completely

invalidates the proposition that there exists an armchair for which, there exist two non-negative integers, x and r such that the armchair is equivalent to $4^r(8x+7)$.

The converse's proof requires more complicated tiers of mathematics, and thus, cannot be fully proved, end-to-end here. These papers describe parts of the proof in detail, but do not show it end to end either: (https://pollack.uga.edu/finding3squares-6.pdf, https://www.ams.org/journals/proc/1957-008-02/S0002-9939-1957-0085275-8/S0002-9939-1957-0085275-8.pdf), requiring theorems that are further found elsewhere.

7 Sums of 4 squares

For the previous two sections, the overarching sets were discriminatory, not allowing every non-negative integer. However, a British mathematician named Edward Waring believed that as the number of squares in the sum increases, the corresponding set eventually becomes none other than simply just every non-negative integer. It turned out that this happened rather early, only at four squares...

Lemma 6. *Euler's four-square-identity: Similar to Diophantus's Identity, if an integer is a sum of four squares and so is another, their product is also a sum of four squares. In other words,* $(m^2+n^2+o^2+p^2)*(q^2+r^2+s^2+t^2) = (mq+nr+os+pt)^2+(mr-nq+ot-ps)^2+(ms+nt-oq-pr)^2+(mt-ns+or-pq)^2$.

Proof: This can be demonstrated algebraically. If an integer is a sum of four squares it can be said to be $m^2+n^2+o^2+p^2$. Another integer that's a sum of four squares can be written as $q^2+r^2+s^2+t^2$. There product is therefore, by the distributive property, $m^2q^2+m^2r^2+m^2s^2+m^2t^2+n^2q^2+n^2r^2+n^2s^2+n^2t^2+o^2q^2+o^2r^2+o^2s^2+o^2t^2+p^2m^2+p^2n^2+p^2o^2+p^2t^2$. Isolate $m^2q^2+n^2r^2+o^2s^2+p^2t^2$, and designate the remaining expression as d. Note that when expanded by the distributive property, $(mq+nr+os+pt)^2 = m^2q^2+2mqnr+2mqos+2mqpt+n^2r^2+2nros+2nrpt+o^2s^2+2ospt$, which is just the former plus $2mqnr+2mqos+2mqpt+2nros+2nrpt+2ospt$. Thus, the expression which is the product of the sums of four squares can be restated as $(mq+nr+os+pt)^2+d-2mqnr-2mqos-2mqpt-2nros-2nrpt-2ospt)$. As for d, $m^2r^2+n^2q^2+o^2t^2+p^2s^2$ can now be isolated from it, with the remainder of d being represented by c.

Expanding $(mr-nq-ot+ps)^2$ reveals $m^2r^2-2mrnq-2mrot+2mrps+n^2q^2+2nqot-2nqps+o^2t^2-2otps+p^2s^2$, so $m^2r^2+n^2q^2+o^2t^2+p^2s^2 = (mr-nq+ot-ps)^2+2mqnr+2mrot-2mrps-2nqot+2nqps+2ospt$, with $2mrnq$ and $2otps$ being rearranged. Note that the rearrangement causes the terms to be the additive identity of $-2mqnr$ and $-2ospt$, so those can be cancelled out. Thus, the product of the sums of four squares can now be said to be $(mq+nr+os+pt)^2+(mr-nq+ot-ps)^2+c-2mqos-2mqpt-2nros-2nrpt+2mrot-2mrps-2nqot+2nqps$.

The next isolation can be $m^2s^2+n^2t^2+o^2q^2+p^2r^2$, which, when performed, leaves the remainder as simply $m^2t^2+n^2s^2+o^2r^2+p^2q^2$. For the former expression, $(ms+nt-oq-pr)^2 = m^2s^2+2msnt-2msoq-2mspr+n^2t^2-2ntoq-2ntpr+o^2q^2+2oqpr+p^2r^2$, so the former expression is $(ms+nt-oq-pr)^2-2mnst+2msoq+2mspr+2ntoq+2ntpr-2oqpr$. With $2msoq$ being rearranged to $2mqos$, it cancels out the term, $-2mqos$ shown in the expression at the end of the last paragraph. $2mspr$ can similarly be rearranged to $2mrps$ to cancel out $-2mrps$, and $2ntoq$ to $2nqot$ to cancel out $-2nqot$. With $2ntpr$ being rearranged to $2nrpt$ to similarly cancel out a term in the expression, the expression becomes $(mq+nr+os+pt)^2+(mr-nq+ot-ps)^2+(ms+nt-oq-pr)^2+m^2t^2+n^2s^2+o^2r^2+p^2q^2-2mqpt-2nros+2mrot+2nqps-2mnst-2oqpr$. The terms in the expression that are not a square of a polynomial with four terms can be rewritten to be $(mt-ns+or-pq)^2$, so the whole product can be represented by $(mq+nr+os+pt)^2+(mr-nq+ot-ps)^2+(ms+nt-oq-pr)^2+(mt-ns+or-pq)^2$, which is a sum of four squares.

Lemma 7. *For any odd prime, there is a multiple of it such that the multiple is a sum of four squares, but the multiple is less than the square of the odd prime. In other words, for an odd prime, f, there exists a positive integer k such that fk is a sum of four squares, but $kf < f^2$.*

Proof: For an odd prime, f, $g := \frac{f-1}{2}$. Note that g is necessarily a positive integer because f is odd and positive. It can be said that for all integers that are the square of a non-negative integer less than or equal to g, for any two of them, x and y, it cannot be the case where $x \equiv y \pmod{f}$ with x and y being distinct. This is because if that was the case, $f|x-y$. If x_1 and y_1 are the respective square-roots of x and y, $f|(x_1+y_1)(x_1-y_1)$, but as f is a prime, meaning that one of the prime factorizations of the specified divisors of x^2-y^2 either contains p or $x^2-y^2=0$. It is impossible for them to be distinct, as x_1 and y_1 are given as positive integers less than or equal to g, so x_1+y_1's maximum value is $2g$, which is less than f, and thus can't be a multiple of it. They are said to be non-negative integers, meaning that x_1+y_1 is 0 at the least. As neither can be negative, they are both 0, making them equal. If x^2-y^2 is 0 by virtue of $x_1-y_1=0$, then $x_1=y_1$. If they are equivalent, there squares are as well, meaning that $x=y$

If squares of distinct integers less than or equal to g never have the same remainder when divided by f, the negative value of the remainder, or it subtracted from f, is also always distinct, so the additive inverses of the squares of distinct integers less than or equal to g also never have the same remainder when divided by f. Numbers one less than these integers(or in other words, $-h^2-1$ where $0 \leq h \leq e$ and h is an integer) also have the same property, henceforth.

As there are $g+1$ squares of non-negative integers less than or equal to g, and $g+1$ integers of the form $-h^2-1(0 \leq h \leq e$ and h is an integer), there are $2g+2 = f+1$ of these. As there are only f possible remainders when dividing by f, the pigeonhole principle can prove that two of the integers have to have the same remainder, or in other words, because there are $f+1$ of these

integers and f remainders, two of the integers have to have the same remainder as otherwise one would have no remainder as that is impossible. However, as shown, distinct squares of integers less than or equal to g cannot have the same remainder, nor can distinct integers of the form $-h^2-1 (0 \leq h \leq e$ and h is an integer), meaning that the two integers with the same remainder has to have one of each to avoid having both of one set.

If two integers have the same remainder when divided by f, there difference is divisible by f, so if a square of an integer less than or equal to g is w^2, $w^2-(-h^2-1) = w^2+h^2+1$. $d := w^2+h^2+1 = w^2+h^2 = 1^2 = 0^2$, and $f|d$. Also, $w, h \leq g$, meaning that $d = w^2+h^2+1 \leq 2g^2+1$. In addition, $2g^2+1 < f^2 = (2g+1)^2 = 4g^2+4g+1$, as $g > 0$ on account of f being a prime, so if $g = 0$, $f = 1$, which cannot be the case, and if it is less, f is negative, which similarly is untrue. Henceforth, $d \leq 2g^2+1 < f^2$, and $d < f^2$.

Theorem 4. *For any non-negative integer, w, there exist four (not necessarily distinct) integers, g, h, i, j, such that $g^2+h^2+i^2+j^2 = w$.*

Proof: From the above Lemma, it can be said that for an odd prime f, a multiple of it less than f^2 is a sum of four squares. In other words, for an integer k, where $0 < k < f$, jk is a sum of four squares. Thus, $g^2+h^2+i^2+j^2 := kf$. If k is even, so is kf, and of g, h, i, j, it cannot be the case where either only one of them is odd or all three of them are. This is because an integer's parity matches its squares(because even numbers $\equiv 0 \pmod 2$ and $0^2 = 0$, and odd numbers $\equiv 1 \pmod 2$, and $1^2 = 1$), and one odd added to three evens or three odds added to one even produces an odd sum(for an algebraic representation, $(2w+1)+2x+2y+2x = 2(w+x+y+z)+1$, and $(2w+1)+(2x+1)+(2y+1)+2z = 2(w+x+y+z)+3 = 2(w+x+y+z+1)+1)$.

Therefore, there are three cases, that g, h, i, j are all even, that they are all odd, or that two of them are even, and the other two odd. In the first case, g^2+h^2 and i^s+j^2 are sums of even squares, and thus, sums of even integers, and thus, even. They are also curtains, so they are even curtains. In the second case, let g, h be the odd integers and i, j be the even integers.. Following the logic of the first case, i^2+j^2 is an even curtain. g^2+h^2 is too, because it is the sum of odd squares, or the sum of odd integers, and that is even$(2x+1+2y+1 = 2(x+y+1)$. Following this logic, if all are odd, g^2+h^2 and i^2+j^2 are still even curtains,

By Fermat's Theorem of two squares, an integer is a curtain if and only if all the primes that are one less than a multiple of 4 have an even exponent. However, 2 is not one of those primes, so if 2 is removed from a curtain's prime factorization(if the curtain is divided by 2), the exponents of its primes one less than a multiple of 4 would not be affected, and thus, half of a curtain is still a curtain as long as the former curtain was even. This means that when fk is split into two even curtains, both can be divided by two to result in two curtains nonetheless, of which, add to $f * \frac{k}{2}$, which is a sum of two curtains and thus a sum of four squares. If $\frac{k}{2}$ is also even, this process can be repeated until an odd integer results from the repeated halving of k. Let this odd integer be denoted

as m. If k was not even, meaning that the process could not have happened, $m := k$. In either case, fm is a sum of four squares

If $m > 1$, let a, b, c, d be defined as integers such that $a \equiv g \pmod{m}$, $b \equiv h \pmod{m}$, $c \equiv i \pmod{m}$, and $d \equiv j \pmod{m}$, but $\frac{-m}{2} < a, b, c, d < \frac{m}{2}$(note that because l is odd, they cannot be exactly $\frac{m}{2}$ or its negative value, as they have to be integers). As all of their absolute values are less than $\frac{m}{2}$, each of their squares are less than $\frac{m^2}{4}$. This means that $a^2 + b^2 + c^2 + d^2 < 4 * \frac{m^2}{4} = m^2$. In addition, $m|a^2 + b^2 + c^2 + d^2$, as $a^2, b^2, c^c, d^2 \equiv g^2, h^2, i^2, j^2 \pmod{m}$ respectively on account of each of a, b, c, d being congruent to a respective value of g, h, i, j with respect to the modulus of m, and $g^2 + h^2 + i^2 + j^2 = fm$, so $m|g^2 + h^2 + i^2 + j^2$. But as $(a^2 + b^2 + c^2 + d^2) < m^2$, for $n := \frac{(a^2+b^2+c^2+d^2)}{m}$, $n < m$.

If $n = 0$, $a^2 + b^2 + c^2 + d^2 = mn = m * 0 = 0$, but the only way this is happening is if $a, b, c, d = 0$, as squares cannot be negative, and if a square is 0, so is its square-root. However, if that is the case, $g, h, i, j \equiv 0 \pmod{m}$, meaning that $m|g, h, i, j$, which means that $m^2|g^2, h^2, i^j, j^2$, so $m^2|g^2 + h^2 + i^2 + j^2 = mp$. However, if $m^2|mp$, $\frac{mp}{m^2} = \frac{p}{m}$ is an integer. Primes are only divisible by themselves and 1, but in this hypothetical, $m >$ 1m and m is a factor of k, meaning that $m \leq k$, and $k < f$ by the Lemma above this Theorem, meaning that $m < f$ and $n \neq 0$. Therefore, $0 < n < m$.

By Euler's four-square identity, $mn * fm = (a^2 + b^2 + c^2 + d^2)(g^2 + h^2 + i^2 + j^2) = (ag + bh + ci + dj)^2 + (ah - bg + cj - di)^2 + (ai + bj - cg - dh)^2 + (aj - bi + ch - dg)^2$. Note that $m|ah - bg$, as bg and ab have a difference of a multiple of bm on account of g and a having a difference of a multiple of them(they have the same remainder when divided by m based on how a is defined). ab and ah have a difference of a multiple of am on account of b and h having a difference of m by how b is defined. Thus, $ah - bg$ is a multiple of bm added to a multiple of am, which is ultimately a multiple of m. The same logic can be applied to $cj - di$, $ai - cg$,$bj - dh$, $aj - dg$, and $ch - bi$ on account of all of them also being a difference of a two products where for a factor in of them, there is a factor in the other that shares its remainder when divided by m.

Henceforth, all of those differences are divisible by m, which means that certain sums of those differences, those being $ah - bh + cj - di$, $ai - cg + bj - dh$, or to rearrange, $ai + bj - cg - dh$, and $aj - dg + ch - bi$, or to rearrange, $aj - bi + ch - dj$ are all divisible by m. In addition, $m|ag + bh + ci + dj$, as $ag \equiv g^2 \pmod{m}$ on account that $g \equiv a \pmod{m}$, so the products of each of g and a and g have the same remainder when divided by m. The same logic follows such that $bh \equiv h^2 \pmod{m}$, $ci \equiv i^2 \pmod{m}$, and $dj \equiv j^2 \pmod{m}$, Thus, $ag + bi + ci + dj \equiv g^2 + h^2 + i^2 + j^2 \equiv fm0 \pmod{m}$, so $m|ag + bh + ci + dj$. As $ag + bh + ci + dj$, $ah - bg + cj - di$, $ai + bj - cg - dh$, and $aj - bi + ch - dg$ are all divisible by m.

Thus, if $x := \frac{ag+bh+ci+dj}{m}$, $y := \frac{ah-bg+cj-di}{m}$, $z := \frac{ai+bj-cg-dh}{m}$, and $r := \frac{aj-bi+ch-dg}{m}$, $x^2+y^2+z^2+r^2 = \frac{(ag+bh+ci+dj)^2+(ah-bg+cj-di)^2+(ai+bj-cg-dh)^2+(aj-bi+ch-dg)^2}{m^2}$, and the numerator of the expression to the right is $mn * fm$ as demonstrated at the beginning of the second-last paragraph. Thus, $x^2 + y^z + z^2 + r^2$ is

$\frac{mn*fm}{m^2} = fn$.

Therefore, if $m > 1$ and m is odd, there exists an integer n, where $0 < n < m$, such that nf is also a sum of four squares. The procedure done to k can be done to n, where m_1 results after repeatedly halving n if it is even and if otherwise, $m_1 := n$, then n_1 can be derived from the same procedure from which n was derived from m. As $n_1 < m_1 \leq n$, to $n_1 < n$, this algorithm always reduces an integer, but never to 0 as demonstrated in the fourth-last paragraph. Thus, this algorithm eventually produces 1, as that's what happens when an integer has to reduce but not reach 0. As it always produces 1, $1 * f$ is a sum of four squares. As f can be any odd prime, all odd primes are thus, the sum of four squares. In addition, $2 = 1^2 + 1^2 + 0^2 + 0^2$, so all primes are the sum of four squares. By Euler's four-square identity, this also means that all composites are, as every composite, by definition, is a product of two or more (not necessarily distinct) primes, and the identity proves that the product of sums of four squares is a sum of four squares. In addition, $0 = 0^2 + 0^2 + 0^2 + 0^2$ and $1 = 1^2 + 0^2 + 0^2 + 0^2$, so 0, 1, and every prime and composite are a sum of four squares, which accounts for every non-negative integer.

This proof required a length explanation, but there is a simpler proof however, but this proof requires assuming the Legendre-Gauss theorem. While not proved in this paper, it is not simply a conjecture, and thus, can be taken to be true. If it still in poor taste to use a theorem which this paper did not prove, that is why this proof is simply an alternate. The theorem has been proven before the Legendre-Gauss theorem by Joseph-Louie Lagrange in the 18th century regardless, this proof only existing to provide a simpler demonstration.

Alternate Proof: Let X be the set for which if and only if for any non-negative integer, x, there exist four (not necessarily distinct) integers, g, h, i, j, such that $g^2 + h^2 + i^2 + j^2 = x$.

Firstly, if for a non-negative integer, a, $a \in A$, there exist 3 integers, x, y, and z, where $x^2 + y^2 + z^2 = a$, by the definition of A. Furthermore, $x^2 + y^2 + z^2 + 0^2 = x^2 + y^2 + z^2$, or a. Therefore, $a \in X$.

By the Legendre-Gauss Theorem, any non-negative integer, t, is not an armchair only if there exist two non-negative integers, x and r, where $w = 4^r * (8x + 7)$. If $r = 0$, $w = 4^0 * (8x + 7)$, or simply $8x + 7$, and as x is an integer, t can only be a non-armchair if it is 7 mod 8. Otherwise, $4|4^r$, and thus, $4|(4^r * (8x + 7))$, so $4|g$, meaning that t can only be a non-armchair if it is 0 or 4 mod 8. As both cases are possible, the conclusion is that t can only be a non-armchair if it is 0, 4, or 7 mod 8, and otherwise, $w \in X$.

However, if $w \equiv 7 \pmod 8$, $w - 1$ is 6 mod 8, and thus, an armchair. Therefore, there exist 3 integers, x, y, and z, where $x^2 + y^z + z^z = w - 1$ If 1 is added to both sides of the expression, but written as as 1^2 for the left side, $x^2 + y^2 + z^2 + 1^2 = w - 1 + 1 = w$, and thus, $w \in X$.

Furthermore, if $w \equiv 4 \pmod 8$, but not an armchair, there exist two non-negative integers, x and r, where $w = 4^r * (8x + 7)$, but $r > 0$, as if t was simply $8x + 7$, it would be 7 mod 8 rather than 0 or 4. However, let $v = 8x + 7$. $v \equiv 7 pmod 8$, and therefore, $v \in X$, so there exist 4 not necessarily distinct integers, g, h, i, and j, where $g^2 + h^2 + i^2 + j^2 = v$. As $4^r * v = w$, $4^r * (g^2 + h^2 +$

$i^2 + j^2) = w = 4^r(g^2) + 4^r(h^2) + 4^r(i^2) + 4^r(j^2) = w$. In addition, $4^r = (2^2)^r = 2(2r) = (2^r)^2$. Thus, $(2^r)^2(g^2) + (2^r)^2(h^2) + (2^r)^2(i^2) + (2^r)^2(j^2) = w$. The equation can be rewritten as $(2^r g)^2 + (2^r h)^2 + (2^r i)^2 + (2^r j)^2 = w$, and therefore, $w \in X$.

Thus, for any non-negative integer, b, $b \in X$ if it is either 0, 4, or 7 mod 8 or otherwise. This is a disjunction of a proposition and its complement, so X contains all non-negative integers, and therefore, for any non-negative integer, t, there exist four (not necessarily distinct) integers, g, h, i, j, such that $g^2 + h^2 + i^2 + j^2 = w$.

8 Sums of increasing squares

So far, all the main sections focused on a fixed number of squares. However, when the fix is loosened around the number of squares, but a new regulation is added on what squares are allowed to be added, which is that all the squares must be of consecutive positive integers, the behavior of the sum can still be analyzed. The first step as to how is to take a look at the next level of exponents, none other than cubes.

Lemma 8. $\sum_{k=1}^{n} k^2 = \frac{(n+2)(n+1)(n)}{3} - \frac{(n+1)(n)}{2}$, *if n is a positive integer.*

Proof: $((x+2)^3 - (x+1)^3) - ((x+1)^3 - x^3)$ can be solved algebraically. The difference between x^3 and $(x+1)^3$ is $3x^2 + 3x + 1$, and of $(x+1)^3$ and $(x+2)^3$ is $3x^2 + 9x + 7$, making the difference between their differences $6x + 6 = 6(x+1)$.

For example, for $x = 0$, there is a difference of $6(x+1) = 6$ between $1^3 - 0^3$ and $2^3 - 1^3$, which is indeed true, $(8-1) - (1-0) = 7 - 1 = 6$. As $1^3 - 0^3 = 1$, that can be said to be the initial value of differences. From there, 6 is added to get $2^3 - 1^3$, and from there, $6(1+1) = 12$ can be added to get $3^3 - 2^3$. Thus, each difference of cubes is essentially $1 + 6 + 12...6n$, where n^3 is the cube that's being subtracted. If each difference of cubes can be written as a line in that format, an overall cube, which is just 0 with all the differences up to it added can be written as a triangle, of which the first five rows are depicted below:

1				
1	6			
1	6	12		
1	6	12	18	
1	6	12	18	24

For a positive integer, n n^3 can be calculated by adding every term in the first n rows of the triangle. However, that still is not on the topic of the sum of increasing squares, so the triangle will have to be altered.

The left-most column of the triangle can be shaved off to leave the table as simply of multiples of 6s, where the first five rows are as follows:

6				
6	12			
6	12	18		
6	12	18	24	
6	12	18	24	30

Unfortunately, the triangle no longer corresponds to cubes. Instead, the sum of all terms in the first n rows is $(n+1)^3-(n+1)$. As removing the left-most column also removed the top-most row, the nth row here refers to the $n+1$th row on the original triangle, hence the first term being $(n+1)^3$. Also, the left-most column would have added $n+1$ if it was still there, as each element in it is 1, and as said, the nth row would be the $n+1$th row in the original triangle, so $n+1$ is subtracted to account for its loss.

This triangle is still not useful in conveying the sum of increasing squares however, so more operations have to be one. Another one will be to divide each term by 3, changing the triangle's appearance to:

2				
2	4			
2	4	6		
2	4	6	8	
2	4	6	8	10

The expression that conveys the sum of all terms in the first n rows of this triangle has a simple change from the last one, simply being divided by 3 to match that being done to all the terms, so the corresponding expression for this one is $\frac{((n+1)^3-(n+1))}{/}3$.

The last step is to subtract every term by 1. When this is done, each row of the triangle is the sum of consecutive odds as follows:

1				
1	3			
1	3	5		
1	3	5	7	
1	3	5	7	9

This may seem pointless at first, but note that each row, when added up, is a square. Differences of squares are simpler than differences of cubes, with $(x+1)^2 = x^2 = x^2+2x+1-x^2 = 2x+1$, meaning that they are just odd numbers that increase by 2 for the next set of squares. 3 is 2^2-1^2, so each square is just 1 with increasing odds, starting with 3, added.

However, a new expression is needed for this triangle. As 1 is subtracted from each term, the overall loss is the amount of cells in the first n rows of a triangle. As discovered allegedly by Gauss as a schoolboy, this amount, $\sum_k^n k$, or $1+2.....n$, is half of $(1+2...n)+(n+(n-1)....1) = (n+1)(n)$. $\frac{(n+1)(n)}{2} = \frac{(n^2+n)}{2}$, which is the loss for the first n rows. Thus, the expression dictating the sum of terms in the first n rows is $\frac{((n+1)^3-(n+1))}{3} - \frac{(n^2+n)}{2}$.The form can be changed if

necessary. As said, $\frac{(n+1)(n)}{2} = \frac{(n^2+n)}{2}$, so the former can be used instead. To change the first term to a similar format, as a product of first-degree powers of n, the numerator can be altered to $n^3+3n^2+3n+1-(n+1) = n^3+3n^2+2n = n(n^2+3n+2) = n(n+1)(n+2)$. Thus, the sum of squares up to n^2 is $\frac{n(n+1)(n+2)}{3} - \frac{(n(n+1))}{2}$.

9 References

(Bertrand, Mike, Euler proves Fermat's theorem on the sum of two squares 2016 Sep 7, https://nonagon.org/ExLibris/euler-proves-fermats-theorem-sum-two-squares)

(Pollack, Paul, and Schorn, Peter,DIRICHLET'S PROOF OF THE THREE-SQUARE THEOREM: AN ALGORITHMIC PERSPECTIVE 2016 Sep 7, https://nonagon.org/ExLibris/euler-proves-fermats-theorem-sum-two-squares)

(Ankeny, NC, SUMS OF THREE SQUARES, Massachusetts Institute of Technology, https://www.ams.org/journals/proc/1957-008-02/S0002-9939-1957-0085275-8/S0002-9939-1957-0085275-8.pdf)