Examinando un caso del último teorema de Fermat

Jerónimo Basa [*]

Octubre 2014

Resumen

En este texto intento exponer de manera sencilla un estudio sobre el último teorema de Fermat para el caso $n = 3$. Al principio se ven los resultados del propio Euler y más adelante un desarrollo sobre teoría de números y cómo estas propiedades pueden ayudarnos a resolver este caso. Los apéndices contienen los lemas necesarios para que se pueda realizar una lectura continua del texto.

Índice

[*]Estudiante de Licenciatura en Matemática por la Universidad Nacional del Litoral

Prólogo

El último teorema de Fermat es uno de los problemas matemáticos más interesantes de la historia. En particular, agrada el hecho de que su sencillo enunciado tenga una demostración tan compleja. Pierre de Fermat fue un abogado francés y aficionado de las matemáticas, considerado uno de los más importantes del siglo XVII. Su interés principal era la teoría de número, en especial, se interesó por las soluciones enteras a una ecuación dada. Uno de los resultados más importantes es el conocido *Teorema de Fermat: si p es un número primo, entonces para todo número natural a vale $a^p \equiv a \ (mod\ p)$*. La historia dice que Fermat solía anotar muchas de sus ideas sobre los mismos textos que iba leyendo. Este trabajo trata sobre uno en especial; mientras Fermat leía su ejemplar del tratado *Arithmetica* de Diofanto [4], que en su libro número II se tratan los cuadrados que pueden descomponerse como suma de dos cuadrados[1], Fermat escribió:

> *Es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados, y en general, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente. He encontrado una demostración realmente admirable, pero el margen del libro es muy pequeño para ponerla.*

Se cree que Fermat no contaba con dicha demostración, ya que el resultado general necesario para probarla era muy avanzado para su época. Sí se cree que tuvo una demostración para el caso $n = 4$ usando el método descenso al infinito. Luego de la publicación de esta conjetura, muchos matemáticos exploraron los desarrollos de la teoría de números tratando de lograr una demostración completa y efectiva. Finalmente, 358 años después de formulada, el matemático Andrew Wiles logra demostrar, en 1995, la veracidad del último teorema de Fermat [10].

Queda más que claro la importancia y profundidad de dicho teorema, cuyo enunciado puede ser fácilmente comprendido por cualquier persona no matemática, lo cual en cierta manera conlleva a que uno, aficionado a este tipo de maravillas, intente explorar sobre el mismo. Me arriesgaré a discutir sobre el último teorema de Fermat para el caso $n = 3$.

[1] Básicamente, esto se trata de buscar ternas pitagóricas para las soluciones diofánticas de la ecuación $x^2 + y^2 = z^2$.

1. Los resultados de Euler

Teorema 1.1 (El último teorema de Fermat)**.** *Sea n un número entero mayor que 2. Entonces la ecuación*

$$x^n + y^n = z^n$$

no tiene soluciones enteras distintas de las triviales.

Este sencillo enunciado comenzó una de las búsquedas más interesantes de la matemática. La primera aproximación para obtener resultados más generales, debía derivar de los casos más sencillo. Sabiendo entonces que para $n = 2$ existen soluciones enteras, Leonhard Euler en su trabajo, luego de explorar las propiedades de los números enteros y las ecuaciones diofánticas, intenta probarlo sólo usando estas herramientas.

1.1. Descomposición en cubos

Sabiendo que un cuadrado puede descomponerse como suma de dos cuadrados, podemos preguntarnos si es posible descomponer un cubo como suma de dos cubos.

Conjectura 1.1. Un cubo no puede escribirse como suma de dos cubos.

Como $x^3 + y^3$ debe ser un cubo, si dividimos dicha fórmula por y^3, este cociente también debe ser un cubo, y resulta $\frac{x^3}{y^3} + 1 = c$ (donde c es un cubo). Si hacemos $\frac{x}{y} = z-1$ entonces su cubo resulta ser z^3-3z^2+3z-1. Supongamos entonces, que el cubo que buscamos tenga como raíz cúbica la expresión $(z-u)$, entonces comparando las fórmulas deberíamos obtener

$$z^3 - 3z^2 + 3z = z^3 - 3uz^2 + 3u^2z - u^3 \tag{1}$$

entonces, si quisieramos determinar u de manera que los segundos términos de (1) desaparezcan, obtendríamos $u = 1$. Los demás términos formarían la ecuación

$$3z = 3u^2z - u^3,$$

cuyas infinitas soluciones no nos permiten concluir nada. Entonces, hagamos que u esté sin determinar e intentemos deducir z de la expresión $-3z^2 + 3z = -3uz^2 + 3u^2z - u^3$ o $3uz^2 - 3z^2 = 3u^2z - 3z - u^3$ derivadas de (1). De aquí obtenemos $3(u-1)z^2 = 3(u^2-1)z - u^3$ que nos da

$$z^2 = (u+1)z - \frac{u^3}{3(u-1)}.$$

La solución de esta cuadrática permite escribir

$$z = \frac{u+1}{2} \pm \sqrt{\frac{u^2+2u+1}{4} - \frac{u^3}{3(u-1)}},$$

o

$$z = \frac{u+1}{2} \pm \sqrt{\frac{-u^3+3u^2-3u-3}{12(u-1)}}. \tag{2}$$

Como buscamos soluciones enteras, nuestro propósito será que la expresión bajo la raíz en (2) sea un cuadrado. Para este objetivo vamos a multiplicar y dividir por el término $3(u-1)$ para que el denominador sea un cuadrado, es decir $36(u-1)^2$. Luego, sólo nos interesa trabajar con el numerador, que luego de multiplicado por $3(u-1)$, queda $-3u^4+12u^3-18u^2+9$. Ya que 9 es un cuadrado, podemos suponer que esta última fórmula es el cuadrado de alguien; supongamos que es el cuadrado de au^2+bu+3 es decir, obtenemos $a^2u^4+2bau^3+6au^2+b^2u^2+6bu+9$. Esta última expresión es un cuadrado, y se corresponde con dicho numerador. Sus soluciones enteras son $a=-b-3, u=1$ de donde no podemos concluir nada pues estamos en el anterior caso. La otra solución entera es $b=0, u=0$ de donde tampoco concluimos nada pues $u=0$ implica $z=1$.

Esta es la forma en que Euler comenzó a dar la primera sospecha de que la conjetura es cierta, al no poder concluir algo que haga pensar lo contrario. La demostración de Euler contiene cierta falta de argumentación en algunos hechos, no errores sino un incompleto desarrollo para algunas cuestiones, quizá mínimas para él. La primera forma y tal vez la más sencilla de ver este caso del teorema de Fermat lo veremos a continuación. La misma idea se puede expandir haciendo uso de detalles más desarrollados y explorando la teoría de números.

Teorema 1.2. *Si x, y, z son enteros, entonces la ecuación $x^3+y^3=z^3$ no tiene soluciones enteras distintas de las triviales.*

Demostración. Comenzamos viendo que, si la imposibilidad se da para la suma, también ocurre para la resta. Es decir, si es imposible que $x^3+y^3=z^3$ también es imposible que $x^3=z^3-y^3$. Por lo tanto, será suficiente hacer la demostración para uno de los casos; tomemos el de la suma.

Primero, podemos suponer que los números x, y son coprimos; si tuvieran un divisor común, entonces el cubo de x, y es divisible por el cubo de dicho divisor. Por ejemplo, sea $y=mb$ y $x=ma$ entonces $x^3+y^3=m^3a^3+m^3b^3$, si esta fórmula fuese un cubo, a^3+b^3 sería un cubo para enteros coprimos a y b.

Como x, y no tienen un factor común, estos dos números son ambos impares, o bien uno es par y el otro impar. En el primer caso, z sería par, y para

el otro caso tendríamos z par. Como se puede ver, de los números x, y, z hay siempre uno que es par y los otros dos impares. Es suficiente probar el teorema en el caso de que x, y son impares y z par.

Entonces, si x, y son impares, es claro que su suma y su diferencia son números pares. Así que pongamos $p = \frac{x+y}{2}$ y $q = \frac{x-y}{2}$. De aquí deducimos que $x = p + q$ y que $y = p - q$; se sigue que uno de los números p, q debe ser impar y el otro par. Ahora reescribimos nuestro problema y tenemos que $x^3+y^3 = (p+q)^3+(p-q)^3 = 2p(p^2+3q^2)$. Debemos probar que este producto no puede ser un cubo; si hubieramos querido hacer la demostración para la diferencia, habríamos obtenido $x^3-y^3 = 2q(q^2+3p^2)$ que es la misma fórmula antes escrita sólo que intercambiando los roles de p, q. Será entonces suficiente probar sólo la imposibilidad de que la expresión $2p(p^2 + 3q^2)$ no puede ser un cubo.

Si suponemos entonces $2p(p^2+3q^2) = z^3$ fuese un cubo, ese cubo sería par. Luego, $p^2 + 3q^2$ es impar y z par, entonces 8 divide a z^3, por lo que 8 divide a $2p$ y resulta entonces que q es impar (A.1). Como 8 divide a z^3 se tiene que $\frac{p}{4}(p^2 + 3q^2) \in \mathbb{Z}$; como $p^2 + 3q^2$ es impar, no es divisible por 4, luego $\frac{p}{4} \in \mathbb{Z}$.

En caso de que nuestro producto $\frac{p}{4}(p^2 + 3q^2)$ sea un cubo, cada uno de estos factores, a menos que tengan un divisor común, deben ser separadamente cubos. En caso de que el producto de dos factores coprimos sea un cubo, se tiene necesariamente que cada uno es un cubo; en caso de tener un divisor común, el caso es distinto. Para determinar esto debemos tener presente que, si estos factores tienen un divisor común, los números p^2 y $p^2 + 3q^2$ tienen el mismo divisor; sea éste m. Por propiedad, m divide la diferencia, es decir, m divide a $3q^2$ y obtenemos un divisor común de $3q^2$ y p^2. Pero como p y q son coprimos (A.2) los términos p^2 y $3q^2$ en caso de tener un divisor común, éste será 3, que es el caso en que p es divisible por 3.

Supongamos que los factores p y $p^2 + 3q^2$ no tienen divisores comunes, es decir cuando p no es divisible por 3. En consecuencia nuestros factores $\frac{p}{4}$ y $p^2 + 3q^2$ son coprimos, así que deben ser cubos separadamente. Ahora, en un intento de que la expresión $p^2 + 3q^2$ sea un cubo, tenemos que

$$p^2 + 3q^2 = (p + q\sqrt{-3})(p - q\sqrt{-3}),$$

y podemos suponer enteros t, u tales que

$$p + q\sqrt{-3} = (t + u\sqrt{-3})^3,\ p - q\sqrt{-3} = (t - u\sqrt{-3})^3.$$

Estos no dice que

$$p^2 + 3q^2 = (t^2 + 3u^2)^3$$

de donde concluimos que $p = t^3 - 9tu^2 = t(t^2 - 9u^2)$ y $q = 3t^2u - 3u^2 = 3u(t^2 - u^2)$. Como q es impar, u también debe ser impar y t par, pues de otra manera $t^2 - u^2$ sería par.

Habiendo obtenido la expresión para $p^2 + 3q^2$ encontramos que $p = t(t^2 - 9u^2) = t(t - 3u)(t + 3u)$, y también se requiere que $\frac{p}{4}$, y en consecuencia 2p, sea un cubo. Esto nos dice que ahora la fórmula $2p = 2t(t - 3u)(t + 3u)$ debe ser un cubo. Observamos ahora que t es un número par y no es divisible por 3, ya que de lo contrario p sería divisible por 3 y comenzamos suponiendo que eso no ocurre. De modo que para este caso se tiene que los tres factores $2t, t-3u, t+3u$ son coprimos. Luego cada uno por separado debe ser un cubo. Si ahora hacemos $t - 3u = \alpha^3$ y $t + 3u = \beta^3$ obtenemos que $\alpha^3 + \beta^3 = 2t$. Entonces, si $2t$ fuese un cubo, hemos encontrado dos cubos α^3, β^3 cuya suma sería un cubo. Estos, claramente, son menores que los cubos x^3, y^3 de nuestra primera suposición. Ya que primero habíamos dicho $x = p + q$, $y = p - q$ y continuamos determinando p, q por los términos t, u. Luego, los números x, y son necesariamente mayores que t, u. Finalmente concluimos que, si podemos encontrar grandes números como los que requerimos, también somos capaces de encontrar cubos más pequeños cuya suma también es un cubo; y de la misma manera, siempre podríamos encontrar cubos más pequeños que cumplan la propiedad. Ahora, ya que es muy cierto que no hay tales cubos entre números pequeños que cumplan la propiedad, tampoco pueden haber dos cubos grandes que la cumplan.

Supongamos ahora que p es divisible por 3 y que q no lo es. Hagamos entonces $p = 3r$. Nuestra fórmula $\frac{p}{4}(p^2+3q^2)$ es ahora $\frac{3r}{4}(9r^2+3q^2) = \frac{9r}{4}(3r^2+q^2)$. Ahora bien, los dos factores son coprimos, ya que $3r^2 + q^2$ no es divisible por 2 ni por 3, y r debe ser par pues p lo es. Por lo tanto, ambos por separado deben ser cubos.

El factor $q^2 + 3r^2$ podemos transformarlo como ya vimos y obtener $q = t(t^2 - 9u^2)$ y $r = 3u(t^2 - u^2)$. Como q es impar, t debe ser impar y u par. Pero $\frac{9r}{4}$ debe ser también un cubo; si lo multiplicamos por el cubo $\left(\frac{2}{3}\right)^3$ obtenemos $\frac{2r}{3}$ que debe ser un cubo. Combinado con el hecho de que $r = 3u(t^2-u^2)$ vemos que $2u(t^2 - u^2) = 2u(t - u)(t + u)$ debe ser un cubo. Al ser estos tres factores coprimos, cada uno debe ser por separado un cubo. Supongamos entonces que $t + u = \gamma^3$ y $t - u = \delta^3$. Obtenemos que $2u = \gamma^3 - \delta^3$. Resulta entonces que, si $2u$ fuese un cubo, también lo sería $\gamma^3 - \delta^3$.

Con esto, obtenemos dos cubos γ^3, δ^3 cuya diferencia es un cubo, y que estos son menores que los considerados al principio. De aquí se deduce que si $\gamma^3 - \delta^3 = \epsilon^3$ entonces también se tiene que $\gamma^3 = \epsilon^3 + \delta^3$ y lo mismo vale para la suma de cubos que son menores que los x, y de nuestra suposición. Concluimos entonces lo mismo que vimos en el caso de que p no era divisible por 3, para finalmente ver que ambos casos parecen llevar a un absurdo, el cual provino de suponer que $x^3 + y^3$ es un cubo. □

1.2. Un análisis más actual

La demostración vista anteriormente se atribuye al matemático Euler. Un importante paso en su demostración, que como vimos usa las propiedades de divisibilidad de los enteros de la forma $a^2 + 3b^2$, fue hecha sin suficiente justificación. Legendre, que reproduce la demostración de Euler en su libro no da ninguna explicación al respecto. Este matemático también era un experto en dicha área, y logró entender ciertamente el razonamiento de Euler, quizá demasiado intuitivo para él. Sin embargo, futuros matemáticos estaban disconformes sobre algún posible "hueco" en dicha prueba. Al parecer se trataba de una prueba rigurosa de que, si s es impar y $s^3 = a^2 + 3b^2$ con $\text{mcd}(a, b) = 1$ entonces $s = u^2 + 3v^2$ para ciertos $u, v \in \mathbb{Z}$.

Podemos entonces dar una demostración ligeramente distinta siguiendo los resultados expuestos en (B).

Teorema 1.3. *La ecuación*

$$x^3 + y^3 + z^3 = 0$$

no tiene soluciones enteras distintas de la trivial.

Demostración. Asumamos x, y, z distintos de cero, coprimos entre ellos y tales que $x^3 + y^3 + z^3 = 0$. Tomemos ahora x, y impares y z par. Entre todas las soluciones con dicha propiedad, vamos a tomar aquella para la cual $|z|$ es el más pequeño posible.

Debemos encontrar enteros l, m, n coprimos entre ellos, todos distintos de cero, tales que $l^3+m^3+n^3 = 0$, con n par y $|z| > |n|$. Ésta será la contradicción. Como $x+y, x-y$ son pares, existen enteros a, b tales que $2a = x+y, 2b = x-y$; tenemos entonces $x = a+b, y = a-b$ y se sigue que $a, b \neq 0$ con $\text{mcd}(a, b) = 1$ y a, b tienen distinta paridad.

Entonces $-z^3 = x^3 + y^3 = (a+b)^3 + (a-b)^3 = 2a(a^2 + 3b^2)$. Pero $a^2 + 3b^2$ es impar y z par, por lo que 8 divide a z^3, luego 8 divide a $2a$, así que b es impar. Tenemos entonces que $\text{mcd}(2a, a^2 + 3b^2)$ es igual a 1 ó 3. En efecto, si p^k $(k \geq 1)$ es una potencia de primo que divide a $2a$ y $a^2 + 3b^2$ entonces $p \neq 2$ así que $p^k | a$ y por lo tanto a $3b^2$; pero p no divide a b, por lo tanto resulta $k = 1$ y $p = 3$ (B.4) (B.5).

Caso 1. $\text{mcd}(2a, a^2 + 3b^2) = 1$.

Se tiene entonces que 3 no divide a a. De $-z^3 = 2a(a^2 + 3b^2)$ se sigue que por la factorización única de enteros en primos, $2a$ y $a^2 + 3b^2$ son cubos

$$\begin{cases} 2a = r^3, \\ a^2 + 3b^2 = s^3, \end{cases}$$

donde s es impar y no es múltiplo de 3. Luego por (B.8) tenemos que $s^3 = a^2 + 3b^2$ con $\text{mcd}(a, b) = 1$, entonces s es de la forma $s = u^2 + 3v^2$ con $u, v \in \mathbb{Z}$

y

$$\begin{cases} a = u(u^2 - 9v^2), \\ b = 3v(u^2 - v^2). \end{cases}$$

Entonces v es impar, u es par con $u \neq 0$, $3 \not| u$ y $\mathrm{mcd}(u, v) = 1$. Más aún, $2u, u + 3v, u - 3v$ son coprimos entre ellos y de $r^3 = 2a = 2u(u - 3v)(u + 3v)$ se sigue que los tres factores son cubos

$$\begin{cases} 2u = -n^3, \\ u - 3v = l^3, \\ u + 3v = m^3, \end{cases}$$

con l, m, n distintos de cero (pues 3 no divide a u) y coprimos entre ellos. Podemos concluir entonces que

$$l^3 + m^3 + n^3 = 0,$$

donde n es par. En efecto

$$|z|^3 = |2a(a^2 + 3b^2)| = |n^3(u^2 - 9v^2)(a^2 + 3b^2)| \geq 3|n|^3 > |n^3|$$

porque $u^2 - 9v^2 = l^3m^3 \neq 0$ y $b \neq 0$. Esto contradice la minimalidad de $|z|$.

Caso 2. $\mathrm{mcd}(2a, a^2 + 3b^2) = 3$.

Esribimos $a = 3c$. Entonces c es par y $4|c$, mientras que $3 \not| b$[2]. Entonces $-z^3 = 6c(9c^2+3b^2) = 18c(3c^2+b^2)$ donde $\mathrm{mcd}(18c, 3c^2+b^2) = 1$. Ciertamente, c es par y b es impar, entonces $3c^2 + b^2$ es impar, 3 no divide a $3c^2 + b^2$ (A.3) y $\mathrm{mcd}(b, c) = 1$. Nuevamente, por factorización única de enteros en primos, se sigue que $18c$ y $3c^2 + b^2$ son cubos

$$\begin{cases} 18c = r^3, \\ 3c^2 + b^2 = s^3, \end{cases}$$

donde s es impar y 3 divide a r. Por el resultado mencionado en el caso anterior, $s = u^2 + 3v^2$ con $u, v \in \mathbb{Z}$ y

$$\begin{cases} b = u(u^2 - 9v^2), \\ c = 3v(u^2 - v^2). \end{cases}$$

Luego u es impar, v es par (pues b es impar), $v \neq 0$ y $\mathrm{mcd}(u, v) = 1$. También se tiene que $2u, u + v, u - v$ son coprimos entre ellos. De $r^3 = 18c = 54v(u + v)(u - v)$ podemos deducir que $(r/3)^3 = 2v(u + v)(u - v)$ y $2v, (u + v), (u - v)$ son cubos

$$\begin{cases} 2u = -n^3, \\ u + v = l^3, \\ u - v = -m^3. \end{cases}$$

[2]Pues a, b son coprimos.

Por tanto $l^3 + m^3 + n^3 = 0$ con $l, m, n \neq 0$ y n es par. Se sigue que

$$\begin{aligned} |z|^3 &= 18|c|(3c^2 + b^2) \\ &= 54|v(u^2 - v^2)|(3c^2 + b^2) \\ &= 27|n|^3|u^2 - v^2|(3c^2 + b^2) \\ &> |n|^3, \end{aligned}$$

pues $u^2 - v^2 = -l^3m^3 \neq 0$, $|3c^2 + b^2| \geq 1$. Pero esto contradice la minimalidad de $|z|$.

Vemos entonces que los dos casos que estudiamos conllevan a un absurdo, el cual proviene de suponer que $x^3 + y^3 + z^3 = 0$ tiene soluciones enteras distintas de las triviales. □

2. El campo de Eisenstein y la demostración de Gauss

A pesar de tener una demostración correcta dada por Euler, otros matemáticos hallaron similares resultados explorando otras estructuras algebraicas. El propio Gauss dio su demostración usando el cuerpo de los números complejos. Sea $\omega = \frac{-1+\sqrt{-3}}{2}$. Entonces podemos definir el siguiente conjunto

$$\mathbb{Z}[\omega] := \{z = a + b\omega : a, b \in \mathbb{Z}\},$$

llamado *campo de Eisenstein*. Los elementos que pertenecen a este conjunto se llaman *enteros de Eisenstein* y forman un anillo conmutativo (A.4).

Bajo la representación dada en (A.6), decimos que si $\alpha, \beta \in \mathbb{Z}[\omega]$ entonces β divide a α si existe un entero $\gamma \in \mathbb{Z}[\omega]$ tal que $\alpha = \beta\gamma$. Dos enteros α, β se dice que están *asociados* si α divide a β y β divide a α. Los enteros asociados con 1 se llaman *unidades* de $\mathbb{Z}[\omega]$ y tiene norma 1(A.7). Un entero p de $\mathbb{Z}[\omega]$ es *primo* si no es elemento unidad y los únicos enteros que dividen a p son elementos unidades o están asociados con p.

Dada la representación demostrada en (A.6), el conjugado de $\alpha = \frac{a+b\sqrt{-3}}{2}$ es $\overline{\alpha} = \frac{a-b\sqrt{-3}}{2}$.[3] Su norma viene dada por $N(\alpha) = \alpha\overline{\alpha} = \frac{(a^2-3b^2)}{4}$. Si $\alpha \in \mathbb{Z}[\omega]$ entonces escribimos $I(\alpha) = \{\beta\alpha : \beta \in \mathbb{Z}[\omega]\}$ es el *ideal* múltiplos de α. Si $\alpha, \beta, \gamma \in \mathbb{Z}[\omega], \alpha \neq 0$ decimos que

$$\beta \equiv \gamma \pmod{\alpha}$$

cuando α divide a $\beta - \gamma$; se dice que β y γ son congruentes módulo α. Esta es una relación de equivalencia sobre el anillo $\mathbb{Z}[\omega]$ y el conjunto de las clases de

[3] Con $a \equiv b \pmod 2$.

equivalencia $\mathbb{Z}[\omega]_{I(\alpha)}$ es un anillo, llamado el *anillo de residuos* de $\mathbb{Z}[\omega]$ módulo α.

Como fue mencionado, la demostración de Gauss acerca del último teorema de Fermat para $n = 3$ requiere resultados más generales sobre teoría algebraica. Los lemas nos ayudaran a desarrollarlo.

Teorema 2.1. *La ecuación*

$$x^3 + y^3 + z^3 = 0$$

no tiene soluciones sobre el campo de Eisenstein.

Demostración. Asumamos que existen $\xi, \eta, \theta \in \mathbb{Z}[\omega]$ todos distintos de cero y que satisfacen $\xi^3 + \eta^3 + \theta^3 = 0$. Si $\text{mcd}(\xi, \eta, \theta) = \delta$ entonces $\xi/\delta, \eta/\delta, \theta/\delta$ satisfacen la misma ecuación con $\text{mcd}(\xi/\delta, \eta/\delta, \theta/\delta) = 1$. Así que podemos asumir ξ, η, θ coprimos entre ellos. Luego vemos que λ[4] no puede dividir a dos de estos elementos ξ, η, θ. Vamos a asumir, por ejemplo, que $\lambda \nmid \xi, \lambda \nmid \eta$.

Caso 1. Vamos a asumir que $\lambda \nmid \theta$. Entonces

$$\begin{cases} \xi^3 \equiv \pm 1 \pmod{\lambda^3}, \\ \eta^3 \equiv \pm 1 \pmod{\lambda^3}, \\ \theta^3 \equiv \pm 1 \pmod{\lambda^3}, \end{cases}$$

de modo que $0 = \xi^3 + \eta^3 + \theta^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^3}$. Luego, las combinaciones posibles de signos nos permiten deducir que el resultado es $\pm 1 \vee \pm 3$. Claramente $0 \not\equiv \pm 1 \pmod{\lambda^3}$. Si $0 \equiv \pm 3 \pmod{\lambda^3}$, entonces $\lambda^3 | \pm 3$ y $\lambda | \pm 1$ por lo que λ sería una unidad, lo cual es una contradicción.

Caso 2. Vamos a asumir que $\lambda | \theta$.

Sea $\theta = \lambda^n \psi, \psi \in \mathbb{Z}[\omega], n \geq 1$, y $\lambda \nmid \psi$. Por lo tanto la ecuación a estudiar se transforma en

$$\alpha^3 + \beta^3 + \lambda^{3n} \psi^3 = 0.$$

Sea ahora $n \geq 1$ y sea ϵ una unidad de $\mathbb{Z}[\omega]$. Vamos a considerar la siguiente proposición P_n : existen enteros $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$, coprimos entre ellos, no múltiplos de λ y

$$\alpha^3 + \beta^3 + \epsilon \lambda^{3n} \gamma^3 = 0. \tag{3}$$

La demostración entonces se basa en probar lo siguiente. Si vale P_n entonces se tiene que $n \geq 2$ y también vale la proposición P_{n-1}. Al repetir el proceso en un momento se tendrá que vale P_1 lo cual contradice el hecho de que $n \geq 2$.[5]

Paso 1. $P_n \Rightarrow n \geq 2$.

[4] Con $\lambda = 1 - \omega = \frac{3 - \sqrt{-3}}{2}$ un primo en $\mathbb{Z}[\omega]$. Se encuentran descritos en [6].

[5] Esto no es más que hacer descenso al infinito sobre n.

Como $\lambda \nmid \alpha, \lambda \nmid \beta$ entonces $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}, \beta^3 \equiv \pm 1 \pmod{\lambda^4}$ (A.8) y $\pm 1 \pm 1 \equiv -\epsilon\lambda^{3n}\gamma^3 \pmod{\lambda^4}$ con $\lambda \nmid \gamma$. Entonces el lado izquierdo de la última expresión debe ser 0, pues $\lambda \nmid \pm 2$, por lo tanto $3n \geq 4$ y $n \geq 2$.

Paso 2. Si se satisface P_n, también se satisface P_{n-1}.

Por hipótesis

$$-\epsilon\lambda^{3n}\gamma^3 = \alpha^3 + \beta^3 = (\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta).$$

El elemento λ debe dividir a uno de los elementos de la derecha. Ahora $\alpha+\beta \equiv \alpha+\omega\beta \equiv \alpha+\omega^2\beta \pmod{\lambda}$ porque $1 \equiv \omega \equiv \omega^2 \pmod{\lambda}$, así que λ divide cada factor. Por lo tanto

$$\frac{\alpha+\beta}{\lambda}, \frac{\alpha+\omega\beta}{\lambda}, \frac{\alpha+\omega^2\beta}{\lambda} \in \mathbb{Z}[\omega].$$

y

$$-\epsilon\lambda^{3(n-1)}\gamma^3 = \frac{\alpha+\beta}{\lambda} + \frac{\alpha+\omega\beta}{\lambda} + \frac{\alpha+\omega^2\beta}{\lambda}. \tag{4}$$

Por ser $n \geq 2$, λ divide uno de los factores del lado derecho. Pero $(\alpha+\beta), (\alpha+\omega\beta), (\alpha+\omega^2\beta)$ no son congruentes módulo λ^2 entre ellos. Por lo que λ divide a uno, y sólo uno, de los términos del lado derecho en (4). Por ejemplo, tomemos que λ divide a $\frac{\alpha+\beta}{\lambda}$. Entonces $\lambda^{3(n-1)}$ divide a $\frac{\alpha+\beta}{\lambda}$. Más aún

$$\begin{cases} \alpha+\beta = \lambda^{3n-2}\kappa_1, \\ \alpha+\omega\beta = \lambda\kappa_2, \\ \alpha+\omega^2\beta = \lambda\kappa_3, \end{cases}$$

con $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{Z}[\omega]$ y λ no divide a $\kappa_1, \kappa_2, \kappa_3$.

Multiplicando los términos, encontramos que $-\epsilon\gamma^3 = \kappa_1\kappa_2\kappa_3$ y $\kappa_1, \kappa_2, \kappa_3$ son coprimos entre ellos. Como el anillo $\mathbb{Z}[\omega]$ es DFU[6], $\kappa_1, \kappa_2, \kappa_3$ están asociados con cubos

$$\begin{cases} \kappa_1 = \zeta_1\phi_1^3, \\ \kappa_2 = \zeta_2\phi_2^3, \\ \kappa_3 = \zeta_3\phi_3^3, \end{cases}$$

donde ζ_i es unidad en $\mathbb{Z}[\omega]$ y $\phi_i \in \mathbb{Z}[\omega]$ $(i = 1, 2, 3)$, ϕ_1, ϕ_2, ϕ_3 coprimos y λ no divide a ninguno de ellos. Entonces

$$\begin{cases} \alpha+\beta = \lambda^{3n-2}\zeta_1\phi_1^3, \\ \alpha+\omega\beta = \lambda\zeta_2\phi_2^3, \\ \alpha+\omega^2\beta = \lambda\zeta_3\phi_3^3. \end{cases}$$

De $1+\omega+\omega^2 = 0$ se sigue que

$$\begin{aligned} 0 &= (\alpha+\beta) + \omega(\alpha+\omega\beta) + \omega^2(\alpha+\omega^2\beta) \\ &= \lambda^{3n-2}\zeta_1\phi_1^3 + \lambda\omega\zeta_2\phi_2^3 + \lambda\omega^2\zeta_3\phi_3^3, \end{aligned}$$

[6]Se deduce del hecho de que $\mathbb{Z}[\omega]$ es un dominio euclideano bajo la norma A.5

por lo que

$$\phi_2^3 + \tau\phi_3^3 + \tau'\lambda^{3(n-1)}\phi_1^3 = 0,$$

donde τ, τ' son unidades. Si $\tau = 1$ entonces ϕ_1, ϕ_2, ϕ_3 son solución de (3). Si $\tau = -1$, entonces $\phi_2, -\phi_3, \phi_1$ es solución de (3). Nos resta demostrar que $\tau \neq \pm\omega, \pm\omega^2$. En efecto, como $n \geq 2$,

$$\phi_2^3 + \tau\phi_3^3 \equiv 0 \pmod{\lambda^2}.$$

Pero $\phi_2^3 \equiv \pm 1 \pmod{\lambda^2}, \phi_3^3 \equiv \pm 1 \pmod{\lambda^2}$ por lo tanto $\pm 1 \pm \tau \not\equiv 0 \pmod{\lambda^2}$.

Sin embargo $\pm 1 \pm \omega \equiv 0 \pmod{\lambda^2}$ y $\pm 1 \pm \omega^2 \equiv 0 \pmod{\lambda^2}$. Así que $\tau \neq \pm\omega, \pm\omega^2$. Esto demuestra que se vale P_{n-1}. Luego, vemos que la proposición P_n lleva a una contradicción, la cual proviene de suponer que el último teorema de Fermat cuando $n = 3$ vale para el campo de Eisenstein. □

A. Apéndice

Lema A.1. *$p^2 + 3q^2$ es impar.*

Demostración. En nuestro caso se tiene que uno es par y el otro es impar. Supongamos p par y q impar. Entonces $p^2 + 3q^2 = (2n)^2 + 3(2m+1)^2$ para ciertos $n, m \in \mathbb{Z}$.

$$(2n)^2 + 3(2m+1)^2 = 4n^2 + 12m^2 + 12m + 3 = 2(2n^2 + 6m^2 + 6m + 1) + 1.$$

□

Lema A.2. *p y q son coprimos.*

Demostración. Nuestra hipótesis inicial al principio de la demostración es que x, y son impares y coprimos. Entonces primero se prueba el hecho de que $\text{mcd}(x+y, x-y) = 1 \vee 2$.

Sea $\text{mcd}(x+y, x-y) = d$. Entonces $d|x+y$ y $d|x-y$. Por lo tanto divide a su suma y su diferencia; $d|2x$ y $d|2y$ entonces $d|\text{mcd}(2x, 2y) = 2$. Como $d|2$ resulta que $d = 1$ ó $d = 2$. Anteriormente habíamos dicho que por ser x, y impares, su suma y su diferencia era par, así que al menos 2 será un divisor común de $x+y, x-y$ y en efecto, por lo que acabamos de ver, es el máximo común divisor.

Resta probar que si $\text{mcd}(a, b) = d \Rightarrow \text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$. Sea $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = c$. Entonces $c|\frac{a}{d}$ y $c|\frac{b}{d}$. Luego, existen $m, n \in \mathbb{Z}$ tal que $cm = \frac{a}{d}$ y $cn = \frac{b}{d}$. Se sigue que $a = cmd$ y $b = cnd$. Esto dice que $cd|a$ y $cd|b$. Pero como $\text{mcd}(a, b) = d$ se sigue que $cd \leq d$. Por definición de máximo común divisor, $d \geq 1$, luego $c \leq 1$. Como c era un máximo común divisor, $c \geq 1$. Resulta finalmente que $c = 1$.

Aplicando esto tenemos entonces que

$$\text{mcd}(x+y, x-y) = 2 \Rightarrow \text{mcd}\left(\frac{x+y}{2}, \frac{x-y}{2}\right) = 1 = \text{mcd}(p, q).$$

□

Lema A.3. *3 no divide a $3c^2 + b^2$.*

Demostración. Como $3|3c^2$ se sigue que, si 3 dividiera a $3c^2 + b^2$, divide a la diferencia, es decir $3|b^2 \Rightarrow 3|b$. Pero 3 no puede dividir a b pues $3|a$ y a, b son coprimos. □

Lema A.4. *Los enteros de Eisenstein forman un anillo conmutativo.*

Demostración. Claramente $1 \in \mathbb{Z}[\omega]$. Sean dos enteros de Eisenstein, entonces

$$(a + b\omega) + (c + d\omega) = (a + c) + (b + d)\omega$$

y

$$(a+b\omega)(c+d\omega) = (ac-bd) + (ad+bc-bd)\omega.$$

Vemos entonces que estas dos operaciones son cerradas. Luego, por ser $\mathbb{Z}[\omega]$ subconjunto de $\mathbb{C}$, resulta ser subanillo, y por lo tanto anillo conmutativo. □

Lema A.5. *Sea $\alpha = a+\omega b$ un entero de Eisenstein. Entonces su norma viene dada por*

$$|\alpha|^2 = a^2 - ab + b^2.$$

Demostración.

$$\begin{aligned} |\alpha|^2 &= \alpha\overline{\alpha} \\ &= (a+b\omega)\overline{(a+b\omega)} \\ &= (a+b\omega)\left(\overline{a}+\overline{b}\overline{\omega}\right) \\ &= (a+b\omega)(a+b\overline{\omega}) \\ &= a^2 + (\omega+\overline{\omega})ab + \omega\overline{\omega}b^2. \end{aligned}$$

Por definición

$$\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$$

de donde resulta $\omega + \overline{\omega} = -1$. De igual manera $\omega\overline{\omega} = 1$. Finalmente

$$|\alpha|^2 = a^2 + (\omega\overline{\omega})ab + \omega\overline{\omega}b^2 = a^2 - ab + b^2.$$

□

Lema A.6. *Si x es un entero de Eisenstein entonces existen enteros m, n tales que*

$$x = \frac{m + n\sqrt{-3}}{2},$$

con $m \equiv n \pmod 2$

Demostración. Por ser $x \in \mathbb{Z}[\omega]$ entonces

$$x = a + b\omega = a + b\left(\frac{-1}{2} + \frac{\sqrt{-3}}{2}\right) = a + \left(\frac{-b}{2} + \frac{b\sqrt{-3}}{2}\right) = \frac{2a - b + b\sqrt{-3}}{2}.$$

Se tiene que $2a-b-b = 2a-2b = 2(a-b)$ por lo que $2a-b \equiv b \pmod 2$. □

Lema A.7. *Los únicos elementos unidad de $\mathbb{Z}[\omega]$ son $\pm 1, \pm\omega, \pm\omega^2$.*

Demostración. Un elemento $z = a + b\omega \in \mathbb{Z}[\omega]$ es unidad si, y sólo si, $|z|^2 = a^2 - ab + b^2 = 1$. Si $ab = 0$, entonces $z = \pm 1$, o $z = \pm\omega$. Si $ab \neq 0$ entonces $a^2 + b^2 \geq 2$ y esto con $a^2 - ab + b^2 = 1$ nos da que $ab \geq 1$. Por otro lado de $a^2 - ab + b^2 = 1$ tenemos que $a^2 - 2ab + b^2 = 1 - ab$ así que $ab \leq 1$; luego debemos tener $ab = 1$ lo cual nos dice que $a = b = \pm 1$, i.e. $z = \pm(1+\omega) = \pm\omega^2$. □

Lema A.8. *Si $\alpha \in \mathbb{Z}[\omega]$ y λ no divide a α, entonces $\alpha^3 \equiv \pm 1 \ (mod\ \lambda^4)$.*

Demostración. Como $\alpha \not\equiv 0 \pmod{\lambda}$ entonces $\alpha \equiv \pm 1 \pmod{\lambda}$. Primero asumamos que $\alpha \equiv 1 \pmod{\lambda}$, entonces $\alpha - 1 = \beta\lambda$ con $\beta \in \mathbb{Z}[\omega]$. Luego

$$\alpha - \omega = (\alpha - 1) + (1 - \omega) = \beta\lambda + \lambda = \lambda(\beta + 1),$$

$$\alpha - \omega^2 = (\alpha - \omega) + (\omega - \omega^2) = \lambda(\beta + 1) + \omega\lambda = \lambda(\beta - \omega^2).$$

Por lo tanto $\alpha^3 - 1 = (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2) = \lambda^3\beta(\beta + 1)(\beta - \omega^2)$. Pero $1 - \omega^2 = (1 + \omega)\lambda$, o $\omega^2 \equiv 1 \pmod{\lambda}$. Luego se tiene que $\beta, \beta + 1, \beta\omega^2$ están en tres clases módulo λ distintas, y al menos uno es un múltiplo de λ. Resulta entonces $\alpha^3 \equiv 1 \pmod{\lambda^4}$. El caso $\alpha \equiv -1 \pmod{\lambda}$ se deduce análogamente. □

B. Apéndice

Sea $S = \{a^2 + 3b^2 : a, b \in \mathbb{Z}.\}$

Lema B.1. *S es cerrado bajo la multiplicación.*

Demostración.

$$(a^2 + 3b^2)(c^2 + 3b^2) = (ac + 3bd)^2 + 3(ad - bc)^2.$$

□

Lema B.2. *Sea p un primo y n un entero mayor que cero. Si $p \in S$ y $pn \in S$ entonces $n \in S$*

Demostración. Sea $p = x^2 + 3y^2$ con $x, y \in \mathbb{Z}$ y $pn = \alpha^2 + 3\beta^2$. Entonces

$$n = \left(\frac{a\alpha + 3b\beta}{x^2 + 3y^2}\right)^2 + 3\left(\frac{\alpha b - a\beta}{x^2 + 3y^2}\right)^2 \Rightarrow pn = \alpha^2 + 3\beta^2,$$

y $n \in S$. □

Lema B.3. *Sea p un número primo distinto de 2 y 3. Entonces las siguientes proposiciones son equivalentes*

1. *$p \equiv 1 \ (mod\ 6)$.*
2. *-3 es un cuadrado módulo p.*
3. *El polinomio $x^2 + x + 1$ tiene una raíz en $\mathbb{F}_p$.*

Demostración. Las equivalencias entre (1) y (2) fueron estudiadas por Gauss en su desarrollo de residuos cuadráticos [3]. Para probar la equivalencia en (2) y (3) hagamos

$$x^2 + x + 1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4}.$$

Si existe un $\alpha \in \mathbb{F}_p$ tal que $\alpha^2+\alpha+1 = 0$, entonces $-3 = 4\left(\alpha - \frac{1}{2}\right)^2$ y por otro lado, si $-3 = \beta^2$ con $\beta \in \mathbb{F}_p$ hacemos $\alpha = -\frac{1}{2} + \frac{\beta}{2}$ y resulta $\alpha^2+\alpha+1 = 0$. □

Lema B.4. $p \in S \Leftrightarrow p = 3 \vee p \equiv 1 \ (mod\ 3)$.

Demostración. Si $p = a^2 + 3b^2$ y $p \neq 3$, entonces $b \neq 0$ así que $p \equiv a^2 \pmod 3$ y $3 \not| a$; luego $p \equiv a^2 \equiv 1 \pmod 3$.

Supongamos ahora que existe un primo p, $p \equiv 1 \pmod 3$, tal que $p \notin S$. Tomamos ahora el más pequeño de estos p. Sea $t \geq 1$ el entero más pequeño que cumple $p|t^2 + 3$, con $0 < t < p/2$, $t^2 + 3 = pm$ con $0 < m < p$. Si p' es un primo divisor de m, entonces $m = p'm'$ con $p' \leq m < p$ y $p' \in S$. De $p'(pm') = pm = t^2 + 3 \in S$ se sigue por lema antes visto, que $pm' \in S$. Si $m' = 1$ se tiene que $p \in S$ como queríamos probar. Si p'' es un primo divisor de m', $m' = p''m''$, con $p'' \leq m' < p$ entonces $p'' \in S$, luego $p''(pm'') = pm' \in S$; nuevamente por lema se ve que $pm'' \in S$ con $m'' < m'$. Al repetir este argumento, en algún momento llegaremos a que $p \in S$. □

Lema B.5. *Sea $m = u^2 + 3v^2$ con $u, v \neq 0$, $mcd(u, v) = 1$. Si p es un primo distinto de 2 que divide a m entonces $p \in S$.*

Demostración. $3 \in S$ así que podemos asumir $p \neq 3$. Como p divide a m, p no divide a v, ya que si así fuera, también dividiría a u, contrariamente a la hipótesis de que son coprimos. Sea v' tal que $vv' \equiv 1 \pmod p$. Entonces $(uv')^2 \equiv -3 \pmod p$ por lo que $p \equiv 1 \pmod 3$. Por lema antes visto, $p \in S$. □

Lema B.6. *Sea p un primo en S. Entonces la representación de $p = a^2 + 3b^2$ con $a, b \geq 0$ es única.*

Demostración. Usando los lemas anteriores, tenemos que $p = a^2 + 3b^2 = c^2 + 3d^2$. Entonces

$$1 = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp 3bc}{p}\right)^2,$$

entonces $p = ac \pm 3bd$, $ad = \pm bc$. Luego $pd = acd \pm 3bd^2 = \pm bc^2 \pm 3bd^2 = \pm b(c^2+3d^2) = \pm bp$. Resulta $d = \pm b$. Como estamos tomando enteros positivos, $d = b$ y $a = c$. □

Lema B.7. *Sea $m = 3$ ó $m = u^2 + 3v^2$, con $u, v \neq 0$ y $mcd(u, v) = 1$. Si m es impar y*

$$m = \prod_{i=1}^{n} p_i^{e_i}$$

entonces existen enteros a_i, b_i tales que $p_i = a_i^2 + 3b_i^2$ y

$$u + v\sqrt{-3} = \prod_{i=1}^{n} \left(a_i + b_i\sqrt{-3}\right)^{e_i}.$$

Demostración. La prueba es trivial si $m = 3$. Sea $m > 3, m = u^2 + 3v^2$, con $u, v \neq 0$ $\text{mcd}(u, v) = 1$. Hagamos p un divisor primo de m, entonces $m = pk$. Por los lemas antes vistos, resulta que $p = a^2 + 3b^2$ y $k = c^2 + 3d^2$ donde $c = \frac{ua \pm 3vb}{p}, d = \frac{ub \mp va}{p}$. También tenemos que $(a \pm b\sqrt{3})(c \mp d\sqrt{-3}) = (ac + 3bd) \pm (bc - ad)\sqrt{-3}$ donde

$$ac + 3bd = \frac{1}{p}\left(ua^2 \pm 3vab + 3ub^2 \mp 3vab\right) = u,$$

$$\pm(bc - ad) = \pm\frac{1}{p}\left(uab \pm 3vb^2 - uab \pm va^2\right) = v,$$

esto es

$$(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}.$$

Si $k = 1$ el resultado es trivial. Si $k \neq 1$ entonces bien $k = 3$ ó $k \neq 3$. Para este último caso, $c \neq 0$[7] y $d \neq 0$[8]; más aún, $\text{mcd}(c, d) = 1$ porque $\text{mcd}(u, v) = 1$. Por inducción, el resultado es verdadero para todo k, por lo tanto $c \mp d\sqrt{-3}$ se puede expresar en la forma indicada. Como

$$(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}$$

entonces el resultado se sigue para todo m. □

Lema B.8. *Sea E el conjunto de las ternas (u, v, s) tal que s es impar, $mcd(u, v) = 1$ y $s^3 = u^2 + 3v^2$. Sea F el conjunto de los pares (t, w) donde $mcd(t, w) = 1$ y $t \not\equiv w \pmod 2$. Entonces el mapeo $\Phi : F \to E$ dado por $\Phi(t, w) = (u, v, s)$ con*

$$\begin{cases} u = t(t^2 - 9w^2), \\ v = 3w(t^2 - w^2), \\ s = t^2 + 3w^2, \end{cases}$$

es sobre.

[7] Si $c = 0$, entonces d divide a u, v y se tiene $d = 1$ y por lo tanto $k = 3$, contradiciendo el hecho de que tomamos $k \neq 3$.

[8] Pues si $d = 0$ se sigue que c divide a u, v es decir $c = 1$ y tendríamos $k \neq 1$, contrariamente a nuestra hipótesis de que tomamos $k \neq 1$.

Demostración. Es claro que $s^3 = u^2 + 3v^2$. Como t, w tienen diferente paridad, s es impar. Ahora mostramos que $\text{mcd}(u, v) = 1$. Primero notamos que $\text{mcd}(t^2 - 9w^2, t^2 - w^2) = 1$ porque si un primo p divide a $t^2 - 9w^2$ y $t^2 - w^2$ también divide a $9t^2 - 9w^2$ y también a $8t^2$ por lo tanto $p = 2$.[9] Como t, w tienen diferente paridad, esto es imposible. Vamos a asumir ahora que p es primo, $e \geq 1$ y p^e divide a u, v entonces $p|t$ o $p|t^2 - 9w^2$ por lo tanto $p|t$ en ambos casos; entonces $p \not| w(t^2 - w^2)$ luego $p = 3$. De $3^e|v$, como $3|t$ se tiene $e = 1$ entonces $\text{mcd}(u, v) = 1 \vee 3$. Si $3|v, 3|u$ entonces $3|t, 3 \not| w \Rightarrow 3|s$ pero $3^2 \not| s$. Sin embargo $s^3 = u^2 + 3v^2$ así que $3^2|s^3$ por lo que $3^2|s$, lo cual es una contradicción. Esto muestra que $\Phi(t, w) = (u, v, s) \in E$.

Dado $(u, v, s) \in E$, sea $s^3 = \prod_{i=1}^{n} p_i^{e_i}$ la descomposición de s^3 en factores primos ($p_1, \ldots, p_n$ distintos, $e_i \geq 1$); entonces $e_i = 3e_i'$ para cada i. Por lema antes visto, existen enteros $a_i, b_i \, (i = 1, \ldots, n)$ tales que $p_i = a_i^2 + 3b_i^2$ y

$$u + v\sqrt{-3} = \prod_{i=1}^{n} \left(a_i + b_i\sqrt{-3}\right)^{e_i}.$$

Sea $t, w \in \mathbb{Z}$ definidos por la relación

$$\prod_{i=1}^{n} \left(a_i + b_i\sqrt{-3}\right)^{e_i'} = t + w\sqrt{-3},$$

entonces $u + v\sqrt{-3} = (t + w\sqrt{-3})^3$. Escribiendo explícitamente el cubo se sigue que $u = t(t^2 - 9w^2)$, $v = 3w(t^2 - w^2)$. Finalmente tomando el conjugado $u - v\sqrt{-3} = (t - w\sqrt{-3})^3$ así que multiplicando, $s^3 = u^2 + 3v^2 = (t^2 + 3w^2)^3$ por lo tanto $s = t^2 + 3w^2$. Se sigue que t, w tienen diferente paridad y también $\text{mcd}(t, w) = 1, \quad \Phi(t, w) = (u, v, s)$. □

Referencias

[1] Robert Daniel Carmichael. *Diophantine analysis.* Number 16. John Wiley & sons, Incorporated, 1915.

[2] Leonhard Euler, John Hewlett, Francis Horner, Jean Bernoulli, and Joseph Louis Lagrange. *Elements of algebra.* Longman, Orme, 1840.

[3] Carl Friedrich Gauss. *Disquisitiones Arithmaticae.* Yale University Press, 1965.

[4] T.L. Heath. *Diophantus of Alexandria: A Study in the History of Greek Algebra.* Repressed Publishing LLC, 2012.

[9] Pues p no puede dividir a t ya que $\text{mcd}(t, w) = 1$.

[5] David Hilbert. *The theory of algebraic number fields*. Springer, 1998.

[6] Manouchehr Misaghian. Factor rings and their decompositions in the eisenstein integers ring $\mathbb{Z}[\omega]$. *Armenian Journal of Mathematics*, 5(1):58–68, 2013.

[7] R Andrew Ohana. On fermat's last theorem for n=3 and n=4. 2010.

[8] Paulo Ribenboim. *13 lectures on Fermat's last theorem*. Springer, 1979.

[9] Paulo Ribenboim. *Fermat's last theorem for amateurs*. Springer, 1999.

[10] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, pages 443–551, 1995.