Premios del Departamento de Matemáticas de la Universidad Autónoma de Madrid para Estudiantes de Secundaria

Tercera Edición, 2008/2009

TRABAJO: Un geoplano algo irracional

GANADOR EN LA CATEGORÍA DE E.S.O.

AUTORES:

- Germán García Butenegro
- Olmo Fernández García

TUTORES:

- Carlos Usón Villalba

CENTRO: IES Batalla de Clavijo (La Rioja)

Un geoplano algo irracional.

Introducción y antecedentes:

Desconocemos que existan antecedentes. El problema de partida parecía algo simple: ¿Cuántas cuerdas de distinta longitud se pueden trazar en una trama cuadrada 4x4? Y no parece que, si alguien intentó resolverlo en algún momento su solución haya pasado a la historia de las matemáticas. Y perviva en algún sitio.

Pero cuidado… porque pronto llegó la generalización y, a partir de ahí las preguntas se amontonaron a nuestro alrededor y de hecho todavía nos persiguen… De forma que, después de intentar responder a algunas llegamos a la conclusión de que nuestro verdadero primer problema era éste:

¿Existe alguna trama de puntos en la que sea posible trazar las raíces cuadradas de todos los números enteros?

Es decir, ¿podemos encontrar un entramado de puntos en el que sea posible representar, mediante un línea que una dos de ellos, todos y cada uno de los radicales cuadráticos? En un principio intentamos organizarlo como un proceso tal como fueron apareciendo los resultados en clase, aunque después nos dimos cuenta de que el sistema que vamos a mostrar ahora es mucho más práctico.

Resultados:

A lo largo del desarrollo del problema, los resultados obtenidos aparecen destacados en color naranja.

1.- Trama cuadrada en 2D:

-¿Cuántas longitudes distintas se pueden crear en una trama cuadrada de dimensiones NxN?

Empezamos por el proceso más lógico, es decir, comprobándolos uno a uno y remarcando en verde las distancias nuevas que íbamos obteniendo:

- **1x1= 2 distancias.**
- **2x2= 5 distancias.**
- **3x3= 9 distancias.**
- **4X4= 14 distancias**
- **5x5= 20 distancias**

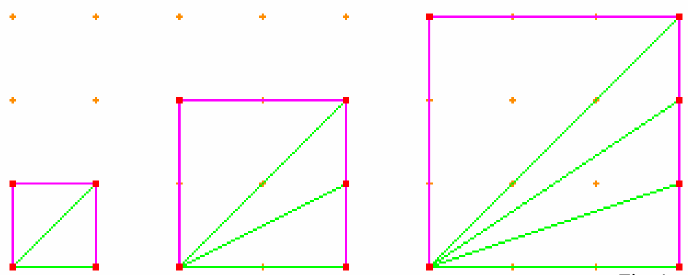


Fig. 1

Los resultados forman una progresión aritmética de orden dos, ya que, partiendo de un vértice y uniéndolo con los puntos del lado opuesto, se obtienen todas las posibilidades que no estaban en la trama anterior (Fig. 1).

¿Existen garantías de esto?

Sí, porque las líneas que terminan en el interior venían ya dadas por geoplanos anteriores, y las que empiezan y terminan en los lados son producto de las que salen del vértice. Con cada cuadrado de lado n se añaden (n+1) longitudes nuevas. Es decir, el número de longitudes de un cuadrado de lado n viene dado por la progresión [2, 2+3, 2+3+4,…, 2+3+4+…+(n+1)]
Ahora sólo queda dar una fórmula:
C_{NxN}= (n+1) sumorial −1 u, homólogamente,

$C_{N\,x\,N} = \frac{n(n+3)}{2} = \frac{n^2+3n}{2}$ **= • $_{n+1}$−1 ya que, si nos fijamos bien se corresponde con los números triangulares menos una unidad.**

Ahora bien, ¿cómo sabemos que en esas tramas hemos trazado TODAS las distancias posibles?

Porque el cuadrado es una figura simétrica; si cogemos solo medio geoplano usando como eje la diagonal y trazamos todas las distancias posibles, al hacer después la simetría axial con la diagonal como eje obtenemos TODAS las distancias por duplicado.(Fig. 1,5)

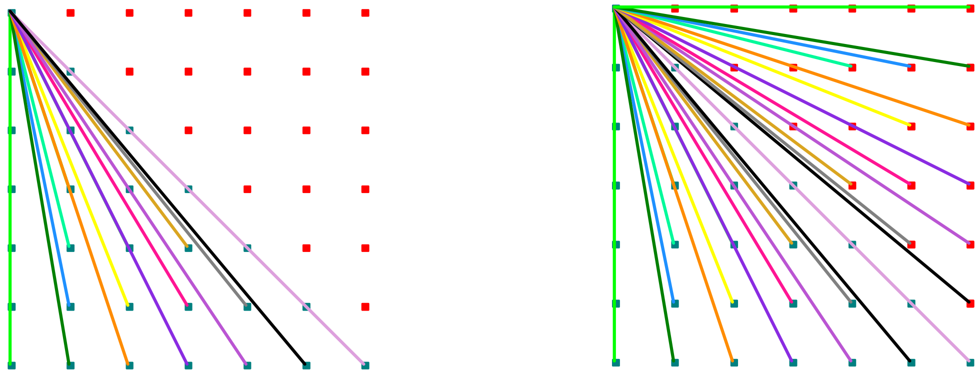


Fig 1,5

Planteamiento 2, ¿qué longitudes pueden aparecer en un geoplano?

- **Los números naturales: 1, 2, 3…**
- **Unas raíces concretas: √2, √5, √10, √17…**

Vale, salen unas cuantas raíces. Pero, ¿pueden salir todas?

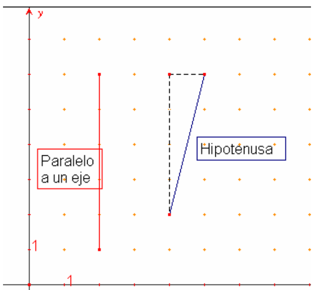
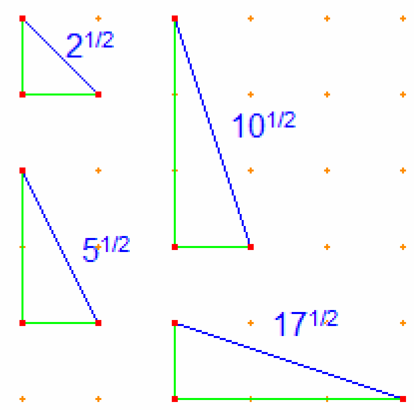


Fig. 2



No. Sin ir más lejos, √3 no puede salir, ya que para obtenerlo necesitaríamos un triángulo rectángulo de catetos 1 y √2. Y, uniendo dos puntos de la trama, no sale.
Vale. O sea, que sólo salen unas cuantas raíces veamos qué tienen en común…
Son las raíces de la suma de dos cuadrados perfectos
Ah, son las raíces de los Números

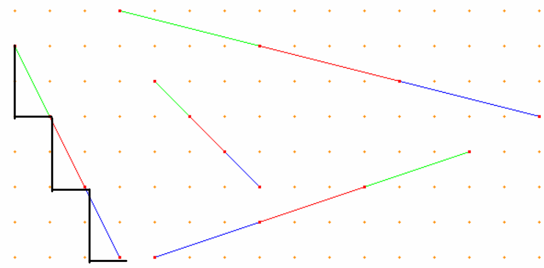
Pitagóricos, es decir, las raíces de aquéllos que se pueden expresar como la suma de dos cuadrados perfectos.

Lo que da pie a una primera hipótesis:
H1: En una trama cuadrada aparecen sólo las distancias diagonales de rectángulos de lados enteros (números pitagóricos)

Demostración:

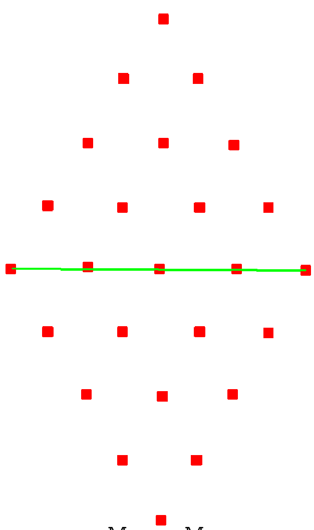
Cualquier segmento en un geoplano puede ser, o bien paralela a un eje, o bien determinado por las coordenadas enteras de sus vértices, es decir, puede ser la hipotenusa de un triángulo rectángulo de catetos enteros *(Fig. 2).*

Un momento, también salen los múltiplos de √2. ¿Son Pitagóricos?
Comprobémoslo en un caso concreto:
$2\sqrt{2}=\sqrt{(4\cdot 2)}=\sqrt{8}$
Ah, pues sí, pero… ¿podemos generalizar eso que hemos hecho arriba? Es decir, ¿para todo P pitagórico, KP pertenece a Þ?



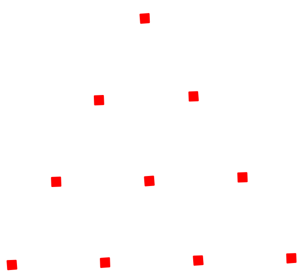
Demostración gráfica: **Cada múltiplo se construye en base a la repetición del triángulo que ha generado el pitagórico de partida.**

Es decir, KP pertenece a P, luego: Los múltiplos de los números Pitagóricos también son Pitagóricos.
Pues tenemos un problema, ya que no podemos alcanzar todas las raíces cuadradas de un números naturales mediante este procedimiento, o dicho de otra forma: No todos los irracionales cuadráticos son expresión de una distancia en una trama cuadrada
¿Existirá una trama de otro tipo en la que figuren como distancias entre sus puntos todos los irracionales cuadráticos? **En el plano, puesto que los únicos polígonos regulares que lo teselan son cuadrados, triángulos y hexágonos, y estos últimos se pueden descomponer en triángulos, la única trama "regular" que nos queda por revisar es la triangular. A ello:**



Trama isométrica en 2D:

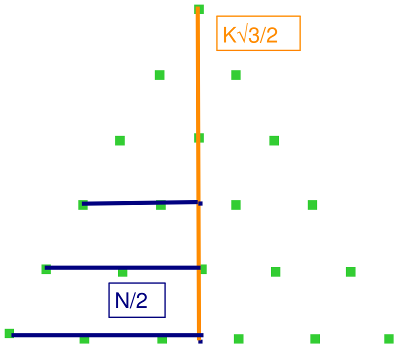
Introducción:
Como se puede apreciar, la "única" diferencia es el motivo de la trama, que es diferente. Igual que en el cuadrado, usamos medio geoplano.



Un geoplano algo irracional.

En un principio lo intentamos con rombos (derecha) por aquello de que se parecían más al cuadrado y quizás hubiese alguna analogía, pero intuimos que con triángulos era un poco más práctico. Y en efecto lo era, ya que nos permitía sacar distancias aplicando el teorema de Pitágoras de forma sencilla.

Ahora, en naranja y verde señalamos las distancias nuevas por cada nivel, desde el 0. Con lo que obtenemos:



Nivel	Distancias nuevas
0	1
1	1
2	2
3	2
4	3
5	3

Esto parece una sucesión de recurrencia, de la que se puede obtener con relativa facilidad un término general. O, mejor dicho, dos:

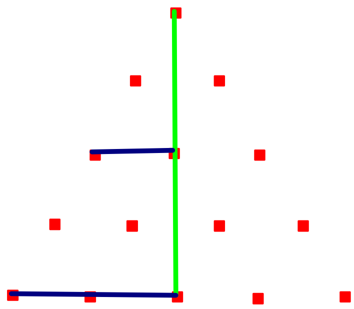
-SI N -Nivel- es par → → → → $\frac{N}{2}+1$

-Si N es impar → → → → → $\frac{N+1}{2}$

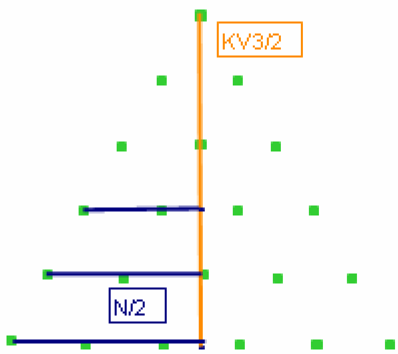
Un ejemplo: Nivel 6. Distancias NUEVAS:
6/2+1 = 4
Otro: Nivel 5. Distancias NUEVAS: 5+1/2 =3
¡Bien, funciona!

Tras crear un par de distancias, con 6 niveles, caímos en la cuenta de que, para calcular las distancias del punto superior al resto de puntos, usando el Teorema de Pitágoras, se mostraban dos regularidades:

- El cateto mayor, la línea verde, es un múltiplo de $\frac{\sqrt{3}}{2}$
- El cateto menor, la línea azul, es un múltiplo de $\frac{1}{2}$



Significa que, por ejemplo, en el nivel 3, el cateto mayor es 3(√3/2) y el cateto menor puede ser ½ ó 3/2; en el nivel 4, el cateto mayor es 4(√3/2) y el menor, 2/2 ó 4/2.
A raíz de estos cálculos, nos dimos cuenta de que, para toas las distan-



cias, estábamos usando la misma fórmula.
¿La misma fórmula? ¡Ah! Es verdad.

$$\sqrt{\left(K\frac{\sqrt{3}}{2}\right)^2+\left(\frac{N}{2}\right)^2}$$

Esta fórmula, en la que K es el nivel y N el numerador del cateto menor, tiene un par de condiciones o trabas:

- **K y N son ambos pares o impares.**
- **K es SIEMPRE mayor o igual que N.**

Dada la primera condición, empezaremos cuando K y N son pares.
Pensándolo bien, al ser K par, se simplifica con el 2, y N también, quedando: $\sqrt{\left(P\sqrt{3}\right)^2+M^2}=\sqrt{3P^2+M^2}$ **, siendo P = K/2 y M = N/2.**
Emitimos ahora un trocito del diálogo inmediatamente posterior al descubrimiento

- **O sea, que hemos saltado la barrera de los Pitagóricos**
- **… y menudo salto. Habrá que ponerles nombre, ¿no?**
- **Vale. ¿Qué nombre se te ocurre?**
- **Pues…los *Números de Apoyo*, porque los descubrimos en clase de apoyo.**
- **No es mala idea.**

Pues, allá vamos con los Números de Apoyo:

$$\sqrt{3\cdot 2^2+0^2}=\sqrt{12}$$

$$\sqrt{3\cdot 2^2+2^2}=4$$

$$\sqrt{3\cdot 4^2+2^2}=\sqrt{52}$$

$$\sqrt{3\cdot 4^2+2^2}=8$$

$$\sqrt{3\cdot 6^2+2^2}=\sqrt{112}$$

Tras estos intentos, nos dimos cuenta de que habíamos cometido un error de dimensiones ionosféricas: estaba contando P y M como K y N.
El otro día, nos dimos cuenta del error, re-ampliamos el término general y desarrollamos el inicial, obteniendo: $\sqrt{(K\frac{\sqrt{3}}{2})^2+(\frac{N}{2})^2}=\sqrt{\frac{3K^2+N^2}{4}}$ **, que, por cierto, evita liarnos con P y M, ya que con K y N basta.**
Ahora, la sucesión completa de los Números de Apoyo, ya que antes, sólo salían la mitad de términos:

$$\sqrt{\frac{3\cdot 2^2+0^2}{4}}=\sqrt{3} \qquad \sqrt{\frac{3\cdot 2^2+2^2}{4}}=2 \qquad \sqrt{\frac{3\cdot 4^2+0^2}{4}}=\sqrt{12}$$

$$\sqrt{\frac{3\cdot 4^2+2^2}{4}}=\sqrt{13} \qquad \sqrt{\frac{3\cdot 4^2+4^2}{4}}=4$$

Que no salen todos es obvio: √7 no sale. Pero ¿Cuáles salen? Dejamos de momento la pregunta en el aire y seguimos buscando una trama más dispuesta a permitir nuestro objetivo. Podríamos tomar tramas arbitrarias, pero nos decantamos por subir de dimensión.

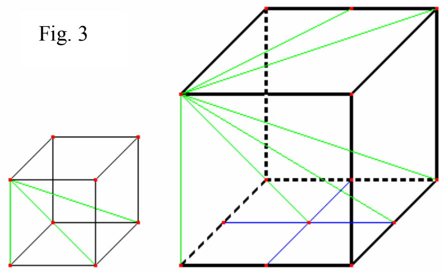
Evolucionemos a la tercera dimensión: los cubos

Trama cuadrada en 3D (Cúbica)

¿Cuántas distancias aparecen?

Comprobemos los primeros casos *(Fig. 3)*:
Siguiendo el mismo modelo, la precipitación hizo que al principio nos dejáramos algunas longitudes, concretamente las que van hacia los puntos interiores de la base -en azul- pero nos dimos cuenta y lo cambiamos.

Fig. 3



- 1x1x1: 3 longitudes
- 2x2x2: 9 longitudes
- 3x3x3: 19 longitudes

Vamos incorporando 6, 10, 15 Lo que da pie a otra primera hipótesis:

H1: Cada paso añade el número triangular de orden n+1 de nuevas distancias, con lo que se obtienen los números tetraédricos de orden n+1 a los que hay que restarles una unidad.

Demostración: Si nos fijamos y vamos colocando un cubo dentro de otro de arista dos y este dentro de otro de arista tres, etc. las nuevas distancias van formando tetraedros (números tetraédricos) que son la suma de números triangulares, luego cada vez vamos añadiendo un número triangular.

Esto nos da pie a pensar que en cuatro dimensiones sumaremos cada vez un número tetraédrico de distancias nuevas. Pero eso habría que ver si se cumple, de momento nos enfrentamos a una progresión aritmética de orden tres cuyo término de lugar "n", por tanto, es la suma de los n-1 anteriores de una aritmética de orden dos.

1 2 3 4 5 6 7 8 9 10 … Naturales

1 3 6 10 15 21 28 36 45 55….Tiangulares

1 4 10 20 35 56 84 120 … Tetraédricos

Disposición que se puede ver por diagonales en un triángulo de Pascal.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

Con lo que resulta muy fácil encontrar el término general:

$T_n=\bullet_{n-1}+T_{n-1}$ es decir $T_n=C_3^{n+2}=\dfrac{n(n+1)(n+2)}{3*2}$

¿Qué distancias aparecen?

Primero intentamos comprobar las que iban surgiendo en cada cubo, pero después nos dimos cuenta de que así no íbamos a llegar a ningún lado. El profesor nos recomendó que buscásemos una especie de teorema de Pitágoras para 3 dimensiones, porque estos segmentos también están delimitados por coordenadas enteras. Comenzamos por comprobar algunos casos:

- **1x1x1:** $\sqrt{3}$
- **1x1x2:** $\sqrt{6}$
- **1x2x2:** $\sqrt{9}$
- **2x2x2:** $\sqrt{12}$

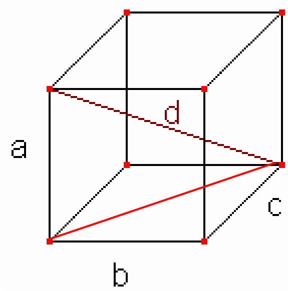


Fig. 4

No sale $\sqrt{7}$, estamos como antes, no es una trama "completa". Salen: ¿Las raíces de los múltiplos de 3? No parece lógico, tratándose de sumar cuadrados…o igual sí. Un momento, ¡puede ser sencillamente eso, la raíz de la suma de los cuadrados de las coordenadas, igual que en 2D!

Vamos a intentar comprobarlo:

$\sqrt{c^2+b^2}^{\,2}+a^2=d^2$ *(Fig. 4)*, es decir $a^2+b^2+c^2=d^2$

¡Es así de sencillo! Un procedimiento similar podría servir para calcular distancias cualesquiera en un geoplano de N dimensiones. De esa forma podemos pensar en una trama hipercúbica. Con lo que solo nos quedaría averiguar cuál es el menor número de cuadrados perfectos en los que se puede dividir un número cualquiera. Si ese número es finito hemos acabado y si no lo es hay que buscar otro tipo de tramas. Probemos con cuatro.

1→1+0+0+0	11→9+1+1+0	21→16+4+1+0	31→25+4+1+1
2→1+1+0+0	12→9+1+1+1	22→16+4+1+1	32→16+16+0
3→1+1+1+0	13→9+4+0+0	23→9+9+4+1	33→25+4+4+0
4→4+0+0+0	14→9+4+1+0	24→16+4+4+0	34→25+4+4+1
5→4+1+0+0	15→9+4+1+1	25→25+0+0+0	35→25+9+1+0
6→4+1+1+0	16→16+0+0+0	26→25+1+0+0	36→36+0+0+0
7→4+1+1+1	17→16+1+0+0	27→25+1+1+0	37→36+1+0+0
8→4+4+0+0	18→16+1+1+0	28→25+1+1+1	38→36+1+1+0
9→4+4+1+0	19→16+1+1+1	29→25+4+0+0	39→36+1+1+1
10→4+4+1+1	20→16+4+0+0	30→25+4+1+0	40→36+4+0+0

Llegamos así hasta el 64; aparecían todos los números, aunque nos podíamos morir de hambre antes de poder generalizarlo. Entonces, El profesor nos recomendó usar el álgebra para ver si era posible demostrar que, tal como creíamos, era posible expresar cualquier número como suma de cuatro cuadrados perfectos, o, lo que es lo mismo, que todos los números naturales son Pitagóricos en cuatro dimensiones.

Y esto nos lleva a otra reflexión, cuando menos curiosa… si se mantuviera esa relación que hemos encontrado, las nuevas distancias obtenidas en una trama hipercúbica en cuatro dimensiones seguirían la sucesión de los números tetraédricos en 4D, que aparece en el triángulo de Pascal, después de restarles una unidad. Si eso es así, la suma de todos esos números nos daría infinito, pero un infinito igual al que resulta de "contar" todos los números naturales, Cosa que no sucedería con los tetraédricos en 3D, ni con los triangulares. Pero tampoco con los tetraédricos en cinco, seis o más dimensiones (que también aparecen en el Triángulo de Pascal). En este caso sobrarían distancias, lo que querría decir que esas distancias que sobran son números naturales que se repiten, es como si la proyección en cuatro dimensiones de un poliedro en cinco no dejase más huella que los puntos que ya tenía en esa proyección. Dicho de otro modo: es como si un tetraedro se proyectase en el plano de su base sólo con tres puntos. Porque, si no es así, ¿qué otros irracional no cuadráticos aparecen?

Pero volvamos a ver si efectivamente se cubren todos los irracionales cuadráticos. Independientemente del orden en que se coloquen puede suceder que uno de ellos sea par, que lo sean dos, tres o los cuatro:

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2f)^2+(2g)^2+(2h)^2}=\sqrt{4e^2+4f^2+4g^2+4h^2}=\sqrt{4(e^2+f^2+g^2+h^2)} \\ b\in p & \textit{Con cuatro pares aparecen los múltiplos de cuatro } n\equiv 0 \bmod(4) \\ c\in p & \\ d\in p & \end{array}$$

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2f)^2+(2g)^2+(2h+1)^2}=\sqrt{4e^2+4f^2+4g^2+4h^2+4h+1}=\sqrt{4(e^2+f^2+g^2+h^2+h)+1} \\ b\in p & \textit{Con tres pares surgen los } n\equiv 1 \bmod(4) \\ c\in p & \\ d\notin p & \end{array}$$

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2f)^2+(2g+1)^2+(2h+1)^2}=\sqrt{4e^2+4f^2+4g^2+4g+1+4h^2+4h+1}= \\ b\in p & =\sqrt{4(e^2+f^2+g^2+g+h^2+h)+2} \\ c\notin p & \textit{Con dos pares aparecen los } n\equiv 2 \bmod(4) \\ d\notin p & \end{array}$$

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2f+1)^2+(2g+1)^2+(2h+1)^2}=\sqrt{4e^2+4f^2+4f+1+4g^2+4g+1+4h^2+4h+1}= \\ b\notin p & =\sqrt{4(e^2+f^2+g^2+g+h^2+h)+3} \\ c\notin p & \textit{Con un número par surgen los } n\equiv 3 \bmod(4) \\ d\notin p & \end{array}$$

Se observa claramente que da igual el orden en el que se coloquen dichos cuadrados, puede ser que sea par uno, dos, tres o los cuatro, lo que nos lleva a que TODOS, absolutamente TODOS los números naturales se pueden expresar a priori como la suma de cuatro cuadrados perfectos, no hay ninguno que quede excluido. Lo que no significa que sea posible.

No hace falta comprobar más casos, porque ya hemos comprobado que podrían aparecer todos. Lo que faltaría por probar es lo contrario, es decir si podría descomponerse un número N en la suma de cuatro cuadrados perfectos en función de su resto al ser dividido entre cuatro. Es evidente que si ese número es un múltiplo de cuatro se tendría que descomponer como suma de cuatro cuadrados de números pares y que si el resto al dividirlo por cuatro fuese 3 con un par y tres impares y así sucesivamente pero, de momento, no se nos ocurre un método de hacer esa descomposición.

En este punto decidimos volver a los Pitagóricos y tratar de saber más de ellos: ¿Cuáles son?, ¿es la suma de dos de ellos un pitagórico?... A esta última pregunta es fácil dar respuesta. Resulta obvio que no ya que 5 y 10 son pitagóricos pero 15 no lo es ya que 15= 15+0 = 14+1 = 13+2 =12+3 = 11+4 = 10 + 5 = 9+6 = 8+7. A la otra no tanto…

Estudio de los pitagóricos en dos dimensiones.

Si la tomamos de la misma manera que la anterior, nos damos cuenta de que, al haber sólo tres posibilidades, es imposible que cubra las cuatro necesarias… no van a poder salir los que dan resto tres al dividirlos entre cuatro, ya que no se conseguirían con dos pares (n≡0mod(4)), ni con dos impares (n≡2mod(4)), ni con uno par y otro impar (n≡1mod(4)).

Los 4x + 3 no pueden ser pitagóricos porque es imposible que de dos números TRES sean impares. Un poco más abajo está desarrollado este punto con más detalle.

Por tanto, los números de la forma 4x + 3 NUNCA JAMÁS pueden ser pitagóricos.

Introducimos aquí un cambio en la orientación del problema y nos desviamos para comprobar las propiedades de los números "tramarios".
¿Qué tienen en común los números que aparecen en las sucesivas tramas?
Empecemos por la cuadrada. Recordemos:

- **Números pitagóricos, forma** $J = A^2 + B^2$

1.-Allá vamos. Primer caso: A y B son pares:

$$\left.\begin{matrix} A = 2K \\ B = 2N \end{matrix}\right\} J = A^2 + B^2 = 4K^2 + 4N^2 = 4\left(K^2 + N^2\right) \equiv \dot{4}$$ **J es un múltiplo de 4.**

2.-Segundo caso: A y B son impares

$$\left.\begin{matrix} A = 2K+1 \\ B = 2N+1 \end{matrix}\right\} J = (2K+1)^2 + (2N+1)^2 = 4K^2 + 4K + 4N^2 + 4N + 2 = 2\left(2K^2 + 2K + 2N^2 + 2N + 1\right) \equiv \dot{2}$$

Es decir, J es un número par.

3.-Ahora, la coctelera: A par, B impar:

$$\left.\begin{matrix} A = 2K \\ B = 2N+1 \end{matrix}\right\} J = A^2 + B^2 = (2K)^2 + (2N+1)^2 = 4K^2 + 4N^2 + 4N + 1 = 4\left(K^2 + N^2 + N\right) + 1 \equiv 1 \bmod (4)$$

Esto quiere decir que, si lo divides entre cuatro, te da 1 de resto. Se lee: congruente con 1 módulo 4.

En este momento nos damos cuenta de que si A, B y C forman una terna pitagórica, ya que:

$A^2 + B^2 = C^2 \quad \Rightarrow \quad (KA)^2 + (KB)^2 = (KC)^2$ **cualquier múltiplo de ellos también, por lo que debemos buscar ternas pitagóricas que no se puedan simplificar, lo que se llama ternas pitagóricas primitivas.**

Ahora que sabemos que A, B y J forman una terna pitagórica primitiva, es decir, cuyos integrantes tienen 1 por MCD, establecemos relaciones de sentido inverso fijándonos en los desarrollos anteriores; es decir, al revés:

- **1.-Si J es múltiplo de 4, A y B han de ser pares.**
- **2.- Si J es impar, A y B deben ser un par y un impar, indistintamente.**
- **3.-Si J es par no múltiplo de 4, A y B son impares.**

Por tanto:

H_1: Si p es primo e impar, p es pitagórico $\leftrightarrow p \equiv 1 \bmod 4$

H_2: Si p primo, $p \equiv 1 \bmod 4$ **se puede escribir como suma de dos cuadrados perfectos de forma única.**

H_3: Todo número primo impar se puede expresar de una única forma como diferencia de dos cuadrados.
H_4: Como trabajamos con ternas pitagóricas, es decir con ternas que no se pueden simplificar, podemos estudiar la paridad de los elementos que la conforman:

a) **Si a, b, c es una terna pitagórica primitiva** $a^2+b^2=c^2 \rightarrow$ **c es impar.**
b) **Si a, b, c es una terna pitagórica primitiva** $a^2+b^2=c^2 \rightarrow$ **a es par y b impar (o viceversa)**
c) **Si a, b, c es una terna pitagórica primitiva** $a^2+b^2=c^2 \rightarrow c^2 \equiv 1 \bmod 4$.
d) **Si a, b, c es una terna pitagórica primitiva** $a^2+b^2=c^2 \leftrightarrow a=m^2-n^2,\ b=2\cdot m\cdot n,\ c=m^2+n^2$.

Demostración de la H_1:

$\rightarrow)p\neq 2\rightarrow$ **p impar** $\rightarrow$ si $a^2+b^2=p$, **a es impar y b par o al revés pues de lo contrario la suma de dos pares** o dos impares daría un número par$\rightarrow$ $a=2k+1$ y $b=2n$ $\rightarrow a^2+b^2=4k^2+4k+4n^2+1=4(k^2+k+n^2)+1=4m+1=p$.

$\leftarrow)$ **En sentido contrario deberíamos ver que se cumple que si p=4m+1 entonces p es pitagórico. Sabemos que todos los números primos son de la forma 4m+1 ó 4m-1. Demostrar esto es equivalente a probar que todos los del tipo 4m+1 son pitagóricos lo que hacemos en H_2.**

Demostración de la H_2:

Veamos que si p=4m+1 entonces se puede expresar de una única forma como suma de cuadrados. Es decir: *Un primo de la forma 4m+1 es la hipotenusa de uno y sólo un triángulo rectángulo de lados enteros*.
Si hay un primo de la forma 4m+1 que no posee dicha propiedad, entonces habrá un primo menor de la forma 4m+1 que no la posea. Luego, puesto que n es arbitrario, debe haber uno aún menor. Descendiendo a través de todos los valores positivos de n uno debe alcanzar m=1 y así el primo 4·1+1 = 5. Entonces 5 no puede cumplir la propiedad requerida[1]. Pero puesto que 5 se puede expresar como la suma de dos cuadrados y sólo de una manera, así sucede con todo primo que es de la forma 4m+1.

Esa es la idea en la que se basa el descenso infinito: Un método de demostración ideado por Fermat (el del famoso teorema) y que es una especie de método de reducción al absurdo aplicado a los números naturales y a lo bestia: Si queremos demostrar algo, suponemos que hay un número natural n para el que la afirmación es falsa, y a partir de ahí tenemos que demostrar que esa falsedad se cumple para un número natural menor que él. De esta forma, como n es un número general, se puede continuar el razonamiento hasta que se agoten los naturales, ya que vamos descendiendo, o hasta encontrar un número concreto que para el que no es falsa la propiedad que tratamos de demostrar y, aplicando la reducción al absurdo, obtenemos lo que queríamos: que la propiedad es cierta.

[1] Más abajo veremos una demostración de cómo se encuentra ese proceso que a nosotros no nos salió.

Demostración H_3:
Que se puede escribir como diferencia de cuadrados es fácil puesto que lo puede hacer cualquier número impar: $2n+1=(n+1)^2-n^2$. Aplicando la ley del descenso infinito, si hubiera un primo que no se pudiera escribir de forma única, querría decir que $2n+1=(n+1)^2-n^2= a^2-b^2$ con $b\neq n$ entonces si la n la reducimos en 8 unidades, por ejemplo, tendríamos: $2n-15=(n-7)^2-(n-8)^2= = a^2-(b^2+8)$ y b^2+8 podría ser un cuadrado ya que $b^2+8=p^2 \Rightarrow p^2-b^2=8$ con lo que sirve con coger b y p de forma que $(p-b)(p+b)=4\cdot 2$, eso es p=3 y b=1 con lo que si existiese uno con dos soluciones distintas debería haber uno menor aún que tampoco lo cumpliera y así sucesivamente, pero esto es imposible, porque llegamos al 3=4-1 que sí lo cumple.

Demostración H_4:

a) **Si c2 fuera par** $\to 2\,|\,c^2 \to 2\,|\,c \to 4\,|\,c^2 \to a^2+b^2 = 4n \to$ **a es par y b es par # con ser terna primitiva.**

b) **Si a y b fueran ambas impares** $a=2k+1$ y $b=2n+1 \to a^2+b^2 = 4(k^2+k+n^2+n)+2$ **con lo que c no sería impar. Tampoco pueden ser ambas pares puesto que si** $a=2k$ y $b=2n \to a^2+b^2 = 4(k^2+n^2)$ **con lo que c no sería impar.**

c) **Como** $a=2k+1$ y $b=2n \to a^2+b^2 = 4(k^2+4k+n^2)+1$.

d)$\to$) $c^2- b^2 = a^2$ **y suponemos a par y b impar (c siempre es impar).**

$(c-b)(c+b)=a^2$; **(Impar-Impar)(Impar+Impar)=(Par)(Par)=4s es decir múltiplo de 4** $\to a^2=4s=4k^2$ **puesto que es un cuadrado, s es cuadrado perfecto** $\to a^2=4k^2=2n^22m^2 \to k^2=n^2m^2 \to$ **podemos tomar esos factores como si fueran los anteriores.**

$$\left.\begin{array}{l}2n^2=c-b\\2m^2=c+b\end{array}\right\}\to\left.\begin{array}{l}2(n^2+m^2)=2c\\2(m^2-n^2)=2b\end{array}\right\}\to\left.\begin{array}{l}n^2+m^2=c\\m^2-n^2=b\end{array}\right\}\to a^2=(n^2+m^2)^2-(m^2-n^2)^2=4n^2m^2.$$

$\leftarrow$) $a=m^2-n^2$, $b=2\cdot m\cdot n$, $c= m^2+n^2$ y $a^2+b^2=c^2 \to (m^2-n^2)^2+4n^2m^2=(m^2+n^2)^2$.

Tras examinar algunos casos concretos también formulamos, algunas hipótesis sencillas acerca de los que se pueden expresar como suma de cuadrados, que se deducen de todo esto:

H_1: No se pueden los de la forma $x^2\cdot$ imposible, porque es lo mismo que $x\cdot$•imposible, si sacamos la x de la raíz.

H_2: Todos los de la forma 4x + 1 se pueden expresar como suma de 2 cuadrados.

H_3: No se puede ninguno de la forma 4(2x + 1) +2, es decir, 8x +6 = 4x + 3.

Vamos a ver qué pasa con los de la forma $a^2+b^2+c^2=d^2$ **(es decir, cuáles son y no cuáles pueden ser, cosa que ya sabemos)**
Algunos números que no aparecen y podrían aparecer teóricamente son:

- **Los de la forma 8x+7**
- **Los que resultan de multiplicarlos por 4**

Veamos por qué:
Los de la forma 8x+7 pertenecen al grupo 4x+3, es de-

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2f)^2+(2g)^2}=\sqrt{4e^2+4f^2+4g^2}=\sqrt{4(e^2+f^2+g^2)} \\ b\in p & Con\ tres\ pares\ aparecen\ los\ múltiplos\ de\ cuatro \equiv 0 \bmod(4) \\ c\in p & \end{array}$$

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2f)^2+(2g+1)^2}=\sqrt{4e^2+4f^2+4g^2+4g+1}=\sqrt{4(e^2+f^2+g^2+g)+1} \\ b\in p & Con\ dos\ pares\ surgen\ los\ n\equiv 1\bmod(4) \\ c\notin p & \end{array}$$

$$\begin{array}{ll} a\in p & \sqrt{(2e)^2+(2g+1)^2+(2h+1)^2}=\sqrt{4e^2+4g^2+4g+1+4h^2+4h+1}= \\ b\notin p & =\sqrt{4(e^2+g^2+g+h^2+h)+2} \\ c\notin p & Con\ un\ par\ aparecen\ los\ n\equiv 2\bmod(4) \end{array}$$

$$\begin{array}{ll} a\notin p & \sqrt{(2f+1)^2+(2g+1)^2+(2h+1)^2}=\sqrt{4f^2+4f+1+4g^2+4g+1+4h^2+4h+1}= \\ b\notin p & =\sqrt{4(+f^2+f`+g^2+g+h^2+h)+3} \\ c\notin p & Sin\ ningún\ número\ par\ surgen\ los\ n\equiv 3\bmod(4) \end{array}$$

cir: $4(x^2+y^2+z^2+x+y+z)+3$
Para que fuera de la forma indicada, tendría que ser $4[2w+1]+3$**, es decir, la primera parte debería ser impar. Pero esto es imposible, ya que el cuadrado de un número no puede tener factores primos que el inicial no tenga, por tanto, es imposible que nos salga ya que: x^2+x es siempre par y lo mismo sucede con y^2+y, z^2+z.**

Los de la forma 4(8x+7) tampoco pueden debido a que es un múltiplo de 4 y ésos son de la forma 4(y^2+x^2+z^2), que se ha comprobado arriba que no puede ser ya que 8x+7 no pueden escribirse y la suma de sólo dos cuadrados de números impa-res genera múltiplos de 2, que no es el caso.

Para la fórmula $\frac{3k^2+n^2}{4}$ vamos a ver qué es lo que nos puede salir:
Si los dos son impares:

$$\frac{3(2f+1)^2+(2m+1)^2}{4} = \frac{12f^2+12f+3+4m^2+4m+1}{4}=3(f^2+f)+(m^2+m)+1$$

Que es un número par ya que en $3(f^2+f)+(m^2+m)+1$ **el primer paréntesis es impar y lo sigue siendo al multiplicar por tres, el segundo es par, la suma de ambos impar y, al aña-dirle 1 se vuelve par. Veamos si podemos saber algo más en relación a cuatro.**
Si en esta ecuación f y m son ambas impares:

$$\frac{3[2(2v+1)+1]^2+[2(2w+1)+1]^2}{4}=\frac{3(4v+3)^2+(4w+3)^2}{4}=\frac{48v^2+72v+27+16w^2+24w+9}{4}=$$
$$=12v^2+18v+4w^2+6w+4$$

Que no aporta nada.
Si f es par y m impar:

$$\frac{3[2(2v)+1]^2+[2(2w+1)+1]^2}{4}=\frac{3(4v+1)^2+(4w+3)^2}{4}=\frac{48v^2+24v+3+16w^2+24w+9}{4}=$$
$$=12v^2+6v+4w^2+6w+3$$

Que tampoco muestra relación con 4, al menos aparentemente.
Si f es impar y m es par:

$$\frac{3[2(2v+1)+1]^2+[2(2w)+1]^2}{4}=\frac{3(4v+3)^2+(4w+1)^2}{4}=\frac{48v^2+72v+27+16w^2+8w+1}{4}=$$
$$=12v^2+18v+4w^2+2w+7=6(2v^2+3v)+2(2\omega^2+\omega+3)+1$$

Que tampoco da pistas nuevas.
Si f y m son ambas pares nos sale que:

$$\frac{3[2(2v)+1]^2+[2(2w)+1]^2}{4}=\frac{3(4v+1)^2+(4w+1)^2}{4}=\frac{48v^2+24v+3+16w^2+8w+1}{4}=$$
$$=12v^2+6v+4w^2+2w+1$$

Hemos visto que si K y N son ambos impares sólo sabemos que el resultado es impar. Si K y N pares.

$$\left.\begin{cases}K=2f\\ N=2m\end{cases}\right\}\Rightarrow\frac{3(2f)^2+(2m)^2}{4}=\frac{12f^2+4m^2}{4}=3f^2+m^2=p^2$$

Si p=2 tememos dos soluciones:

$$\begin{array}{l}3f^2+m^2=4\\ f=0\Rightarrow m\ \ =2\end{array}\quad \textbf{y al contrario}\quad \begin{array}{l}3f^2+m^2=4\\ m=0\Rightarrow 3f^2=4\neq\end{array}\quad \textbf{también}\quad \begin{array}{l}3f^2+m^2=4\\ f=1\Rightarrow m=1\end{array}$$

Podemos discutir la paridad de f y m.

Caso 1: f es par, m es impar:

$$\left.\begin{array}{l}f=2s\\ m=2t+1\end{array}\right\}3(2s)^2+(2t+1)^2=p^2\Rightarrow 3\cdot 4s^2+4t^2+4t+1=p^2\equiv 1\bmod(4)\Rightarrow p\equiv 1\bmod(4)$$

En resumen:

$$\left.\begin{cases}K=2f=4s\equiv 0\bmod(4)\\ N=2m=4t+2\equiv 2\bmod(4)\end{cases}\right\}\Rightarrow p^2\equiv 1\bmod(4)\ y\ p\equiv 1\bmod(4)$$

Caso 2: f es impar, m es par:

$$\left.\begin{array}{l}f=2s+1\\ m=2t\end{array}\right\}p^2=3(2s+1)^2+(2t)^2=3\cdot 4s^2+3\cdot 4s+4t^2+3=p^2\equiv 3\bmod(4)\Rightarrow No\ \exists\ p$$

En resumen:

$$\left.\begin{cases}K=2f=4s+2\equiv 2\bmod(4)\\ N=2m=4t\equiv 0\bmod(4)\end{cases}\right\}\Rightarrow p^2\equiv 3\bmod(4)\ y\ p\ no\ \exists$$

Caso 3: f es par, m par:

$$\left.\begin{array}{l}f=2s\\ m=2t\end{array}\right\}3(2s)^2+(2t)^2=p^2\Rightarrow 3\cdot 4s^2+4t^2=p^2\equiv 0\bmod(4)\Rightarrow\begin{cases}p\equiv 0\bmod(4)\\ p\equiv 2\bmod(4)\end{cases}$$

En resumen:

$$\left.\begin{cases}K=2f=4s\equiv 0\bmod(4)\\ N=2m=4t\equiv 0\bmod(4)\end{cases}\right\}\Rightarrow p^2\equiv 0\bmod(4)\ y\begin{cases}p\equiv 0\bmod(4)\\ p\equiv 2\bmod(4)\end{cases}$$

Caso 4: f es impar, m es impar:

$$\left.\begin{matrix} f = 2s+1 \\ m = 2t+1 \end{matrix}\right\} p^2 = 3(2s+1)^2 + (2t+1)^2 = 3\cdot 4s^2 + 3\cdot 4s + 4t^2 + 4t + 1 + 3 \Rightarrow p^2 \equiv 0\,\mathrm{mod}(4)$$

$$\Rightarrow \begin{cases} p \equiv 0\,\mathrm{mod}(4) \\ p \equiv 2\,\mathrm{mod}(4) \end{cases}$$

En resumen:

$$\left\{\begin{matrix} K = 2f = 4s+2 \equiv 2\,\mathrm{mod}(4) \\ N = 2m = 4t+2 \equiv 2\,\mathrm{mod}(4) \end{matrix}\right\} \Rightarrow p^2 \equiv 0\,\mathrm{mod}(4)\ y \begin{cases} p \equiv 0\,\mathrm{mod}(4) \\ p \equiv 2\,\mathrm{mod}(4) \end{cases}$$

Conclusiones:

- **Si f es par y m es impar, p^2 es congruente con 1 módulo 4.**
- **Si f es impar y m es par, p^2 es congruente con 3 módulo 4.**
- **En los demás casos, p^2 sale múltiplo de 4.**

Por tanto, con este modelo nunca podremos expresar los números cuadrados congruentes con 4 módulo 2, que son los pares que no son múltiplos de 4. Y como, cuando K y N son impares obteníamos números impares, no es posible obtener cuaternas pitagóricas para números pares.

En la trama isométrica (triangular), NO se puede encontrar la raíz (recordemos que trabajamos con raíces) de ningún par no múltiplo de 4.

Pero eso es lógico pues p^2 nunca puede ser congruente con cuatro módulo dos puesto que p no existiría. Si nos fijamos en p la cosa es mucho más interesante:
los números p≡1mod(4) precisarían para ser obtenidos que k≡0mod(4) y N≡2mod(4). Los p que son congruentes con 0mod(4) precisan que ambas (k y N) sean pares. Si ambas son impares y pretendemos que nos salgan números congruentes con 3 módulo 4:

$$3f^2 + 3f + m^2 + m + 1 = 3 + 4s \Rightarrow 3(f^2 + f - 1) + m^2 + m + 1 \equiv 0\,\mathrm{mod}(4)$$

$$\Rightarrow \begin{cases} \{f^2 + f - 1 \equiv 1\,\mathrm{mod}(4)\ y\ m^2 + m + 1 \equiv 1\,\mathrm{mod}(4) \\ \{f^2 + f - 1 \equiv 0\,\mathrm{mod}(4)\ y\ m^2 + m + 1 \equiv 0\,\mathrm{mod}(4) \\ \{f^2 + f - 1 \equiv 2\,\mathrm{mod}(4)\ y\ m^2 + m + 1 \equiv 2\,\mathrm{mod}(4) \\ \{f^2 + f - 1 \equiv 3\,\mathrm{mod}(4)\ y\ m^2 + m + 1 \equiv 3\,\mathrm{mod}(4) \end{cases} \Leftrightarrow \begin{cases} \{f^2 + f \equiv 2\,\mathrm{mod}(4)\ y\ m^2 + m \equiv 0\,\mathrm{mod}(4) \\ \{f^2 + f \equiv 1\,\mathrm{mod}(4)\ y\ m^2 + m \equiv 3\,\mathrm{mod}(4) \\ \{f^2 + f \equiv 3\,\mathrm{mod}(4)\ y\ m^2 + m \equiv 1\,\mathrm{mod}(4) \\ \{f^2 + f \equiv 4\,\mathrm{mod}(4)\ y\ m^2 + m \equiv 2\,\mathrm{mod}(4) \end{cases}$$

$$3f^2 + 3f + m^2 + m + 1 = 3 + 4s \Rightarrow 3(f^2 + f - 1) + m^2 + m + 1 \equiv 0\,\mathrm{mod}(4)$$

$$\Leftrightarrow \begin{cases} \{f \equiv 1\,\mathrm{mod}(4)\ y\ m \equiv 0\,\mathrm{mod}(4) \\ \{f \equiv 0\,\mathrm{mod}(4)\ y\ m \equiv 1\,\mathrm{mod}(4) \\ \{f \equiv 3\,\mathrm{mod}(4)\ y\ m \equiv 1\,\mathrm{mod}(4) \end{cases}$$

Nada impide que puedan existir.

Faltaría demostrar que: ***Todo entero positivo es una suma de cuatro cuadrados perfectos.*** **Los intentos no fueron muy eficaces y miramos en Internet a ver si alguien sabía algo sobre el tema y… ¡vaya sorpresa! El teorema lleva el nombre**

de Lagrange lo que quiere decir que se conoce demostración desde tiempos de Napoleón.

Esto nos resultó muy sorprendente porque, cuando iniciamos el trabajo, el profesor nunca nos dijo que estos temas habían sido estudiados con anterioridad y nada nos hacía pensar que así fuera puesto que nuestro problema de partida era poco interesante para las Matemáticas, o al menos, eso nos parecía a nosotros. Ahora nos hemos dado cuenta de que cualquier pregunta por aparentemente sencilla que parezca puede resultar interesante desde el punto de vista de esta ciencia.

Internet surge en nuestro apoyo. Y nos permite ofrecer una demostración, que al parecer, lleva el sello de Lagrange, y que nosotros no supimos obtener por nosotros mismos. Después de verla no cabe duda que no mereció la pena el tiempo que perdimos en tratar de obtenerla, pero nos permitió sacar algunas conclusiones y plantearnos nuevas preguntas, algunas de las cuales también habían obtenido respuesta de otros matemáticos famosos, como veremos al final.

Demostración:
Antes de abordar el problema se demuestra que: $(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = (aA+bB+cC+dD)^2 + (aB-bA+cD-dC)^2 + (aC-bD-cA+dB)^2 + (aD-dA+bC-cB)^2$
De lo que obtenemos que el producto de dos números que son la suma de cuatro cuadrados es también suma de cuatro cuadrados.
Por tanto, sólo hay que probarlo con primos impares puesto que las potencias de dos son la suma de 4 cuadrados perfectos al ser cada potencia de dos o es un cuadrado o la suma dos: 2^{2n} ó $2^{2n+1}=2^{2n}+2^{2n}=(2^n)^2+(2^n)^2$, por ejemplo: 32=16+16. Los números pares, a su vez se pueden descomponer en producto de dos y como se cumple que:
$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)=(aA+bB+cC+dD)^2+(Ab-bA+cD-dC)^2+(Ac-bD-cA+dB)^2+(Ad-bA+cB-dC)^2$ cualquier producto de dos factores primos será posible descomponerlos usando esta propiedad.
Además según el pequeño teorema de Fermat $a^{p+1}\equiv 1 \bmod (p)$

Primos congruentes con 1 mod 4

Comenzaremos mostrando que si p es un primo y $p\equiv 1 \pmod 4$, entonces existe un número a tal que $a^2 \equiv (-1) \bmod (p) \equiv (p-1) \bmod (p)$. Diremos que -1 es un residuo cuadrático mod *p*.
Una forma de ver esto es lo siguiente:
Si *a*, *b*, y *c* son tres enteros y *p* no divide a *a*, entonces $ab\equiv ac \pmod p$ implica que $b=c \pmod p$. La razón es que las condiciones implican que *p* divide a $ab-ac$ y *p* no divide a *a*, así que *p* divide *a* $b-c$, que es la conclusión. Ahora para cada *a* tal que $0<a<p$ los números $a, 2a, 3a, \ldots, (p-1)a$ son todos no congruentes entre sí mod *p*, y por lo tanto deberán ser congruentes a $1, 2, 3, \ldots, p-1$ en algún orden. Tomando el producto de todos los enteros en ambos conjuntos, vemos que $a^{p-1}(p-1)! = (p-1)! \pmod p$. Como *p* no divide ningún factor de $(p-1)!$, se pude cancelar para concluir que $a^{p-1}\equiv 1 \pmod p$ (pequeño teorema de Fermat).

Luego si a no es divisible por p, si hacemos $b=a^{(p-1)/2}$, entonces $b^2\equiv 1 (\mathrm{mod}\ p)$.Esto significa que p divide a $(b^2-1)=(b-1)(b+1)$, es decir, $a^{(p-1)/2}=b=\pm 1 (\mathrm{mod}\ p)$
El polinomio $x^{(p-1)/2}-1$ puede tener como máximo $(p-1)/2$ raíces al igual que el otro factor de $x^{p-1}-1 = (x^{(p-1)/2}-1)\ (x^{(p-1)/2}+1)$. Como el polinomio tiene p-1 raíces (1, 2, ..., p-1), se concluye que exactamente (p-1)/2 de los factores deben satisfacer la ecuación $x^{(p-1)/2} = -1\ (\mathrm{mod}\ p)$. Hasta ahora, este argumento es válido para todos los primos impares.
El siguiente paso está limitado a los primos p, para los cuales 4 divide a p-1.
Si $a^{(p-1)/2}=-1(\mathrm{mod}\ p)$ y hacemos $b=a^{(p-1)/4}$, entonces $b^2=-1(\mathrm{mod}\ p)$, como queremos.
Ahora a^2+1^2 es un múltiplo de p, digamos $a^2+1^2=kp$. Como $a<=p-1$, vemos que $a^2+1<p$ así que $k<p$. Ahora describiremos un procedimiento que continúa produciendo soluciones de $a^2+b^2=kp$, pero con valores menores de k hasta $k=1$ que es lo que necesitamos. Asumiendo que tenemos un par a y b, sean a' y b' los residuos menores absolutos a mod k y b mod k, respectivamente. Esto significa que a' y b' son enteros en el rango $(-k/2,\ k/2]$. De ellos sigue que $a'2+b'^2<=k^2/2$. Además, $a'^2+b'^2=a^2+b^2=0(\mathrm{mod}\ k)$ porque $a=a'(\mathrm{mod}\ k)$ y $b=b'(\mathrm{mod}\ k)$. Así $a'^2+b'^2=mk$ con $m<k$. Multiplicando, encontramos que $(a^2+b^2)(a'^2+b'^2)=mk^2p$.

Ahora tenemos la identidad, $(a^2+b^2)(a'^2+b'^2) = (aa'+bb')^2+(ab'-ba')^2$, como $aa'+bb' = a^2+b^2 = 0\ (\mathrm{mod}\ k)$ y $ab'-ba' = ab-ba = 0\ (\mathrm{mod}\ k)$ sigue que ambos términos del miembro derecho son divisibles por k y así $((aa'+bb')/k)^2 + ((ab'-ba')/k)^2 = mp$

Primos congruentes con 3 mod 4

En este caso, comenzaremos buscando números a y b tales que $a^2+b^2+1 = 0\ (\mathrm{mod}\ p)$. Esto es lo mismo que $b^2=-1-a^2\ (\mathrm{mod}\ p)$. No es difícil probar que existe como mínimo una solución a $y^2=-1-x^2\ (\mathrm{mod}\ p)$. Para verlo, primero observe que los cuadrados $0^2,\ 1^2,\ ...,\ ((p-1)/2)^2$ tienen todos distintos residuos mod p ya que $a^2 = b^2\ (\mathrm{mod}\ p)$ implica que p divide a $(a^2-b^2)=(a+b)(a-b)$ y de aquí que $a = b\ (\mathrm{mod}\ p)$ o $a = -b\ (\mathrm{mod}\ p)$, lo que es imposible para dos números distintos en el rango $[0,(p-1)/2]$. Así aquellos cuadrados tienen $(p+1)/2$ residuos distintos. Por razones similares, los números $-1-0^2,\ -1-1^2,\ ...,\ -1-((p-1)/2)^2$ tienen $(p+1)/2$ residuos distintos. Como hay p a lo sumo, los dos conjuntos de residuos se solapan y hay como mínimo una solución a $x^2+y^2+1 = 0\ (\mathrm{mod}\ p)$. Para los primos que son congruentes a 3 mod 4, existe una manera muy sencilla de construir una raíz cuadrada de cualquier número que sea un residuo cuadrático. Consideremos un número a, no divisible por p. Suponiendo que $a = b^2\ (\mathrm{mod}\ p)$. Luego $a^{(p+1)/2} = b^{p+1} = b^2b^{p-1} = b^2 \equiv a\ (\mathrm{mod}\ p)$ de lo que podemos ver que $(a^{(p+1)/4})^2 \equiv a\ (\mathrm{mod}\ p)$ y entonces $a^{(p+1)/4}$ es una raíz cuadrada de a mod p o de -a.
Una vez que tenemos x y y tales que $x^2+y^2+1 = 0\ (\mathrm{mod}\ p)$, podremos reemplazarlos por residuos menores absolutos y podemos suponer que $|x| < (p-1)/2$ y $|y| < (p-1)/2$ de lo que se

puede ver que $x^2+y^2+1 < p^2/2$. Así obtenemos valores iniciales de a,b,c,d para los cuales $a^2+b^2+c^2+d^2 = kp$ con $k < p$.

Si $k > 1$ debemos encontrar una nueva solución con un valor menor de k. Consideraremos el caso de k impar y par separadamente.

Supongamos que k es impar. En ese caso, sean a', b',c', y d' los residuos absolutos menores de a, b, c, y d mod k. Entonces cada uno de |a'|, |b'|, |c'| y |d'| es <= (k-1)/2 así que $a'^2+b'^2+c'^2+d'^2 \le (k-1)^2$ mientras: $a'^2+b'^2+c'^2+d'^2 = a^2+b^2+c^2+d^2 = 0 \pmod k$

Luego $a'^2+b'^2+c'^2+d'^2 = mk$ con $m < k$. Entonces:

$mk^2p = (a^2+b^2+c^2+d^2)\ (a'^2+b'^2+c'^2+d'^2) = (aa'+bb'+cc'+dd')^2 + (ab'-ba'+dc'-cd')^2 + (ac'-ca'+bd'-db')^2 + (ad'-a'd+cb'-bc')^2$ y, de una manera similar al primer caso, cada término es divisible por k, de lo que concluimos que

$mp = ((aa'+bb'+cc'+dd')/k)^2 + ((ab'-ba'+dc'-cd')/k))^2 + ((ac'-ca'+bd'-db')/k)^2 + ((ad'-a'd+cb'-bc')/k)^2$ lo que completa la construcción.

Cuando k es par, el argumento anterior falla específicamente en el caso a'=b'=c'=d'=k/2 ya que entonces $a'^2+b'^2+c'^2+d'^2 = k^2$. Como $a^2+b^2+c^2+d^2 = kp$ es par ninguno o dos o los cuatro valores de a, b, c y d son pares. En cualquier caso podemos intercambiar los valores de forma que a±b y c±d sean pares y entonces:

$((a+b)/2)^2 + ((a-b)/2)^2 + ((c+d)/2)^2 + ((c-d)/2)^2 = (k/2)p$ lo que completa la prueba.

Curiosidades:

- Como decíamos antes, algunas dudas que nos iban surgiendo ya estaban demostradas por matemáticos importantes. Lo cual nos sorprendió porque estas cosas parecían bastante sencillas y poco trascendentes.

- Así, por ejemplo, Legendre demostró que un número entero positivo puede expresarse como suma de tres cuadrados si y sólo si ese número no es de la forma $4^k(8m+7)$. Aunque en principio la prueba estaba incompleta, Gauss la completó poco después.
- En 1834 Jacobi encontró el número exacto de formas en las que se puede expresar un número entero positivo n como suma de cuatro cuadrados. Este número es 8 veces la suma de los *divisores* de n si n es impar y 24 veces la suma de los divisores impares de n si n es par.
- *Todo número entero positivo puede ser expresando como suma de, como mucho, 3 números triangulares, 4 números cuadrados, 5 números pentagonales, etc.* Gauss demostró el resultado para números triangulares y Cauchy demostró el resto.

- **Otra de las generalizaciones es la siguiente: dados números naturales a, b, c podemos resolver la ecuación $n = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ para cualquier n siendo las x enteras. Es más, hay 54 elecciones de a, b, c , d para cada n. Suponiendo que a • b • c • d.**
- **Como puede verse el teorema de los cuatro cuadrados es un caso particular cuando a=b=c=d=1. La solución general de este problema fue dada por *Ramanujan*, aunque en realidad él dio una elección más, pero en este caso la ecuación no tiene solución para n=15.**

Hemos elegido los más sorprendentes y, después de ver la demostración de los cuatro cuadrados, nos desanimamos a seguir buscando en esta dirección y dimos por concluido el trabajo.

Conclusiones:

Hemos remarcado en naranja los diferentes teoremas que hemos ido encontrando pero si tenemos que elegir a modo de resumen algunos de ellos nos quedamos con los siguientes:

- En el plano, y usando tramas regulares, tenemos dos situaciones: Si la trama es cuadrada no se pueden encontrar distancias entre dos puntos que sean la raíz cuadrada de un múltiplo de 4 más 3. Por eso no obteníamos $\sqrt{3}$, ni $\sqrt{7}$.

- En trama isométrica las cosas son más complicadas y, en cualquier caso no salen las raíces de los números pares que no sean múltiplos de cuatro.

- En trama cúbica no pueden aparecer los de la forma 8x+7=4(2x+1)+3, por eso, por ejemplo, no salía $\sqrt{7}$.

- En trama hipercúbica se obtienen todos porque todo número natural es pitagórico en la cuarta dimensión.

Bibliografía:

No es que podamos presumir de haber usado mucha bibliografía puesto que no encontramos libro alguno que tratara del tema tal como estaba planteado, pues no vimos libros de tramas ni nada parecido. Sólo al final del trabajo recurrimos a Internet. Entre las páginas visitadas, las más interesantes fueron:

- http://gaussianos.com/descenso-infinito-un-metodo-de-demostracion-poco-conocido/
- http://gaussianos.com/el-teorema-de-los-cuatro-cuadrados/
- http://www.iesmurgi.org/matematicas/materiales/numeros/node8.html

- http://es.wikipedia.org/wiki/Descenso_infinito
- *www.pedagogica.edu.co/proyectos/geometria/docs/XVI/descenso_infinito.pdf*
- http://www.alpertron.com.ar/4CUADR.HTM#primo14ían.