UNIVERSIDAD DEL BIOBIO
FACULTAD DE EDUCACIÓN Y HUMANIDADES
PEDAGOGÍA EN EDUCACIÓN MATEMÁTICA

ALGUNAS ECUACIONES DIOFÁNTICAS

Memoria para optar al Título de Profesor de Educación media en Educación Matemática

Autores

Andrea Carolina Esnida Muñoz
Jorge Andres Barahona Sandoval
José Esteban Padilla Padilla

Profesor Guía

Sr. Ivo Basso Basso

Chillán, 2009

AGRADECIMIENTOS

En principio, queremos agradecer al profesor, Señor Ivo Basso, quien ha sido parte de nuestra formación profesional como profesor de asignatura y hoy como profesor guía de nuestra tesis, que representa la última etapa que vivimos como estudiantes de Pedagogía en Educación Matemática. De igual forma, dentro del cuerpo docente que nos acompañó en este camino, encontramos a una profesora, que para nosotros fue muy importante en nuestra formación, la Señora Sara Pascual Pizarro, pues nos entregó las herramientas para fundar las bases didácticas en nuestra labor docente, a través de la rigurosidad, capacidad de crítica, objetividad, dentro de muchas otras cosas implícitas que encontramos en sus clases y fuera de ellas.

Por otra parte, aprovechamos esta oportunidad para hacer presente que nada de lo que hemos vivimos como estudiantes dentro de esta etapa, habría sido posible sin nuestras familias, pues ellos han sido un apoyo constante y fundamental, dándonos ánimo cuando pensábamos que ya no podíamos más, cada vez que teníamos un problema nos ayudaron a solucionarlo y lo más importante el cariño y la dedicación hacia nosotros.

Finalmente, por esas cosas fortuitas, poco predecibles de la vida, hoy más que compañeros de carrera, de tesis, podemos decir que somos un grupo de amigos que al pasar de los días, de los años fuimos compartiendo tantas cosas, experiencias de vida, problemas, desilusiones, alegrías, tardes de estudio, cuantos paseos, tantas personas que han pasado por nuestra vida. Por esto y otras cosas más, gracias a los que nos ha tocado vivir, que nos ha hecho crecer como personas y de igual forma, como amigos.

Índice

1. INTRODUCCIÓN

Las Ecuaciones Diofánticas, reciben su nombre gracias al matemático griego Diofanto de Alejandría quien vivió entre los años 200/214 a 284/298, dato que no se sabe con exactitud. Este matemático fue considerado el padre del álgebra, aunque es más conocido por su trabajo en aritmética relacionado con la solución de ecuaciones algebraicas y sobre la teoría de los números, más información respecto de su vida no se maneja mucha.

Diofanto escribió "La Aritmética"distribuidos en trece libros dedicados a la resolución de ecuaciones algebraicas, buscando de esta manera dar métodos para encontrar sus soluciones enteras o racionales a estas, cabe mencionar que de los 13 libros sólo se conocen los seis primeros. El contenido de estos libros consiste en una colección de problemas, en todos estos el matemático griego presenta una solución única y no establece distinción entre problemas determinados e indeterminados, de igual forma, no existe ningún orden en cuanto a la naturaleza de los problemas o los métodos de resolución. Algunos ejemplos de los problemas que trataba en su libro son: ¿Qué números son suma de dos números al cuadrado? ¿Qué números son suma de tres números al cubo?.

Estas ecuaciones son las que tanto sus coeficientes como sus soluciones se encuentran en el conjunto de los números enteros; su clasificación viene de la mano con el número de incógnitas y el grado que estas contemplen. Algunas de estas ecuaciones son: La ecuación Pitagórica, en la cual nuestro objetivo principal es saber si existe alguna fórmula general que nos permita conocer todos los trios que son solución de la ecuación $x^2 + y^2 = z^2$

Las Ecuaciones y Curvas Elípticas, sobre un cuerpo K son en general expresiones del siguiente tipo:

$$y^2 = x^3 + ax^2 + bx + c$$

Con $a, b, c \epsilon K$. Si el cuerpo $K = Q$, entonces estamos en el caso racional. La forma de las soluciones de la ecuación elíptica tiene su origen en la fórmula general de la ecuación cuadrática y su discriminante es también muy similar.

Además analizaremos El Teorema de Fermat, el que afirma que la expresión $x^n + y^n = z^n$ con $x, y, z \epsilon Z$ y $n \epsilon N$ no tiene solución para $n > 2$. Durante más de 350 años fueron muchos los intentos de demostración de la conjetura de Fermat, interviniendo en el estudio del problema tanto matemáticos de la talla de Euler, Dirichlet, Legendre, Gauss o Kummer, como otros menos conocidos. Todos ellos, en un esfuerzo épico en la historia de la Matemática, intentaron la prueba del enunciado para ciertas condiciones parciales, para ciertos exponentes n de la ecuación diofántica. Para algunos de estos exponentes se logró el propósito, pero la demostración general de esta proposición permanecería fatalmente inalcanzable a los esfuerzos de la comunidad matemática. Hasta que a mediado de los años 90, el matemático inglés, profesor en Princenton, Andrew John Wiles consistió, en definitiva, en estudiar a fondo la conjetura de Taniyama-Shimura y tratar de dar con una demostración de su falsedad.

Entre los años 1986 y 1993, desarrollando un aparato matemático de gran complejidad, A. Wiles se dedicó al estudio de la Conjetura de Taniyama-Shimura, hasta comunicar a la comunidad científica, en 1993, que habia logrado la prueba. Un análisis detallado del trabajo presentado por Wiles descubrió un fallo sustancial en la argumentación, que le hizo revisarlo con la ayuda de su discípulo Richard Taylor, revisión que le costó un año de trabajo. Finalmente, en 1994, la prueba de Andrew Wiles del Teorema de Fermat, fue aceptada.

Este texto no pretende estudiar todas las Ecuaciones Diofánticas existentes, sino más bien mostrar la solución de algunos de los diversos tipos de Ecuaciones Diofánticas que se conocen; este trabajo se llevará a cabo con la utilización de las herramientas de la Teoría de Números, entre las cuales podemos destacar divisibilidad, congruencias, entre otras.

2. FORMULACIÓN DEL PROBLEMA

En innumerables ocasiones, nos enfrentamos a ecuaciones no particulares (sin solución única), las cuales poseen infinitas soluciones en el campo numérico de los números reales, por lo que los estudiantes descansan en el hecho de encontrar una o más soluciones en éste campo, pero sabemos que estas ecuaciones, como por ejemplo la pitagórica, posee soluciones enteras. Frente a esto nace la pregunta ¿Cómo encontrar las soluciones en el campo numérico de los enteros para estas ecuaciones?, ¿Existen formas generales de encontrar estas soluciones en algunas ecuaciones conocidas?

El planeamiento anterior, es el motivo de este trabajo, el cual pretende revisar algunas ecuaciones algebraicas y buscar sus soluciones en el campo de los números enteros y en alguna de estas encontrar un patrón para localizar estas soluciones. Estas ecuaciones, cuyas soluciones encontramos en los números enteros, son trabajadas desde miles de años, su precursor fue Diofanto de Alejandría, por lo que este tipo de ecuaciones, las cuales estudiaremos, son llamadas Ecuaciones Diofánticas.

3. OBJETIVOS

"Mostrar las soluciones de algunas Ecuaciones Diofánticas en su forma general".

"Mostrar el progreso histórico hasta la actualidad del trabajo realizado en Ecuaciones Diofánticas".

4. LA ECUACIÓN $x^2 + y^2 = z^2$

El Teorema de Pitágoras ha merecido la atención de muchos matemáticos, especialmente en la antigüedad, actualmente están registrados unas 370 demostraciones de este teorema, desde su aparición 500 a.c. desarrollado por Pitágoras.

Quizás ningún teorema de la amplia matemática, ha recibido demostraciones como este teorema, de todas ellas la más famosa, sin duda, es la de Euclides. El Teorema de Pitágoras aparece por doquier en la matemática, éste es la base de una multitud de teoremas geométricos, de la trigonometría y la geometría analítica. La ecuación Pitagórica $x^2 + y^2 = z^2$ es la ecuación de la circunferencia,del mismo modo, la base de la fórmula $\cos^2 \alpha + \sin^2 \alpha = 1$ y el origen del análisis indeterminado de Diofanto y Fermat.

También puede ser el germen del dramático alumbramiento de la inconmensurabilidad de la Escuela Pitagórica. No sólo ha sido útil en la matemática, sino también en la vida cotidiana; el famoso Galileo Galilei utilizó el Teorema de Pitágoras para determinar la medida de algunas montañas lunares, para conocer la altura de un edificio, sabiéndo la medida de la sombra que proyecta y la distancia del punto más alto del edificio al extremo de la sombra. En general, este teorema se puede utilizar para hallar longitudes en donde intervienen triángulos rectángulos. En el presente documento se muestra una de las demostraciones de la Ecuación Pitagórica y el análisis de las distintas soluciones.

Si tenemos la ecuación $x^2 + y^2 = z^2$ y la dividimos por z^2 entonces obtenemos:

$$\frac{x^2}{z^2}+\frac{y^2}{z^2}=\frac{z^2}{z^2}$$

Ahora asignamos las siguientes variables: $\frac{x}{z}=x'$, $\frac{y}{z}=y'$
Entoces reemplazando tenemos:

$$x'^2 + y'^2 = 1 \tag{1}$$

Así el problema es reducido a las soluciones (x',y') de esta ecuación

$$y'^2 = 1 - x'^2 = (1 - x')(1 + x')$$

Luego, dividimos la expresión anterior por $(1 + x')^2$, lo que nos da como resultado:

$$\frac{y'^2}{(1 + x')^2} = \frac{(1 - x')(1 + x')}{(1 + x')^2}$$

$$\left(\frac{y'}{(1 + x')}\right)^2 = \frac{(1 - x')}{(1 + x')}$$

Supongamos que $t = \frac{y'}{1+x'}$, entonces tendriamos

$$t^2 = \frac{(1-x')}{(1+x')}$$

$$t^2(1+x') = (1-x')$$

$$t^2 + t^2x' = 1 - x'$$

$$x't^2 + x' = 1 - t^2$$

$$x'(t^2+1) = 1 - t^2$$

$$x' = \frac{1-t^2}{t^2+1}$$

como $t = \frac{y'}{(1+x')}$

entonces reemplazamos x' y entonces tendríamos

$$t = \frac{y'}{1 + \frac{1-t^2}{t^2+1}}$$

$$t = \frac{y'}{\frac{(t^2+1)+1-t^2}{t^2+1}}$$

$$t = \frac{y'}{\frac{2}{t^2+1}}$$

$$t = \frac{y'(t^2+1)}{2}$$

Por lo tanto tenemos que $y' = \frac{2t}{t^2+1}$

Entonces, ahora sabemos que:

$$x' = \frac{1-t^2}{1+t^2}, \quad y' = \frac{2t}{1+t^2} \tag{2}$$

donde quedan x' e y' en función de t.

Una solución especial de esta ecuación es $x' = -1$, $y' = 0$, pues así $x'^2 + y'^2 = 1$ la cual representa una circunferencia de radio 1, otro punto particular de la circunferencia es $x' = 1$, $y' = 0$.

La fórmula (2) donde t es un racional, da la solución general de la ecuación $x'^2 + y'^2 = 1$, en números racionales y, por lo tanto ellas dan el principio de la solución general de la ecuación:

$$x^2 + y^2 = z^2, \tag{3}$$

en los números enteros.

En relación a lo anterior, veremos la transición de las soluciones racionales de $x'^2 + y'^2 = 1$ a las soluciones enteras de $x^2 + y^2 = z^2$.

Consideremos $t = \frac{q}{p}$, donde p y q son primos relativos; como $x' = \frac{1 - t^2}{1 + t^2}$, $y' = \frac{2t}{1 + t^2}$, ahora tenemos:

$$x' = \frac{x}{z} = \frac{p^2 - q^2}{p^2 + q^2}, \quad y' = \frac{y}{z} = \frac{2pq}{p^2 + q^2} \tag{4}$$

y se puede escoger

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

Entonces tenemos una solución en los enteros de la ecuación $x^2 + y^2 = z^2$, pero puede ocurrir que x, y, z sean múltiplos comunes de esos números. Si los tres números, $p^2 - q^2$, $2pq$ y $p^2 + q^2$ tienen un factor común mayor que 1, podemos dividirlo por ese factor común y todavía conseguir una solución entera de la ecuación.

Consideramos dos posibilidades para los primos relativos p y q.

(i) Primero, supongamos que uno de ellos es par y el otro es impar, luego los números $p^2 - q^2$, $2pq$ y $p^2 + q^2$ no tienen un factor en común mayor que 1, ya que tal factor tendría que ser impar (desde que $p^2 - q^2$ es impar) y dividiría a $(p^2 - q^2) + (p^2 + q^2) = 2p^2$; de modo similar dividiría a $2q^2$ y esto es imposible puesto que p y q son primos relativos.

De aquí en este caso tenemos:

$$x = m(p^2 - q^2), \quad y = 2mpq, \quad z = m(p^2 + q^2), \tag{5}$$

donde m es entero.

Ahora consideramos la posibilidad de que p y q sean ambos impares, en este caso si ponemos $p + q = 2P$ y $p - q = 2Q$, los números P y Q son primos relativos. Uno de ellos es par y el otro impar ya que $P + Q = p$, es impar. Sustituyendo en términos de P y Q tenemos:

$$\frac{x}{z} = \frac{2PQ}{P^2 + Q^2}, \qquad \frac{y}{z} = \frac{P^2 - Q^2}{P^2 + Q^2}$$

Después de cancelar un factor 2. La posición es, por lo tanto, de la misma forma como antes, excepto que x e y son intercambiables y P y Q toman el lugar de p y q.

Conclusión, todas las soluciones de $x^2 + y^2 = z^2$ están dadas por:

$$x = m(p^2 - q^2), \qquad y = 2mpq \qquad \text{y} \qquad z = m(p^2 + q^2)$$

donde m, p y q son enteros, p y q son primos relativos y uno de estos es par y otro impar.

Esas son la Fórmulas de Euclides. La solución simple (aparte de la solución trivial con uno de los ceros desconocidos) es x=3, y=4, z=5, que surge con m=1, p=2 y q=1.

La primitiva que es la solución con x, y, z primos relativos y por lo tanto m=1 son (3,4,5), (5,12,13), (8,15,17), (7,24,25), (21,20,29), (9,40,41).

Puesto que la fórmula para t (tomando m=1) es $z^2 = p^2 + q^2$, nosotros podemos tomar z un cuadrado perfecto y eligiendo p y q por conveniencia y tan sólo obtener una solución paramétrica para $x^2 + y^2 = z^4$, la repetición del proceso permite dar solución para $x^2 + y^2 = z^k$, donde k, es algún número mayor que 2.

5. LA ECUACIÓN $ax^2 + by^2 = z^2$

Consideremos:

$$ax^2 + by^2 = z^2 \tag{6}$$

donde a y b son números naturales, ninguno de los cuales es un cuadrado perfecto. Tal ecuación puede no tener solución (aparte para la solución $x = y = z = 0$).

Por ejemplo la ecuación:

$$2x^2 + 3y^2 = z^2$$

no tiene solución.

Se puede suponer que x, y, z no tienen un factor en común mayor que 1, de donde se sigue que en particular ni x ni z es divisible por 3. Pero luego la congruencia $2x^2 \equiv z^2 \pmod 3$ es imposible, puesto que 2 no es residuo cuadrático del módulo 3.

Consideraciones similares se aplican a la ecuación general (6), y estas dan las condiciones de congruencia que deben ser satisfechas para que la ecuación tenga solución. Podemos suponer que a y b son libres de cuadrados, esto es, no divisible por algún cuadrado mayor que 1, pues la introducción de factores cuadrados en a y b no afecta la solución de la ecuación.

Si la ecuación tiene solución, podemos dividir por algún factor común de x, y, z, y obtener una solución en la cual x, y, z no tenga algún factor común mayor que 1.

La ecuación implica la congruencia $ax^2 \equiv z^2 \pmod b$. Ahora x y b deben ser primos relativos pues ellos tienen un factor primo en común, este primo divide a x y z, y por lo tanto su cuadrado divide a by^2, y como b es libre de cuadrados cualquiera este requeriría que el número primo divida a y lo cual es imposible.

Multiplicando la congruencia por x'^2, donde $xx' \equiv 1 \pmod b$, obtenemos una congruencia de la forma:

$$a \equiv \alpha^2 (mod \quad b), \tag{7}$$

Donde $\alpha = x'z$. Similarmente

$$b \equiv \beta^2 (mod \quad a) \tag{8}$$

para un cierto entero β. Eso es, a debe ser un residuo cuadratico (mod b) y b debe ser un residuo cuadrático (mod a).

Si a y b tienen un factor común $h > 1$, hay otra congruencia además de (7) y (8) la cual necesita tener solución si la ecuación (6) tiene solución. Elijamos $a = ha_1$ y $b = b_1 h$, de modo que a_1, b_1 y h son primos relativos en pares. Para cualquier solución de (6), z necesita ser divisible por h, de este modo $a_1x^2 + b_1y^2$ necesita ser dividible por h.

Multiplicando por $b_1x'^2$, obtenemos una congruencia de la forma:

$$a_1x^2 + b_1y^2 = hM \quad /b_1x'^2 \quad \text{(cierto M)}$$
$$a_1b_1(x'^2x^2) + b_1^2y^2x'^2 = hMb_1x'^2$$

Pero se sabe que:

$$x'x \equiv 1(mod\ \ b)$$

entonces

$$x'^2x^2 \equiv 1(mod\ \ b)$$

además, por definición de congruencia se tiene:

$$x'^2x^2 - 1 = Pb \quad \text{(cierto P)}$$
$$x'^2x^2 = 1 + Pb$$

Reemplazando $x'^2x^2 = 1 + Pb$ en $a_1b_1(x'^2x^2) + b_1^2y^2x'^2 = hMb_1x'^2$ obtenemos:

$$a_1b_1(1 + Pb) + (b_1yx')^2 = hB \quad \text{(cierto B)}$$
$$a_1b_1 + a_1b_1Pb + \gamma^2 = hB$$
$$a_1b_1 + hC + \gamma^2 = hB \quad \text{(cierto C)}$$
$$a_1b_1 + \gamma^2 = hB - hC$$
$$a_1b_1 + \gamma^2 = hD \quad \text{(cierto D)}$$

por lo que se concluye que:

$$a_1b_1 \equiv -\gamma^2(mod \quad h) \tag{9}$$

El hecho que las congruencias (7), (8), y (9) necesitan tener solución impone restriciones a a y b, las cuales son necesarias para la solución de la ecuación (6). Es de ninguna manera obvio que si las congruencias tienen solución entonces la ecuación tiene solución.

Si cualquier a ó b es 1, la ecuación obviamente tiene solución. Si $a = b$ las condiciones de congruencia (7) y (8) son trivialmente satisfechas y (9) se reduce a $1 \equiv -\gamma^2 \pmod{a}$, esto implica que a es representable como $p^2 + q^2$ y la ecuación se satisface por $x = p$, $y = q$, $z = p^2 + q^2$.

Se puede suponer ahora que $a > b > 1$. El plan de la prueba deriva de (6) una ecuación similar con la misma b pero con a reemplazada por A, donde $0 < A < a$ y A, b satisfacen las mismas tres condiciones de congruencia como a y b. La repetición de los procesos debe llevarnos eventualmente a una ecuación en la cual ya bien uno de los coeficiente es 1 o los dos coeficientes son iguales a A. Como se ha visto, tal ecuación tiene solución.

Por hipótesis, la congruencia (8) tiene solución. Elegimos una solución β la cual satisface $|\beta| \leq \frac{1}{2}a$. Como $\beta^2 - b$ es múltiplo de a, se puede asignar:

$$\beta^2 - b = aAk^2 \tag{10}$$

donde k y A son enteros y A es libre de cuadrados (todos los factores cuadrados son absorvidos en k^2). Notamos que k es primo relativo con b pues b es libre de cuadrados. Observamos que A es positivo pues si

$$aAk^2 = \beta^2 - b > -b > -a$$

de donde $Ak^2 \geq 0$ y por lo tanto > 0 pues b no es un cuadrado perfecto.

Si sustituimos y y z en términos de nuevas variables Y y Z en:

$$z = bY + \beta Z, \quad y = \beta Y + Z \tag{11}$$

encontramos que:

$$z^2 - by^2 = (\beta^2 - b)(Z^2 - bY^2)$$

En vista de (10), la ecuación (6) se transforma en

$$ax^2 = aAk^2(Z^2 - by^2)$$

Eligiendo $x = kAX$ la nueva ecuación es:

$$AX^2 + bY^2 = Z^2$$

Si esta ecuación tiene solución entonces también la tiene (6); pues la sustitución (11) y la ecuación $x = kAX$ da valores enteros no todos cero, para x, y, z en términos de X, Y,Z.

Nota: la forma de la sustitución (11) es sugerida escribiendo:

$$z - y\sqrt{b} = (\beta - \sqrt{b})(Z - Y\sqrt{b})$$

El nuevo coeficiente A es positivo y libre de cuadrados y satisface:

$$A=\frac{1}{ak^2}(\beta^2-b)<\frac{\beta^2}{ak^2}\leqq\frac{\beta^2}{a}\leqq\frac{1}{4}a$$

y por lo tanto A es menor que a. Queda por ser probado que A y b satisfacen las condiciones de congruencia análogas a (7), (8), (9). La análoga de (8) es obvia, puesto que $b\equiv\beta^2 \pmod{A}$ por (10).

Pero al probar el análogo de (7), observamos que (10) puede ser dividido a través de h, obteniendo

$$h\beta_1^2 - b_1 = a_1Ak^2$$

también (7) es equivalente $a_1\equiv h\alpha_1^2 \pmod{b_1}$. Por lo tanto:

$$h\beta_1^2\equiv hA(\alpha_1 k)^2 \pmod{b_1}$$

y desde que h, k, a_1 son todos primos relativos con b_1, se sigue que A es congruente a un cuadrado (mod b_1) también $-a_1Ak^2\equiv b_1 \pmod{h}$ y en vista de (9) y el hecho que k, a_1, b_1 son todos primos relativos a h, se sigue que A es congruente a un cuadrado (mod h) y por lo tanto también (mod b), obteniendo el análogo de (7).

Para la prueba del análogo de (9) con A en lugar de a, sea H como el más alto factor común de A y b, y ponemos $A = HA_2$, $b = Hb_2$. La ecuación (10) puede ser dividida por H dando:

$$H\beta_2^2 - b_2 = aA_2k^2$$

por lo tanto:

$$-A_2b_2\equiv a(A_2k)^2 \pmod{H}$$

como $a\equiv\alpha^2 \pmod{H}$ por (7), esto significa que $-A_2b_2$ es congruente a un cuadrado (mod H), lo cual es el análogo de (9).

Se tiene ahora que demostrar que el coeficiente A y b satisface una condición similar de congruencia impuesta sobre a y b. El método de prueba ya aclarado, por lo tanto aplicado y establecida la solubilidad de la ecuación (6).

Para la ilustración de la prueba anterior, aplicaremos el proceso a la ecuación:

$$41x^2 + 31y^2 = z^2 \tag{12}$$

como los coeficeintes son primos relativos, hay unicamente dos condiciones de congruencia.

$$41\equiv\alpha^2 \pmod{31}$$

$$31\equiv\beta^2 \pmod{41}$$

Ambas tienen solución, con $\alpha \equiv \pm 14 \pmod{31}$ y $\beta \equiv \pm 20 \pmod{41}$.

Siguiendo el método, debemos escoger un valor para β y entonces definir A y k por (10).

En la teoría, suponemos $|\beta| \leq \frac{1}{2}a$ y así tomamos $\beta = 20$.

Tenemos:

$$\beta^2 - b = 400 - 31 = 4 \times 41$$

de esto $k = 3$ y $A = 1$ (el hecho que $A = 1$ quiere decir que el proceso necesitará una repetición adicional).

La nueva ecuación derivada desde (12) es $X^2 + 31Y^2 = Z^2$ y tomamos la solución obvia $X = 1$, $Y = 0$, $Z = 1$. La relación entre x, y, z y X, Y, Z con los coeficientes ahora en uso, son:

$$z = 31Y + 20Z, \quad y = 20Y + Z, \quad x = 3X.$$

Esto nos da la solución $x = 3$, $y = 1$, $z = 20$ para la ecuación original (12).

Ahora se retoma la teoría general. Se ha probado que la solubilidad de la congruencia (7), (8), (9) es necesaria y suficiente para la solubilidad de la ecuación (6), sobre la suposición que a y b son cuadrados perfectos. Legendre facilmente dedujo desde estos resultados la condición necesaria y suficiente para la solución de la ecuación:

$$ax^2 + by^2 = cz^2$$

Donde a, b, c son números naturales. Sobre la suposición que a, b, c son cuadrados perfectos y primos relativos en pares (los cuales no son serias restricciones aquí), la condición es que las tres congruencias:

$$bc \equiv \alpha^2 \pmod{a}, \quad ca \equiv \beta^2 \pmod{b}, \quad ab \equiv \gamma^2 \pmod{c}.$$

todas tienen solución.

Concluiremos en ésta sección con algunas observaciones sobre cuestiones generales de las congruencias y de las condiciones de solubilidad de Ecuaciones Diofánticas. Cualquier ecuación diofántica da lugar a una congruencia en cualquier módulo que queramos seleccionar, y tal congruencia debe ser soluble si la ecuación es soluble. Por lo general hay sólo un número finito de módulos para los cuales la solubilidad de la congruencia impone alguna condición sobre los coeficientes de la ecuación.

Se han demostrado varios casos en los cuales se demuestra que una ecuación no tiene solución por consideraciones de congruencia. Es a veces posible demostrar la no solubilidad de una ecuación usando una congruencia a un módulo que depende de las incógnitas en la ecuación. Esto es la idea subyacente de la prueba dada por V. A. Lebesgue en 1869, que la ecuación:

$$y^2 = x^3 + 7$$

no tiene solución en los enteros. Primero, x debe ser impar desde que un número de la forma $8k + 7$ no puede ser cuadrado. Ahora escriba la ecuación como:

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4).$$

El número $x^2 - 2x + 4 = (x - 1)^2 + 3$ es de la forma $4k + 3$. De ahí esto tiene algún factor primo q de aquella forma, y ya que la congruencia $y^2 + 1 \equiv 0 \pmod{q}$ no tiene solución, la ecuación propuesta no tiene solución.

6. LA ECUACIÓN $ax^2 + by^2 + cz^2 = 0$

Aunque el problema que damos acerca de esta ecuación proviene de Legendre, la prueba es reciente, adaptada de un paper de Mordell.

Teorema 1 *Sean a, b, c enteros no nulos, tal que el producto* ***abc*** *es un cuadrado cualquiera. La condición necesaria y suficiente para que* $ax^2 + by^2 + cz^2 = 0$ *tenga una solución en los enteros; x, y, z no deben ser nulos y a, b, c no tienen el mismo signo. Luego* $-bc, -ac, -ab$ *son residuos cuadráticos módulo a, b, c, respectivamente.*

Antes de dar la prueba de estos resultados, estableceremos 2 lemas:

Lema 1 *Sean* λ, μ, ν *números reales positivos, el producto* $\lambda\mu\nu = m$, *siendo m un entero. Entonces alguna congruencia* $\alpha x + \beta y + \gamma z \equiv 0$ *(mod m) tiene una solución x, y, z (no todas nulas) tal que* $|x| \leq \lambda$, $|y| \leq \mu$, $|z| \leq \nu$.

Prueba: dejamos el rango de x desde $0, 1...[\lambda]$, y desde $0, 1...[\mu]$, z desde $0, 1...[\nu]$. Con esto se obtiene $(1 + [\lambda])(1 + [\mu])(1 + [\nu]) > \lambda\mu\nu = m$[1] y desde ahí deben haber aproximadamente dos soluciones, x_1, y_1, z_1 y x_2, y_2, z_2 tal que:

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \text{ (mod m)}.$$

Luego se tiene:

$$\alpha(x_1 - x_2) + \beta(y_1 - y_2) + \gamma(z_1 - z_2) \equiv 0 \text{ (mod m)},$$

$$|x_1 - x_2| \leq [\lambda] \leq \lambda \; |y_1 - y_2| \leq \mu, \quad |z_1 - z_2| \leq \nu$$

Lema 2 *Supongamos que* $ax^2 + by^2 + cz^2$ *es representable en factores lineales módulo m y módulo n, que es:*

$$ax^2 + by^2 + cz^2 \equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z) \text{ (mod m)}$$

$$ax^2 + by^2 + cz^2 \equiv (\alpha_3 x + \beta_3 y + \gamma_3 z)(\alpha_4 x + \beta_4 y + \gamma_4 z) \text{ (mod n)}$$

Si $(m, n) = 1$ entonces $ax^2 + by^2 + cz^2$ se puede representar en factores lineales módulo mn.

Prueba: Podemos cambiar $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ para satisfacer:

$$\alpha \equiv \alpha_1, \beta \equiv \beta_1, \delta \equiv \gamma_1, \alpha' \equiv \alpha_2, \beta' \equiv \beta_2, \gamma' \equiv \gamma_2 \text{ (mod m)}$$

$$\alpha \equiv \alpha_3, \beta \equiv \beta_3, \delta \equiv \gamma_3, \alpha' \equiv \alpha_4, \beta' \equiv \beta_4, \gamma' \equiv \gamma_4 \text{ (mod n)}$$

[1] Sea x e y, números reales, entonces tenemos: (1) $[x] \leq x < [x] + 1$, $x - 1 < [x] \leq x$, $0 \leq x - [x] < 1$

entonces la congruencia

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' \beta y + \gamma' z)$$

sostiene módulo m y módulo n y por lo tanto sostiene módulo mn.

Prueba del Teorema 1: si $ax^2 + by^2 + cz^2 = 0$ tiene una solución x_0, y_0, z_0, no todos nulos, entonces a, b, c no son de igual signo. Dividiendo x_0, y_0, z_0 por (x_0, y_0, z_0) tenemos una solución x_1, y_1, z_1 con $(x_1, y_1, z_1) = 1$.

Probaremos que $(c, x_1) = 1$. Si esto no fuera así habría un primo p dividiendo a c y x_1. Luego $p \nmid b$ entonces p/c y abc es un cuadrado cualquiera.

Por lo tanto p/by_1^2 y $p \nmid b$ de esto p/y_1^2, p/y_1 y entonces $p^2/(ax_1^2 + by_1^2)$ entonces p^2/cz_1^2. Pero c es un cuadrado cualquiera, entonces p/z_1. Se concluye que p es un factor de x_1, y_1 y z_1, al contrario $(x_1, y_1, z_1) = 1$. En consecuencia tenemos $(c, x_1) = 1$.

Sea u elegido para satisfacer $ux_1 \equiv 1$ (mod c). Entonces la ecuación $ax_1^2 + by_1^2 + cz_1^2 = 0$ implica que $ax_1^2 + b_1^2 \equiv 0$ (mod c), y multiplicando esto por $u^2 b$ obtenemos $u^2 b^2 y_1^2 \equiv -ab$ (mod c). Así hemos establecido que $-ab$ es un residuo cuadrático módulo c. Una prueba similar muestra que $-bc$ y $-ac$ son residuos cuadráticos módulo a y b respectivamente.

Se asume que $-bc$, $-ac$, $-ab$ son residuos cuadráticos módulo a, b, c respectivamente. Note que esta propiedad no cambia si a, b, c son reemplazados por sus negativos. Como a, b, c no son del mismo signo, podemos cambiar los signos de todos ellos, si necesariamente, en orden tenemos uno positivo y dos negativos. Entonces, con un cambio de notación, se puede arreglar esto, de modo que a sea positivo y b y c sean negativos.

Si definimos r como una solución de $r^2 \equiv -ab$ (mod c), y a_1 como una solución de $aa_1 \equiv 1$ (mod c), estas soluciones existen debido a suposiciones sobre a, b, c. Entonces se puede escribir:

$$\begin{gathered} ax^2 + by^2 \equiv aa_1(ax^2 + by^2) \equiv a_1(a^2x^2 + aby^2) \\ \equiv a_1(a^2x^2 - r^2y^2) \equiv a_1(ax - ry)(ax + ry) \equiv (x - a_1ry)(ax + ry) \text{ (mod c)}, \end{gathered}$$

$$ax^2 + by^2 + cz^2 \equiv (x - a_1ry)(ax + ry) \text{ (mod c)}.$$

Así $ax^2 + by^2 + cz^2$ es el producto de dos factores lineales módulo c, y similarmente de módulo a y módulo b. Aplicando el Lema 2 dos veces, concluimos que $ax^2 + by^2 + cz^2$ puede ser escrito como el producto de dos factores lineales módulo abc. Entonces existen números α, β, γ, α', β', γ' tales que:

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \text{ (mod } abc)$$

Ahora aplicamos el Lema 1 para la congruencia

$$\alpha x + \beta y + \gamma z \equiv 0 \pmod{abc}$$

usando $\lambda = \sqrt{bc}$, $\mu = \sqrt{|ac|}$, $r = \sqrt{|ab|}$. Así obtenemos una solución x_1, y_1, z_1 de la congruencia anterior con $|x_1| \leq \sqrt{bc}, |y_1| \leq \sqrt{|ac|}, |z_1| \leq \sqrt{|ab|}$. Pero a, b, c son un cuadrado cualquiera, así $\sqrt{bc}$ es un entero sólo si es 1, y similarmente para $\sqrt{|ac|}$ y $\sqrt{|ab|}$. Por lo tanto tenemos:

$$|x_1| \leq \sqrt{bc},\ x_1^2 \leq bc \text{ con igualdad posible sólo si b=c=-1}$$

$$|y_1| \leq \sqrt{|ac|},\ y_1^2 \leq -ac \text{ con igualdad posible sólo si } a = 1, c = -1$$

$$|z_1| \leq \sqrt{|ab|},\ z_1^2 \leq -ab \text{ con igualdad posible sólo si } a = 1, b = -1$$

Por lo tanto, si a es positivo y b y c son negativos, tenemos $b = c = -1$,

$$ax_1^2 + by^2 cz_1^2 \leq ax_1^2 < abc,$$

y además

$$ax_1^2 + by_1^2 + cz_1^2 \geq by_1^2 + cz_1^2 > b(-ac) + c(-ab) = -2abc.$$

Dejando a un lado el caso especial cuando $b = c = -1$, tenemos:

$$-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc$$

Ahora x_1, y_1, z_1 es una solución de:

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}$$

Así las inecuaciones de arriba implican que:

$$ax_1^2 + by_1^2 + cz_1^2 = 0 \text{ ó } ax_1^2 + by_1^2 + cz_1^2 = -abc$$

En el primer tenemos una solución de $ax^2 + by^2 + cz^2 =$. En el segundo caso verificamos fácilmente que x_2, y_2, z_2, definido por $x_2 = y_2 = z_2 = 0$ luego $z_1^2 + ab = 0$, $z_1^2 - ab = 0$ y $z_1 = \pm 1$, $z = 0$ es una solución.

Finalmente podemos disponer del caso especial $b = c = -1$. Las condiciones sobre a, b, c ahora implica que -1 es un residuo cuadrático módulo a, en otras palabras, que $R(a)^2$ es positivo. Por lo anterior esto implica que $Q(a)$ es positiva y por lo tanto que la ecuación $y^2 + z^2 = a$ a una solución y_1, z_1. Entonces $x = 1$, $y = y_1$, $z = z_1$ es una solución de $ax^2 + by^2 + cz^2 = 0$ desde $b = c - 1$.

[2]Sea $R(n)$ que denota el número de raíces de $s^2 \equiv -1 \pmod{n}$. Entonces $P(n) = R(n)$ para $n > 1$, $P(1) = 2$, $R(1) = 1$, $Q(1) = 4$, $Q(n) = 4R(n)$ para $n \geq 1$, y $N(n) = 4 \sum_{d^2|n} R(n/d^2)$

7. CURVAS ELÍPTICAS

La teoría de las curvas elípticas es una de las creaciones más interesantes de las matemáticas del siglo XX, aunque sus antecedentes se remontan hasta la matemática griega. Uno de los investigadores más conocidos que se relaciona con las curvas elípticas es Louis Mordell (1962). Estas curvas se definen mediante ecuaciones cúbicas, éstas han sido usadas para probar el último teorema de Fermat y se emplea también en la criptografía y en la factorización de enteros. Estas curvas no son elipses, las curvas elípticas son ”regulares", es decir ”no-singulares", lo que significa que no tienen ”Cúspides"ni auto intersecciones.

Por ejemplo la ecuación $y^2 = x^3 + 7$, es una curva elíptica.

La ecuación general corresponde a la ecuación de Weierstrass, tradicionalmente escrita como:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{13}$$

esto es simplificable. Primero reemplazamos y por $\frac{1}{2}(y - a_1x - a_3)$, y entonces multiplicamos por 4, para eliminar los denominadores, y la ecuación se reduce a:

$$y^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + 2(2a_4 + a_1a_3)x + (a_3^2 + 4a_6). \tag{14}$$

Si reemplazamos x por $\frac{x - 3(a_1^2 + 4a_2)}{36}$ e y por $\frac{y}{108}$, luego multiplicamos por $108^2 = \frac{36^3}{4}$ para eliminar denominadores reducimos la ecuación a la forma:

$$y^2 = x^3 - Ax - B. \tag{15}$$

Si los a_i con $i = 1, 2, ..,6$ son enteros, lo son A y B.

No obstante, la transformación de (13) a (15) no necesariamente lleva a soluciones enteras, pero hay una conexión cercana entre las soluciones racionales y las enteras (en la cual ningún factor común puede ser cancelado entre X, Y y Z los cuales no todos son 0) de:

$$Y^2Z = X^3 - AXZ^2 - BZ^3. \tag{16}$$

Si tenemos una solución racional $x = \frac{n_x}{d_x}$ e $y = \frac{n_y}{d_y}$ de (15), con n_x este perteneciente a los enteros, entonces podemos sustituir estos valores en (15) y multiplicando por $d_x^3d_y^3$ simplificamos denominadores, tenemos:

$$\frac{n_y^2}{d_y^2} = \frac{n_x^3}{d_x^3} - A\frac{n_x}{d_x}, \text{ multiplicamos por } /d_x^3 d_y^3$$

$$n_y^2 d_x^3 d_y = n_x^3 d_y^3 - A n_x d_x^2 d_y^3 - B d_x^3 d_y^3$$

Si hacemos, $X = n_x d_y$, $Y = n_y d_x$ y $Z = d_x d_y$, obtenemos (16) y X, Y, Z son enteros. Sin embargo, ellos tendrán un factor en común, el cual podemos demostrar que es d_y^3, y así el factor d_x^3 es suficiente para simplificar denominadores.

Inversamente, dada una solución de (16), si se divide por Z^3 y aplicamos las mismas sustituciones en otro sentido, es decir, reemplazamos X por $n_x y_d$, etc., entonces se obtiene (15). Por supuesto esto no se utiliza cuando $Z = 0$ y efectivamente la solución $X = 0$, $Y = 1$, $Z = 0$, la cual no corresponde a una solución racional de (15), es conocida.

El discriminante en las ecuaciones cuadráticas es $d = b^2 - 4ac$. Hay uno similar también llamado discriminante en la ecuación elíptica y se denota por $\Delta = 16(4A^3 - 27B^2)$. Las ecuaciones con $\Delta = 0$ son un caso especial, desde que el lado derecho de la igualdad (15) se puede factorizar como $(x - 2\alpha)(x + \alpha)^2$ (donde α es una raíz cuadrada de $\frac{A}{3}$, la cual como Δ=0, es también una raíz cúbica de $\frac{B}{2}$).

Si escribimos $y' = \frac{y}{(x + \alpha)}$, entonces buscamos las soluciones de $y'^2 = x - 2\alpha$, y existe un x, por lo tanto un y, para cada valor de y'. El caso donde $\Delta = 0$ y $A \neq 0$ es conocido como un nodo, desde que la curva se cruza a si misma, mientras que el caso donde $\Delta = A = 0$ (por lo tanto $B = 0$) es conocido como una cúspide.

De aquí en adelante se asumirá que Δ es no nulo, en otras palabras que la ecuación es no singular.

Hay una interpretación geométrica llamativa de las ecuaciones elípticas, conocida como curvas elípticas, la cual es fundamental para la mayor parte de la teoría, incluyendo muchos de los resultados que dejaremos sin prueba. Si dibujamos el gráfico de (15), se obtiene una de las de las dos formas de la Fig. 1, dependiendo del signo de Δ.

Esta claro en geometría que cada linea recta (excepto vertical), que intersecta la curva en dos puntos P y Q también debe intersectar la curva en un tercer punto R (no necesariamente diferentes). Lo más interesante es que, si P y Q tienen coordenadas racionales, entonces R también debe tenerlas. Si P y Q tienen coordenadas racionales, entonces la ecuación de la recta que los une debe tener coficientes racionales, es decir, $y = lx + m$. Sustituyendo esto en (15) nos da una ecuación cúbica racional para x. Pero, esta ecuación tiene dos soluciones racionales (que provienen de P y Q) y por lo tanto debe tener una tercera solución, puesto que, el producto de las tres soluciones es el negativo del coeficiente de x^0. Así R tiene una coordenada x racional

desde que la ecuación de la recta es racional, una coordenada y racional. Esto entrega caminos para conseguir nuevas soluciones racionales, a partir de soluciones antiguas.

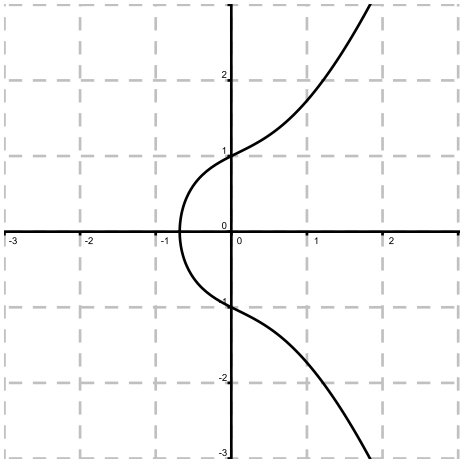

Figura 1: $y^2 = x^3 + x + 1, \Delta > 0$

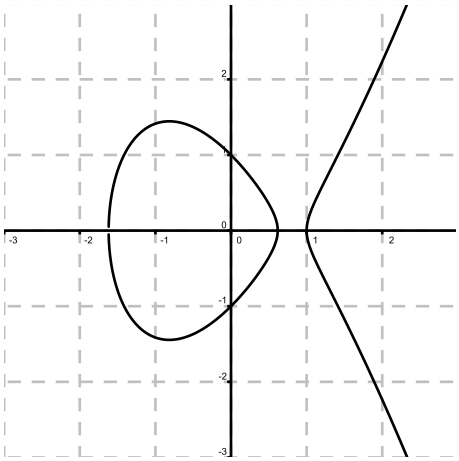

Figura 2: $y^2 = x^3 - 2x + 1, \Delta < 0$

Primero, se realizarán dos observaciones geométricas. Se excluirá el caso de una recta vertical, puesto que, no parece cruzar a la curva en un tercer punto, aunque de la misma manera que ”lineas paralelas se encuentran en el infinito", se podría decir que la recta también encuentra la curva en el infinito.

En términos de las ecuaciones (15) y (16), este punto sería la ”solución al infinito", $X = 0$, $Y = 1$ y $Z = 0$; llamado normalmente el punto O. Del mismo modo, para que una recta sea vertical, P y Q deben tener igual coordenada en x, y por lo tanto, los cuadrados de la coordenada de y son iguales, así uno es el negativo del otro.

La segunda observación geométrica concierne varios casos especiales en donde $P = Q$. En este caso, el significado geométrico correcto de ”la recta que conecta P y Q” es ”la tangente a la curva en P". Con esta interpretación se puede deducir que el tercer punto también tiene coordenadas racionales.

Se define una operación, la cual llamaremos + por las razones que se verán más adelante, sobre los puntos de una curva elípticas dada. Si R es el tercer punto, en la recta que pasa por P y Q, y R' es el punto con igual coodenada en x como R, pero cuya coodenada de y es:

$$P + Q = R'. \tag{17}$$

Aritmeticamente, si se asume que $P = (x_1, y_1)$, $Q = (x_2, y_2)$ y $R' = (x_3, y_3)$, y que la curva está dada por (15), entonces:

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= \frac{y_2 - y_1}{x_2 - x_1} x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \end{aligned} \tag{17'}$$

cuando x_1 es diferente de x_2, y

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 - A}{2y_1}\right)^2 - x_1 - x_2 \\ y_3 &= \frac{3x_1^2 - A}{2y_1}(x_1 - x_3) - y_1 \end{aligned} \tag{17''}$$

cuando $P = Q$. Por supuesto, si $P = Q'$ la respuesta es 0.

A partir de esta definición $R + R' = 0$, y O es el equivalente a cero para la adición ordinaria, por lo tanto tiene sentido escribir $-R$ en vez de R'. Está claro que la definición geométrica (17) (y puede ser comprobado de las fórmulas (17') y (17'')) que $P + Q = Q + P$, es decir, la + es conmutativa y asociativa (la prueba de esta propiedad es muy laboriosa o requiere usar ordenador). Entonces + tiene todas las propiedades algebraicas habituales y escribiremos $2P$ en vez de $P + P$, etc.

No se sigue que todas las propiedades aritméticas de +, se cumplan. Por ejemplo es posible para P diferente de O, que $2P$ sea igual a O.

Un ejemplo de esto es la curva $y^2 = x^3 - 63x - 162$ que tiene tres de tales puntos P $(-6, 0)$, $(-3, 0)$ y $(9, 0)$. Es claro geométricamente que unicamente tales puntos sobre una curva de la forma de (15) son aquellos con $y = 0$, por lo tanto la coodenada x debe ser la raiz cúbica del lado derecho, y ellos son por lo tanto 0, 1 y 3. Este resultado es por lo tanto verdadero para cualquier curva elíptica desde que ellos pueden ser transformado a la forma (15).

De cualquier manera, los puntos en la curva elíptica no necesitan ser puntos de torción, es decir, tener múltiplos que son O. Por ejemplo en la curva $y^2 = x^3 - 2$, hay un punto obvio $P = (3, 5)$, $5^2 = 3^3 - 2$. Podemos calcular con un ordenador.

$$2P = \left(\frac{129}{100}, \frac{-383}{1000}\right)$$

$$3P = \left(\frac{164323}{29241}, \frac{-66234835}{5000211}\right)$$

$$4P = \left(\frac{2340922881}{58675600}, \frac{113259286337279}{4494455096000}\right)$$

Y puede ser probado que la ecuación continúa indefinidamente.

Consideramos la curva

$$y^2 = x^3 - 11. \tag{18}$$

Luego obviamente los puntos $P = (3, 4)$ y $Q = (15, 58)$ están en la curva. Algunos primeros múltipos de P son:

$$\left(\frac{345}{64}, \frac{-6179}{512}\right), \quad \left(\frac{861139}{23409}, \frac{799027820}{358177}\right) \quad \text{y} \quad \left(\frac{22125642465}{9774090496}, ...\right)$$

Mientras que los dos primeros múltiplos de Q son:

$$\left(\frac{51945}{13456}, \frac{10647157}{1560896}\right) \quad \text{y} \quad \left(\frac{50491376191}{22468511025}, \frac{1987488229342114}{9774090496}, ...\right)$$

En realidad, se puede mostrar que todos los múltiplos de P son distintos de los múltiplos de Q, y así tenemos a partir de esto, un sistema bi-dimensional de puntos racionales sobre la curva: $aP + bQ$ para cualquier entero a y b; con $a = b = 0$ da el punto al infinito. Esto es posible y Mestre ha demostrado que:

$$y^2 - 246xy + 36599029y = x^3 - 19339780x - 36239244$$

tiene al menos 12 puntos independientes. Su trabajo ha llegado a ser extendido por Nagao y por Fermigier: el último ha encontrado una curva con al menos 22 puntos independientes. En este ejemplo A tiene 33 dígitos y B tiene 50. Se ha conjeturado, para algunos n, se puede encontrar una curva con al menos n puntos racionales independientes sobre ella. De cualquier manera, solo hay un número finito de puntos independientes, un resultado que fué probado por Mordell, y después generalizado por Weil. No es conocido un algoritmo para saber exactamente cuantos puntos independientes están allí. Se puede mostrar que las curvas con un gran números de puntos independientes son, en cierto sentido, raras".

Los ejemplos de arriba pueden dar al lector la impresión que es fácil encontrar puntos, al menos sobre curvas elípticas simples; nada podría ser más lejano que la verdad. Por ejemplo, Bremner y Cassels mostraron que el punto más simple sobre $y^2 = x^3 + 877x$ es ...

$$\left(\frac{3754945281271621...}{6215987776...}, \frac{256256...}{49007802...}\right)$$

8. EL ÚLTIMO TEOREMA DE FERMAT

La última conjetura de Fermat o bien como generalmente ha sido nominada, El Último Teorema de Fermat, afirma sencillamente que la expresión $x^n + y^n = z^n$, con $x, y, z \epsilon N$ y $n \epsilon N$ no tiene solución para $n > 2$, es decir, que si x^n e y^n son potencias perfectas de números enteros, $x^n + y^n$ no es potencia perfecta de números enteros cuando es $n > 2$. Pierre Fermat tenía la costumbre de anotar en los márgenes de los textos, es así como dejó en uno de los márgenes de la Aritmética de Diofanto, esta conjetura muy simple de explicar, pero tan difícil de demostrar que ha tenido al mundo científico de cabeza durante 300 años.

Lo curioso es que en dicho margen, Fermat escribió que poseía una demostración "maravillosa", que sin embargo, no cabía en el estrecho margen del libro de Diofanto. Este hecho ha presentado históricamente un enigma, pues las generalidades posteriores a la vista de la dificultad de dar con una demostración "maravillosa", no se plantearon que el doctor Fermat se quedó olímpicamente con lo personal, o bien, estaba en un craso error al considerar que disponía de algún tipo de demostración.

Todos los intentos realizados en los 3 siglos siguientes a la muerte de Fermat, tanto de encontrar una demostración de la veracidad de la conjetura, como de encontrar un caso que la contradijera, han resultado fallidos. Es así que, desde 1908 existía un premio de 100.000 marcos que habría de entregarse a la persona que lograra demostrar la conjetura. El premio administrado por la Universidad de Gotinga, se ofrecía por la demostración, no por encontrar un ejemplo que rechace la conjetura. En el año 1997 se hizo entregar al profesor Andrew Wiles de dicho premio.

La demostración del Último Teorema de Fermat a mano de Andrew Wiles, fue uno de los logros matemáticos más prominentes de finales del siglo pasado, y sin duda uno de los eventos científicos que recibió la mayor atención de los medios de comunicación y del público en general.

El logro de Wiles ha sido realmente contundente y su demostración es un verdadero tour de forcé[3], matemático digno de la mayor admiración. La historia personal de Wiles en relación con el último teorema de Fermat, es sin duda dramática, tanto por haberse él puesto como meta desde joven la resolución del problema y haberlo logrado después de décadas, como por los largos años que dedicó en completa soledad a su prueba y el error que se descubrió en ella en el último momento.
La mayor parte de los conocimientos de los descubrimientos del Teorema de Fermat han sido sacado de los comentarios que él escribió sobre el margen de su copia de la aritmética de Diofanto.

Frente a la ecuación $x^2 + y^2 = z^2$ en el libro de Diofanto, Fermat escribio: "sin embargo, es imposible escribir un cubo como la suma de dos cubos ($x^3 + y^3 \neq z^3$), así también, un número elevado a la cuarta potencia es imposible escribirla como la suma de dos números elevados

[3]Proeza

a su cuarta potencia, respectivamente ($x^4 + y^4 \neq z^4$), y en general cualquier potencia más allá de la segunda, como la suma de dos potencias similares. Para esto he descubierto una prueba realmente maravillosa, pero el margen es demasiado pequeño para contenerlo". Esta es la famosa conjetura de Fermat, generalmente llamado el Último Teorema de Ferma: la ecuación

$$x^n + y^n = z^n \tag{19}$$

no tiene ninguna solución en los números naturales si n es un número entero mayor que 2.

Como se ha mencionado anteriormente, a pesar de los esfuerzos de muchos de los mejores matemáticos de los 300 años pasados, permanecio no probado como una proposición general hasta que Wiles anunciara una prueba en 1993. Probablemente Fermat confundía en el pensamiento de esto, él tenía una prueba.

La atracción del problema está en parte en la simplicidad seductora de su formulación, por esta razón esto ha obsesionado a muchos aficionados cuya seguridad en sí mismo ha sido mayor que su capacidad matemática, y esto seguramente tiene la distinción de ser el problema arítmetico para el cual el mayor número de pruebas incorrectas ha sido propuesto.

Siempre parecía probable que cualquier nuevo método inventado para la prueba de la conjetura del Teorema de Fermat conduciría a nuevos acontecimientos importantes en la teoría de números.

Esto fue ampliamente realizado en el caso del trabajo de Kummer (1810 - 93). Kummer creyó al principio que él había demostrado la conjetura de Fermat. El error en sus argumentos fue advertido por Dirichlet, y los esfuerzos de Kummer para reparar el error lo condujeron a crear una teoría nueva y extensa, en el campo de los números algebraicos ideales. La prueba de Wiles del Último Teorema de Fermat es en realidad importante para dar un paso adelante en la teoría de curvas elípticas.

En un desarrollo elemental como este, debemos contentarnos por la prueba de la verdad de la conjetura del Teorema de Fermat para algún valor particular de n

El caso más simple para tratar es $n = 4$, donde Fermat demostró que la ecuación no tiene solución.

Por otro lado, Fermat demostró, de forma general, que la ecuación:

$$x^4 + y^4 = z^2 \tag{20}$$

no tiene ninguna solución en los números naturales, y su prueba es un ejemplo excepcional de su técnica de pendiente infinita, que es simplemente otra forma del principio de prueba por la inducción. De cualquier solución hipotética de la ecuación en los números naturales, Fermat sacó otro con un valor más pequeño de z. La repetición de este proceso conduce tarde o temprano a una contradicción, ya que una secuencia de números naturales que dismunuye, no puede hacerlo indefinidamente.

El principio es el mismo como el método de Legendre, pero aquí esto es usado en la demostración de que no tiene soluciones, mientras que allí eso fue usado para demostrar que sí tiene solución.

Si se supone que x, y, z son los números naturales que satisfacen (20), podemos suponer también que x e y no tienen ningún otro factor común mayor que 1. Luego, los números x^2, y^2, z constituyen una solución primitiva de $X^2 + Y^2 = Z^2$, por lo tanto, ellos son expresiones posibles como (posiblemente depués del intercambio x e y

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

Donde p y q son números naturales y primos relativos, donde uno es par y el otro impar. Mirando la primera ecuación, y recordando que cualquier cuadrado debe ser congruente a 0 ó 1 (mod 4), aca vemos que p debe ser impar y q par. Poniendo $q = 2r$, tenemos:

$$x^2 = p^2 - (2r)^2,\ (\frac{1}{2}y)^2 = pr$$

Donde p y r son primos relativos y su producto es un cuadrado perfecto, cada uno de ellos debe ser un cuadrado perfecto. Si ponemos $p = v^2$ y $r = w^2$, la primera ecuación se hace

$$x^2 + (2w^2)^2 = v^4$$

Esta ecuación es algo similar a (20) en su forma general. Cuando un razonamiento similar es aplicado otra vez a la nueva ecuación, obtenemos exactamente (20). La última ecuación implica:

$$x = P^2 - Q^2,\ 2w^2 = 2PQ,\ v^2 = P^2 + Q^2$$

Donde P y Q son números enteros y primos relativos, donde uno es par y el otro impar. Entonces $PQ = w^2$,P y Q de ben ser cuadrado perfecto.

Colocando $P = X^2$, $Q = y^2$, la tercera ecuación es:

$$X^4 + Y^4 = v^2$$

que es la primera forma de (20). En esta ecuación X, Y, v son números naturales y

$$v^2 = p < \sqrt{z}$$

De donde $v < z$. En vista de lo que fue dicho antes, esto es suficiente para demostrar que la ecuación (20) no tiene solución.

Hasta los años ochenta, las investigaciones sobre el problema del Teorema de Fermat, casi todas habian estado basadas en el trabajo de Kummer. Ellos mostraron pruebas que si la n satisface cualquiera de una serie de condiciones, entonces la ecuación (19) no tiene solución. Es suficiente para considerar los valores primos de $n > 2$, porque algún número mayor que 2 es dibisible por algunos números primos mayores que 2, o sea divisible por 4; y si la ecuación no tiene solución para algún valor de n es un Fortiori que no tiene solución para cualquier múltiplo de aquel valor. Hasta ahora, siempre que un número n no satisfaga alguno de los criterios existentes, ello como generalmente es posible de encontrar otro criterio que se enfrentaría con el número n.

Se ha visto que la ecuación cuadrática $x^2 + y^2 = 1$ tiene infinitas soluciones en los números racionales, y con esto, si podemos encontrar una solución racional de una cónica, podemos encontrar infinitas de estas. Esto mismo es verdadero para algunas curvas elípticas, con más precisión, si se puede encontrar una "no *torción*", en un punto racional, podemos encontrar infinitos. Mordell conjeturó que algunas curvas, las más complicadas, sólo podrían tener finitas soluciones. Esto finalmente fue demostrado por Falting en 1983, que muestra para $n > 3$ $x^n + y^n = 1$ tiene sólo finitas soluciones racionales.

Frey sugirió en 1985, que la existencia de una solución no trivial de $u^p + v^p = w^p$ implica la existencia de una curva no modular elíptica, $y^2 = x(x + u^p)(x - v^p)$ conocido como la curva de Frey. Esta sugerencia fue mostrada por Ribet en 1986. Esta curva es semiestable y en 1993 Whiles anunció una prueba que cada curva semiestable elíptica es modular, el caso semiestable conjeturado por Taniyama, Shimura y Weil. De ahí ninguna solución no trivial de $u^p + v^p = w^p$ puede existir.

8.1. LA ECUACIÓN $x^4 + y^4 = z^2$

Se demostrará ahora la inposibilidad de solución de la ecuación $x^4 + y^4 = z^2$ en los números enteros positivos. El argumento es indirecto, en lo que se refiere a suponer que existe una solución en los enteros positivos, y esto conducirá a una contradicción. Asumiendo al menos una solución, suponemos que x, y, z denota una solución positiva tal que ninguna otra solución tiene un valor más pequeño que z. La contradicción se obtiene sacando otra solución positiva en los números enteros con un valor de z más pequeño aún. Primero se establece el $m.c.d(x, y, z) = 1$. Ya que si p es primo y divide a x, y y z entonces $p^4/(x^4 + y^4)$ de modo que p^4/z^2 y p^2/z. Esto seguiría con $(x/p)^4 + (y/p)^4 = (z/p^2)^2$, contradiciendo el caracter mínimo de z.

En particular se observa que x, y, z no son todos pares. Si x e y fueran impares tendríamos $x^4 \equiv y^4 \equiv 1 \pmod 8$ y $z^2 \equiv 2 \pmod 8$ que es imposible. Si x e y son pares, z sería par, y entonces concluiríamos que x ó y es par o impar. Se presume que x es par e y impar.

Después se escribe $y^4 = (z - x^2)(z + x^2)$ y observe esto $(z - x^2)$ y $(z + x^2)$ son primos relativos. Puesto que si p divide a ambos, esto divide su producto, y^4, su suma $2z$ y su diferencia $2x^2$. Esto es imposible porque y es impar y el $m.c.d(x, y, z) = 1$. De ahí $(z - x^2)$ y $(z + x^2)$ son las cuartas potencias de números enteros positivos, u^4 y v^4, $(u, v) = 1$. Así se tiene:

$$z - x^2 = u^4, z + x^2 = v^4, (v^2 - u^2)(v^2 + u^2) = 2x^2$$

Ahora u y v son impares porque $(z - x^2)$ y $(z + x^2)$ son impar, y de ahí $v^2 + u^2 \equiv 2 \pmod 4$. También ningún p impar primo divide a ambos lados $(v^2 - u^2)$ y $(v^2 + u^2)$ desde entonces $(u, v) = 1$ y $(v^2 - u^2)$ es un cuadrado perfecto, es decir, $(v^2 - u^2) = a^2$, $(v^2 + u^2) = 2b^2$ con a y b positivos.

Se tiene que $v = r^2 + s^2$, $u = r^2 - s^2$ y $a = 2rs$ donde r y s son números enteros positivos. Ahora $v^2 + u^2 = 2b^2$ implica $r^4 + s^4 = b^2$, y ya que esto tiene la misma forma que $x^4 + y^4 = z^2$, tenemos una contradicción si se demuestra que $z > b$.

Ahora $u = v = 1$ es imposible porque esto implica $x^2 = 0$, y $u^4 + v^4 > u^2 + v^2$ y tenemos

$$z = \frac{1}{2}(u^4 + v^4) > \frac{1}{2}(u^2 + v^2) = b^2 \geq b$$

que completa la prueba de la proposición siguiente.

Teorema 2 *Las únicas soluciones enteras de $x^4 + y^4 = z^2$ son las soluciones triviales $x = 0$, $z = \pm y^2$ e $y = 0$, $z = \pm x^2$.*

A veces llaman en método usado en la prueba de este teorema "la prueba por la pendiente" ó "el método de Fermat de la pendiente infinita". Este tipo de prueba, que también ocurre en otros sitios en la teoría de números, está basado en el principio que cada juego no vacío de enteros positivos contiene la mayor parte de elementos.

El hecho que $x^4 + y^4 = z^2$ no tiene ninguna solución positiva implica que $x^4 + y^4 = z^4$ no tiene ninguna solución positiva. Esto es un caso particular de una afirmación famosa de Fermat, en el cual él afirmó en una nota marginal que él podría demostrar esto para cada número entero $n > 2$, la ecuación $x^n + y^n = z^n$ no tiene más soluciones en los números enteros, que la trivial al menos una variable es cero. Esta proposición aún es una conjetura para muchos valores de n. Se conoce como el Último Teorema de Fermat o el gran Teorema de Fermat.

El hecho que $x^3 + y^3 = z^3$ no tiene solución en los enteros positivos implica la misma cosa para $x^n + y^n = z^n$, si n es cualquier múltiplo de 3. Así si el teorema de Fermat se cumple para los números primos impares, también se sostiene para todos los enteros $n > 2$.

Un aviso que El último Teorema de Fermat es verdadero para cualquier exponente menor que 100000, fue publicado por S. Wagstaff, en el Notices of the Amer Math Society, 23, A-53 (1976).

Tales resultados son obtenidos ingeniosamente combinando teorias con técnicas del ordenador.

El Teorema 2 es ampliado en los problemas siguientes, para mostrar que ninguna de las ecuaciones:

$$x^4 + y^4 = z^2$$

$$x^4 - 4y^4 = z^2$$

$$x^4 - y^4 = z^2$$

$$x^4 + 4y^4 = z^2$$

tiene una solución en los números enteros positivos. Basta demostrar sólo para una de las dos primeras de estas ecuaciones, y también para las últimas dos ecuaciones, puesto que identidades algebráicas pueden ser utilizadas para establecer la equivalencia en cada par.

Haciendo un leve cambio en la notación, ahora se demuestra que si hay una solución de $x^4 + y^4 = z^2$ en los enteros positivos, entonces hay también una solución de $u^4 - 4v^4 = w^2$ en los números enteros positivos, e inversamente.

Comenzando con $x^4 + y^4 = z^2$, y elevando al cuadrado ambos lados, ponemos

$$z^4 - 4(xy)^4 = (x^4 - y^4)^2$$

Esta ecuación es de la forma $u^4 - 4v^4 = w^2$.

A la inversa, si elevamos al cuadrado ambos lados de $u^4 - 4v^4 = w^2$ y reorganizamos los términos, resulta $w^4 + (2uv)^4 = (u^4 + 4v^4)^2$, que es de la forma $x^4 + y^4 = z^2$.

La equivalencia de las ecuaciones $x^4 - y^4 = z^2$ y $x^4 + 4y^4 = z^2$ puede ser demostrada de un modo análogo.

9. LA ECUACIÓN $x^3 + y^3 = z^3 + w^3$

Si bien la ecuación $x^3 + y^3 = z^3$ es un caso especial de la ecuación de Fermat, es insoluble, la ecuación $x^3 + y^3 = z^3 + w^3$ tiene infinitas soluciones enteras, con soluciones obvias $x = z$ ó $x = w$ ó $x = -y$. Una fórmula que entrega soluciones, fue encontrada en el año 1591 (Vieta), siendo descubierta una fórmula más general por Euler entre los años 1756 – 1760. Luego, Bienet en 1841 simplifica la fórmula.

Para resolver la ecuación

$$x^3 + y^3 = z^3 + w^3 \tag{21}$$

Utilizamos las siguientes igualdades $x + y = X$; $z - w = W$; $x - y = Y$; $z + w = Z$.

La ecuación obtenida es:

$$X(X^2 + 3Y^2) = Z(Z^2 + 3W^2) \tag{22}$$

Existe una identidad que expresa que el producto de dos números de la forma $X^2 + 3Y^2$ tiene la misma forma:

$$(X^2 + 3Y^2)(Z^2 + 3W^2) = (XZ + 3YW)^2 + 3(YZ - XW)^2$$

Si se multiplica (22) por $X^2 + 3Y^2$ y dividimos por Z, se obtiene:

$$\frac{X}{Z}(X^2 + 3Y^2)^2 = (XZ + 3YW)^2 + 3(YZ - XW)^2$$

Esto muestra que el número racional $\frac{X}{Z}$ es de la forma $p^2 + 3q^2$ donde p y q son números racionales dados por:

$$p = \frac{XZ + 3YW}{X^2 + 3Y^2}, \quad q = \frac{YZ - XW}{X^2 + 3Y^2} \tag{23}$$

Simplificando algebraicamente, elegimos $Z = 1$ y consideramos X, Y y W como números racionales. En (23), con $Z = 1$, obtenemos:

$$pX + 3qY = 1$$

$$pY - qX = W$$

Esto nos muestra que podemos expresar Y y W en términos de p, q y X, donde $X = p^2 + 3q^2$. Obtenemos:

$$3qY = 1 - pX$$

$$3qW = p - X^2$$

Si volvemos a los originales x, y, z, w y removemos los denominadores obtenemos:

$$\begin{cases} x = 1 - (p - 3q)(p^2 + 3q^2), \\ z = p + 3q - (p^2 + 3q^2)^2, \end{cases} \qquad \begin{cases} y = -1 + (p + 3q)(p^2 + 3q^2), \\ w = -(p - 3q) + (p^2 + 3q^2)^2, \end{cases} \tag{24}$$

Estas son la fórmula de Euler y Bienet. Para racionales p y q cualesquiera, ellas nos dan racionales x, y, z, w, que satisfacen la ecuación (21) y muestra que reciprocamente cada solución racional de (21) es proporcional a una solución dada por estas fórmulas.

Si en particular se da a p y q valores enteros, obtenemos soluciones enteras de (21), pero esto no es una razón suficiente para esperar que cada solución entera sea obtenida de esta forma. Una solución particular, obtenida al utilizar $p = 1$, $q = 1$ es $x = 9$, $y = 15$, $z = -12$, $w = 18$, esto corresponde curiosamente a que $3^3 + 4^3 + 5^3 = 6^3$.

Los valores $p = 4$, $q = 1$ corresponde a:

$$3^3 + 60^3 = 22^3 + 59^3.$$

La solución más simple de (21) con x, y, z, w, todos positivos es:

$$1^3 + 12^3 = 9^3 + 10^3 (= 1729)$$

El número 1729 es el más pequeño expresable como la suma de dos cubos enteros positivos, de dos diferentes formas.

Una identidad interesante (Mahler 1936), es obtenida al colocar $p = 3q$. Esto da $x = 1$, $y = -1 + 72q^3$, $z = 6q - 144q^4$. Escribiendo $2q = t$, se obtiene la identidad:

$$(1 - 9t^3)^3 + (3t - 9t^4)^3 + (9t^4)^3 = 1$$

Lo interesante de esto, es el hecho que muestra que el número 1 puede ser representado de infinitas formas como la suma de tres cubos enteros. Existe una identidad similar para el número 2. No se sabe de alguna identidad que exprese el número 3 como una suma de tres cubos enteros, de infinitas formas y las formas que conocemos:

$$1^3 + 1^3 + 1^3$$

$$4^3 + 4^3 + (-5)^3$$

Sería apropiado mencionar en este punto, otro problema no resuelto. No todos los números pueden ser representados como la suma de tres cubos enteros, y así ningún número congruentes a 4 ó 5 (mod 9) pueden ser así representados.

Otro problema es: ¿Es cada número representable como la suma de cuatro cubos enteros?

A pesar de muchas tentativas, ésto todavía no está resuelto.

Finalmente, hay un camino simple de expresar un número, como la suma de cinco cubos enteros.

Tenemos que

$$(x+1)^3 + (x-1)^3 + (-x)^3 + (-x)^3 = 6x$$

De ahí cualquier múltiplo de 6 es representable por cuatro cubos enteros.

Ahora, cualquier número puede ser reducido a un múltiplo de 6 restándole un cubo conveniente. Verdaderamente, es fácil ver que $n - n^3$ es siempre un múltiplo de 6.

Esto lleva al resultado que cada número es representable por la suma de 5 cubos, como por ejemplo:

$$18 = (-2)^3 + (-4)^3 + (13)^3 + (26)^3 + (-27)^3$$

$$846 = (42)^3 + (-112)^3 + (-33)^3 + (111)^3 + (-2)^3$$

Esto se cree que fué probado por primera vez por Oltramere en 1894.

10. ECUACIÓN DE PELL

La ecuación $x^2 - dy^2 = N$, con enteros d, N y x e y incognitas, es lo que llamamos la ecuación de Pell. Si d es negativo, puede tener sólo un número finito de soluciones. Si d es un cuadrado perfecto, digamos d=a^2, la ecuación se reduce a $(x - ay)(x + ay) = N$ y nuevamente tiene sólo un número finito de soluciónes. El caso más interesante de la ecuación surge cuando d es un entero positivo y no es un cuadrado perfecto. Para este caso, se usarán fracciones simples continuas.

Jhon Pell fue un matemático inglés que vivió durante el siglo XVII. Se ha cuestionado el por qué, la ecuación que nos convoca lleva su nombre, pués, Euler asoció un método de resolución de este tipo de ecuaciones a Pell en vez de a Brouncker, el verdadero propietario de dicho método. En los tiempos de Euler, él era un escritor muy leído, por lo que la inclusión de este fallo en uno de sus libros provocó que esta asociación errónea se difundiera ampliamente y con rapidez.

La antigua Grecia fué el escenario donde se gesta el estudio de la ecuación de Pell. Algunos trabajos de Arquímedes muestran el conocimiento de alguna solución para el caso $d = 3$ e incluso se conjetura que los griegos poseían más nociones sobre el asunto, lo cual no se puede asegurar pues no se tienen documentos que lo corroboren. De lo que sí se posee conocimento, es del estudio sobre esta ecuación realizada en la antigua India. Brahmagupta encontró la solución más pequeña para el caso $d = 92$ y Bháscara una técnica general para encontrar soluciones.

Es importante mencionar a Pierre de Fermat quien profundizó el estudio de la ecuación de Pell. En 1657, al final de su carrera, envió el siguiente desafío a los matemáticos ingleses:

"Dado un número cualquiera, que no es un cuadrado, existe un número infinito de cuadrados tal que si el cuadrado es multiplicado por el número dado y la unidad es añadida al producto el resultado es un cuadrado. Dicho de otro modo, dado d que no es un cuadrado, existen infinitos cuadrados, x^2, tales que si los multiplicamos por d y añadimos 1 a este producto, el resultado es un cuadrado, digamos y^2"

Esto nos lleva a la ecuación $dx^2 + 1 = y^2$ que es precisamente la ecuación de Pell.
Al parecer, en la época de Diofanto se tomaban las soluciones válidas para estas ecuaciones como racionales.Ésto último hizo que los ingleses resolvieran muy pronto el desafío propuesto, pero Fermat había incluido en su desafío un preámbulo donde explicaba que se pedían soluciones enteras, pero esta explicación debió extraviarse y no llegó a sus destinatarios.

Fermat tuvo que aclarar este punto a los ingleses en el momento que recibió las soluciones. Los ingleses se indignaron, pues ellos concideraban que ésto era un cambio de las condiciones del problema, de igual forma, se dedicaron a resolverlo. Wallis y Brouncker son al parecer los que tuvieron más dedicación a ello.

En este y en algún otro desafío aparecían separados tres casos particulares de la ecuación de Pell. Explícitamente los casos $d = 61, 109, 149$. La razón del porque estos casos, es que es más complicado el análisis para $d < 200$. Esto nos indica que Fermat debía poseer un método general para resolver la ecuación de Pell.

Los ingleses, al parecer Brouncker (o al menos Wallis se lo atribuye a él), consiguieron resolver los casos particulares y además dieron un procedimiento general para llegar a la solución para cualquier valor de d. Pero, este método poseía un problema, al igual que el de Fermat, quizás fuera el mismo y era que en ningún momento se demostraba que el método funcionara siempre. Se aplicaba a una ecuación con un d concreto y se obtenían las soluciones, mas no se demostraba que el método era válido para todos los casos. Esto toma bastante importancia, pués el mismo Euler fracasó al intentar demostrar este hecho y hubo que esperar más de un siglo para que Lagrange consiguiera dicha prueba.

Lagrange ha sido el primero en probar que $x^2 + dy^2 = 1$ tiene infinitas soluciones si d es un entero positivo fijo, no un cuadrado perfecto.

Se expanderá $\sqrt{d}$, en una fracción continua [4] con h_n/k_n convergentes, y con q_n definido por la ecuación [5] con $\xi_0 = \sqrt{d}, q_o = 1, m_0 = 0$.

Teorema 3 *En los párrafos anteriores mencionamos el caso que nuestro* $\boldsymbol{d}$ *fuera un entero positivo, no siendo cuadrado perfecto, pues bien, en este caso tenemos que* $h_n^2 - dk_n^2 = (-1)^{n-1}q_{n+1}$ *para otro entero* $n \geq 1$.

De las ecuaciones [6] [5] , se tiene:

$$\sqrt{d} = \xi_0 = \frac{\xi_{n+1}h_n + h_{n-1}}{\xi_{n+1}k_n + k_{n-1}} = \frac{(m_{n+1} + \sqrt{d})h_n + q_{n+1}h_{n-1}}{(m_{n+1} + \sqrt{d})k_n + q_{n+1}k_{n-1}}$$

[4]Teorema: si el entero positivo d no es un cuadrado perfecto, la expansión en fracción simple continua de $\sqrt{d}$ es de la forma $\sqrt{d} = \langle a_0, \overline{a_1, a_2, ..., a_{r-1}, 2a_0}\rangle$, con $a_0 = [\sqrt{d}]$. Además con $\xi = \sqrt{d}$, $q_0 = 1$, $m_0 = 0$, en ecuaciones con x en los reales del tipo $x > 1$, y $x + x^{-1} < \sqrt{5}$, entonces $x < \frac{1}{2}(\sqrt{5} + 1)$ y $x^{-1} > \frac{1}{2}(\sqrt{5} - 1)$.

[5]Definición: si x es real, $x > 1$, y $x + x^{-1} < \sqrt{5}$, entonces $x < \frac{1}{2}(\sqrt{5} + 1)$ y $x^{-1} > \frac{1}{2}(\sqrt{5} - 1)$.

[6]Definición: sea $\theta = \langle a_0, a_1, a_2...\rangle$ fracción simple continua. Entonces $a_0 = [\theta]$. Además si θ_1 denota $\langle a_1, a_2, a_3, ...\rangle$ entonces $\theta = a_0 + \frac{1}{\theta_1}$.

Simplificando esta ecuación y separando esto en una parte racional y una parte puramente irracional. Cada una de las partes debe ser cero, entonces conseguimos dos ecuaciones y podemos eliminar m_{n+1} de ellos. El resultado final es:

$$h_n^2 - dk_n^2 = (h_n k_{n-1} - h_{n-1}k_n)q_{n+1} = (-1)^{n-1}q_{n+1}$$

Donde se usa [7] en el último paso.

Colorario 1 *Tomando* $\boldsymbol{r}$ *como la longitud del período de la expanción de* $\sqrt{d}$ *para* $n \geq 0$.

$$h_{nr-1}^2 - dk_{nr-1}^2 = (-1)^{nr}q_{nr} = (-1)^{nr}$$

n posee infinitas soluciones para $x^2 - dy^2 = 1$ en los enteros, condicionando a d que sea un número positivo y no un cuadrado perfecto.

Podemos ver que el Teorema 3 nos da soluciones para la ecuación de Pell en ciertos valores de N. En particular, el colorario anterior, nos da infinitas soluciones de $x^2 - dy^2 = 1$ para el uso de un valor nr. Si r es impar, el colorario anterior nos da infinitas soluciones de $x^2 - dy^2 = -1$, utilizando un entero impar $n \geq 1$.

El próximo teorema muestra que muchas soluciones de $x^2 - dy^2 = \pm 1$ pueden ser obtenidas a partir de la expansión de fracciones simples continuas de $\sqrt{d}$. Pero primero se realizará la siguiente observación: a parte de cada solución trivial como $x = \pm 1, y = 0$ de $x^2 - dy^2 = 1$, todas las soluciones de $x^2 - dy^2 = N$ disminuyen dentro del conjunto de cuatro combinaciones de signos $\pm x$,$\pm y$. De ahí es suficiente hablar de las soluciones positivas $x > o, y > 0$.

Teorema 4 *Sea* $\boldsymbol{d}$ *un entero positivo no cuadrado perfecto, y sea la expansión de la fracción continua de* $\sqrt{d}$ *convergente a* h_n/k_n. *Sea* N *un entero que satisfaga* $|N| < \sqrt{d}$. *Luego, alguna solución positiva* $x = s, y = t$ *de* $x^2 - dy^2 = N$ *con* $(s, t) = 1$ *satisfaciendo* $s = h_n, t = k_n$ *para algunos enteros positivos* n.

Prueba: Sea E y M enteros positivos tal que $(E, M) = 1$ y $E^2 - \rho M^2 = \sigma$, donde $\sqrt{\rho}$ es irracional y $o < \sigma < \sqrt{\rho}$. Aquí ρ y σ son números reales, no necesariamente enteros. Entonces:

$$\frac{E}{M} - \sqrt{\rho} = \frac{\sigma}{M(E + M\sqrt{\rho})}$$

y aquí

$$0 < \frac{E}{M} - \sqrt{\rho} < \frac{\sqrt{\rho}}{M(E + M\sqrt{\rho})} = \frac{1}{M^2(E/(M\sqrt{\rho})) + 1}$$

[7] Teorema: la ecuación $h_i k_{i-1} - h_{i-1}k_i = (-1)^{i-1}$ y $r_1 - r_{i-1} = \dfrac{(-1)^{i-1}}{k_i k_{i-1}}$ para $i \geq 1$. Las identidades: $h_i k_{i-2} - h_{i-2}k_i = (-1)^i a_i$ y $r_i - r_{i-2} = (-1)^i a_i k_i k_{i-2}$ para $i \geq 1$. La fracción h_1/k_1 es reducida, esto es $(h_i, k_i) = 1$.

También $0 < E/M - \sqrt{\rho}$ implica que $E/(M\sqrt{\rho}) > 1$, y por lo tanto

$$|\frac{E}{M} - \sqrt{\rho}| < \frac{1}{2M^2}$$

Por [8], E/M es convergente en la fracción continua de la expansión de $\sqrt{\rho}$.

Si $N > O$, tomamos $\sigma = N, \rho = d, E = s, M = t$, y el teorema se cumple en este caso.

Si $N < 0$, entonces $t^2 - (1/d)s^2 = -N/d$ y tomando $\sigma = -N/d, \rho = 1/d, E = t, M = s$. Se descubre que t/s es convergente en la expansión de $1/\sqrt{d}$. Entonces [9] muestra que s/t es convergente en la expansión de $\sqrt{d}$.

Teorema 5 *Toda solución positiva de $x^2 - dy^2 = \pm 1$ se encuentra entre $x = h_n, y = k_n$ donde h_n/k_n son convergentes de la expanción $\sqrt{d}$. Si r es el punto final de la expanción de $\sqrt{d}$ y si r es par, cuando $x^2 + dy^2 = -1$ no tiene soluciones, todas las soluciones positivas de $x^2 - dy^2 = 1$ son dadas por $x = h_{nr-1}, y = k_{nr-1}$ para $n = 1, 2, 3....$ Por otro lado si r es impar, cuando $x = h_{nr-1}, y = k_{nr-1}$ dan todos soluciones positivas para $x^2 - dy^2 = -1$ con $n = 1, 3, 5, ...$ y todas soluciones positivas de $x^2 - dy^2 = 1$ con $n = 2, 4, 6, ...$*

Prueba: La secuencia de pares $(h_0, k_0), (h_1, k_1), ...$ incluirá todas las soluciones positivas de $x^2 + dy^2 = 1$. Además, $a_0 = [\sqrt{d}] > 0$ entonces la secuencia $h_0, h_1, h_2, ...$ es estrictamente creciente. Si denotamos x_1, y_1 como la primera solución que aparece, entonces para muchas otras soluciones x, y tendremos $x > x_1$ y de ahí también $y > y_1$. Habiendo encontrado esta solución positiva menor, mediante fracciones simples continuas, podemos encontrar todas las soluciones positivas restantes por un método más simple.

Teorema 6 *Sea x_1, y_1 las soluciones positivas menores de $x^2 + dy^2 = 1$, **d** un entero positivo no cuadrado perfecto. Entonces, todas las soluciones positivas estan dadas por x_n, y_n para $n = 1, 2, 3, ...$ donde x_n e y_n son enteros definidos por $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.*

Los valores de x_n e y_n son determinados por la expansión de la potencia y la comparación de las partes racionales y las partes puramente irracionales. Por ejemplo, $x_3 + y_3\sqrt{d} = (x_1 + y_1\sqrt{d})^3$ entonces $x_3 = x_1^3 + 3x_1y_1^2d$ e $y_3 = 3x_1^2y_1 + y_1^3d$.

[8] Teorema: sea ξ el cual denota algun número irracional. Si éste es un número racional a/b con $b \geq 1$ tal que: $|\xi - \frac{a}{b}| < \frac{1}{2b^2}$. Tenemos que si a/b es igual a una de las convergencias de la expansión de la fracción simple continua de ξ.

[9] Teorema: el n-ésimo número convergente de $1/x$ es el recíproco de el $(n-1)$ número convergente de x, si x es algún número real >1.

Prueba: Primero se establece que x_n, y_n es una solución. Tenemos $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pues la conjugación de un producto es el producto de la conjugación. Entonces podemos escribir

$$x_n^2 - y_n^2 d = (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) = (x_1 - y_1\sqrt{d})^n(x_1 + y_1\sqrt{d})^n = (x_1^2 - y_1^2 d)^n = 1$$

A continuación se mostrará que muchas soluciones pueden ser obtenidas. Supongamos que existen soluciones positivas s, t que no estan en la secuencia $\{x_n, y_n\}$. Luego, ambos $x_1 + y_1\sqrt{d}$ y $s + t\sqrt{d}$ son mayor que 1, deben existir algunos enteros m , tal que, $(x_1 + y_1\sqrt{d})^m \leq s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}$. No se puede tener $(x_1 + y_1\sqrt{d})^m = s + t\sqrt{d}$, por que esto implicaría que $x_m + y_m\sqrt{d} = s + t\sqrt{d}$, y luego $s = x_m, t = y_m$. Ahora

$$(x_1 - y_1\sqrt{d})^m = (x_1 + y_1\sqrt{d})^{-m},$$

y podemos multiplicar la desigualdad anterior por $(x_1 - y_1\sqrt{d})^m$ para obtener

$$1 < (s + t\sqrt{d})(x_1 - y_1)^m < x_1 + y_1\sqrt{d}$$

Definiendo los enteros a y b por $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$ tenemos,

$$a^2 - b^2 d = (s^2 - t^2 d)(x_1^2 - y_1^2)^m = 1$$

entonces a, b son una solución de $x^2 - dy^2 = 1$ tal que, $1 < a + b\sqrt{d} < x_1 + y_{1\sqrt{d}}$. Pero, tenemos $0 < (a + b\sqrt{d})^{-1}$, y luego $0 < a - b\sqrt{d} < 1$. Ahora, tenemos

$$a = \frac{1}{2}(a + b\sqrt{d}) + \frac{1}{2}(a - b\sqrt{d}) > \frac{1}{2} + 0 > 0,$$
$$b\sqrt{d} = \frac{1}{2}(a + b\sqrt{d}) - \frac{1}{2}(a - b\sqrt{d}) > \frac{1}{2} - \frac{1}{2} = 0,$$

entonces a, b es una solución positiva. Anteriormente $a > x_1, b > y_1$, pero esto contradice $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$ y entonces la suposición anterior es falsa. Todas las soluciones positivas son dadas por x_n, y_n, para $n = 1, 2, 3, ...$

Podemos notar que la definición de x_n, y_n puede ser extendida a cero y un negativo n, estos dan soluciones no positivas.

Para un N distinto de 1, hay ciertos resultados que pueden ser demostrados, pero aquellos no son tan completos como los que se han mostrado, los cuales son verdadero para el caso de $N = 1$. Por ejemplo, si x_1, y_1 es la solución positiva más pequeña de $x^2 - dy^2 = 1$, y si $r_0^2 - ds_0^2 = N$, estos enteros r_n, s_n pueden der definidos por $r_n + s_n\sqrt{d} = (r_0 + s_0\sqrt{d})(x_1 + y_1\sqrt{d})^n$, y es fácil demostrar que r_n, s_n son soluciones de $x^2 - dy^2 = N$. Como sea, aquellos no nos asegura que todas las soluciones positivas pueden ser obtenidas por este camino, comenzando desde un r_0, s_0 fijo.

Referencias

[1] Introduction to the theory of numbers, Ivan Niven Zuckerman, N.Y.: John Wiley, 1980.

[2] Introducción a la teoría de los números, Pettofrezzo, Anthony J., Englewood Cliffs, N.J.: Prentice-Hall, 1972.

[3] El teorema de Fermat y sus Historias, Leo Corry, 2006.

[4] Sobre la conjetura de Fermat, file///cl/casanchiya/mat/wiles/Fermat.htm