SOBRE EL TEOREMA DE FERMAT DE LA SUMA DE DOS CUADRADOS

Sonia Carolina Maldonado Dávila

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE CIENCIAS

ESCUELA DE MATEMÁTICAS

BUCARAMANGA

2006

SOBRE EL TEOREMA DE FERMAT DE LA SUMA DE DOS CUADRADOS

Sonia Carolina Maldonado Dávila

Monografía presentada como requisito para optar al
título de Licenciada en Matemáticas

Director

Edilberto José Reyes

Msc en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE CIENCIAS

ESCUELA DE MATEMÁTICAS

BUCARAMANGA

2006

A mi hijo Andrés

AGRADECIMIENTOS

Doy mi más profundo agradecimiento:

- A **Dios**,
- A **mis padres Rafael y Sonia**,
- A **mi esposo Alexander**,
- Al profesor **Edilberto Reyes**,
- A **los profesores**, por su contribución en mi formación académica.
- A **mis familiares y amigos**, que de una u otra forma estuvieron conmigo, brindándome su ayuda y cooperación en el transcurso de mi carrera .
- A la **UIS**, institución que me dio la oportunidad de formarme profesionalmente.

TÍTULO: SOBRE EL TEOREMA DE FERMAT DE LA SUMA DE DOS CUADRADOS[*]

AUTOR: MALDONADO DÁVILA Sonia Carolina[**]

PALABRAS CLAVES: suma de cuadrados, teorema de Fermat, números primos,prolongaciones, criterio de Euler.

DESCRIPCIÓN

En esta monografía encontraremos un análisis del artículo: Smith y el teorema de Fermat sobre la suma de dos cuadrados. En este artículo Smith realiza la demostración del teorema de Fermat: Todo numero que supere a un múltiplo de 4 en 1 se compone de dos cuadrados; el cual actualmente se enuncia, todo primo de la forma $4n + 1$ es suma de dos cuadrados.Tambien se realiza la demostración de la unicidad que Gauss enuncia en el teorema mencionado anteriormente, e igualmente realiza una demostración rigurosa del criterio de Euler; pues éste también se basa en los primos de la forma $4n + 1$.

Todas las pruebas que muestra Smith estan basadas en las prolongaciones; tema que èl define en éste artículo, mostrando todas sus propiedades y aplicando éstos conceptos en el desarrollo de algunos ejemplos, para que así el lector vea claramente en qué consiste su teoria y su fácil aplicación. En el desarrollo de la demostración Smith ve la necesidad de enunciar y probar varios lemas que apoyan sus teorias, justificando claramente todos los pasos realizados en el proceso de la misma. Además se presentan demostraciones de otros autores como son Stewart y Shanks con el fin de mostrar las diferencias y las semejanzas en el desarrollo de la prueba.

---

[*]Monografía

[**]Facultad de Ciencias. Escuela de matemáticas. Director: Edilberto José Reyes.

TITLE: ABOUT THE FERMAT SUM OF TWO SQUARES THEOREM[*]

AUTHOR: MALDONADO DÁVILA Sonia Carolina[**]

KEY WORDS: Sum of squares, Fermat theorem, prime numbers, continuant, Euler criterion.

DESCRIPTION

In this monographic, we will find an analysis about H.J.S.Smith and the Fermat sum of two squares theorem. In this article Henry John Stephen Smith gives a demonstration of the fermat theorem, all number that exceed in one a multiple of four, is formed by two squares; this theorem present that all prime which is represented by the form $4n + 1$ is the sum of two squares, also it gives the demonstration of the uniqueness that Gauss mentioned in the last theorem, in the same way makes an extensive demonstration related to Euler criterion, because it is also based on the primes, which has the form $4n + 1$.

All the proofs that were made by Smith are based on the continuant, which are defined in the article showing all its properties and applying these concepts to solve some examples, in this way the reader can understand his theory and see how easy are their applications. In the development of the demonstration Smith mentioned and proved some lemmas that support his theory, justifying each step during the process. Besides it present demonstrations of other authoress as soon as Stewart and Shanks, with in order to to point out the differences and the similarity in the elaboration of the proof.

---

[*]Monograph

[**]Faculty of sciences. Mathematics school. Director: Edilberto José Reyes.

CONTENIDO

Introducción

Se dice que un entero positivo es primo si tiene exactamente dos divisores positivos. Quien más investigó y publicó teoremas sobre estos números fue FERMAT, el gran matemático creador de la teoría de números.

Los descubrimientos de FERMAT relacionados con los números primos han contribuido al desarrollo de muchas áreas de las matemáticas, especialmente en la teoría de grupos y la teoría de ecuaciones algebraicas. Debido a la gran importancia de sus resultados, muchos matemáticos han sentido gran atracción por estudiarlos e incluso formular nuevas hipótesis tomando como base las ya existentes.

Uno de los últimos teoremas de FERMAT, considerado por muchos uno de los más bellos, dice que todo número que supera a un múltiplo de 4 en 1 se compone de 2 cuadrados. Actualmente se enuncia así: Todo número primo de la forma 4n+1 es suma de dos cuadrados. Desafortunadamente FERMAT no llegó a demostrarlo, despertando así el interés de muchos matemáticos por desarrollar una prueba. Gauss, por ejemplo, modifica el teorema de los dos cuadrados enunciando la unicidad de los dos enteros positivos que lo hacen verdadero, y Euler se basa en los primos de esta forma para enunciar su criterio, el cual permite encontrar soluciones de una ecuación cuadrática.

Una prueba muy elemental del teorema de FERMAT la dio HENRY JOHN STEPHEN

SMITH 1826-1883, quien utilizó conocimientos elementales de álgebra, propiedades de los determinantes y el teorema fundamental de la aritmética para crear una construcción que le pemite formular la demostración.

H.J.S SMITH fue un gran matemático, su formación académica era extensa. Estudió en las mejores universidades de la época, entre las que están la universidad de Oxford, y

publicó muchos trabajos, destacándose un reporte sobre la teoría de números, su contribución en el desarrollo de la integración de funciones discontinuas[***] y la introduccion del primer ejemplo de lo que hoy es llamado el conjunto de Cantor.

Gracias a todos estos conocimientos SMITH no solo demuestra el teorema de FERMAT: también demuestra la unicidad de Gauss y el criterio de Euler. Una presentación moderna de la demostración de SMITH la hace Francis W. CLARKE en su artículo *"H.J.S Smith and the Fermat two squares theorem"*, publicado en la número 106 del mes de septiembre de 1999 de la American Mathematica Monthly. El trabajo que hemos realizado consiste en analizar detalladamente ese artículo llenando algunos pasos que el autor ha omitido por considerarlos obvios.

[***]H.J.S.Smith, The collected mathematical papers of Henry John Stephen Smith: I y II. OXFORD, 1894

Capítulo 1

PRELIMINARES

1.1. El estudio de H. J. Smith

Para realizar la demostración al teorema de Fermat, Smith utilizó conocimientos básicos de álgebra elemental, incluyendo las simples propiedades de los determinantes y el teorema fundamental de la aritmética. Él combina estos resultados con las prolongaciones, teoría que desarrolló usando estudios basados en las fracciones continuas y utilizando los determinantes para definirlas. Con las prolongaciones logra una demostración sencilla y completa del teorema de Fermat.

Debido a que Gauss enuncia la unicidad del teorema de Fermat, Smith plantea una demostración de este resultado. Y como los primos en los que se basa este teorema son de la forma $4n+1$, Smith también realiza una demostración del criterio de Euler para la cual aplica las prolongaciones.

1.2. Conceptos elementales de álgebra y teoría de números

Definición 1.1. *Un entero positivo $p > 1$ se denomina primo si tiene exactamente dos divisores positivos: p y 1*

Definición 1.2. *Sean a y b enteros, sin que ambos sean ceros. El conjunto de todos los divisores comunes de a y b es un conjunto de números enteros cuyo máximo se denomina el Máximo Común Divisor de a y b, cuya notación es (a, b).*

Definición 1.3. *Si a y b son enteros, no ambos cero y tales que $(a, b) = 1$, decimos que a y b son primos relativos.*

Teorema 1.1. *Sean a y b enteros, con $b > 0$. Entonces existen enteros únicos q y r, tales que $a = bq + r$, con $0 \leq r < b$.*

Demostración.

Primero demostraremos la existencia: Sea $S = \{z \in \mathbb{Z} | z = a - bx, x \in \wedge z \geq 0\}$.
Veamos que $S \neq \varnothing$. Consideremos los dos casos posibles para a, es decir, $a \geq 0$ y $a < 0$. En el primer caso tenemos, tomando $x = 0$, $z = a - b$,$0 = a \geq 0$, así que $S \neq \varnothing$. En el segundo, y puesto que $b > 0$ es lo mismo que $b \geq 1$ ó $1 - b \leq 0$, tomando $X = a$ tendremos $z = a - b.a = a(1 - b) \geq 0$, y por consiguiente $S \neq \varnothing$.
Ahora bien, por el principio del buen orden S tiene un mínimo r, y en consecuencia

existe un entero q tal que $a - bq = r$ con $0 \leq r$.

De otra parte, puesto que $r = min(S)$ tenemos $r - b = (a - bq) - b = a - (q + 1)b < 0$, y por tanto $r < b$.

Ahora demostremos la unicidad. Supongamos que, $a = bq + r = bq' + r'$, con $0 \leq r < b$ y $0 \leq r' < b$. Si suponemos $q' < q$, entonces $q'+1 \leq q$, y por lo tanto $r = a-bq \leq a-b(q'+1) = (a-bq')-b = r'-b < 0$, que evidentemente es una contradicción. Similarmente, si suponemos $q < q'$, obtenemos otra contradicción, luego necesariamente $q = q'$, y tambien $r = r'$.

□

Definición 1.4. ALGORITMO DE EUCLIDES ***(ver, por ejemplo, [3])*** *Si a , b son enteros tales que, $0 < b < a$, aplicando el algoritmo de la división y escribiendo*

$$a = bq_1 + r_1, 0 \leq r_1 < b \text{ si } r_1 = 0,$$

tenemos a/b, y $(a, b) = b$; si no, se aplica nuevamente el algoritmo para obtener

$$b = r_1q_2 + r_2, 0 \leq r_2 < r_1 \text{ si } r_2 = 0;$$

entonces, $r_1 = (r_1, b) = (a, b)$; si no, se repite el proceso hasta llegar a lo sumo en b pasos a un residuo cero.

Ejemplo 1.1.

Encontrar $(687, -234)$. *Aplicando el algoritmo de Euclides tenemos*

$$687 = (234)(2) + 219,$$
$$234 = (219)(1) + 15,$$
$$219 = (15)(14) + 9,$$
$$15 = (9)(1) + 6,$$

$$9 = (6)(1) + 3,$$
$$6 = (3)(2) + 0;$$

por lo tanto, $(687, -234) = 3$.

Definición 1.5. *Sean a y b enteros cualquiera, y n un entero positivo; si $(a-b)/n$ decimos que a y b son congruentes módulo n, y escribimos*

$$a \equiv b \pmod{n}.$$

Teorema 1.2. Teorema fundamental de la aritmética *Todo entero $n > 1$ o es primo o se puede factorizar como producto de primos. Este producto es único, salvo por el orden de los factores.*

Demostración.

Sea S el conjunto de todos los números naturales que son primos, o, que pueden escribirse como producto de primos. Claramente, $S \subseteq \{k \in \mathbb{N} | k \geq 2\}$, y además tenemos :

1. $2 \in S$, porque 2 es un número primo.

2. Supongamos, que $n \geq 2$, y que $k \in S$ para todo k, tal que $2 \leq k < n$.
   Veamos que $n \in S$. Si n es primo, entonces $n \in S$. Si no es primo,
   existen, r y t, tales que $n = rt$ con $2 \leq r < n$, y $2 \leq t < n$; por hipótesis, ellos
   o son primos, o producto de primos. En consecuencia, n es producto de primos,
   y así $n \in S$.

Ahora probemos la unicidad de la factorización, salvo por el orden. Usaremos inducción sobre n:

Para $n = 2$, claramente la representación es única. Supongamos ahora que para todo entero k, con $2 \leq k < n$, la representación es única, y supongamos que, $n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$, donde, p_i y q_i son primos con

$$p_1 \leq p_2 \leq \dots \leq p_s \text{ y } q_1 \leq q_2 \leq \dots \leq q_t.$$

Así $(q_1 q_2 \dots q_t)/p_1$, y entonces $p_1 = q_j$ para algún j, por lo tanto, $q_1 \leq p_1$.
Analogamente, $(p_1 p_2 \dots p_s)/q_1$, y entonces $q_1 = p_i$ para algún i, y por lo tanto $p_1 \leq q_1$.
Lo anterior demuestra que $p_1 = q_1$. Cancelando tenemos

$$n/p_1 = p_2 p_3 \dots p_s = q_2 q_3 \dots q_t.$$

Como $n/p_1 < n$, la hipótesis de inducción garantiza que estas dos representaciones de n/p_1 son idénticas, y en consecuencia $s = t$, y para cada i, $p_i = q_i$.
Por el principio de inducción matemática la prueba queda completa.

□

Proposición 1.1. Segundo principio de inducción matemática. *Sea a un número natural, $S \subseteq \{k \in \mathbb{N} \ / \ k \geq a\}$ que satisface:*

1. $a \in S$
2. *Para cada $n > a, n \in S$ siempre que $k \in S$ para todo k en los naturales, tal que $a \leq k < n$.*

Entonces

$$S = \{k \in \mathbb{N} \mid k \geq a\}.$$

Demostración.

La demostracion es por contradicción. Supongamos que $S \neq \{k \in \mathbb{N} | k \geq 0\}$, y sea $T = \{k \in \mathbb{N} | k \geq a\} - S$. Luego $T \neq \varnothing$, y por el principio del buen orden, tiene un mínimo m. Además, puesto que $a \in S$, entonces $m > a$, y para todo k tal que $a \leq k < m$, la minimalidad de m nos garantiza que $k \in S$, y por la segunda condición concluimos que $m \in S$, lo cual es una contradicción.

□

1.2.1. La función determinante

La función determinante es una función con valores reales de una variable matricial, en el sentido de que asocia un número real $f(X)$ a una matriz X (ver, por ejemplo, [4]). Las matrices que se utilizan en este artículo son las de orden superior; para poder desarrollarlas se utilizan las permutaciones. Así, una matriz A de $n \times n$, tiene $n!$ productos elementales, estos productos son de la forma $a_{1j1}a_{2j2}\ldots a_{njn}$, donde $(j_1, j_2, \ldots, j_n)$, es una permutación del conjunto $\{1, 2, 3, \ldots, n\}$. Por un producto elemental con signo de A, se entenderá un producto elemental $a_{1j1}a_{2j2}\ldots a_{njn}$, multiplicado por $+1$ ó por -1. Si $(j_1, j_2, \ldots, j_n)$ es una permutación par, se usa el signo $+$, y si $(j_1, j_2, \ldots, j_n)$ es una permutación impar, se usa el signo $-$. Ahora ya es posible definir la función determinante. (Las demostraciones de lo que sigue se encuentran en un buen texto de álgebra lineal).

Definición 1.6. *Sea A una matriz cuadrada. La función determinante se denota por $det(A)$ y se define como la suma de los producos elementales de Acon signo. El número $det(A)$ se denomina determinante de A.*

Teorema 1.3. Operaciones elementales en los renglones sobre un determinante. *Sea A una matriz $n \times n$. Tenemos entonces:*

- *Si B es la matriz que se obtiene cuando un solo renglón o una sola columna de A se multiplica por un escalar k, entonces $det(B) = kdet(A)$.*
- *Si B es la matriz que se obtiene cuando se intercambian dos renglones o dos columnas de A, entonces $det(B) = -det(A)$.*
- *Si B es la matriz que se obtiene cuando un múltiplo de un renglón de A se suma a otro renglón, o cuando un múltiplo de una columna se suma a otra columna, entonces $det(B) = det(A)$.*

Otro resultado que se aplica a las operaciones en renglones es el desarrollo por cofactores.

Definición 1.7. *Si A es una matriz cuadrada, entonces el menor del elemento a_{ij} se denota por M_{ij}, y se define como el determinante de la submatriz que queda después de quitar el i-ésimo renglón y la j-ésima columna de A. El número $(-1)^{i+j}M_{ij}$ se denota por C_{ij}, y se denomina cofactor del elemento a_{ij}.*

Ejemplo 1.2.

Considérese la matriz general de 3×3, y desarrollese por cofactores

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}.$$

Entonces,

$$det(A) = a_{11}(a_{22}a_{33} - a_{23}a_{32}) + a_{21}(a_{13}a_{32} - a_{12}a_{33}) + a_{31}(a_{12}a_{23} - a_{13}a_{22}).$$

Debido a que las expresiones entre paréntesis son justamente los cofactores C_{11}, C_{22} *y* C_{33}, *se tiene que*

$$det(A) = a_{11}C_{11} + a_{21}C_{21} + a_{31}C_{31}$$

Teorema 1.4. *El determinante de una matriz* A $n \times n$ *se puede calcular multiplicando los elementos de cualquier renglón por sus cofactores y sumando los productos resultantes; es decir, para cada* 1, i, n *y* 1, j, n *se tiene que*

$$det(A) = a_{j1}C_{j1} + a_{i2}C_{i2} + \cdots + a_{nj}C_{nj}$$

es el desarrollo por cofactores a lo largo del i*-ésimo renglón.*

Ejemplo 1.3. *Evaluar el* $det(A)$ *mediante el desarrollo por cofactores a lo largo del primer renglón de la matriz*

$$A = \begin{vmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{vmatrix}.$$

$$det(A) = \begin{vmatrix} 3 & 1 & 0 \\ -2 & -4 & 3 \\ 5 & 4 & -2 \end{vmatrix} = 3\begin{vmatrix} -4 & 3 \\ 4 & -2 \end{vmatrix} - 1\begin{vmatrix} -2 & 3 \\ 5 & -2 \end{vmatrix} + 0\begin{vmatrix} -2 & -4 \\ 5 & 4 \end{vmatrix} =$$

$$= 3(-4) - 1(-11) + 0 = -1$$

1.2.2. Residuos cuadráticos

A continuación se mostrará la solución de los residuos generales de la congruencia cuadrática módulo m (ver, por ejemplo [5]), y finalmente la solución de las congruencias cuadráticas puras módulo primos. Se tomará una notación algo diferente, y se considerará como un problema típico el desarrollo de congruencia cuadrática pura, $x^2 \equiv a \pmod{p}$, con $(a, p) = 1$ y p primo impar.

El caso, $a \equiv 0 \pmod{p}$ es trivial, teniendo como única solución $x \equiv 0 \pmod{p}$, la cual no está incluida en la discusión. Comenzaremos con las siguientes definiciones útiles

Definición 1.8. *Si la congruencia* $x^2 \equiv a \pmod{m}$*, tiene una solución, entonces* a *se denomina un residuo cuadrático módulo* m*; si no es solución, entonces* a *se denomina un no-residuo cuadrático módulo* m*.*

Ejemplo 1.4.

1. 1 *es residuo cuadrático mod*(13)*; para* 1 *el residuo cuadrático mod*(13) *es el cuadrado* ± 1*.*

2. *4 es residuo cudrático mod*(13)*; para* 4 *el residuo cuadrático mod*(13) *es el cuadrado* ± 2.

Las demostraciones de los siguientes 3 teoremas se pueden encontrar en [3]; se omiten debido a que las preliminares utilizadas en las demostraciones no se requieren en nuestro trabajo.

Teorema 1.5. *Exactamente la mitad de los residuos diferentes de* 0 *módulo p son residuos cuadráticos módulo p.*

Teorema 1.6. *El entero,* $a \equiv 0 \pmod{p}$ *es o no es un residuo cuadrático módulo p; deacuerdo con esto se tiene:*

$$a^s \equiv 1 \pmod{p},\ o,\ a^s \equiv -1 \pmod{p},\ donde\ s = (p-1)/2.$$

Teorema 1.7. *El producto ab es o no es residuo cuadrático módulo p, si y solo si, exactamente 1, a ó b no son residuos cuadráticos módulo p.*

El símbolo de Legendre

Para mostrar que si un entero a es o no es un residuo cuadrático módulo p, se encuentra conveniente usar una función especial de teoría de números, conocida como el símbolo de Legendre.

Definición 1.9. *Sea* (a/p)*, con sus valores definidos como sigue:*

1. $(a/p) = +1$*, si a no es congruente con* $0 \pmod{p}$*, y si ,a es un residuo cuadrático módulo p.*

2. $(a/p) = -1$*, si* a *no es un residuo cuadrático módulo* p*.*

Por supuesto, es esencial, que al usar el símbolo de Legendre (definición anterior) se tenga cierta cautela, y no se debe interpretar el símbolo como una simple fracción en paréntesis; para nuestro conocimiento ya se tiene la definición, y ahora se enunciarán los teoremas que muestran la diferencia entre una simple fracción y el símbolo de Legendre.

Teorema 1.8. *Si* $a \equiv b \pmod{p}$*, entonces* $(a/p) = (b/p)$*.*

Demostración.

Como $a \equiv b \pmod{p}$, entonces por residuos cuadráticos sabemos que si $x^2 \equiv a \pmod{p}$ las dos congruencias tienen exactamente la misma solución, si la hay; así que $x^2 \equiv b \pmod{p}$, luego, $(a/p) = (b/p)$.

□

Teorema 1.9. $(a/p) \equiv a^2 \pmod{p}$.

Demostración.

Es una consecuencia directa de la definición del símbolo de Legendre,y del teorema 1,6

□

Teorema 1.10. $(ab/p) = (a/p)(b/p)$.

Demostración.

Este resultado se obtiene cambiando el teorema 1,7 en términos del símbolo de Legendre.

□

Teorema 1.11. $(c^2b/p) = (b/p)$.

Demostración.

Este es un caso especial del teorema 1,7; haciendo uso del hecho de que $a = c^2$ es obviamente un residuo cuadrático, de manera que, $(c^2/p) = 1$.

□

Capítulo 2

DEMOSTRACIÓN DE SMITH DEL TEOREMA DE FERMAT

En este capítulo se definen y se prueban todos los resultados obtenidos por Smith, así como las demostraciones de los dos teoremas que se enuncian a continuación. Para lograr un mejor entendimiento, y ver claramente la aplicación de los resultados que se presentan, desarrollaremos algunos ejemplos.

2.1. Dos teoremas fuertes

Teorema 2.1. Fermat y Gauss

Sea p un número primo tal que $p \equiv 1 \pmod 4$; entonces existen enteros positivos u, v únicos y primos entre sí, tales que

$$p = u^2 + v^2.$$

Teorema 2.2. (*Criterio de Euler) Sea p un número primo tal que $p \equiv 1 \pmod 4$;*

entonces:

1. *La ecuación cuadrática* $x^2 \equiv -1 \pmod{p}$ *tiene dos únicas soluciones,* x_0 *y* x_1 *en* $\mathbb{N}$*, tales que* $1 < x_0 < (p-1)/2$ *y* $(p-1)/2 < x_1 < p$*, con* $x_1 = p - x_0$*.*

2. *Todas las otras soluciones son congruentes a* x_0 *ó* $x_1(mod(p))$

2.2. Definición de prolongación y sus propiedades

Definición 2.1. *Sea* n *un número natural; si se toma* q_r *en los naturales, donde* $r = 1, 2, \ldots, n$*, entonces se define* $[.] : \mathbb{N}^n \to \mathbb{N}$ *por el determinante*

$$[q_1, q_2, \ldots, q_{n-1}, q_n] =: \begin{vmatrix} q_1 & 1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & 1 & \cdots & 0 & 0 \\ 0 & -1 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & -1 & q_n \end{vmatrix}.$$

Nótese que

$$[q_1] = q_1;$$
$$[q_1, q_2] = q_1 q_2 + 1;$$
$$[q_1, q_2, q_3] = q_1 q_2 q_3 + q_1 + q_3.$$

Lema 2.1. *Sea* n *un número natural tal que* $n \geq 2$*; entonces:*

I. $[q_1, q_2, \ldots, q_n] = [q_1][q_2, q_3, \ldots, q_n] + [q_3, \ldots, q_n]$.

II. $[q_1, q_2, \ldots, q_n] \in \mathbb{N}$.

III. $[q_1, q_2, \ldots, q_n] = [q_n, \ldots, q_2, q_1]$.

IV. $[q_2, q_3, \ldots, q_n] < [q_1, q_2, \ldots, q_n]$.

V. $[q_2, q_3, \ldots, q_n] y\ [q_1, q_2, \ldots, q_n]$ *son primos relativos.*

VI.

$$[q_1, \ldots, q_{s-1}, q_s, q_{s+1}, q_{s+2}, \ldots, q_n] = [q_1, \ldots, q_{s-1}, q_s][q_{s+1}, q_{s+2}, \ldots, q_n] + [q_1, q_2, \ldots, q_{s-1}][q_{s+2}, \ldots, q_n].$$

Demostración.

I. Por la definición tenemos que

$$[q_1, q_2, \ldots, q_n] = \begin{vmatrix} q_1 & 1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & 1 & \cdots & 0 & 0 \\ 0 & -1 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & 1 & q_n \end{vmatrix}.$$

Desarrollando el determinante por la fila 1 obtenemos el siguientes resultado:

$$[q_1, q_2, \ldots, q_n] = q_1 \begin{vmatrix} q_2 & 1 & \cdots & 0 & 0 \\ -1 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & q_{n-1} & 1 \\ & 0 & \cdots & 1 & q_n \end{vmatrix} - (1) \begin{vmatrix} -1 & 1 & \cdots & 0 & 0 \\ 0 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & q_{n-1} & 1 \\ 0 & 0 & \cdots & 1 & q_n \end{vmatrix};$$

luego se tiene que

$$[q_1, q_2, \ldots, q_n] = [q_1][q_2, q_3, \ldots, q_n] + [q_3, \ldots, q_n].$$

II. Aplicando el segundo principio de inducción matemática, para

$$n = 1, \quad \text{se tiene por definición que } [q_1] = q_1 \in \mathbb{N};$$

$$n = 2, \quad [q_1, q_2] = q_1 q_2 + 1 \in \mathbb{N} \text{ así hasta}$$

$$[q_1, q_2, \ldots, q_r], \text{ con } r = n - 1 \in \mathbb{N};$$

luego, por el segundo principio de inducción tenemos que $[q_1, q_2, \ldots, q_n] \in \mathbb{N}$.

III. Aplicando la definición tenemos que

$$[q_1, q_2, \ldots, q_{n-1}, q_n] =: \begin{vmatrix} q_1 & 1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & 1 & \cdots & 0 & 0 \\ 0 & -1 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & -1 & q_n \end{vmatrix}.$$

Por las propiedades de los determinantes podemos decir que el determinante anterior es igual a

$$\begin{vmatrix} q_1 & 1 & 0 & \cdots & 0 & 0 \\ -1 & q_2 & 1 & \cdots & 0 & 0 \\ 0 & -1 & q_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & q_{n-1} & 1 \\ 0 & 0 & 0 & \cdots & -1 & q_n \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 & \cdots & -1 & q_n \\ 0 & 0 & 0 & \cdots & q_{n-1} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & -1 & q_3 & \cdots & 0 & 0 \\ -1 & q_2 & 1 & \cdots & 0 & 0 \\ q_1 & 1 & 0 & \cdots & 0 & 0 \end{vmatrix} =$$

$$= [q_n, q_{n-1}, \ldots, q_2, q_1].$$

IV. Por la propiedad 1, tenemos que

$$[q_1, q_2, \ldots, q_n] = [q_1][q_2, q_3, \ldots, q_n] + [q_3, \ldots, q_n],$$

y como

$$[q_1] \in \mathbb{N},\ [q_2, q_3, \ldots, q_n] \in \mathbb{N} \text{ y } [q_3, \ldots, q_n] \in \mathbb{N},$$

podemos concluir que

$$[q_1, q_2, \ldots, q_n] > [q_2, q_3, \ldots, q_n].$$

v. Por la primera propiedad sabemos que

$$[q_1, q_2, \ldots, q_n] = [q_1][q_2, q_3, \ldots, q_n] + [q_3, \ldots, q_n];$$

ahora, supongamos que existe un número natural d tal que $[q_1, q_2, \ldots, q_n]/d$; pero por la igualdad anterior $([q_1][q_2, q_3, \ldots, q_n] + [q_3, \ldots, q_n])/d$, entonces

$$[q_1][q_2, q_3, \ldots, q_n]/d \text{ y } [q_3, \ldots, q_n]/d;$$

pero no se puede asegurar que d divida a $[q_1]$ y a $[q_2, q_3, \ldots, q_n]$ a la vez, luego si, d no divide a $[q_2, q_3, \ldots, q_n]$, concluimos que $[q_1, q_2, \ldots, q_n]$ y $[q_2, q_3, \ldots, q_n]$ son primos relativos.

VI. Por definición se tiene

$$[q_1,\ldots,q_{s-1},q_s,q_{s+1},q_{s+2},\ldots,q_n]=\begin{vmatrix} q_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0\\ -1 & q_2 & 1 & 0 & \cdots & 0 & 0 & 0\\ 0 & -1 & q_3 & 1 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & -1 & q_s & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & -1 & \cdots & \cdots & q_{n-1} & 1\\ 0 & 0 & 0 & 0 & \cdots & \cdots & -1 & q_n \end{vmatrix};$$

aplicando las propiedades de los determinantes a la fila s, se tiene

$$[q_1,\ldots,q_{s-1},q_s,q_{s+1},q_{s+2},\ldots,q_n]=[q_1,...,q_{s-1},q_s][q_{s+1},q_{s+2},...,q_n]$$
$$+[q_1,q_2,...,q_{s-1}][q_{s+2},...,q_n],$$

pues los demás términos se reducen a cero.

□

2.3. El algoritmo de Euclides

Algoritmo 1: Sean r y s números naturales primos entre sí, con $s < r$, y escribamos: $r/s = q_1 + t/s$, donde $(0 < t < s)$, $s/t = q_2 + u/t$, donde $(0 \leq u < t)$,..., $v/w = q_n + 0/w = q_n$ para algún n en $\mathbb{N}$, con $n \geq 2$, q_i en $\mathbb{N}$, donde $i = 1, 2, 3, \ldots, n$ y $q_n \geq 2$. Así, un número racional $r/s > 1$ está asociado a un conjunto de enteros positivos $\{q_1, q_2, ..., q_n\}$ que satisfacen el algoritmo. En pocas palabras tenemos:

Lema 2.2. *Sea $\{q_1, q_2, \ldots, q_n\}$ un conjunto de enteros positivos, con $n \geq 2$, y $q_n \geq 2$; entonces hay un único número racional $r/s > 1$ cuyo algoritmo euclídeo da el conjunto $\{q_1, q_2, \ldots, q_n\}$; además, r/s está determinado por*

$$r/s = [q_1, q_2, \ldots, q_n]/[q_2, q_3, \ldots, q_n];$$

aquí r y s son primos relativos, y están dados por

$$r = [q_1, q_2, \ldots, q_n] \text{ y } s = [q_2, q_3, \ldots, q_n].$$

Demostración.

Definamos

$$r/s = [q_1, q_2, \ldots, q_n]/[q_2, q_3, \ldots, q_n];$$

ahora, aplicando la propiedad 1 del lema 2.1 tenemos

$$[q_1, q_2, \ldots, q_n] = [q_1][q_2, q_3, \ldots, q_n] + [q_3, \ldots, q_n]$$

y

$$[q_2, q_3, \ldots, q_n] = [q_2][q_3, q_4, \ldots, q_n] + [q_4, \ldots, q_n];$$

aplicando el procedimiento n-veces se llega a que

$$r = [q_1, q_2, \ldots, q_n] \quad \text{y} \quad s = [q_2, q_3, \ldots, q_n],$$

y por la propiedad 5 del lema 2.1 sabemos que r y s son primos relativos.

□

2.4. Demostración de Smith del teorema de Fermat

Despues de definir y de mostrar todas las propiedades que sobre las prolongaciones enunció Smith, estamos preparados para estudiar y entender la demostración que él realizó del teorema "Suma de dos cuadrados"de Fermat, el cual se enuncia así:

Teorema de Fermat

Sea p un número primo tal que $p \equiv 1 \pmod 4$. Entonces existen enteros positivos u y v, primos entre sí y tales que

$$p = u^2 + v^2.$$

Demostración.

Sea p un número primo, con $p \equiv 1 \pmod 4$; entonces se tiene que $p = 4r + 1$. Tomando $\mu \in \{1, 2, 3, \ldots, 2r\}$, y considerando el conjunto de números racionales $\{p/\mu\}$ con $2 < p/\mu \leq p$, aplicando el Algoritmo 1 a p/μ se obtiene una representación de la forma

$$p/\mu = [q_1, q_2, \ldots, q_n]/[q_2, q_3, \ldots, q_n],$$

donde n y $\{q_1, q_2, \ldots, q_n\}$ dependen de la escogencia de μ, y donde

$$p = [q_1, q_2, \ldots, q_n] \text{ y } \mu = [q_2, q_3, \ldots, q_n];$$

de las propiedades anteriores tenemos que $q_1 \geq 2$ y $q_2 \geq 2$.
Ahora, tomemos uno de los racionales p/μ con $\mu \in \{1, 2, 3, \ldots, 2r\}$; entonces se obtiene la siguiente cadena de razonamientos, usando la propiedad 3 del Lema 2.1:

$$p/\mu = [q_1, q_2, \ldots, q_n]/[q_2, q_3, \ldots, q_n];$$

entonces

$$[q_1, q_2, \ldots, q_n] = p = [q_n, q_{n-1}, \ldots, q_1],$$

luego

$$[q_n, q_{n-1}, \ldots, q_1]/[q_{n-1}, q_{n-2}, \ldots, q_1] = p/\nu;$$

esto se obtiene del lema 2.2 con $1 < \nu < p/2$, y por la propiedad 1 del Lema 2.1, luego $\nu \in \{2, 3, \ldots, 2r\}$. Este razonamiento para los pares de elementos del conjunto $\{2, 3, \ldots, 2r\}$ da para cada miembro μ del conjunto un único compañero ν. Así, debe existir al menos un λ tal que el compañero se obtuvo aplicando el razonamiento anterior. Entonces

$$[q_1, q_2, \ldots, q_n]/[q_2, q_3, \ldots, q_n] = p/\lambda = [q_n, q_{n-1}, \ldots, q_1]/[q_{n-1}, q_{n-2}, \ldots, q_1],$$

y aplicando el Algoritmo 1 a ambos lados se obtiene $p = [q_1, q_2, \ldots, q_n]$, con la propiedad palindrómica. Si tenemos

$$q_i = q_{n+1-i} \text{ con } (i = 1, 2, 3, \ldots, n), \text{ y si } n = 2t + 1,$$

entonces $n \geq 3$ y $p = [q_1, q_2, \ldots, q_{s-1}, q_s, q_{s-1}, \ldots, q_1]$; aplicando la propiedad 6 del Lema 2.1,

$$[q_1, q_2, \ldots, q_{s-1}, q_s, q_{s-1}, \ldots, q_1] = [q_1, q_2, \ldots, q_{s-1}, q_s][q_{s-1}, \ldots, q_n] +$$
$$+ [q_1, q_2, \ldots, q_{s-1}][q_{s-2}, \ldots, q_1]$$

luego

$$p = [q_1, q_2, \ldots, q_{s-1}]([q_1, q_2, \ldots, q_{s-1}, q_s] + [qs - 1, \ldots, q_1]);$$

entonces p se representa como el producto de dos factores que son más grandes que 1, pero $p = 4r + 1$, luego llegamos a una contradicción. Por lo tanto, $n = 2t$, luego

$$p = [q_1, q_2, \ldots, q_s, q_s, \ldots, q_1] \text{ con } q_1 \geq 2.$$

Si aplicamos la propiedad 6 del Lema 2.1,

$$p = [q_1, q_2, \ldots, q_s][q_s, \ldots, q_1] + [q_1, q_2, \ldots, q_{s-1}][q_{s-1}, \ldots, q_1],$$

entonces

$$p = [q_1, q_2, \ldots, q_s]^2 + [q_1, q_2, \ldots, q_{s-1}]^2,$$

y por la propiedad 1 del Lema 2.1 tenemos que $[q_1, q_2, \ldots, q_s]$ y $[q_1, q_2, \ldots, q_{s-1}]$ son primos relativos.

□

Ejemplo 2.1.

1. $p = 13 \quad 13 = 4 * 3 + 1 \quad , r = 3, \quad luego \quad \mu \in \{2, 3, 4, 5, 6\}.$

   Para $\mu = 2,$ *se tiene*

   $$13/2 = 6 + 1/2,$$

   $$2 = 2 + 0,$$

   luego

   $$\mu = 2 \ , q_1 = 6 \ , q_2 = 2 \ , n = 2;$$

   Para $\mu = 3,$ *se tiene*

   $$13/3 = 4 + 1/3,$$

   $$3 = 3 + 0,$$

   luego

   $$\mu = 3 \ , q_1 = 4 \ , q_2 = 3 \ , n = 2;$$

   Para $\mu = 4,$ *se tiene*

   $$13 = 3 + 1/4,$$

$$4 = 4 + 0,$$

luego

$$\mu = 4 \ , q_1 = 3 \ , q_2 = 4 \ , n = 2;$$

Para $\mu = 5$, *se tiene*

$$13/5 = 2 + 3/5,$$

$$5/3 = 1 + 2/3,$$

$$3/2 = 1 + 1/2,$$

$$2 = 2 + 0,$$

luego

$$\mu = 5 \ , q_1 = 2 \ , q_2 = 1 \ , q_3 = 1 \ , q_4 = 2 \ , n = 4;$$

Finalmente para $\mu = 6$, *se tiene*

$$13/6 = 2 + 1/6,$$

$$6 = 6 + 0,$$

luego

$$\mu = 6 \ , q_1 = 2 \ , q_2 = 6 \ , n = 2;$$

así que $13 = [2, 1, 1, 2] = [2, 1][1, 2] + [2, 2],$

$$13 = [2, 1]^2 + [2]^2 = 3^2 + 2^2.$$

2. $p = 17 \quad 17 = 4 * 4 + 1 \ , \ r = 4,$ *luego* $\mu \in \{2, 3, 4, 5, 6, 7, 8\}.$

Para $\mu = 2$, *se tiene*

$$17/2 = 8 + 1/2,$$

$$2 = 2 + 0,$$

luego

$$\mu = 2\ , q_1 = 8\ , q_2 = 2\ , n = 2;$$

Para $\mu = 3$, *se tiene*

$$17/3 = 5 + 2/3,$$

$$3/2 = 1 + 1/2,$$

$$2 = 2 + 0,$$

luego

$$\mu = 3\ , q_1 = 5\ , q_2 = 1\ , q_3 = 2\ , n = 3;$$

Para $\mu = 4$, *se tiene*

$$17/4 = 4 + 1/4,$$

$$4 = 4 + 0,$$

luego

$$\mu = 4\ , q_1 = 4\ , q_2 = 4\ , n = 2;$$

Para $\mu = 5$, *se tiene*

$$17/5 = 3 + 2/5,$$

$$5/2 = 2 + 1/2,$$

$$2 = 2 + 0,$$

luego

$$\mu = 5\ , q_1 = 3\ , q_2 = 2\ , q_3 = 2\ , n = 3;$$

Para $\mu = 6$, *se tiene*

$$17/6 = 2 + 5/6,$$

$$6/5 = 1 + 1/5,$$

$$5 = 5 + 0,$$

luego

$$\mu = 6\ , q_1 = 2\ , q_2 = 1\ , q_3 = 5\ , n = 3;$$

Para $\mu = 7$, *se tiene*

$$17/7 = 2 + 3/7,$$
$$7/3 = 2 + 1/3,$$
$$3 = 3 + 0,$$

luego

$$\mu = 7 \ , q_1 = 2 \ , q_2 = 2 \ , q_3 = 3 \ , n = 3;$$

Finalmente para $\mu = 8$, *se tiene*

$$17/8 = 2 + 1/8,$$
$$8 = 8 + 0,$$

luego

$$\mu = 8 \ , q_1 = 2 \ , q_2 = 8 \ , n = 2;$$

así que $17 = [4, 4] = 4^2 + 1,$

$$17 = 4^2 + 1^2.$$

Corolario 2.1. *Sea* p *un número primo tal que* $p \equiv 1 \pmod 4$*; entonces hay exactamente* $2r$ *distintas prolongaciones y representaciones de* p*, donde*

$$p = [q_1, q_2, ..., q_n] \ \textit{con} \ q_n \geq 2.$$

Demostración.

Sea $\mu \in \{1, 2, ..., 2r\}$, entonces por el lema 2.2 se tiene

$$p/\mu = [q_1, q_2, ..., q_n]/[q_2, q_3, ..., q_n] \text{ con } p = [q_1, q_2, ..., q_n] \text{ y } q_n \geq 2.$$

Si las representaciones de p son distintas, entonces $p/\mu = p/\nu$ con $\mu \neq \nu$.
Como

$$p = [q_1, q_2, ..., q_n] \text{ con } q_n \geq 2 \text{ y si } n = 1,$$

entonces

$$q_n = q_1 = p, \text{ y si se toma } \mu = 1 \text{ con } n \geq 2,$$

así que

$q_n \geq 2$; luego, de las propiedades 1 y 3 del Lema 2.1 se obtiene la desigualdad

$$[q_2, q_3, ..., q_n] \leq ([q_1, q_2, ..., q_n] + 1)/2,$$

la cual debemos demostrar. Viéndola de otro modo,

$$2[q_2, q_3, ..., q_n] - 1 \leq [q_1, q_2, ..., q_n];$$

como

$$[q_1, q_2, ..., q_n] = [q_n, q_{n-1}, ..., q_1] = [q_n][q_{n-1}, q_{n-2}, ..., q_1] + [q_{n-2}, q_{n-3}, ..., q_1],$$

con

$$[q_n] \geq 2 \text{ y } [q_{n-2}, q_{n-3}, ..., q_1] > 1,$$

entonces

$2[q_2, q_3, ..., q_n] - 1 \leq [q_1, q_2, ..., q_n]$, luego se tiene que $[q_2, q_3, ..., q_n] \in \{2, ..., 2r\}$.

□

Para $p = 13$, se obtuvieron seis representaciones:

$$13 = [13] = [6, 2] = [4, 3] = [3, 4] = [2, 6];$$

luego

$$13 = [2, 1, 1, 2] = \begin{vmatrix} 2 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & -1 & 2 \end{vmatrix}.$$

2.5. Demostración de Smith del criterio de Euler

Antes de realizar la demostración del criterio de Euler, Smith enuncia y demuestra un lema que es clave en el desarrollo de la demostración. Debido a la complejidad de la misma, la demostración está dividida en dos partes.

El criterio de Euler

Sea p un número primo tal que $p \equiv 1 \pmod 4$; entonces:

1. La ecuación cuadrática $x^2 \equiv -1 \pmod{p}$ tiene dos únicas soluciones, x_0 y x_1, en los números naturales, tales que $1 < x_0 < (p-1)/2$ y $(p-1)/2 < x_1 < p$, con $x_1 = p - x_0$.

2. Todas las otras soluciones son congruentes a x_0 ó $x_1(mod(p))$.

Lema 2.3. *Sea n un número natural con $n \geq 2$, y $\{q_1, q_2, ..., q_n\}$ un conjunto de enteros positivos; si*

$$I_n(q_1, q_2, ..., q_n) =: [q_1, q_2, ..., q_n][q_2, q_3, ..., q_{n-1}] - [q_1, q_2, ..., q_{n-1}][q_2, q_3, ..., q_n],$$

entonces

$$I_n(q_1, q_2, ..., q_n) = (-1)^n.$$

Demostración.

Por una propiedad del Lema 2.1 tenemos que

$$I_2(q_1, q_2) = [q_1, q_2] - [q_1][q_2] = q_1q_2 + 1 - q_1q_2 = 1.$$

Para el caso general, de la propiedad 6 del Lema 2.1 se tiene

$$[q_1, q_2, ..., q_n] = [q_1, q_2, ..., q_{n-1}]q_n + [q_1, q_2, ..., q_{n-2}],$$

$$[q_2, q_3, ..., q_n] = [q_2, q_3, ..., q_{n-1}]q_n + [q_2, q_3, ..., q_{n-2}];$$

multiplicando la primera ecuación por $[q_2, q_3, ..., q_{n-1}]$ y la segunda por $[q_1, q_2, ..., q_{n-1}]$, y definiendo la multiplicación como en el lema anterior, tenemos

$$I_n(q_1, q_2, ..., q_n) = [q_1, q_2, ..., q_{n-2}][q_2, q_3, ..., q_{n-1}]$$
$$- [q_2, q_3, ..., q_{n-2}][q_1, q_2, ..., q_{n-1}] = -I_{n-1}(q_1, q_2, ..., q_{n-1})$$

repitiendo la aplicación de este último resultado,

$$I_n(q_1, q_2, ..., q_n) = (-1)^r I_{n-r}(q_1, q_2, ..., q_{n-r}),$$

con $r \in \{1, 2, ..., n-2\}$; si tomamos $r = n-2$, y usando el procedimiento anterior, tenemos

$$I_n(q_1, q_2, ..., q_n) = (-1)^{n-2} I_2 = (-1)^n,$$

entonces

$$I_n(q_1, q_2, ..., q_n) = (-1)^n.$$

□

Ahora sí estamos en condición de iniciar la demostración del criterio de Euler.

Demostración. Primera parte.

Tomando un número primo p con $p \equiv 1 \pmod 4$, de la demostración del teorema 2.1 podemos escribir p como sigue

$$p = [q_1, q_2, ..., q_s, q_s, ..., q_1] \text{ con } s \geq 1 \text{ y } q_1 \geq 2.$$

Ahora, definiendo $x_0 \in \mathbb{N}$ por

$$x_0 = [q_2, q_3, ..., q_s, q_s, ..., q_1],$$

aplicando la propiedad 1 del Lema 2.1 se tiene que para $q_1 \geq 2, 1 < x_0 < (p-1)/2$, y aplicando el resultado del Lema 2.3 con $n = 2s$ obtenemos

$$\begin{aligned}&[q_1, q_2, ..., q_s, q_s, ..., q_1][q_2, q_3, ..., q_s, q_s, ..., q_2]- \\ &- [q_1, q_2, ..., q_s, q_s, ..., q_2][q_2, q_3, ..., q_s, q_s, ..., q_1] = (-1)^{2s} = 1\end{aligned}$$

de la definición de p y x_0 y la propiedad 3 del lema 2.1 se tiene el resultado

$$p[q_2, q_3, ..., q_s, q_s, ..., q_2] - x_0^2 = 1,$$

entonces

$$x_0^2 \equiv -1 \pmod{p};$$

además se tiene que $1 < x_0 < (p-1)/2$, lo que completa la demostración de la primera parte.

□

Ejemplo 2.2.

Si $p = 13$, *entonces*

$$p = [q_1, q_2, ..., q_s, q_s, ..., q_1] = [2, 1, 1, 2],$$

$$x_0 = [q_2, q_3, ..., q_s, q_s, ..., q_1] = [1, 1, 2] = 1 * 1 * 2 + 1 + 2 = 5,$$

$$[q_2, q_3, ..., q_s, q_s, ..., q_2] = [1, 1] = 1 * 1 + 1 = 2;$$

entonces, de

$$1 < x_0 < (p - 1)/2$$

tenemos

$$1 < 5 < (13 - 1)/2 = 1 < 5 < 6,$$

luego

$$p[q_2, q_3, ..., q_s, q_s, ..., q_2] - x_0^2 = 13 * 2 - 5^2 = 1$$

y

$$x_0^2 = 25 = 26 - 1 \equiv -1 \pmod{p}.$$

Demostración. Segunda parte.

Supongamos que r es otra solución de la ecuación cuadrática:

$$x^2 \equiv -1 \pmod{p}, \text{ con } r \neq x_0 \text{ y } r \neq p - x_0;$$

sin perder generalización, podríamos suponer que r es el mínimo residuo positivo módulo p. Entonces $r^2 \equiv x_0^2 \equiv -1 \pmod{p}$, y p divide a $r^2 - x_0^2 = (r - x_0)(r + x_0)$; como p es primo, entonces p divide a $r - x_0$, ó, a $r + x_0$. El formar el caso implica que $r \equiv x_0 \pmod{p}$, pero como r y x_0 son los menores residuos positivos se sigue que $r = x_0$, o en el último caso,

$$r \equiv -x_0 \equiv p - x_0 \pmod{p},$$

y, como r y $p - x_0$ son los menores residuos positivos, se tiene que $r = p - x_0$.
Esta contradicción completa la prueba del teorema 2.2.

□

2.6. Demostación de Smith del teorema de Gauss

En esta sección se completa la demostración del teorema de Fermat y Gauss. Aquí, Smith realiza la demostración de la unicidad que plantea Gauss en el teorema mencionado anteriormente. El teorema de Fermat y Gauss nos dice:

Sea p un número primo tal que $p \equiv 1 \pmod{4}$; entonces existen enteros positivos u y v,

únicos y primos entre sí, tales que

$$p = u^2 + v^2.$$

Demostración.

Sea p un número primo con $p \equiv 1 \pmod 4$; suponiendo que existen 2 primos relativos con representación de dos cuadrados,

$$p = u^2 + v^2 \text{ y } p = s^2 + r^2 \text{ con } u < v \text{ , } s < r,$$

aplicando el Algoritmo 1 a los números racionales v/u y r/s, obtenemos

$$1 < v/u = [q_1, q_2, \ldots, q_n]/[q_2, q_3, \ldots, q_n]$$

y

$$1 < r/s = [t_1, t_2, \ldots, t_m]/[t_2, t_3, \ldots, t_m];$$

entonces

$$u = [q_2, q_3, \ldots, q_n],\ v = [q_1, q_2, \ldots, q_n],\ s = [t_2, t_3, \ldots, t_m],\ r = [t_1, t_2, \ldots, t_m],$$

y por lo tanto, por la propiedad 6 del Lema 2.1, tenemos

$$\begin{aligned} p = u^2 + v^2 &= [q_2, q_3, \ldots, q_n]^2 + [q_1, q_2, \ldots, q_n]^2 = \\ &= [q_n, \ldots, q_2, q_1, q_1, \ldots, q_n], \end{aligned}$$

$$p = s^2 + r^2 = [t_2, t_3, \ldots, t_m]^2 + [t_1, t_2, \ldots, t_m]^2$$
$$= [t_m, \ldots, t_2, t_1, t_1, \ldots, t_m]$$

la parte 1 del teorema 2.2 garantiza que las prolongaciones

$$[q_{n-1}, \ldots, q_1, q_1, \ldots, q_{n-1}, q_n]$$

y

$$[t_{m-1}, \ldots, t_1, t_1, \ldots, t_{m-1}, t_m]$$

son ambas soluciones de la ecuación cuadrática $x^2 \equiv -1 \pmod{p}$, y satisfacen que $1 < x < (p-1)/2$. De la unicidad de esta solución tenemos

$$[q_{n-1}, \ldots, q_1, q_1, \ldots, q_{n-1}, q_n] = [t_{m-1}, \ldots, t_1, t_1, \ldots, t_{m-1}, t_m] = \rho,$$

así que

$$1 < p/\rho = [q_n, \ldots, q_2, q_1, q_1, \ldots, q_n]/[q_{n-1}, \ldots, q_1, q_1, \ldots, q_{n-1}, q_n] =$$
$$= [t_m, \ldots, t_2, t_1, t_1, \ldots, t_m]/[t_{m-1}, \ldots, t_1, t_1, \ldots, t_{m-1}, t_m],$$

luego

$$1 < p/\rho = [t_m, \ldots, t_2, t_1, t_1, \ldots, t_m]/[t_{m-1}, \ldots, t_1, t_1, \ldots, t_{m-1}, t_m];$$

aplicando el Algoritmo 1 a ambas prolongaciones tenemos que $m = n$, y $q_i = t_i$, con $i = 1, 2, \ldots, n$; por lo tanto, $u = s$ y $v = t$, estableciéndose la unicidad del resultado.

□

Capítulo 3

OTRAS DEMOSTRACIONES DEL TEOREMA DE FERMAT

En este capítulo encontraremos algunas de las demostraciones más conocidas del teorema de Fermat; también se hará una pequeña comparación entre las propiedades que utilizó Smith, y las que utilizaron los demás autores.

3.1. Demostración de B. M. Stewart

Primero se mostrarán dos lemas:

Lema 3.1. *Sea p un número primo tal que $p \equiv 1 \pmod 4$; entonces existen enteros x, y y m que son solución de la ecuación $x^2 + y^2 = mp$, donde $0 < m < p$.*

Demostración.

Por propiedades de residuos cuadráticos se puede decir que

$$(-1/p) = +1, \text{ si } p = 4k + 1,$$

luego existe un entero y tal que

$$1 + y^2 \equiv 0 \pmod{p};$$

se puede encontrar un

$$a \equiv \pm y \pmod{p}, \text{ tal que } |a| < p/2,$$

entonces

$$0 < mp = 1 + a^2 < 1 + p^2/4 < p^2, \text{ luego } 0 < m < p,$$

estos enteros 1, a y m satisfacen el lema.

□

Lema 3.2. *Si p es primo de la forma $4k + 1$, y si $x^2 + y^2 = mp$ con $1 < m < p$, entonces existen enteros x_1, y_1 y M tales que*

$$x_1^2 + y_1^2 = Mp \text{ con } 1 \leq M < m.$$

Demostración.

Si m es par se debe tener que $x \equiv y \pmod{2}$, y se podría reescribir la ecuación de la hipótesis así:

$$((x+y)/2)^2 + ((x-y)/2)^2 = (m/2)p.$$

Como tenemos que

$$x_1 = (x+y)/2,\ y_1 = (x-y)/2 \text{ y } M = m/2,$$

se satisface el lema.

Si m es impar, se puede modificar el algoritmo de la división para escribir

$$x = am + a_1,\ |a_1| < m/2;\ y = bm + b_1,\ |b_1| < m/2.$$

Si estas expresiones son sustituidas en

$$(a^2+b^2)(a_1^2+b_1^2) = A^2 + B^2, \text{ con } A = aa_1 + bb_1,\ B = ab_1 - ba_1,$$

se encuentra que

$$a_1^2 + b_1^2 + 2Am + (a^2+b^2)m^2 = mp.$$

Luego hay un entero M no negativo, tal que $a_1^2 + b_1^2 = Mm$; se puede escribir

$$M + 2A + (a^2+b^2)m = p,\ M^2 + 2AM + (a^2+b^2)(a_1^2+b_1^2) = (M+A)^2 + B^2 = Mp.$$

Si $M = 0$ se tendría que $a_1 = b_1 = 0$, o sea que m^2 podría dividir a $x^2 + y^2 = mp$, y m podría dividir a p. Pero como p es primo y $1 < m < p$, se genera una contradicción. Entonces se tiene que $1 \leq M$, pero $Mm = a_1^2 + b_1^2 < m^2/2 < m^2$, y por lo tanto $M < m$.

Luego $x_1 = M + A$, $y_1 = B$ y M son enteros que satisfacen la condición del lema.

□

Demostración. Al teorema de fermat.

Por el Lema 3.1 podrímos encontrar enteros x y y tales que

$$x^2 + y^2 = mp, 1 \leq m < p;$$

en el caso $m > 1$, podríamos aplicar el Lema 3.2 un número finito de veces (digamos con $m > M = M_1 > M_2 > ... > M_k = 1$), descendiendo hasta obtener $x_k^2 + y_k^2 = p$.

□

3.2. Demostración de Daniel Shanks

Para realizar la demostración Shanks no necesitó enunciar lemas particulares, pues toda su demostración se basa en conceptos elementales de teoría de números.

Demostración.

Sea p un número primo tal que $p \equiv 1 \pmod 4$; existe $s < p$ tal que $(s^2 + 1)/p$.
Escribamos $s = a_0$ y $1 = b_0$, luego $pq_0 = a_0^2 + b_0^2$. Se deduce que $q_0 < p$, si $q_0 = 1$, entonces $p = a_0^2 + b_0^2$, si no, q_0 divide a a_0 y a b_0; escogiendo el residuo negativo o positivo que tenga menor magnitud, tenemos

$$a_0 = r_0 q_0 + \alpha_0, \;\; b_0 = s_0 q_0 + \beta_0,$$

donde α_0 y β_0 son residuos. Por lo tanto, satisfaciendo $|x| \leq 1/2q_0$, no son ambos residuos cero. Pero si $\alpha_0 = \beta_0 = 0$, se tiene $p/q_0, 1 < q_0 < p$, lo que es imposible. Ahora, si se define a q_1 por $q_0 q_1 = \alpha_0^2 + \beta_0^2$, y si $0 < q_1 \leq 1/2q_0$, por resultados anteriores se sabe que

$$pq_0^2 q_1 = (a_0^2 + b_0^2)(\alpha_0^2 + \beta_0^2) =$$
$$= (a_0\alpha_0 + b_0\beta_0)^2 + (a_0\beta_0 - b_0\alpha_0)^2;$$

sustituyendo a a_0 y b_0, y dividiendo por q_0^2, se llega a

$$pq_1 = (r_0\alpha_0 + s_0\beta_0 + q_1)^2 + (r_0\beta_0 - s_0\alpha_0)^2;$$

esto es, si

$$a_1 = |r_0\alpha_0 + s_0\beta_0 + q_1| \text{ y } b_1 = |r_0\beta_0 - s_0\alpha_0|,$$

se tiene

$$pq_1 = a_1^2 + b_1^2;$$

si $q_1 = 1$ se concluye la hipótesis; si no, se continúa el procedimiento, obteniendo

$$q_0 > q_1 > ... > q_n = 1,$$

y, finalmente se llega a

$$p = a_n^2 + b_n^2.$$

Ahora se prueba la unicidad. Sean a, b, c y d enteros positivos tales que $p = a^2+b^2 = c^2+d^2$; entonces

$$p = (ac + bd)^2 + (ad - bc)^2 \text{ y } p^2 = (ac - bd)^2 + (ad + bc)^2;$$

también se tiene que si

$$p = a^2 + b^2 = c^2 + d^2,$$

entonces

$$(p - a^2)d^2 = (p - c^2)b^2$$

ó

$$p(d^2 - b^2) = (ad - bc)(ad + bc).$$

Ahora, si $(ad - bc)/p$, se tiene que $ad - bc = 0$, y entonces $a^2 - b^2 = 0$ ò $b = d$; del mismo modo, si $(ad+bc)/p$, se tiene que $ac = bd$ y $(a, b) = 1$, entonces d/a y c/b. Luego se concluye que $d = a$, y como p es primo, solo se cumple uno de estos dos casos.

□

3.3. Conclusiones

3.3.1. Smith y Stewart

Como ya se ha mencionado anteriormente, Smith basa su demostración en el estudio que realizó sobre las prolongaciones apoyándose en algunos resultados básicos de álgebra y teoría de números, entre los que se destaca el algoritmo de Euclides y las congruencias módulo p. Mientras que la demostración realizada por Stewart solo se basa en resultados algebraicos y de teoría de números, como son la solución de ecuaciones cuadráticas y algunas propiedades de los números primos.

La similitud de las demostraciones radica esencialmente en los conocimientos básicos que se deben tener de las materias mencionadas anteriormente, y en el uso de las congruencias módulo p.

3.3.2. Smith y Shanks

Las herramientas utilizadas por Smith para la demostración del teorema ya fueron mencionadas en la comparación anterior. Shanks se basa principalmente en el algoritmo de la división y sus propiedades, así como en las propiedades de los números primos. Los dos resultados muestran una demostración clara y sencilla del teorema de Fermat; su gran similitud es que todo el desarrollo lo consiguen utilizando el algoritmo de la división.

Bibliografía

[1] **CLARKE F.W.** ”Smith and the Fermat two squares theorem.” *Amer.math.Montly*, **1999.**

[2] **BELL E.T.** *Men of mathematics.* **Victor Gollanez Ltd.,1937.**

[3] **DICKSON L.E.** *History of the theory of numbers* **Chelsea publishing Co.,1966**

[4] **HOWARD A.** *Introducción al Álgebra Lineal .* **Editorial Limusa S.A., 2000.**

[5] **STEWART B.M.** *Theory of numbers.* **The Macmillan Company, 1959.**

[6] **BROWDER F. ”Mathematical developments arising from Hilbert problems”, Procedings of symposia in pure mathematics.** *American Mathematical Society,1976.*

[7] **SHANKDS D.** *Theory of numbers.* **Chelsea Publishing Company, 1978.**