UNA VISIÓN HISTÓRICA DEL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

WILSON ALEJANDRO TRIANA CORDERO
2006240059

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ, D.C. 2012

UNA VISIÓN HISTÓRICA DEL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

TRABAJO DE GRADO ASOCIADO A UN GRUPO DE ESTUDIO

WILSON ALEJANDRO TRIANA CORDERO
2006240059

PROFESORA ASESORA:

LYDA CONSTANZA MORA MENDIETA
Profesora Departamento de Matemáticas U.P.N.

UNIVERSIDAD PEDAGÓGICA NACIONAL
FACULTAD DE CIENCIA Y TECNOLOGÍA
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ, D.C. 2012

AGRADECIMIENTOS

Este trabajo de grado, que implicó mucho esfuerzo, no lo hubiese podido terminar sin el apoyo, principalmente, de Dios; de mi profesora asesora, Lyda Constanza Mora, quien durante su elaboración siempre estuvo constante; a mi madre, Yanet Triana, fuente de inspiración y de ánimo permanente en los momentos difíciles para no dejarme caer; a mi tío Alejandro Triana, a mi familia, a mis profesores que me formaron durante todo este tiempo enseñándome, no solo en la parte profesional sino también en la aspecto personal, y a mis amigos; a todos ellos gracias porque sin su apoyo hubiese sido muy difícil culminar esta etapa de mi vida.

1. Información General	
Tipo de documento	Trabajo de Grado asociado a un grupo de estudio.
Acceso al documento	Universidad Pedagógica Nacional. Biblioteca Central
Titulo del documento	Una visión histórica de Teorema Fundamental de la Aritmética
Autor(es)	TRIANA CORDERO, Wilson Alejandro
Director	MORA MENDIETA, Lyda Constanza
Publicación	Bogotá, D.C., 2012, [62]
Unidad Patrocinante	Universidad Pedagógica Nacional
Palabras Claves	Teoría de Números, Factorización Prima, Gauss, Prestet, al-Farisi, Euclides, Teorema Fundamental de la Aritmética.

2. Descripción
En este trabajo se hace un breve recorrido histórico del Teorema Fundamental de la Aritmética, iniciando desde el año 300 A.C., hasta el año 1801., teniendo en cuenta diferentes personajes que aportaron al tema. Para la realización de este estudio se tuvieron en cuenta diferentes artículos de autores que ya se han interesado en el estudio histórico del TFA y la revisión de algunas fuentes originales.

3. Fuentes
Para la realización de este trabajo, se tiene como base principal el documento publicado por Agargün & Özkan (2001) en la revista Historia Mathematica titulado A Historical Survey of the Fundamental Theorem of Aritmetic. Teniendo en cuenta los diferentes personajes referenciados en la obra citada, se hizo la revisión de otros escritos, para el caso de Euclides, se tuvo en cuenta la obra de Tomas Heath (1908); para el caso de al-Farisi, un artículo de Agargün & Fletcher (1994); para Jean Prestet, se utilizó un artículo de Goldstein (1992) estos dos últimos publicado en la revista Historia Mathematica; para el estudio de los aportes de Leonerd Euler, se revisó el documento Elementos de Algebra, del mismo Euler (1770) cuya traducción

al inglés fue hecha por Jhon Hewlett (1840) y por último, para los aportes de Carl F. Gauss, se tuvo en cuenta la traducción al español de la obra Disquisitiones Arithmeticae hecha por Barrantes, H., Josephy, M. & Ruiz, A (2008).

4.Contenidos

Este trabajo se inicia con una somera biografía de los personajes que están relacionados con el desarrollo del Teorema Fundamental de la Aritmética, seguido de esto, lo que se puede considerar fueron los aportes de Euclides (300 A.C), al-Farisi, Jean Prestet (1689), Leonerd Euler (1770), Legendre (1798) y Carl Friederich Gauss (1801) al planteamiento y demostración del Teorema Fundamental de la Aritmética. Posterior a esto, se presentan las conclusiones que deja este estudio.

5.Metodología

Para la realización de este trabajo de grado, se inicia con la traducción, al español, del artículo “A Historical Survey of the Fundamental Theorem of Arithmetic” (Agargün, A. G y Özkan, E. 2001), luego se procede a estudiar detalladamente tal documento. En el artículo se presentan diferentes momentos históricos en los que el Teorema Fundamental de la Aritmética (TFA) se encuentra implícita o explícitamente; para el caso de Euclides, se consultó la obra de Heat (1908), una traducción al inglés de la obra Los Elementos, se estudiaron las proposiciones y las definiciones relacionadas en el texto principal; del texto principal se tuvo en cuenta la bibliografía empleada por Agargün y Özkan, así que se buscaron los documentos originales de Goldstein (1992), On a Seventeenth Century Versión of The Fundamental Theorem of Arithmetic, Agargün y Fletcher (1994), al-Farisi and the Fundamental Theorem of Arthmetic,luego se hizo la traducción de los documentos y se estudiaron.

6.Conclusiones

En el marco de este trabajo de grado, se encuentra que el teorema fundamental de la aritmética ha estado presente por más de 2000 años, antes de que Gauss en 1801 lo enunciara y demostrara, esto puede ser debido a la intencionalidad de las épocas, el hecho de demostrar no era algo que fuera considerado de vital importancia, lo importante era la utilización de

lo que se conocía para el descubrimiento de nuevas teorías.

Durante el proceso de formalización del Teorema Fundamental de la Aritmética, se ve que varios personajes están implicados con su uso y que no todos corresponden a la misma época, es decir que el TFA es de vital importancia para el desarrollo de los aportes de los diferentes autores mencionados en este trabajo.

El estudio de la historia de las matemáticas es un tema que permite el desarrollo de habilidades referentes a las competencias profesionales del profesor de matemáticas; la búsqueda de fuentes originales o que están más cerca de la verdad histórica del tema o del autor que se estudia, permite que el profesional tenga una perspectiva propia del tema o del autor.

La historia del Teorema Fundamental de la Aritmética, tiene su inicio en el año 300a.c, e involucra a diferentes matemáticos reconocidos, lo que resalta su importancia; en el caso de la teoría de números se evidencia este hecho.

La importancia de un tema o de un teorema, depende del interés del investigador; para algunos autores el Teorema Fundamental de la Aritmética, no era tan importante como para enunciarlo o demostrarlo, sin embargo sí era necesario tenerlo en cuenta y para el desarrollo de sus obras. Se puede pensar que ellos creían que no había necesidad de exponer algo que, se suponía, ya se conocía.

7.Elaborado por:	TRIANA CORDERO, Wilson Alejandro
8.Revisado por:	MORA MENDIETA, Lyda Constanza

Fecha de elaboración del Resumen:	11	11	2012

Tabla de Contenido

Tabla de Contenido vii
Introducción 8
1. PRELIMINARES 8
1.1. Objetivos 8
1.2. Objetivos específicos 8
1.3. Justificación 9
2. PRESENTACIÓN GENERAL DEL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA 11
3. EL APORTE DE EUCLIDES 16
3.1. La obra *Los Elementos* 16
3.2. Los Elementos y el TFA 16
4. EL APORTE DE AL-FARISI 23
5. EL APORTE DE JEAN PRESTET 34
6. EL APORTE DE EULER 38
7. EL APORTE DE LEGENDRE 42
8. EL APORTE DE GAUSS 44
9. CONCLUSIONES 48
Anexo No.1 50
Tabla de ilustraciones 62
Bibliografía 63

Introducción

El Teorema Fundamental de la Aritmética está ligado a las propiedades de la divisibilidad de los enteros, lo que promueve el desarrollo de diferentes temas relacionados, como el de Máximo Común Divisor o Mínimo Común Múltiplo, es decir que tiene un papel relevante en el desarrollo de las propiedades de los números naturales; la importancia del tema y el interés histórico de las matemáticas fueron los que motivaron el inicio de este trabajo.

Para la elaboración de este trabajo, se tomó como documento principal *"A Historical Survey of the Fundamental Theorem of Arithmetic",* publicado en la revista Historia Matematica en el año 2001 y cuyos autores son Agargün y Özkan, la traducción de este documento se presenta como anexo.

La idea principal de este documento es presentar la evolución histórica del Teorema Fundamental de la Aritmética y los principales autores que participaron en dicha evolución, entre los que se encuentran Euclides, al-Farisi, Jean Prestet, Euler, Legendre y Gauss; presentando inicialmente una breve biografía de cada uno, luego se expone el trabajo y los aportes de cada uno con respecto al tema.

En el último apartado de este trabajo se presentarán las conclusiones que deja la realización de este trabajo de grado, relacionado con el estudio histórico del Teorema Fundamental de la Aritmética.

1. PRELIMINARES

1.1. Objetivos

Este trabajo pretende presentar una visión sobre la evolución del Teorema Fundamental de la Aritmética, teniendo en cuenta los personajes involucrados, sus formulaciones, aportes y propuestas de demostración o demostraciones.

1.2. Objetivos específicos

- Identificar los aportes de Euclides, en su obra *Los Elementos*, que le permite a Gauss enunciar el Teorema Fundamental de

la Aritmética.

- Exponer el trabajo más destacado de diferentes autores entre el año 300 A.C. y 1800 acerca del Teorema Fundamental de la Aritmética.

1.3. Justificación

El estudio de la historia de las matemáticas juega un papel importante en la formación docente ya que ayuda tomar conciencia de lo que son realmente las matemáticas, de los cambios que se dan y de la forma de construcción de las mismas.

Esta información histórica de las matemáticas puede contribuir a los profesores (Guacaneme, 2007) a:
Comprender por qué un cierto concepto es difícil para algunos estudiantes y desarrollar alguna estrategia que permita superar la falla detectada.

- Promover un estilo consciente de enseñanza. En la búsqueda histórica de algún tema específico se encuentran diferentes métodos, ya que se encuentran diferentes autores, ciudades y/o comunidades, que están relacionadas con lo búsqueda, lo que debe permitir al docente una mejor aprensión y/o comprensión del tema estudiado.

En esta misma dirección, en los Lineamientos curriculares de Matemáticas(MEN, 1998) se hace hincapié en la importancia de hacer un estudio histórico de temas matemáticos:

> "*El conocimiento de la historia proporciona además una visión dinámica de las matemáticas y permite apreciar cómo sus desarrollos han estado relacionados con las circunstancias sociales y culturales e interconectados con los avances de otras disciplinas, lo que trae consigo importantes implicaciones didácticas: posibilidad de conjeturar acerca de desarrollos futuros, reflexión sobre imitaciones y alcances en el pasado, apreciación de las dificultades para la construcción de nuevos conocimientos*" (p. 14)

Basado entonces en la necesidad del conocimiento histórico-matemático en la formación docente, este trabajo se enmarca en este campo, con el cual se pretende hacer un recorrido histórico del *Teorema Fundamental de la Aritmética desde Euclides (300 A.C) hasta Gauss (1800)* y realizar una recopilación escrita sobre la información hallada alrededor del tema.

El TFA está relacionado con la factorización prima de un número, en este concepto se habla acerca de divisibilidad y es un tema que se

considera fundamental en la enseñanza del sistema de los números naturales(Rico, L. Marín, A. Lupiañez, J. Gomez, P, 2008); algunos contenidos del sistema de los números naturales se presentan en el nivel básico como destrezas para adquirir o afianzar (es el caso del uso del paréntesis y la jerarquía de operaciones o los algoritmos del producto y la división), esto resalta la importancia del estudio del TFAen la educación inicial ya que está relacionado con el algoritmo de la división, que se considera una base, para el estudio de los sistemas numéricos.

2. PRESENTACIÓN GENERAL DEL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

"La factorización prima de cualquier entero positivo $n > 1$ *es única, excepto por el orden en que aparecen los factores primos"*(Pettofrezzo & Byrkit, 1972)

Es el enunciado conocido como Teorema Fundamental de la Aritmética (TFA) y como se observa, está relacionado con el concepto de factorización única. La factorización única se refiere a dos propiedades particulares de un número: la existencia y la unicidad. La existencia hace referencia a la posibilidad de que un número compuesto mayor que 1 pueda ser representado como un producto finito de números primos y la unicidad significa que esta representación es única, sin importar el orden. Según Agargün y Özkan (2001), la factorización única apareció por primera vez como una propiedad de los números naturales.

Son varios los personajes en la historia de las matemáticas que han aportado a la formulación del TFA, en este trabajo se presentan las elaboraciones de algunos de los más destacados, según Agargün y Özkan (2001); éstos, en orden cronológico, son:

- **Euclides**[1] **(330 a.C. - 275 a.C.)**

Ilustración 1: Euclides
Tomada de: http://es.wikipedia.org/wiki/Euclides

Matemático griego. Poco se conoce a ciencia cierta de la biografía de Euclides, pese a ser el matemático más famoso de la antigüedad.

Es probable que Euclides se educara en Atenas, lo que explicaría su buen conocimiento de la geometría elaborada en la escuela de Platón. Enseñó en Alejandría, donde alcanzó un gran prestigio en el ejercicio de su magisterio.

Euclides fue autor de diversos tratados, pero su nombre se asocia principalmente a uno de ellos, *Los Elementos*, que rivaliza por su difusión con las obras más famosas de la literatura universal, como la Biblia o el *Quijote*. Se trata, en esencia, de una compilación de obras de

[1] Euclides recuperado de http://es.wikipedia.org/wiki/Euclides el 11 de Noviembre de 2012

autores anteriores (entre quienes se destaca Hipócrates de Quíos), que las superó de inmediato por su plan general y la magnitud de su propósito[2].

- **Kamal al-DinAbul Hasan MuhammadAl-Farisi (1260-1320)**

Fue un destacado matemático y físico persa. Sus contribuciones a la matemática son en óptica y teoría de números.

Ilustración 2: al-Farisi
Tomada de:
http://ustazbaba.blogspot.com/2009/11/kamal-al-din-al-farisi-ahli-fisika.html

Nació en Tabriz (Irán). Al-Farisi fue discípulo del gran astrónomo y matemático Qutb al-Din al-Shirazi. Su trabajo sobre la óptica fue incitado por una pregunta sobre la refracción de la luz.

Al-Farisi hizo un número de contribuciones importantes a la teoría de números. La teoría más impresionante de su trabajo es sobre números amigos[3]. En el libro *Tadhkira al-ahbab fi bayanal-tahabb* (Memorándum para la prueba de amigabilidad) introdujo un acercamiento importante a un área entera de la teoría de números, introduciendo ideas referentes la factorización y a métodos combinatorios.

- **Jean Prestet (1468 - 1690)**

Nació en Châlon-sur-Saone (Francia). Perteneció al círculo Nicolás Malebranche, primero como su siervo, después como su alumno, desde 1670 hasta la publicación de la primera edición de la *Elemens de Mathématiques* en 1675. Los *Elemens* se difundieron ampliamente. Desde 1675 a 1680, Prestet fue preparado para el sacerdocio en el Oratorio y enviado a diferentes pueblos para enseñar matemáticas. Murió unos meses después de la publicación de su *Nouveaux Elemens*(una segunda edición de *Elemens de Mathématiques*), el 8 de junio de 1690.

Al igual que la primera edición, la segunda se ocupa principalmente

[2]Tomada de http://www.biografiasyvidas.com/biografia/e/euclides.htm, recuperada el 11 de noviembre de 2012

[3] Dos números n y m se dice que son amigos, si n es la suma de los divisores propios de m y si, al mismo tiempo, m es la suma de los divisores propios de n. (Hogendijk, J.P., 1975, pág. 269).

de la aritmética y el álgebra, pero es mucho más larga incluyendo material nuevo, como las propiedades extendidas de combinaciones y divisores; también, en el segundo volumen, los problemas diofánticos son tratados por un uso sistemático del álgebra cartesiana.

La primera versión de la obra de Prestet había sido criticada por varios matemáticos, entre ellos Leibniz, y el desarrollo de la combinatoria en la segunda versión puede reflejar la respuesta de Prestet a la insistencia de Leibniz acerca de un nivel más profundo de la aritmética -lo simbólico-. La segunda versión de Prestet no contiene algún resultado nuevo sobre los temas que escribió, números amigos o perfectos. A veces se le acredita como el descubridor del octavo número perfecto[4], pero esto ya era conocido antes de él.

- **Leonhard Paul Euler (1707- 1783).**

Ilustración 3: Leonhard Paul Euler
Tomada de: http://fr.wikipedia.org/wiki/Fichier:Leonhard_Euler_2.jpg

Fue un matemático y físico suizo. Según varios historiadores, Euler es el principal matemático del siglo XVIII y uno de los más grandes y prolíficos de todos los tiempos.

Vivió en Rusia y Alemania la mayor parte de su vida y realizó importantes descubrimientos en áreas tan diversas como el cálculo o la teoría de grafos. También introdujo gran parte de la moderna terminología y notación matemática, particularmente para el área del análisis matemático, como por ejemplo la noción de función matemática. Asimismo se le conoce por sus trabajos en los campos de la mecánica, óptica y astronomía.

Euler ha sido uno de los matemáticos con más producción escrita; se calcula que sus obras completas reunidas podrían ocupar entre 60 y 80 volúmenes

En la teoría de números, Euler demostró:

[4] $2^{30}\ 2^{31}-1\ = 2.305.843.008.139.952.128$

- Que la suma de los recíprocos de todos los números primos diverge, lo que equivale a decir que $\lim_{x\to\infty}\left(\sum_{p\leq x}\frac{1}{p}\right)=\infty \quad p \in P$.
- Las identidades de Newton, las cuales están relacionadas con las dos diferentes maneras de escribir la raíz de un polinomio.
- El Pequeño teorema de Fermat, uno de los teoremas clásicos de teoría de números relacionado con la divisibilidad.
- El teorema de Fermat sobre la suma de dos cuadrados, el cual establece la relación que hay entre los números primos representables como suma de dos cuadrados.
- Definió la función ϕ de Euler.
- En el año 1772, que $2^{31}-1=2.147.483.647$ es un número primo de Mersenne[5].
- En el año de 1770 publicó su famosa *Introducción al Álgebra*, ésta fue la primera obra que escribió después de haber quedado totalmente ciego. En esta obra Euler, en la primera parte, encontramos un trabajo que relaciona los números reales y algunas operaciones (sumas, restas, proporciones, razones, entre otras); en la segunda parte, expone su trabajo relacionado con la solución de ecuaciones de primer grado, sistemas de ecuaciones con de primer grado, sistemas de ecuaciones lineales con más de una cantidad desconocida y soluciones de las ecuaciones de segundo grado.

Euler, también realizó trabajos pioneros en la distribución de los números primos y en la aplicación del análisis a la teoría de números. Su conjetura, en 1796, del teorema de los números primos fue probada cierta por Hadamard y de la Vallée-Poussin en 1898.

- **Adrien-Marie Legendre (1752 - 1833)**

Ilustración 4: Adrien-Marie Legendre
Tomada de: http://www.nndb.com/people/891/000093612/

Fue un matemático francés. Hizo importantes contribuciones a la estadística, la teoría de números, el álgebra abstracta y el análisis matemático.

En teoría de números, conjeturó y presentó una demostración incompleta de la ley de reciprocidad

[5] Un número primo de Mersenne es de la forma 2^p-1, donde p también es un número primo,

cuadrática probada posteriormente por Gauss,

En el artículo de León (2009) previo al enunciado de esta ley, el autor menciona la siguiente definición:

Si existe un x tal que $x^2 \equiv a\ (mod q)$, se dice que a es un residuo o resto cuadrático de q (o módulo q). Si no existe tal x, se dice que $a$no es un resto cuadrático de q.

Y la ley de reciprocidad cuadrática afirma que, dados p y q dos primos impares distintos:

Si p o q son de la forma $4k + 1$, entonces $p$es un resto cuadrático de $q$si y sólo si $q$es un resto cuadrático de p. Si ambos, p y $q$son de la forma $4k + 3$, entonces $p$es un resto cuadrático de $q$sí y sólo si $q$no es un resto cuadrático de p.

Y en términos de Legendre lo anterior se expresa de la siguiente manera:

$$\frac{p}{q} = -1^{\frac{p-1}{2}\frac{q-1}{2}} \frac{q}{p}$$

- **Johann Carl Friedrich Gauss (1777 - 1855)**

Ilustración 5: Johann Carl Friederich Gauss
Tomada de: http://www.nndb.com/people/891/000093612/

Matemático, astrónomo, geodésico y físico alemán que contribuyó significativamente en muchos campos, incluida la teoría de números, el análisis matemático, la geometría diferencial, la estadística, el álgebra, la geodesia, el magnetismo y la óptica. Considerado «el príncipe de las matemáticas» y «el matemático más grande desde la antigüedad», Gauss ha tenido una influencia notable en muchos campos de la matemática y de la ciencia. Fue de los primeros en extender el concepto de divisibilidad a otros conjuntos.

Gauss fue un niño prodigio, de quien existen muchas anécdotas acerca de su asombrosa precocidad. Hizo sus primeros grandes descubrimientos mientras era apenas un adolescente y completó su magnum opus, *Disquisitiones Arithmeticae* a los veintiún años (1798), aunque no sería publicado hasta 1801. Fue un trabajo

fundamental para que se consolidara la teoría de los números.

Estos son entonces los matemáticos más sobresalientes en la historia del TFA, en los capítulos siguientes se mostrarán en detalle cuáles fueron sus principales aportes en relación con tal teorema.

3. EL APORTE DE EUCLIDES

3.1. La obra *Los Elementos*

Los Elementos es la obra más representativa de Euclides, está dividida en trece libros. Cada libro inicia presentando las definiciones y continúa con la presentación y demostración de las proposiciones. Los contenidos que tratan cada libro[6]son:

- ***Libro I*** *Los fundamentos de la Geometría Teoría de los triángulos, paralelas y el área.*
- ***Libro II*** *Álgebra geométrica*
- ***Libro III*** *Teoría de la circunferencia*
- ***Libro IV*** *Figuras inscritas y circunscritas*
- ***Libro V*** *Teoría de las proporciones abstractas*
- ***Libro VI*** *Figuras geométricas semejantes y proporcionales*
- ***Libro VII*** *Fundamentos de la teoría de los números*
- ***Libro VIII*** *Continuación de proporciones a la teoría de números*
- ***Libro IX*** *Teoría de los números*
- ***Libro X*** *Clasificación de los inconmensurables*
- ***Libro XI*** *Geometría de los sólidos*
- ***Libro XII*** *Medición de figuras*
- ***Libro XIII*** *Sólidos regulares*

Esta obra es considerada por algunos, como la mejor obra de texto escrita, resaltando su antigüedad (300 A.C.), lo que más se destaca es el rigor lógico y aunque se pueden pensar en trabajos de matemáticos anteriores con un rigor del mismo estilo, la desventaja es que no se conoce ningún fragmento.(Duran, 2002)

3.2. Los Elementos y el TFA

Aunque en *Los Elementos* Euclides no hace una mención directa del TFA, los libros VII (Fundamentos de la teoría de los números) y IX (Teoría de los números) incluyen algunas proposiciones que se

[6]Joyce, D.E. (1997). Tomado de http://www.euclides.org/menu/elements_esp/indiceeuclides.htm, recuperado el 11 de noviembre de 2012.

hallan directamente relacionadas con el tema.

El libro VII, que consta de 22 definiciones y 39 proposiciones, contiene un par de proposiciones, la 30 y la 31, asociadas al TFA.

El libro IX, que consta de 36 proposiciones, contiene una proposición, la 14, asociadas al TFA.

En relación con las definiciones relacionadas con el TFA, vale la pena mencionar que Euclides incluye la de número primo y la de número compuesto; así:

D.12[7]**.**Un número primo es aquél que sólo es medido por la unidad.

D.14.Número compuesto es el medido por algún número[8].

Euclides con la palabra mide hace referencia a una relación que existe entre dos números, las definiciones que da, son estas:

- D.3: "Un número es parte de un número, el menor del mayor, cuando mide al mayor"
- D.4: "Pero partes cuando no lo mide"

Utilizando algunos términos actuales, de D.3 y D.4, podemos concluir que la palabra "mide" hace referencia a "divide" y la expresión "un número es parte de un número" se usaría cuando la división es exacta y la expresión "un número es partes de un número" cuando la división tiene un residuo. Estas observaciones, también, las hace Heath en su obra

Con base en esto, se presenta la proposición 30:

> **Proposición VII.30**[9]**:** *"Si dos números, al multiplicarse entre sí, hacen algún número y algún número primo mide a su producto, también medirá a uno de los números iniciales"*

La cual puede reescribirse de la siguiente manera:

[7] En adelante se notarán las definiciones con la letra D y el número de la definición propuesta por Euclides, así "D.1" indicaría la definición 1 del libro VII.
[8] Euclides en D.2, establece que "Un número es una pluralidad compuesta de unidades", lo que deja por fuera que la unidad sea un número.
[9] Esta notación se adoptará durante este escrito e indica el número del libro seguido del número de la proposición.

Proposición VII.30: *"Si el producto de dos números es medido por algún número primo, este número también medirá a alguno de los números iniciales"*

A continuación se presenta el siguiente gráfico, que relaciona las proposiciones que intervienen en la demostración que presenta Euclides en su obra. El origen de la flecha indica la proposición que se utilizan y el final de la flecha indica la proposición en la que se aplica para hacer la demostración; las flechas en las definiciones cumplen el mismo papel.

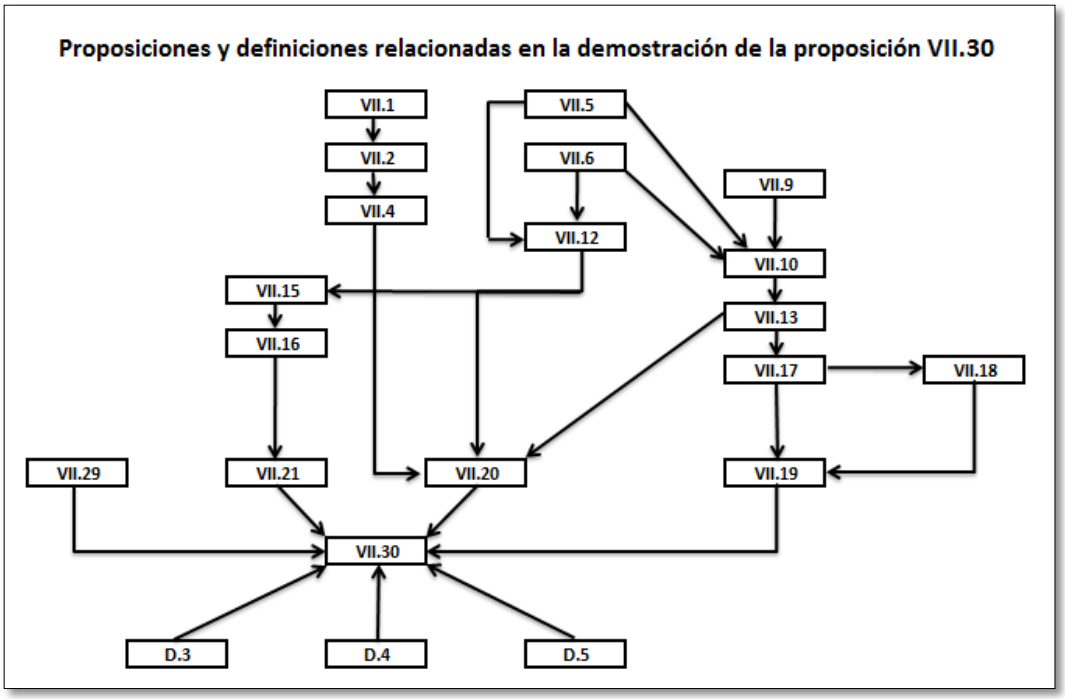

Ilustración 6: Proposiciones y definiciones relacionadas en la demostración de la proposición VII.30

Para darle significado a la Ilustración 6, se presenta la demostración del teorema. Se irán relacionando las proposiciones, como justificación a las afirmaciones que se van haciendo en el proceso.

La demostración presentada por Heath (1908), difiere con la que se presenta a continuación; se han modificado, en algunos casos, su escritura por un lenguaje moderno para facilitar su comprensión.

Demostración:

En el enunciado se plantea que se toman dos números

cualesquiera, sean estos números a y b[10].

Ahora, estos números se multiplican entre sí, lo cual se hace según D.15 ("Se dice que un número multiplica a un número cuando el multiplicado se añade a si mismo tantas veces como unidades hay en el otro y resulta un número…"), obteniendo entonces:

$$a \times b = c$$

Se tiene también otra hipótesis:*"…algún número primo mide a su producto…"*; esto es, existe algún número d que cumple dos condiciones, la primera es que es un número primo y la segunda es que mide al producto de los número dados, es decir que d, mide a c.

Lo que hay que demostrar es que $d$mide a ao a b, para lo cual se supone que d no mide a a.

De la anterior afirmación y basados en la proposición VII.29[11]

Y como $d$es primo y no mide a a, d es primo respecto[12]aa.

De otro lado, dado que d mide a c, entonces podemos decir que:

$$d \times e = c$$

Por lo anterior y como $a \times b = c$, entonces se tiene que:

$$a \times b = d \times e$$

Lo cual podemos reescribirla de la siguiente manera, esto teniendo en cuenta la proposición VII.19[13]:

$$\frac{d}{a} = \frac{b}{e}$$

Ya habíamos concluido, que d y a, son número primos entre sí además dado el paso anterior y laproposición VII.21[14], decimos, entonces, que d y a son los menores de los que guardan la misma razón.

De lo anterior y la proposición VII.20[15], tenemos que:

$$\frac{d}{b}$$

[10] Vale la pena aclarar que estos números son números naturales.

[11] Enuncia: Todo número primo, es primo respecto a todo número al que no mide.

[12] En la D.13, se tiene que Números primos entre sí son los medidos por la sola unidad como medida común

[13] Esta proposición die que: Si cuatro números son proporcionales, el producto del primero y el cuarto será igual al del segundo y el tercero; y si el producto del primero y el cuarto es igual al producto del segundo y el tercero, los cuatro números serán proporcionales.

[14] Que enuncia: Los números que son primos entre sí son los menores de aquellos que guardan la misma razón que ellos.

[15] Esta proposición die que: Los números menores de aquellos que guardan la misma razón que ellos, miden a los que guardan la misma razón el mismo número de veces, el mayor al mayor y el menor al menor.

Y esto quiere decir que si d no mide a a, entonces mide a b y similarmente si partimos de que d no mide a b, llegaremos a que d mide a a. Con lo cual queda demostrado que si d, primo, mide al producto de a y b, entonces mide a a o a b.

Otra de las proposiciones planteadas por Euclides, que se refiere al TFA, como ya se mencionó, es la proposición 31, que se enuncia como sigue:

> ***Proposición VII.31:*** *"Todo número compuesto es medido por algún número primo"*

Para esta demostración, presentada en la traducción hecha por Heath (1908) de los *Elementos,* Euclides solo utiliza la definición de número compuesto.

Demostración:

> Sea $a$un número compuesto, algún número lo medirá. Digamos que es b, si$b$ es primo, la demostración habrá terminado; pero si es compuesto, algún número medirá a b. Digamos que un número lo mide y digamos que éste es c; entonces, c mide a b yb medirá a a, entonces c también medirá a ay si $c$es primo, entonces habríamos terminado, pero si es compuesto, algún número medirá a c, este procedimiento lo repetiremos hasta que encontremos el número que estamos buscando, el número primo que mida al compuesto y el cual también medirá a a, pero, si no es encontrado -el número primo-, una sucesión infinita de números compuestos medirán al número a, cada uno de ellos es menor al anterior lo cual es un imposible en un número[16].
> Entonces algún número primo será encontrado el cual medirá a alguno de los anteriores números que se encuentran en la sucesión de números compuesto que dividen a a, el cual también medirá aa.En este sentido, cualquier número compuesto será medido por algún número primo.

Es evidente la conexión de las anteriores proposiciones con el TFA, si lo vemos de cerca, este enunciado solo menciona que un número

[16] En otras palabras, sí se tiene que a_1 y a_2 son factores de a y no son primos, entonces $a_1 < a$ y $a_2 < a$, ahora si a_3 y a_4 son factores de a_1 y a_2 respectivamente y si se continua hallando factores compuestos de a_3 y a_4, sucesivamente, tendremos que $a > a_1 > a_3 > \cdots > a_k$, pero a_k debe ser mayor que 1 porque a_k es compuesto y es imposible que haya infinitos números mayores que 1 y menores que a, en esto radica la imposibilidad de la sucesión infinita de números compuestos que midan a a.

compuesto puede ser medido por un número primo, pero en consecuencia se puede ver que si el procedimiento se hace hasta que no tengamos números compuestos restantes después de encontrar un número primo que divida al inicial, se habría establecido desde ya el TFA.

En el libro IX que habla sobre la Teoría de los números, también existe una proposición que está relacionada con el TFA, para la demostración de esta proposición Euclides tiene en cuenta la definición de números primo, número compuesto y la proposición VII.30 (que ya se ha demostrado), ésta es:

> ***Proposición IX.14:*** *"Si un número es el menor medido por números primos, no será medido por ningún otro número primo fuera de los que le medían desde un principio."*

Esta proposición se puede considerar como una demostración parcial de la condición de unicidad para el TFA.

Demostración:

> Sea a el número menor medido por los números primos b, c, d;decimos que a no puede ser medido por ningún otro número primo, excepto b, c, d.Pero, si fuera posible, es decir, que sea medido por el número primo $e$tal que e no es el mismo que cualquiera de los números b, c, d,si e mide a a,$f \times e = a$.Pero si dos números son multiplicados y hacen otro número, y cualquier número primo mide a su producto, éste también es medido por alguno de los números originales. Entonces b, c, d medirá a alguno de los números e, f.Pero ninguno de ellos mide a e ya que e es primo, entonces uno de los números b, c, f, medirá a f, el cual es menor que a, pero esto es imposible ya que por hipótesis a es el menor número medido por b, c, d; entonces ningún número primo medirá a a excepto b, c, d.

El TFA está parcialmente en la proposición IX.14 puesto que, como dice Agargün y Özkan (2001),en esta proposición Euclides sólo considera los números compuestos que se pueden escribir como producto de números primos diferentes, al incluir la expresión "*es el menor medido por números primos"*; así, por ejemplo, en términos modernos, $6\,(= 3 \times 2)$, al ser el menor número medido por los números primos 3 y 2, no será medido por ningún otro número primo

distintos a los ya mencionados; pero no se dice algo respecto a los números compuestos que poseen factores repetidos, como por ejemplo el 12 cuya descomposición es $2 \times 2 \times 3$, número que estaría fuera del teorema ya que no es el menor número medido por los números primos 2 y 3, que son sus factores.

Si analizamos detenidamente las proposiciones presentadas, se puede pensar que Euclides veía la necesidad de tener en cuenta, en el estudio de la teoría de números, la descomposición en factores de cualquier número para hallar sus divisores[17] y por la misma razón se debe pensar en la unicidad de la descomposición, ya que si la descomposición no fuera única, se deberían buscar todas las expresiones que representan un mismo número en forma de producto de factores para poder hallar todos los divisores del número.

Como se ve, Euclides, hace un gran aporte a lo que actualmente se conoce como el TFA ya que las tres proposiciones presentadas, en conjunto, están relacionadas con aquel, ya que las tres hacen referencia a la división de un número compuesto por un número primo.

[17] Esto teniendo en cuenta la proposición IX.36 que está relacionada con números perfectos, que son aquellos que cumplen, que la suma de sus divisores menos el divisor propio es igual al mismo.

4. EL APORTE DE AL-FARISI

El mayor aporte de al-Farisia la teoría de números está relacionado con los números amigos y cómo al trabajar con éstos son necesarios sus divisores, al-Farisi inicia un estudio para poder encontrar divisores de números dados utilizando la descomposición en factores de los números y es aquí donde se halla su relación con el TFA.

En su obra se encuentran seis definiciones y nueve proposiciones asociadas al TFA; enseguida se presentan tales definiciones y proposiciones con sus correspondientes demostraciones, en términos del mismo al-Farisi (Brentjes, 1990, citado por Agargün & Fletcher, 1994, pp. 164-170, traducción libre).

Definiciones:

1. Cada número[18] hecho por la multiplicación de un número con otro número, yo lo llamo un número doble. Y si éste es hecho multiplicando un número con otro número y con un tercero, yo lo llamo un triple. Y si éste es hecho al multiplicar un triple con un cuarto, yo lo llamo cuádruple, etcétera.
2. Y los factores de cada [número] compuesto[19] o son iguales o no. Yo llamo a los del primer tipo de factores iguales; el segundo tipo de factores diferentes, ya sea que la totalidad de sus factores sean diferentes, como en el [número] compuesto de $a, b, c,$ o algunos de sus factores son diferentes como en el número compuesto de a, b, b.
3. Y si el número de factores de dos números compuestos son los mismos, y llamo a estos dos [números compuestos] correspondientes en factores, o si no [yo los llamo] diferentes en ellos.
4. Dos números compuestos los cuales tienen la misma descomposición en factores son aquellos que tienen igual correspondencia en factores, donde cada factor repetido en uno de ellos es repetido el mismo número [de veces] en el otro.

[18] Se puede interpretar que al-Farisi hacía referencia a los que hoy llamamos números naturales.

[19] Tengamos en cuenta que al-Farisi, no ha dado una definición de *número compuesto.* Posiblemente se basa en lo propuesto por Euclides, pues al-Farisi se basa en aquel.

5. Las potencias (*the genera*) de un número es su cuadrado y su cubo y así indefinidamente.
6. La cadena de números es la serie de números que inicia con el mismo número, y el segundo su cuadrado, entonces su cubo, y así para el resto de las potencias (*genera*). El número y su potencia (*genera*) son los términos de esta cadena.

Al-Farisi no es riguroso en la escritura de sus proposiciones, muchas veces, como se verá, omite la expresión "primos" utilizando sólo la palabra "factores", no obstante, en las demostraciones sí tiene en cuenta que tales factores deben ser primos. Similarmente utiliza sin distinción, "mide a" y "divide a", posiblemente porque, así como nosotros entendemos actualmente la similitud entre estas expresiones (la primera utilizada por Euclides), al-Farisi también la reconocía.

Proposición 1. *"Cada número compuesto puede necesariamente ser descompuesto en un número finito de factores primos de los cuales éste es el producto"*

Demostración.

> Sea a un número compuesto; ya que éste es un número compuesto, es necesariamente medido por un primo (por VII.31 de los Elementos). Sea éste [primo]b que mide a a con c. Si c es primo entonces esto muestra que a es el resultado de multiplicar el número primo b y el número primo c. Si c es compuesto entonces éste es medido por un primo d *according*[20] al número e [esto es *c= de*]. Si e es primo es claro que a está hecho por la multiplicación de los números primos a, d y e. Por otro lado podemos escribir de forma tal que el factor compuesto esté finalmente descompuesto en dos factores primos. Entonces a está hecho de todos los primos anteriores. Si éstos nunca pueden ser descompuestos en dos factores primos, entonces esto podría, necesariamente, sugerir que un producto finito puede ser un de un producto infinito de números, lo cual es absurdo. Y esto es lo que buscamos.

Según Agargün & Fletcher (1994), esta demostración es la primera prueba de la existencia de la descomposición prima de un número

[20] Esta palabra indica que los números d y e miden a c; pero se decide escribir en inglés por cuanto o hallamos una traducción acorde en lengua castellana.

compuesto dado.

Proposición 2. *"Si hay tres números a, b, c, la razón[21] del primero y el tercero se compone de la razón del primero y el segundo y de la razón del segundo y el tercero"*

La demostración de esta proposición, también la presenta Agargün & Fletcher (1994).

Demostración.

> Digamos que el cuadrado de $b$es h, y el producto de b con a es d, y con c es z. Como d es compuesto –sus factores son a, b– y z es compuesto –sus factores son b, c– la razón de d a z es hecha por la razones de a a b y de b a c de acuerdo con VIII.5[22]. Pero como b fue multiplicado por sí mismo y por a para obtener h y d respectivamente, entonces la razón de a a b es igual a la razón de d a h de acuerdo con VII.18[23], en términos actuales$\frac{a}{b} = \frac{d}{h}$y similarmente, la razón de b a c es igual a la razón de h a z, es decir $\frac{b}{c} = \frac{h}{z}$. Entonces, de $\frac{a}{b} \times \frac{b}{c} = \frac{d}{h} \times \frac{h}{z}$, haciendo las operaciones, simplificar obtenemos la igualdad, la razón de a a c es igual a la razón de d a z, el cual es hecho por las otras dos razones. Y esto era lo que buscábamos.

En suma lo que plantea al-Farisi, en lenguaje moderno, es que $\frac{a}{c} = \frac{a}{b} \times \frac{b}{c}$. Relación que no se encuentra en Euclides (Agargün & Fletcher, 1994, p165).

Proposición 3. *"La razón de la unidad a cualquier número compuesto está hecho por la razón de cada uno de sus factores primos"*

Demostración.

[21] Al-Farisi no ha dado una definición acerca de lo que es una razón.
[22] Esta proposición enuncia que: Los números planos (D.17. Cuando dos números, al multiplicarse entre sí, hacen algún número, el resultado se llama número plano y sus lados son los números que se han multiplicado) guardan entre sí la razón compuesta de las razones de sus lados.
[23]Esta proposición enuncia que: Si dos números, al multiplicar a un número cualquiera, hacen ciertos números, los resultantes guardarán la misma razón que los multiplicados.

Digamos que el número compuesto es a y dejemos que sus factores primos sean los que siguen. Digamos que son dos factores primos b, c; luego decimos que como b fue multiplicado por c para obtener a la razón de b a a es igual a la razón de la unidad a c. Y la razón de la unidad a a es hecha por la razón de la unidad a b y de b a a. Así la razón de la unidad a a está hecha por sus razones de b y c.

Digamos que sus factores [primos] son más de dos, llamémoslos $b, c, d,$ y que el número formado por by $c$es h. La razón de la unidad a h estáhecha por su razón a sus dos factores, refiriéndonos a b y c. Y como a está hecho por h y d, la razón de la unidad a a está hecho por su razón a h y d. Entonces la razón de la unidad a a está hecho por sus razones a b y c y d. Y manera similar podemos probar si los factores son más de tres. Y esto era lo que queríamos demostrar.

Agargün y Fletcher (1994), muestran la demostración anterior de la siguiente manera, usando la proposición 2, que ya se ha presentado:

Si b y c son primos tales que$a = bc$ entonces por la proposición VII.18[24]$\frac{b}{a} = \frac{b}{bc} = \frac{1}{c}$. Con esto ya tenemos tres números – $1, b, a$ – y con la proposición 2 se tiene que

$$\frac{1}{a} = \frac{1}{b} \quad \frac{b}{a}$$

Y si se reemplaza, se tiene lo que se quería demostrar

$$\frac{1}{a} = \frac{1}{b} \quad \frac{1}{c}$$

Proposición 4. *"Cualesquiera dos números compuestos los cuales tienen la misma descomposición en factores son correspondientes*[25]*"*

Demostración.

Sean a y b, cada uno de los cuales está compuesto por los factores c, d, e[26].La causa es que la razón de la unidad a cada

[24] Enuncia que: Si dos números, al multiplicar a un número cualquiera, hacen ciertos (números), los resultantes guardarán la misma razón que los multiplicados.
[25] Esta palabra hace referencia a igualdad.
[26] Para que lo que sigue sea posible c, d y e deben ser primos, pero al-Farisi no lo

uno de ellos está hecho por las razones de cada uno de$c, d, e,$ entonces la razón de la unidad a los dos de ellos son iguales. Por lo tanto ellos son correspondientes. Esto es lo que buscábamos.

En otras palabras:

Como $a = cde$ y $b = cde$de la proposición 3, se tiene que $\frac{1}{a} = \frac{1}{c} \frac{1}{d} \frac{1}{e}$ y $\frac{1}{b} = \frac{1}{c} \frac{1}{d} \frac{1}{e}$, de ahí que $\frac{1}{a} = \frac{1}{b}$ y el paso final, llegar a que $a = b$.

Pero esta última parte es omitida por al-Farisi, según Agargün & Fletcher (1994, p. 167, traducción libre) "*esto supone que podía ser un paso obvio y que no había necesidad de hacer énfasis en él*".

Una parte importante es que al-Farisi usa la proposición 3 para demostrar la proposición 4, nótese, como se indicó antes, que al-Farisi no tiene cuidado de enunciar que los factores c, d, e son primos, algo que sí es importante en el enunciado de la proposición 3.

Proposición 5. *"Cualesquiera dos números compuestos diferentes no tienen la misma descomposición en factores"*

Demostración.

Pero es necesario que los factores primos de uno de ellos sea diferente de los factores primos del otro, o bien algunos de esos factores son diferentes si ellos son diferentes en factores, o ellos son diferentes en el número de repeticiones de alguno de éstos si ellos tienen factores iguales; si no, entonces ellos tienen la misma descomposición en factores y por lo tanto son correspondientes [esto es, idénticos], pero fueron supuestos distintos. Esto es una contradicción. Así que se obtiene lo que deseamos demostrar.

Proposición 6. *"Para cada número compuesto el cual es descompuesto en sus factores primos, los números compuestos de esos factores, dobles o triples y así, hasta el producto de acuerdo con el número de factores menos uno, todos esos son parte*[27] *de*

---

enuncia.

[27] Seguramente al-Farisi utiliza esta expresión teniendo en cuenta las definiciones planteadas por Euclides, en donde dice que un número es parte de un número, el

éste"

Demostración.

> Digamos que el número compuesto es a y su descomposición en factores primos son los números b, c, d, e. Entonces decimos que el número hecho por b y c mide a a, porque si estos son multiplicados con el número hecho por d y e, entonces el resultado es a. Y similarmente para el resto de [los números]dobles y triples. Pero tampoco el producto mencionado ($b \times c \times d \times e$) correspondiente al número de los factores es un divisor de éste [i.e., el número dado] porque el producto de todos los factores no es menor que el número inicial y el producto de todos los factores por otro factor tampoco es divisor del número inicial, ya que esto no es posible debido a la ausencia de un factor adicional. Y así lo que nosotros preguntábamos ha sido establecido. Esto es lo que buscábamos.

Al-Farisi deja claro en esta proposición que el producto de la descomposición en factores de un número no es divisor del número dado, lo que afirma que su intención era encontrar los divisores propios de un número dado, lo que si estaba encaminado a su trabajo posterior (el estudio de los números perfectos).

Proposición 7. *"Si un número no es medido por otro número, entonces tampoco su cuadrado ni cualquiera de sus potencias medirá el producto de éste. Y tampoco su cubo ni cualquiera de sus potencias medirá el producto de su cuadrado"*

Demostración.

> Digamos que a no mide a b. Sea c el cuadrado de a, e es su cubo, h es su cuarta potencia, d el producto de b y a, z el producto de b y c, y t el producto de b y e. Digo que ni c ni las potencias de a miden a d, tampoco e ni las potencias de a miden a z, y tampoco h ni las potencias de a miden a t. La razón es que si a es multiplicado por sí mismo y por b para obtener c y d respectivamente, la razón de c a $d$es igual a la razón de a a b, de acuerdo con VII.18, pero a no mide a b, asíc no mide a d. Similar para e y h y las otras potencias de a, porque si uno de estos mide a d, y c mide su potencia,

menor del mayor, cuando mide al mayor.

entonces c mide a d, y esto es una contradicción. Similarmente, c fue multiplicado por a y b para obtener e y z respectivamente, entonces las razón entre e y z es igual a la razón de a a b. Así e no puede medir a z, similarmente para h y las potencias de a. De la misma manera mostramos que h y las potencias de a no pueden medir a t. Y era lo que se buscaba.

En lenguaje moderno, la proposición anterior, enuncia que si $a \nmid b$ entonces

$$a^2 \nmid ab, \qquad a^3 \nmid ab, \ldots$$

$$a^3 \nmid a^2 b, \qquad a^4 \nmid a^2 b, \ldots$$

$$a^4 \nmid a^3 b, \qquad a^5 \nmid a^3 b, \ldots$$

Al-Farisi establece $c = a^2$, $d = ab$; así $\frac{c}{d} = \frac{a^2}{ab} = \frac{a}{b}$ esto por la proposición VII.18, y $c \nmid d$. Luego $\frac{e}{z} = \frac{a^3}{a^2 b} = \frac{c}{d}$. Por lo tanto sí $e|d$ entonces $e|ad$ o $e|z$. Pero se tendría que$c|d$ lo que es una contradicción.

Proposición 8. *"Si un número compuesto es descompuesto en sus factores primos y un número de ellos no se repite, entonces este número compuesto no será medido por el cuadrado de este número primo ni por una de sus potencias. Y si este factor primo se repite una sola vez entonces entre sus potencias su cuadrado solamente lo medirá, pero no las potencias restantes. Y similarmente si este se repite solo dos veces entonces su cuadrado y cubo solamente lo medirán pero no las potencias restantes y así."*

Demostración.

Digamos que el número compuesto es a. Éste es descompuesto en sus factores primos b, c y d, entonces decimos que b, por ejemplo, ya que no se repite, su cuadrado b^2, no medirá a a. Esto porque b es primo relativo a c y d, así que también es primo relativo del producto de c y d, por VII.24[28]. El número b ha sido multiplicado por sí mismo y por el producto de c y d, para obtener b^2 y a respectivamente,

[28]Esta proposición enuncia que: Si dos números son primos respecto a otro número, también el producto será número primo respecto al mismo número

entonces el cuadrado no medirá a a por VII.25[29], entonces es claro que sus potencias [las de b] no medirán a a.

Digamos que b se repite entre los factores primos de a, y los factores son b, b, c, d. Es evidente que su cuadrado el cual es uno de sus productos dobles lo medirá. Pero decimos que su cubo no lo medirá, como b no mide al producto de c y d como se probó anteriormente, y el cuadrado de b es multiplicado por sí mismo y por$c$ y d el resultado es b^3 y a respectivamente, los cuales tienen la misma razón. Así que el cubo no medirá a a y claramente las demás potencias tampoco pueden medirlo.

Si b se repite dos veces, como por ejemplo,b, b, b, c, d, entonces el cuadrado de b y el cubo de b mide a a, pero no las demás potencias, porque b no mide el producto de c y d, y su cubo es multiplicado por sí mismo y por ellos, para obtener su cuarta potencia y a respectivamente, los cuales tienen la misma razón, así su cuarta potencia no mide a a. Similarmente para el resto de sus potencias, y es lo que se buscaba.

Agargün & Fletcher (1994) enuncian la anterior proposición de la siguiente manera, utilizando un lenguaje moderno:

Sí $a = bcd$, una descomposición prima, entonces $b^2 \nmid a,\ b^3 \nmid a, \ldots$

Sí $a = b^2cd$, una descomposición prima, entonces $b^3 \nmid a,\ b^4 \nmid a, \ldots$

Sí $a = b^3cd$, una descomposición prima, entonces $b^4 \nmid a,\ b^5 \nmid a, \ldots$

Y así.

Proposición 9. *"Cada* [*número*]*compuesto, descompuesto en sus factores primos no tiene otras partes* [*divisores*] *excepto la unidad y sus factores primos y también los* [*números*] *dobles hechos de* [*dos*] *sus factores y si hay más de dos, y también los* [*números*] *triples si hay más de tres y así hasta terminar el producto de números de acuerdo al número de factores menos uno"*

Demostración.

Digamos que a es un número compuesto y su descomposición en factores primo es b, c, d, e. Decimos que no tiene divisores excepto la unidad y b, c, d, e, y los números

[29] Establece que: Si dos números son números primos entre sí, el producto de uno de ellos multiplicado por sí mismo será número primo respecto del que queda.

dobles hechos de b y c, b y d, b y e, c y d, c y e, d y e, y sus números triples hechos de b y c y d, b y c y e, b y d y e, c y d y e y sus productos de acuerdo al número de factores menos uno.

La razón es que si fuera posible que tenga una parte (un divisor) que no sea alguna de las que ya se han mencionado entonces, sea ésta z, que es primo o compuesto. Si éste es primo y mide a a [el cual es] hecho por b,c,d veces e, por VII.30, éste necesariamente mide a uno de sus dos factores (bcd o e), y [este] no puede medir al primo e, luego éste tiene que medir el número hecho de b,c,d. Pero como éste mide este producto el cual está hecho del producto de b y $c$veces el primo d, como en el argumento anterior, éste debe medir el [número] hecho de b,c y ya que éste mide al producto entonces medirá a alguno de estos dos factores primos, o es uno de ellos, en ambos casos es imposible.

Si z es un [número] compuesto, y éste es distinto de los productos anteriormente mencionados, entonces necesariamente sus factores primos no pueden ser idénticos con los factores de dichos productos. Por lo tanto o bien existe, entre los factores primos de z, uno de los cuales no aparece entre los factores de a, o no. Si no existe, o hay entre ellos un factor de z [el cual] que se repite un número [de veces], pero no se repite [tantas veces] entre los factores de a, o uno de los factores de a [el cual] se repite un número [de veces] pero no es repetido [tantas veces] entre los factores de z. Y esos con los tres casos.

Para el primer caso, sea éste [factor] primo distinto de todos los factores de a,h, entonces h es primo y se cumple la contradicción mencionada cuando se supuso z primo.

Para el segundo caso, uno de los factores de z, sea éste b, es repetido [digamos] una vez [en z], y b no se repite en los factores de a. Así el [número] hecho de b y él mismo mide a z, y[así] éste mide a a y [a pesar de que] éste no está repetido en los factores de a, lo cual es imposible. Y similarmente podemos probar una contradicción si éste [i.e., b] es repetido dos o más veces. Y sea *b* repetido dos veces en los factores de z y una vez en los factores de *a*, así [el cubo de b] necesariamente mide a z y mide a a, pero éste no se repite

> más de una vez en sus [i.e., en los de *a*] factores, y esto es una contradicción. Y similarmente la contradicción ocurre cuando el número de veces que se repite *b* en los factores de *z* es más que el número de veces que se repite *b* en los factores de *a*. Si es el tercer caso, me refiero a que alguno de los factores de *a* es repetido el número de veces en éste pero no se repite tantas veces en los factores de z, luego es claro que en este caso, z llega a ser uno de las partes del producto [ya mencionado]. Por lo tanto, el teorema es establecido. Esto es lo que buscábamos.

Las anteriores proposiciones se pueden relacionar de la siguiente manera, como se muestra en esta figura[30]:

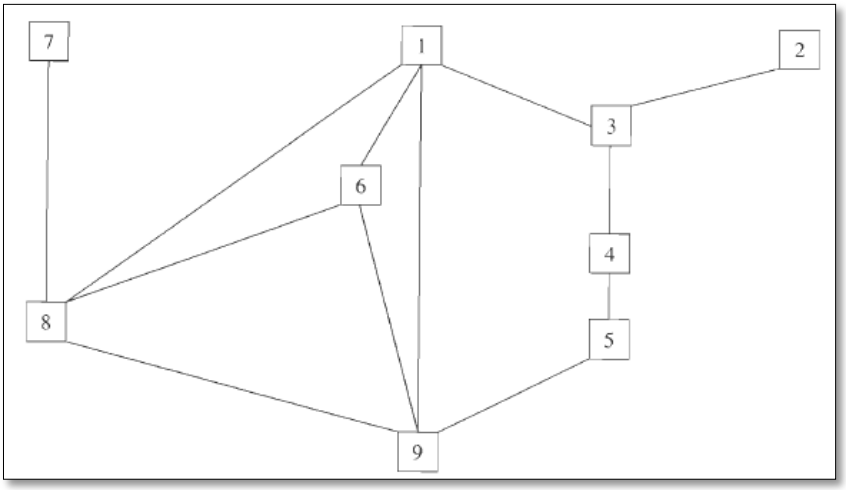

Ilustración 7: Diagrama de las proposiciones utilizadas para demostrar la proposición 9

No cabe duda que al-Farisi se basa en el trabajo de Euclides, los *Elementos,* ya que utiliza algunas de sus proposiciones para demostrar las suyas. Por otro lado se ve que la intención final de al-Farisi era demostrar la proposición 9, en donde asume la existencia de la factorización prima y la consiguiente determinación de todos los divisores.

La proposición 9 se puede considerar como una parte de la demostración del TFA ya que está relacionada con la existencia de la descomposición en factores primos de cualquier número compuesto, pero, como enuncia Rashed (1983, citado por Agargün, 1994), al-Farisi se queda corto porque no enuncia ni demuestra la

[30]Agargün, A. (1994). Al-Farisi and the Fundamental Theorem of Arithmetic.*HistoriaMathematica, 21, 162-173. Pag 171*

unicidad. Agargün y Fletcher (1994) hacen referencia a la misma observación, concluyendo que al-Farisi no tenía intención de demostrar la unicidad del TFA y en consecuencia no la enuncia, y por lo mismo, no le interesaba su demostración. Agargün & Fletcher también expone que al-Farisi pudo pensar que esto era obvio y en consecuencia no era necesario hacerlo.

Otro de los aspectos criticados en la obra de al-Farisi es la falta de rigor debida por ejemplo, al uso ambiguo de palabras como *factor* haciendo referencia a *factores primos*, argumento en el que se basa Rashed (1983) para dudar de su trabajo como matemático.

Una gran diferencia del trabajo de Euclides contrastado con el de al-Farisi es el lenguaje que utiliza, es un poco más simbólico y se puede interpretar con un grado mayor de facilidad, respecto a lo que se halla en Euclides.

5. EL APORTE DE JEAN PRESTET

Los resultados de interés de la obra de Prestet, relacionados con el TFA, se encuentran en el sexto capítulo ("Livre") del primer volumen de *Nouveaux Elemens* (1689). Este capítulo se dedica a la divisióngeneral de magnitudes.

Goldstein (1992) afirma que el autor da varias definiciones análogas a algunas presenten en el libro VII de los *Elementos* de Euclides tales como divisor, divisor común, simple o número primo, número compuesto, etc., luego presenta algunos corolarios. Goldstein relaciona el siguiente teorema y los colorarios con el aporte de Jean Prestet al TFA:

Teorema:*"Si dos números*[31] b y c *son primos relativos, su producto* bc *es el menor número que cada uno de ellos puede dividir exactamente y sin resto"*

Como corolario de este teorema, se encuentran:

Corolario III: *"Si* d *mide exactamente un producto* bc *de dos números* b *&* c *y si c y* d *son primos relativos; el número* d *es un divisor del número* b*. Como* c *&* d *son primos relativos y cada uno de ellos mide exactamente el producto* bc*, su producto* cd *que es el menor número que cada uno de ellos puede medir exactamente es un divisor de* bc*. Si entonces* e *es el exponente integral [i.e., el cociente] de la división de* bc *por* cd*, el número* bc *será igual al producto del divisor* cd *por el exponente integral* e*. Y si se divide cada uno de ellos por* c*, el exponentes de* b *&* de *son iguales o son uno y el mismo número. Pero si se divide* de *por* d*, uno tendrá el exponente integral* e*. Y así* d *es un divisor del número* de *o de* b*."*

Lo anterior se puede resumir en este ejemplo:

d	bc	b	c	cd	e
4	84	12	7	28	3
	cde	de			

[31] Se supone que estos números son naturales, aunque Prestet no lo enuncia.

Goldstein (1992) enuncia que este resultado es seguido por una sucesión de corolarios cuyo objeto es exponer todos los divisores de un número expresado como un producto de factores primos.

Corolario IV: *"Si los dos números diferentes a & b son simples, cada divisor de su plano, o su producto ab, es* 1, *o* a, *o* b *o* ab. *Para llamar* z *un divisor del número plano* ab, *si los números* a *y* z *son primos relativos, el número* z *será un divisor del número simple* b, *es decir* 1 *o* b, *que son los únicos divisores del número simple* b*"*

1	2	3	6	1	2	3	6
1	a	b	ab	1	a	b	ab
		z		z			

Y si los números a y z son relativamente compuestos[32], el simple a será un divisor de z. Y llamando y el exponente integral del divisor de z por a, el producto ay es igual al número z y también medirá a ab, del cual z es un divisor. Y llamando x entonces el exponente integrante de la división del número de ab por ayo z, el producto ayx es igual al número ab. Y dividiendo ayx y ab por a, los exponentes xy & b son iguales o son uno y el mismo número. Y, en consecuencia 1 & b, que son los divisores de b, son también los únicos divisores del número yx. Y así, el divisor y, que es integral, es necesariamente 1 o b, & ay, o z su equivalente, es el número simple $1a$, o el número plano ab. Así que si dos números a y b son simples, cada divisor de su plano ab es uno de los cuatro, $1, a, b, ab$.

1	2	3	6	1	2	3	6
1	a	b	ab	1	a	b	ab
y	z	x	ayx		x	y	z
		yx					yx

[32] Aunque en Goldstein no se encuentra definición de este término, suponemos que significa que éste significa que $a|z$.

En los corolarios V y VI, Prestet presenta enunciados análogos para el producto de tres números simples diferentes ("sólida") y de cuatro números simples ("súper-sólido"), luego cinco, y así sucesivamente, como él dice, infinitamente. Retoma todo esto en el siguiente corolario:

Corolario VII: *"El plano de dos números simples, o el sólido de tres, o el supersólido de cuatro, o el producto de varios, no puede tener ningún divisor simple, excepto la unidad, o uno de los dos, o uno de los tres, o de los cuatro simples, etc., de los que se supone que es el producto"*

En los primeros casos, Prestet da la lista completa de los divisores, se da cuenta de que corresponden a las diferentes combinaciones posibles de los factores simples, uno por uno, de dos en dos, etc. Se vuelve entonces a las potencias del mismo número primo

Corolario VIII: *"Si el número* a*es un simple, los divisores de su cuadrado* aa *es uno de los tres,* $1,\ a,\ aa$*. Y cada divisor de su cubo* a^3 *una de las cuatro,*$1, a, a^2, a^3$ *(...). Y así con los otros hasta el infinito"*

Y concluye con el siguiente corolario:

Corolario IX: *"Si los números* a *y* b *son simples, todos los divisores [de]*aab*es uno de los tres,*$1, a, aa,$ *o uno de los diferentes productos de estos tres por b; es decir, uno de los seis,*$1\ a, aa, 1b, ab, aab$*.Porque que todos los planos alternativos [es decir, obtenidas por multiplicar los diferentes factores de dos en dos] de los simples* a, a, b *son* $aa\&ab$*. [Enunciados análogos para* $aabb;\ aabbb;\ aab^3cc;\ aab^3ccd$*]. Y así, con los otros"*

Se puede interpretar, con lo anterior, que Prestet estaba interesado en responder a la pregunta de cuántos y cuáles son los divisores de un número dado, se puede inferir que le interesaba saber la cantidad ya que en los corolarios IV, VII, VIII y IX trata de numerarlos y caracterizarlos.

Prestet utiliza estos resultados en el resto del capítulo para solucionar diferentes problemas, tales como la búsqueda de todos los divisores de un número entero dado, calcular el número de divisores de un número dado, o la determinación de la medida común de dos números. También explica la noción de un número

perfecto[33].y demuestra la construcción de Euclides para estos números(Goldstein, 1992).

[33] n es un número perfecto si la suma de sus divisores propios es igual a él mismo.

6. EL APORTE DE EULER

La obra de Euler que está relacionada con el TFA es la que publicó en el año de 1770, *Introducción al Álgebra*, obra que escribió después de quedar ciego, esto fue posible gracias a la ayuda de su hijo Juan Alberto Euler. Esta obra consta de dos volúmenes. El tomo I considerado como la primera tentativa para establecer las operaciones fundamentales sobre bases racionales, trata las operaciones aritméticas con números enteros, racionales e irracionales, positivos y negativos, realiza cálculos utilizando logaritmos. El segundo volumen está destinado al análisis diofántico; se encuentran resueltas algunas proposiciones debidas a Fermat. También se encuentra el estudio de las ecuaciones determinadas e indeterminadas, es decir, aquellas que tienen un número finito de soluciones y las que por el contrario tienen infinitas soluciones(Chadid, 1996).

Agargün y Özkan (2001) afirman que Euler en su obra *Introducción al Álgebra,* enuncia parte de la existencia del TFA sin demostrarla, y también da un enunciado parcial de la unicidad análogo a la proposición 9 de al-Farisi y al corolario 9 de Prestet. No obstante consideramos que, como ya se mencionó, en la proposición 9 de al-Farisi no se establece unicidad para la factorización prima, solo se asume la existencia de tal factorización.

Los enunciados relacionados con el aporte de Euler al TFA están en el artículo 41 del capítulo IV de la sección 1 de la parte 1, pero antes de enunciarlos, revisando un poco lo anterior a estos enunciados, se encontró, en la obra de Euler (1770), que él da las definiciones de números primos y números compuestos; así que presentaremos tales definiciones en artículos, como él lo hace.

Capítulo IV

"Artículo 37. Nosotros hemos observado que un producto es generado por la multiplicación de dos o más números juntos, y que estos números son llamados factores. Entonces, los números$a, b, c, d,$ son los factores del producto$abcd.$

Artículo 38. Si, por lo tanto, nosotros consideramos todos los números enteros como producto de dos o más números multiplicados juntos, nosotros pronto encontraremos que algunos de ellos no resultan de una multiplicación, y en consecuencia no tienen factores; mientras otros pueden ser el

producto de dos o más números multiplicados juntos, y en consecuencia tenemos dos o más factores. Así 4 es producido por 2×2; 6 por 2×3; 8 por $2 \times 2 \times 2$; 27 por $3 \times 3 \times 3$; y 10 por 2×5, etc.

Artículo 39. Pero por otro lado, los números $2, 3, 5, 7, 11, 13, 17,$ etc., no pueden ser representados de la misma manera como factores, a menos que para este propósito nosotros hagamos uso de la unidad, y representemos 2, como, 2×1. Pero los números que son multiplicados por 1 terminan siendo el mismo, esto no es propio para reconocer la unidad como factor. Todos los números, así, como $2, 3, 5, 7, 11, 13, 17,$ etc., los cuales no pueden ser representados como factores, son llamados simples, o números primos; mientras que los otros, como $4, 6, 8, 9, 10, 12, 14, 15, 16, 18,$ etc., los cuales pueden ser representados como factores, son llamados números compuestos.

Artículo 40. Los números simples o primos por lo tanto merecen una atención particular, por lo que no son el resultado de la multiplicación de dos o más números. Esto es particularmente digno de observación, ya que si escribimos estos números en sucesión como ellos siguen este orden, así, $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$ etc., nosotros no podemos trazar un orden regular de la secuencia; este incrementa algunas veces mucho, algunas veces poco; y hasta ahora nadie ha podido establecer o descubrir si ellos siguen alguna ley o no" (p.10)

Hasta ahora podemos establecer ciertas diferencias de la presentación de las ideas de Euler con las presentadas por los demás autores, ya que a Euler parece que le interesa establecer un la diferencia que existe entre un número simple y uno compuesto, por lo que inicia dando la definición de factores de un número, además, enuncia que todo número compuesto puede ser escrito como producto de sus factores. Además advierte que la unidad no es considerada como un factor, ya que al multiplicar cualquier número por la unidad sigue siendo el mismo número, enunciado que diferencia a los números *simples* de los compuestos.

Artículo 41. Todos los números compuestos, los cuales pueden ser representados como factores, resultan de los números primos antes mencionados; es decir, todos sus factores son

números primos, estos siempre pueden ser descompuestos y representados por dos o más números primos. Cuando tenemos representado, por ejemplo, el número 30 como 5×6, es evidente que 6 no es un número primo, pero usando el producto de 2×3, podemos tener la representación de 30 como $5 \times 2 \times 3$ o como $2 \times 3 \times 5$; es decir, como factores,de los cuales todos son números primos.

El anterior enunciado se puede considerar como el correspondiente a la existencia del TFA, ya que establece que todo número compuesto puede ser representado como producto de factores primos, sin embargo en el capítulo IV, no se establece una demostración formal de este enunciado, por otro lado parece que a Euler sí le interesaba dejar claro lo que decía y por ello el uso de ejemplos.

En el artículo 42 Euler sólo enuncia la diferencia que se puede encontrar entre los números compuestos, ya que en algunos casos con números mayores, éstos tienen menos factores primos que números compuestos menores.

En el artículo 43 Euler enuncia un método, a través de un ejemplo, para representar un número compuesto como producto de sus factores primos, el método lo ejemplifica con el número 360, Euler (1770) enuncia que:

> "El primer paso consiste en escribir 360 como 2×180, ahora 180 es igual a 2×90 y
>
> | | | |
> |---|---|---|
> | 90 | es lo mismo que | 2×45 |
> | 45 | es lo mismo que | 3×15 |
> | 15 | es lo mismo que | 3×5 |
>
> Por último sólo debemos representar el número 360 como el producto de $2 \times 2 \times 2 \times 3 \times 3 \times 5$."(p.12)

Resumiendo el método, debemos hacer la división del número inicial, digamos x, con el número primo más pequeño, si la división es exacta, lo representamos como $2 \times a$ (siendo a el resultado de la división), si$a$, es simple, el procedimiento habrá acabado, pero si es compuesto, continuamos de nuevo con el número primo 2, si éste no lo divide, procedemos con el siguiente número primo, es decir 3, si la división es exacta representamos a como $3 \times c$ (siendo c el resultado

de la división) y la representación, hasta el momento, sería $2 \times 3 \times c$, si c es simple, habremos terminado, de lo contrario debemos volver a revisar si el número primo 3 divide a c, de lo contrario continuaremos con el siguiente número primo, y así hasta terminar.

Agargün y Fletcher (2001) también mencionan una relación del TFA con el artículo 65 del capítulo VI de la sección 1 de la parte 1 de la misma obra de Euler, que enuncia:

> ***Artículo 65.****Cuando, por lo tanto, hemos representado a cualquier número asumidos por placer, por sus factores simples, será muy fácil para exhibir todos los números por los que es divisible. Sólo tenemos, en primer lugar, que tomar los factores simples uno por uno, para luego multiplicarlos juntos de dos en dos, de tres en tres, de cuatro en cuatro, y así hasta que llegamos al número propuesto.*

Dos interpretaciones diferentes, logradas en el marco de este trabajo de grado, de porqué Agargün y Fletcher (2001) consideran que este enunciado está relacionado con la unicidad del TFA son:

1. El artículo 65 enuncia que podemos encontrar todos los divisores de un número con su escritura como producto de factores simples, sin embargo al tratar de demostrar esto, suponemos que no los encuentro todos esto quiere decir que existen divisores que provienen de otra factorización prima del mismo número, esto es contradictorio porque se supone que la factorización es única.
2. Se puede suponer que Euler partió del supuesto de que la factorización prima de un número es única y por lo tanto es posible afirmar que puedo encontrar todos los divisores a partir de su representación como producto de factores simples.

De alguna manera podemos ver que Euler, al igual que al-Farisi y Prestet, sólo estaba interesado en encontrar todos los divisores de un número dado.

7. EL APORTE DE LEGENDRE

La obra de Legendre relacionada con el TFA es *Théorie des Nombre* (Teoría de Números), la cual fue publicada en 1798; esta obra trata temas relacionados con la teoría de números y es aquí donde Legendre establece el primer caso de aplicación de la ley de reciprocidad cuadrática[34].

Agargün y Özkan (2001) presentan el enunciado y la demostración del enunciado de Legendre, así:

Cualquier número no primo[35] N *puede ser representado por un producto de varios números primos* $\propto, \beta, \gamma$*, etc., cada uno elevado a alguna potencia, por lo que uno supone que* $N = \propto^m \beta^n \gamma^p$*, etc.*

Su demostración es la siguiente

El método a seguir para realizar esta descomposición, consiste en tratar de dividir N *por cada uno de los números primos* $2, 3, 5, 7, 11$*, etc., a partir del más pequeño. Cuando la división tiene éxito con uno de estos números*$\propto$*, se repite tantas veces como es posible, por ejemplo,* m *veces, y llama* P *al último cociente, así tenemos*

$$N = \propto^m P$$

El número P *no puede ser dividido por* $\propto$*, y es inútil tratar de dividir* P *por un número primo menor que* $\propto$*, pero si* P *fuera divisible por* θ*, donde* θ *es menor que* $\propto$*, está claro que* N *también sería divisible por* θ*, en contra de la hipótesis. Por tanto, debemos tratar de dividir* P *por números primos mayores que* $\propto$*, por lo que vamos a obtener en la sucesión*

$$P = \beta^n Q,\ Q = \gamma^p R, \text{etc.},$$

Por lo que tenemos que $N = \propto^m \beta^n \gamma^p$*, etc.*

Con este método podemos encontrar la descomposición en factores primos de cualquier número, este método es similar al presentado por Euler en la sección anterior, sin embargo Legendre usa expresiones generales (contrario a Euler) para representar este

[34]Esta ley permite la determinación de la solvencia de cualquier ecuación de segundo grado en la aritmética modular.

[35] El documento estudiado no presenta una definición para este palabra según Legendre.

método, de alguna forma la manera de escribir Legendre es más "matemática", ya que en la demostración del enunciado Legendre trata de generalizar, que cualquier número se puede escribir de esta manera.

Agargün y Özkan (2001), aseguran que en el artículo X, de la misma obra de Legendre, él establece una manera de encontrar los divisores de un número, partiendo del número dado escrito de la forma factorizada, sin embargo la demostración para este enunciado no es presentada por estos autores:

Un número N se expresa en la forma $\propto^m \beta^n \gamma^p$, etc, cada divisor de N también será de la forma $\propto^\mu \beta^\sigma \gamma^\pi$, etc, donde los exponentes μ, σ, π, etc, no son mayores [uno a uno] que m, n, p, etc.

Es evidente que Legendre intenta, con este enunciado, mencionar todos los divisores de un número dado; al respecto, Agargün & Fletcher mencionan que al mismo tiempo trata de hallar la suma de los divisores encontrados, lo que está relacionado con el trabajo de varios autores que se han mencionado en este trabajo, es decir está relacionado con los números perfectos.

8. EL APORTE DE GAUSS

La obra máxima de Gauss, *Disquisitiones Arithmeticae,* fue escrita en el año 1798 pero publicada en 1801. Gauss en esta obra, además de enunciar y demostrar el TFA, también enuncia que:

- Todo número entero es suma de, a lo sumo, tres números triangulares y de cuatro cuadrados.
- Existe una relación entre los polígonos regulares y su construcción usando regla y compás.

En esta obra también se incluye una nueva teoría, la Aritmética Modular, que consiste en un conjunto de métodos para resolver problemas con números enteros a partir de un conjunto de operaciones aritméticas basadas en la relación de congruencia entre números, Pettofrezzo y Byrkit (1972) definen la relación de congruencia de la siguiente manera:

> Sea$m$un entero positivo. Sia *y* $b$son dos enteros tales que $m|(a-b)$, entonces se dice que $a$es congruente con $b$módulo$m$; esto será denotado por
>
> $$a \equiv b \ (mód\ m)$$
>
> *Si* $m \nmid (a-b)$, entonces se dice que a es incongruente con$b$módulo$m$y será denotado por
>
> $$a \not\equiv b(mód\ m).$$ (p.87)

Hernández (2006) hace una breve descripción de la obra de Gauss, donde menciona la cantidad de secciones y qué contiene cada una:

> Las *Disquisitiones Arithmeticae* tratan sobre números enteros y excluye amenudo a los fraccionarios y siempre a los irracionales. El libro se organiza en siete secciones:
>
> 1. Números congruentes en general
> 2. Las congruencias de primer grado
> 3. Residuos de potencias
> 4. Congruencias de segundo grado
> 5. Formas y ecuaciones indeterminadas de segundo grado
> 6. Aplicaciones de las nociones anteriores
> 7. Ecuaciones de las secciones de un círculo. (p.4)

Hernández establece que en las Secciones I y II, Gauss introduce por primera vez la notación aritmética en congruencias; en las secciones III y IV aborda los residuos cuadráticos y de potencias superiores. Demuestra entre otras cosas el Pequeño Teorema de Fermat y el teorema de Wilson[36]; las últimas secciones, V, VI y VII trata de las formas cuadráticas y sus aplicaciones y ocupan más de la mitad de la obra de Gauss.

El enunciado y demostración del TFA se encuentra, en el artículo 16, en la segunda sección titulada, *"Las congruencias del primer grado".*

Los teoremas previos al TFA son enunciados y demostrados por Gauss (1801, p.1, Sección II), así:

13. Teorema. *El producto de dos números positivos, más pequeños que un número primo dado, no puede dividirse por este número primo.*

> En otras palabras: p primo, y a positivo y $a < p$: entonces no puede encontrarse ningún número positivo b menor que p tal que $ab \equiv 0 \mod p$
>
> Si se niega el teorema, tendremos números $\mathrm{b}, \mathrm{c}, \mathrm{d}$, etc., todos $< p$, tales que $\mathrm{a}b \equiv 0$, $ac \equiv 0$, $ad \equiv 0$, etc., $(mod.p)$. Sea b el menor de todos estos, tal que ningún número menor que b tenga esta propiedad. Es evidente que $\mathrm{b} > 1$: pues si $\mathrm{b} = 1$, entonces $\mathrm{ab} = \mathrm{a} < p$ (por hipótesis) y por lo tanto no es divisible por p. Ahora, como p es primo, no puede dividirse por b pero está comprendido entre dos múltiplos sucesivos de b, mb y $(\mathrm{m}+1)\mathrm{b}$. Sea $p - mb = b'$; así b' será un número positivo y $< b$. Ahora, como suponemos que $ab \equiv 0\,(mod.p)$, también tenemos $mab \equiv 0$ (por art. 7[37]), y restando éste de $ap \equiv 0$ resulta $a(p - mb) = ab' \equiv 0$; esto es: b' tiene que ser uno de los números $b, c, d,$ etc., aunque resulta menor que el menor de tales números, b. Q. E. A.

[36] "El producto de todos los números menores que un número primo dado, aumentado en una unidad es siempre divisible por dicho número"

[37] Si $A \equiv a$, entonces, también $kA \equiv ka$.

14. *Si ni a ni b pueden dividirse por un número primo p, tampoco el producto ab puede dividirse por p.*

Sean α y β los menores residuos positivos de los números a y b, respectivamente, según el módulo p. Ninguno de ellos es cero (por hipótesis). Ahora, si $ab \equiv 0\ (mod.p)$, entonces $\alpha\beta \equiv 0$, puesto que $ab \equiv \alpha\beta$. Pero esto contradice el teorema anterior.

15. *Si ninguno de los números a, b, c, d, etc., puede dividirse por un número primo p, tampoco puede dividirse por p el producto $abcd$ etc.*

Según el artículo anterior, ab no puede dividirse por p; por lo tanto, tampoco abc, ni tampoco $abcd$, etc.

16. Teorema. *Cualquier número compuesto puede resolverse en factores primos de una manera única.*

Demostración. Que cualquier número compuesto pueda resolverse en factores primos, resulta de consideraciones elementales, pero esta supuesto tácitamente, y en general sin demostración, que no puede hacerse de muchas maneras diferentes. Supongamos que algún número compuesto A, que es $= a^{\propto}b^{\beta}c^{\gamma}$ etc., donde $a, b, c,$ etc. denotan números primos diferentes, es resoluble en factores primos de otra manera.
Primero, es claro que no puede aparecer en este segundo sistema de factores ningún otro primo más que a, b, c, etc. puesto que ningún otro primo puede dividir a A, el cual está compuesto de estos primos. De forma semejante, ninguno de los primos a, b, c, etc. puede estar ausente del segundo sistema de primos, puesto que si no, no podría dividir a A (artículo anterior). Así, estas dos resoluciones en factores pueden ser diferentes solamente si un primo aparece más veces en una resolución que en la otra. Sea p un tal primo que aparece m veces en una resolución, y n veces en la otra, y tal que $m > n$. Al disminuir en n el número de factores p en cada sistema quedaran $m - n$ factores p en un sistema mientras que no quedara ninguno en el otro.
Esto es, tenemos dos resoluciones en factores del número $\frac{A}{p^n}$.
El que una de ellas no contenga al factor $p$mientras que la otra lo contenga m — n veces contradice lo que acabamos de demostrar. (pp.13-15)

Se puede interpretar, de la demostración presentada por Gauss, que solo le interesaba demostrar la unicidad de la factorización prima de un número, ya que la existencia de la factorización prima lo considera como elemental, puede ser por el trabajo de los autores previos a él, quienes ya se habían encargado de esta parte.

9. CONCLUSIONES

La investigación realizada durante este trabajo, permitió exponer diferentes autores que están relacionados con el TFA, pero muy seguramente se quedaron varios por mencionar, quizá algunos nos son tan nombrados o posiblemente al igual que con otros matemáticos, simplemente, no han dejado rastro de su trabajo.

Indudablemente, el trabajo de Euclides se puede considerar como pionero, en relación con el TFA. A través de los diferentes artículos estudiados, se pudo observar que la mayoría de los autores mencionados, trabajaban de manera similar (hablando de la estructura de su trabajo), iniciando con definiciones, continuando con los teoremas sustentados en definiciones o teoremas previos (bien sean propios o de otros); la importancia del trabajo de Euclides, se hace más evidente en el trabajo de al-Farisi, quien en sus demostraciones enuncia algunas de las proposiciones presentadas en los *Elementos.*

En algunos casos, los autores que se relacionaron en este trabajo, tienen enunciados similares, sin embargo que sea similar respecto al enunciado, no implica similitud en sus métodos para demostrar o en su notación o en su lenguaje; en el caso de al-Farisi, el lenguaje era un poco complicado y por ello fue necesario modificar el texto y reescribirlo utilizando un lenguaje moderno que permite mejorar la compresión de la obra original, sin querer decir con esto, que utilizando tal lenguaje la comprensión sea sencilla, solo “menos difícil”.

El estudio de la historia del TFA, en principio, fue complicado, a pesar de estar familiarizado el lenguaje de Euclides, el tiempo que se dedicó para entender sus demostraciones fue mucho más, comparado con los otros autores.

Respecto a la rigurosidad, en escritura, se destacan indudablemente, Legendre y Gauss, quienes usan una notación simbólica para generalizar sus ideas y la descomposición en factores primos de número compuestos, a diferencia Euler, quien solo daba ejemplos concretos para enunciar algo.

Relacionando la rigurosidad en las demostraciones, dejando de lado a Prestet ya que no se encontraron evidencias de sus demostraciones, aunque la mayoría de estos autores son reconocidos, algunos nos pueden dejar sorprendidos; cuando vemos

sus trabajos, por lo menos en este aspecto (El TFA) logra asombrar ver que la demostración es un ejemplo concreto, en el caso de Euler para el artículo 41, del capítulo V; claro que esta visión puede depender de la idea de rigurosidad matemática de la época.

El estudio de la Historia de las Matemáticas, no es sencillo, la búsqueda de textos originales o que están más relacionado con el autor que se está estudiando, a veces es complicado, como es el caso de Jean Prestet, no fue sencillo hallar artículos que mencionaran todo respecto a él, biografía, obras y por supuesto lo relacionado con el TFA; por otra parte los documentos que se encontraron, en su mayoría están escritos en otro idioma, lo que dificulta y demora un poco la comprensión de lo que intenta decir cada autor estudiado, sin embargo este ejercicio ratifica lo mencionado por Guacaneme (2011), respecto a los tres *artefactos* a los que allí se hace alusión, se pueden identificar los componentes que se desarrollaron a partir del inicio de la elaboración de este trabajo:

- **Visiones de la actividad matemática:** Este trabajo expone la importancia del TFA con problemas internos de la matemática, ya que éste estaba relacionado con el trabajo posterior de varios autores en relación con los números perfectos.
- **Visiones de los objetos matemáticos:** Se evidenció en algunos casos, nuestras representaciones simbólicas difieren con algunos autores y que el concepto rigor matemático, para el caso de la escritura y de la presentación de las demostraciones, es diferente, en algunos casos, confusa y en otros insuficientes.
- **Competencias profesionales:** En este aspecto y como ya se había mencionado, la elaboración de este trabajo exigió hábitos de lectura (en español e inglés), escritura, escucha y búsqueda de fuentes originales.

Anexo No.1

UN ESTUDIO HISTÓRICO DEL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA[38]

El propósito de este artículo es un estudio comprensivo de la historia del Teorema Fundamental de la Aritmética. Para este objetivo investigamos los pasos más importantes durante el periodo de Euclides a Gauss.

INTRODUCCIÓN

El concepto de factorización única está relacionado con la aritmética griega y aún tiene un papel importante en la moderna teoría de anillos conmutativa. Básicamente, la factorización única consiste de dos propiedades: existencia y unicidad. La existencia significa que un elemento es representado como un producto finito de irreducibles, y la unicidad significa que esta representación es única en cierto sentido. La factorización única apareció por primera vez como una propiedad de los números naturales. Esta propiedad es llamada el Teorema Fundamental de la Aritmética (TFA).

La historia del TFA es extrañamente oscura. Formulamos el TFA como lo siguiente. Cualquier número natural mayor que 1 puede ser representado como un producto de primos de una y solamente una forma (sin importar el orden). Como hemos iniciado, esto no aparece en los *Elementos de Euclides* [Heath, 1908]. Sin embargo, Euclides jugó un papel importante en la historia del TFA. Específicamente, los libros VII y IX contienen proposiciones que están relacionadas con el TFA.

En su *Tadhkirat al-Ahbabfibayan al-tahabb* [Rashed, 1982] al-Farisi, prueba la existencia de una descomposición prima, y después da todo lo que es necesario para probar su unicidad. Su proposición 9 determina todos los divisores de un número dado desde su factorización prima. Un resultado análogo puede ser encontrado en *Nouveaux Elemns de Mathématiques* de Prestet.

Siguiendo a Prestet podemos también mencionar a Euler. En su libro *Vollständige Einleitungzur Algebra* [Euler 1770] Euler asumió la propiedad de la existencia del TFA y declaró un resultado similar al de al-

[38]Agargün, A. G.,Özkan, E. M. (2001) A Historical Survey of the Fundamental Theorem of Arithmetic. *Historia Mathematica 28 (2001). 20 7-214.*
Traducción libre realizada por Wilson Alejandro Triana Cordero en el marco del trabajo de grado **UNA VISIÓN HISTÓRICA DEL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA**

Farisi y Prestet para encontrar todos los divisores. Más tarde Legendre prueba la parte de la existencia del TFA en su libro *Théories des nombres* [Legendre 1798] y asume la unicidad cuando lista los factores de un número dado pero él no declara el TFA explícitamente. El primer enunciado claro y prueba del TFA parece ser dado por Gauss in su *Disquisitiones Arithmeticae*[Gaus 1801]. Después de Gauss, muchos matemáticos propusieron diferentes demostraciones del TFA en sus trabajos [Agargün & Fletcher 1997].

2. EUCLIDES Y EL TFA

Los Elementos de Euclides [Health 1908] consisten de 13 libros. Los libros de aritmética, VII al IX, contienen resultados básicos de la teoría de números. Aunque el TFA no aparece en los *Elementos,* hay dos proposiciones muy significativas, VII.30 y VII.31, las cuales están conectadas con el TFA. Hay una tercera proposición, IX.14, que es un teorema de unicidad. De hecho, el TFA se desprende de las proposiciones VII.30 y VII.31.

VII. 30. Si dos números, al multiplicarse entre sí, hacen algún número y algún número primo mide a su producto, también medirá a uno de los números iniciales. [i.e., si un número primo c mide ab, entonces c mide a o a b, donde "medir" puede ser escrito como "dividir", sin embargo repetir sería más cercano al espíritu de la palabra griega]

VII.31. Cualquier número compuesto es medido por algún número primo.

Fácilmente, obtenemos la existencia (cualquier número mayor que 1 puede ser representado como un producto de primos) por VII.31, y la unicidad (i.e., esta representación es única sin importar el orden) por VII.30. Hoy en día, muchos matemáticos podrían demostrar el TFA usando estas proposiciones. Para la unicidad suponemos $p_1 \dots p_n = q_1 \dots q_m$ son dos descomposiciones primos de algún número entero positivo. Entonces, por VII.30 tenemos que $p_1 \mid q_1$. Similar podemos tener la misma cosa para todos los $p_1 \dots p_n$y q's y de aquí $n = m$. Sin embargo, Euclides no establece el TFA siguiendo las proposiciones en el libro VII.

En el libro IX encontramos la proposición 14 la cual establece que "si un número es menor que su medido por un número primo este no puede ser medido por ningún otro número primo excepto por lo originales"

Hay muchas similitudes entre el TFA y IX.14. La proposición IX.14 es una clase de teorema de unicidad. Esta es una demostración parcial de la condición de unicidad para el TFA, pero es claro que IX.14 no

cubre el caso de números que poseen factores cuadrados. Por esta razón algunos autores (e.g,. [Hendy 1975, Mullin 1965]) han examinado IX.14, y han determinado que los resultados (IX.14 y el TFA) no son técnicamente equivalentes.

Además, tenemos que notar que sin tener en cuenta la descomposición prima IX.14 inicia con la colección de primos mientras que el TFA inicia con un entero. Los puntos de partida de los dos teoremas son completamente diferentes.

Hoy en día, los libros de texto comúnmente toman el TFA como un teorema fundamental. Ellos inician con la definición de números primos y prueban la unicidad de la factorización con los primos. Esto está seguido por las propiedades de los primos relativos enteros y máximo común divisor. Este enfoque parece tener orígenes con Gauss. En teoría de los números de Euclides se organizan las cosas justo en el orden inverso. Euclides inicia con el algoritmo de la división para encontrar el máximo común divisor de enteros, y entonces el obtiene una definición operativa de los primos enteros relativos. De la investigación del inicio de los primos relativos, el eventualmente encuentra resultados sobre los números primos, incluyendo en particular una proposición importante VII.30, y a continuación el afirma la proposición VII.31 (véase arriba) en el orden inverso. En la teoría de Euclides el TFA podría perder mucha de este significado. Lejos de ser fundamental, IX.14 es puesto al final de la teoría de la aritmética de Euclides. No se puede considerar la culminación de cualquier parte importante de la teoría, ni se utiliza en cualquier resultado posterior.

3. AL-FARISI Y EL TFA

Kamal al-Dın al-Farisı, quien murió en 1320 AC, fue un gran matemático persa, físico y astrónomo, el trabajó representando el paso más representativo hacia el TFA hecho después por el matemático Guass. Su resultado apareció *Tadhkirat al-Ahbabfıbayan al-tahabb*(el cual significa “Memorias para un amigo explicando la prueba de amabilidad”. Su asunto fundamental fue los números amigos, y su objetivo fue probar por un método diferente el teorema de Ibn Qurra que dice “si tres número $p = 3.2^{n-1} - 1$, $q = 3.2^{n} - 1$, y $r = 9.2^{2n-1} - 1$ son primos y sí $p, q > 2$, entonces el par $2^{n}pq$ y $2^{n}r$ son amigos” [Hogendijk 1985]. Ibn Qurra (836 – 901) trabajó ligeramente en la descomposición de enteros y los métodos de combinatoria. Al-Farisi fue llevado a desarrollar nuevas ideas en la

teoría de números y el investigó la descomposición de enteros más detalladamente que Ibn Qurra. Después él pudo introducir los métodos de combinatoria esto fue necesario para considerar la existencia de la factorización de un entero como producto de números primos y el uso de la propiedad unitaria para determinar los divisores.

En [Agargün & Fletcher 1994] hicimos una traducción en inglés de sus primeras nueva proposiciones y proporcionan un comentario de los métodos de Al-Farisi. El papel principal de estas nueve proposiciones es conocer y buscar los divisores de un número dado y por lo tanto es una preparación para el trabajo con los números amigos.

Uno puede decir que Euclides tomo el primer paso en la vía para la existencia de la factorización prima, y Al-Farisi tomo el paso final para la actual existencia de la demostración de la factorización prima finita en su primera proposición.

Proposición 1. Cada número compuesto puede ser descompuesto en un número finito de factores primos de los cuales estos son el producto.

Suponga que $a > 1$ es una composición entera. Por lo tanto, para Euclides VII.31 este posee un número divisor primo b. Luego para $1 < c < a$.

$$a = bc$$

Si c es primo, entonces la proposición está demostrada. De lo contrario$c$ tiene un divisor primo d y por $1 < e < c$ nosotros escribimos

$$c = de$$

Si e es primo entonces la proposición está demostrada luego $a = bde$. De lo contrario nosotros repetimos el proceso un número finito de veces y al final descomponemos un factor compuesto en dos factores primos desde un número finito que no puede ser mayor de un producto finito de números. Entonces escribimos para k primo

$$a = bd \cdots k$$

Esta proposición es la primera declaración conocida y prueba de la

existencia de una factorización prima para cualquier número compuesto. Después al-Farisi, Prestet no expone esto, pero lo uso para determinar todos los divisores de un entero dado. Euler expuso y uso esto para encontrar divisores. Eventualmente Legendre expuso y probó esto.

Las proposiciones de al-Farisi de las 2 a la 5 son las siguientes:

Proposición 2. Cuando tres números a, b, c, se dan, la relación de la primera a la tercera se compone de la relación de la primera a la segunda y de la relación de la segunda a la tercera.

Proposición 3. La relación de 1 a cualquier número compuesto se compone de su relación a cada uno de los factores primos.

Proposición 4. Cualquiera de los dos números compuestos que tienen la misma descomposición en factores son idénticos.

Proposición 5. Cualquiera de los dos números compuestos distintos no tienen la misma descomposición en factores.

Después de la Proposición 5 al-Farsi dio el primer paso para determinar todos los divisores de un entero.

Él no consideró el entero propio como un divisor. Allí, al igual que con Prestet y Euler, el principal punto de partida fue la descomposición de primos.

Proposición 6. Si un número compuesto a se descompone en un números primos $b, c, d, e, \cdots, k$, entonces de dos en dos, $ab, bd, be, \cdots$, etc, de tres en tres $bcd, bce, \cdots$ etc, todos ellos son divisores de a.

Entonces, al-Farsi demostró la Proposición 7, que se utiliza para demostrar la Proposición 8.

Proposición 7. Sí $a \nmid b$, entonces para $n = 3,4 \cdots, a^2 \nmid ba$; y $a^n \nmid ba$; $a^3 \nmid ba^2$ y $a^{n+1} \nmid ba^2$; $a^4 \nmid ba^3$ y $n^{n+2} \nmid ba^3$ y así sucesivamente.

Aquí tenemos la Proposición 8, que se utiliza en la proposición siguiente.

Proposición 8. Aquí, sí un número compuesto a es descompuesto en sus factores primos como $a = bcd \ldots k$, entonces si uno de ellos, digamos b, no se repite entonces $b^2 \nmid a$ y para $n = 3,4, \ldots, b^n \nmid a$. Y sí b se repite una sola vez entonces b^2 / a pero $b^n \nmid a$. Y sí b se repite únicamente dos veces entonces $b^2 | a$, $b^3 | a$, pero $b^{n+1} \nmid a$.

Para determinar todos los divisores de un entero compuesto dado , al-Farsi demostró la Proposición 9. En esta proposición se observa que todas las proposiciones anteriores se utilizan directa o

indirectamente. Vemos un resultado similar en Prestet y Euler, pero por supuesto la Proposición 9 se presentó mucho antes, y por lo que sabemos que este es el primer resultado conocido para determinar todos los divisores de un número compuesto. Una vez más el punto de partida principal fue la descomposición prima.

Proposición 9. Sí un número compuesto a *es descompuesto en sus factores primos como* $a = bcdh \cdots kl$*, entonces* a *no tiene divisores excepto* 1 *y* $b, c, d, h, \ldots, k, l$ *y de dos en dos* $bc, bd, \ldots, etc.$*, y de tres en tres* $bcd, bch, \ldots, etc., \ldots$*, y los productos de todos los factores excepto uno:* $cdh \cdots kl, bdh \cdots kl, \ldots, bcdh \cdots k$.

Obviamente $1, b, c, d \ldots, k, l$ son divisores de a. Los otros son inmediatamente divisores de la Proposición 6. Suponer que a tiene otro divisor z el cual es o primo o compuesto. Si z es un primo entonces consideramos a a como $b\,(cdh \cdots l)$ y $z|b(cd \cdots l)$ implica $z|cdh \cdots l$ de Euclides VII.30. Similarmente $z|c(dh \cdots l)$ implica $z|dh \cdots l$. por lo tanto, por el mismo proceso tenemos $z|kl$. Por tanto $z|k$ o $z|l$ y esto implica $z = k$ o $z = l$. Esta es la contradicción. Suponer ahora que z es un número compuesto y este es distinto de los divisores antes dichos. Por tanto, de la proposición 5 existe uno entre los factores primos de z el cual no aparece entre los factores de a, o si este uno factor no existe, entonces hay un factor de z el cual no se repite el mismo número de veces en z y a. Así tenemos tres casos posibles: (i) z tiene un factor primo el cual no aparece entre los factores de a, o si z no tiene ningún factor entonces (ii) un factor de z tiene más repeticiones que un factor de a, o (iii) un factor de a se repite a si mismo mas que un factor de z.

Si se trata de la primera y h es un número primo distinto de todos los factores de a, entonces esto es una contradicción del caso previo, donde z es asumido para ser un número primo.

Si se trata del segundo, que es un factor de z, decimos p, repetir n veces en z pero menos n veces en a, entonces $p^{n+1}|z$ y $p^{n+1}|a$, lo que es imposible, por la proposición 8.

Y si es el tercero, que es, todos los factores de z no se repiten más veces que en los factores de a, entonces z llega a ser divisor de a, lo cual ha sido mencionado, y esto es una contradicción.

Vemos que al-Farisi hace un avance importante hacia el TFA, aunque él no decirlo. Dijo, y demostró la existencia de una parte del TFA, pero no lo hizo del estado y no tenía la intención de demostrar la singularidad de la factorización en números

primos desde que el TFA no era importante para él. Esto no quiere decir que no sabía de la singularidad. Si Al-Farisi había querido expresar y probar la unicidad, habría sido capaz de hacerlo. Al-Farisi sabía que la singularidad muy bien como se puede ver tanto de la declaración y la prueba de su proposición 9. De hecho, demostró la Proposición 9 con el fin de determinar todos los divisores de un número compuesto, y lo utiliza para dar una nueva demostración del teorema de ibn Qurra en números amigos. Sin embargo, mostró todo lo que se necesita para probar la unicidad. Por lo tanto podemos considerar que la Proposición 9 que es equivalente a la parte de unicidad del TFA.

4. EL RESULTADO DE PRESTET

En esta sección nosotros presentamos algunos resultados publicados por Jean Prestet en sus 1689 *Nouveaux Elemens de Mathématiques* [Goldstein 1992]. Ellos confirman que antes de tiempos modernos una factorización prima no era algo de interés en su propio derecho, pero como un medio de encontrar los divisores.

Prestet tampoco declaró la existencia ni la unicidad del TFA. Él fue influenciado por Euclides y se preocupaba por los divisores. Como al-Farisi y Euler él dio a los resultados principales para encontrar todos los divisores de un número dado. En particular su Corolario IX tiene un papel importante. Este resultado nos hace creer que Prestet conoció el TFA. Nosotros pensamos que él pudo haberlo demostrarlo, pero él no se preocupaba por esto.

En Capítulo 6 de su primer volumen, nosotros nos encontramos el siguiente teorema.

TEOREMA. Si dos números b y c son primos relativos, su producto bc es el menor número que cada uno de ellos puede dividir exactamente y sin residuo.

Como un corolario de este teorema Prestet declaró:

COROLARIO III. Si d mide exactamente al producto bc de dos números b y c y si c y d son primos relativos; el número d es un divisor del otro número b.

El objeto del siguiente corolario fue determinar todos los divisores de un número expresado como producto de factores primos.

COROLARIO IV. Si dos números diferentes a y b son simples, cada divisor del plano, o producto ab, es 1, o a, o b, o ab.

Prestet continúa con los corolarios V y VI usando el mismo argumento para un producto de tres números primos diferentes (sólidos) y cuatro números primos (supersólidos), entonces cinco, y así indefinidamente.

En el siguiente corolario él estudió los poderes de algún número primo.

COROLARIO VIII. Si el número a es simple, cada divisor de este cuadrado aa es una de estos tres $1, a, aa$. y cada divisor de este cubo a^3 uno de los cuatro $1, a, a^2, a^3$ $(\ldots)$. Y así con los otros infinitamente.

Finalmente, el da

COROLARIO IX. Si los números a y b son simples, cada divisor de aab de los tres a, a, b es uno de los tres $1, a, aa$ o uno de los diferentes productos de esos tres por b; es decir, uno de los seis $1, a, aa, 1b, ab, aab$. Porque todos planos alternativos [i.e., obtenidos por la multiplicación de diferentes factores dos a dos] de la simple a, a, b son aa y ab. [Declaración análoga para $aabb; aabb; aab^3cc; aab^3ccd$]. Y así con los otros.

Está claro que Prestet no declara el FTA en su trabajo porque su objetivo era hacer explícito la relación entre cualquier factorización de un número dado en primos y todos los posibles divisores. Sin embargo, los resultados de Prestet son cercanos al FTA, y en el sentido de implicando su corolario IX pueden ser considerados como el equivalente a la unicidad de la factorización prima.

5. DECLARACIONES DE EULER

En su *Vollständige Einleitungzur Algebra* [Euler 1770] Leonard Euler afirmó la existencia de una parte del TFA sin probarlo propiamente, y también hizo una declaración para la parte de unicidad análogo a la Proposición 9 de al-Farisi y al Corolario 9 de Prestet.

En el artículo 41 del capítulo IV de la sección I de la parte I Euler afirmó la existencia de la factorización prima y nos proporcionó una prueba parcial de la misma. Pero su prueba omite algunos detalles.

41. Todos los números compuestos, los cuales pueden ser representados como factores, resulta de los números primos antes mencionados; es decir, todos sus factores son números primos, estos siempre pueden ser descompuestos y representados por dos o más números primos. Cuando tenemos representado, por ejemplo, el número 30 como 5×6, es evidente que 6 no es un número primo, pero usando el producto de 2×3, nosotros podemos tener la representación de 30 como $5 \times 2 \times 3$ o como $2 \times 3 \times 5$; es decir, como factores los cuales todos son números primos

En el artículo 43, por ejemplo, Euler da un método para encontrar la descomposición de cualquier número en sus factores primos:

43. Por lo tanto, es fácil de encontrar un método para el análisis de cualquier número, o su solución en sus factores simples. Que se propone, por ejemplo, el número 360; que la representará primero por 2 x 180. Ahora 180 es igual a 2 x 90, y

90	*Es lo mismo que*	2×45
45	*Es lo mismo que*	3×15

Y por último

15	*Es lo mismo que*	3×5

de modo que el número 360 puede ser representado por los factores simples 2 x 2 x 2 x 3 x 3 x 5, ya que todos estos números multiplicados juntos producir 360.

Euler no declaró la unicidad de la factorización en números primos, pero él hizo una declaración relacionada sin prueba en el artículo 65 del Cap. VI de la Secc. 1 de la Parte 1 de Euler [1770].

65.Cuando, por lo tanto, hemos representado a cualquier número asumidos por placer, por sus factores simples, será muy fácil para exhibir todos los números por los que es divisible. Sólo tenemos, en primer lugar, tomar los factores simples uno por uno, para luego multiplicarlos juntos de dos en dos, de tres en tres, cuatro por cuatro, y así hasta que llegamos al número propuesto.

Observamos que Euler sólo estaba interesado en la búsqueda de todos los divisores de un número y que estaba siguiendo la tradición de al-Farsi y Prestet. En el artículo 65, Euler nos dice que todos los divisores de un número se obtienen a partir de los factores primos que aparecen en la representación del número como un producto de números primos y esta es la única manera de tener todos los divisores de la serie. Por lo tanto, esto puede ser considerado como la unicidad de la factorización en primos. Euler también dio un ejemplo al final del artículo 64: Se deduce que 60, o $2\ x\ 2\ x\ 3\ x\ 5$, pueden dividirse no sólo por estos números simples, también por aquellos que están compuestos de dos cualesquiera de ellos; que es decir, por $4, 6, 10$ y 15, y también por aquellos que están compuestos de cualquiera de tres de sus factores simples, es decir, por $12, 20, 30$, y por último también, por sí mismo 60.

6. LEGENDRE

Aquí le tenemos el enunciado de Legendre que se puede encontrar en [Legendre 1798, art. VIII]:

Cualquier número no primo N puede ser representado por un producto de varios números primos $\propto, \beta, \gamma$, etc, cada uno elevado a alguna potencia, por lo que uno supone que $N = \propto^m \beta^n \gamma^p$, etc

Entonces su prueba inmediatamente sigue así:

El método a seguir para realizar esta descomposición, consiste en tratar de dividir N por cada uno de los números primos 2, 3, 5, 7, 11, etc., a partir de la más pequeña. Cuando la división tiene éxito con uno de estos números$\propto$, se repite tantas veces como es posible, por ejemplo, m veces, y llamar P al último cociente, tenemos

$$N = \propto^m P$$

El número P no puede ser dividido por $\propto$, y es inútil tratar de dividir P por un número primo menos que $\propto$, pero si P fuera divisible por θ, donde θ es menor que $\propto$, está claro que N también sería divisible por θ, en contra de la hipótesis. Por tanto, debemos tratar de dividir P por números primos mayores que $\propto$, por lo que vamos a obtener en la sucesión

$$P = \beta^n Q. \qquad Q = \gamma^p R, \text{ etc.,}$$

Por lo que tenemos que $N = \propto^m \beta^n \gamma^p$, etc.

Como vemos en esta prueba, para cualquier número siempre tenemos la misma descomposición en factores primos de acuerdo al método de Legendre. Es evidente que no podemos suponer que esto es equivalente a la parte de la unicidad de la TFA. Sin embargo, una declaración relacionada con la unicidad se da en el artículo X:

Un número N se expresa en la forma $\propto^m \beta^n \gamma^p$, etc, cada divisor de N también será de la forma $\propto^\mu \beta^\sigma \gamma^\pi$, etc, donde los exponentes μ, σ, π, etc, no son mayores [uno a uno] quem, n, p, etc.

En este artículo, de hecho, Legendre se propone a encontrar el número de todos los divisores de un número, y al mismo tiempo la suma de estos divisores. De esta afirmación se puede demostrar la unicidad.

7. GAUSS

Gauss dio la propiedad de factorización única para los enteros positivos en el artículo 16 de su *Arithmeticae Disquisitiones* [Gauss 1801]. En la sección II se abre con el siguiente artículo.

13. Teorema. El producto de dos números positivos, más pequeños que un número primo dado, no puede dividirse por este número primo.

Entonces Gauss reproduce el Teorema VII.32 de los *Elementos* de Euclides y su generalización.

14. si ni a ni b pueden dividirse por un número primo p, tampoco el producto ab puede dividirse por p.

15. Si ninguno de los números a, b, c, d, etc., puede dividirse por un número primo p, tampoco puede dividirse por p elproducto $abcd$ etc.

Aquí tenemos su artículo 16.

16. Teorema. Cualquier número compuesto puede resolverse en factores primos de una manera única

Gauss mismo no especificó una prueba de la existencia de parte del TFA. Afirmó que es claro de las consideraciones elementales, lo cual es correcto. Comenzó su demostración al afirmar que "es evidente a partir de consideraciones elementales que cualquier número compuesto se puede descomponer en factores primos, pero se supone tácitamente y por lo general sin pruebas de que esto no se puede hacer de muchas maneras diferentes". Luego él considera un número compuesto $A == a^{\propto}b^{\beta}c^{\gamma}$ etc., con$a, b, c,$ etc números primos desiguales y mostró que A no puede ser resuelto en factores primos de otra manera con otros primos excepto a, b, c, etc., o que tiene unos números primos que aparecen en una descomposición más frecuencia que en la otra.

Por lo tanto, la primera declaración clara y prueba del TFA parece haber sido dada por Gauss en su *Disquisitiones Arithmeticae*. Desde entonces muchas pruebas diferentes se han dado. En [Agargün & Fletcher 1997], hemos investigado diferentes pruebas del TFA y las clasificamos.

REFERENCIAS

Agargün, A. G. & Fletcher, C. R. 1994. al-Farisi and the Fundamental Theorem of Arithmetic. Historia Mathematica 21, 162-173.

----------1997. The fundamental theorem of arithmetic dissected. Mathematica Gazette 81, No. 490, 53-57.

Euler, L. 1770.*VollständigeEinleitungzur Algebra.* St. Petersburg; French translation with *Additions* by Joseph L. Lagrange. Lyon, 1774; republished in Vol. 7 of Lagrange's *Oeuvres* and in Vol. (1)1 of Euler's *Opera;* English translation *Elements of Algebra* [trans. John Hewlett, London, 1840], reprinted Berlin/Heidelberg/New York: Springer-Verlag, 1985.

Gauss, C. F. 1801.*DisquisitionesArithmeticae.* Leipzig; Translated into English by A. C. Clarke. New Haven, CT: Yale Üniversity Press, 1966.

Goldstein, C. 1992. On a seventeenth century version of the fundamental theorem of arithmetic. *Historia Mathematica* 19, 177-187.

Heath, T. L. 1908. *The Thirteen Books of Euclid's Elements,* Vol. 2. Cambridge, UK: Cambridge University Press.

Hendy, M. D. 1975. Euclid and the Fundamental Theorem of Arithmetic. *Historia Mathematica* 2, 189-191.

Hogendijk, J. P. 1985. Thabit ibn Qurra and the pair of amicable numbers 17296, 18416.*HistoriaMathematica*12, 269-273.

Knorr, W. R. 1976. Problems in the interpretation of Greek number theory: Euclid and the Fundamental Theorem of Arithmetic. *Studies in the History and Philosophy of Science* 7, 353-368.

Legendre, A. M. 1798.*Théorie des Nombres,* 3rd ed. Paris: FirminDidot, 1830; reprinted Paris: Hermann, 1990.

Mullin, A. A. 1965. Mathematico-philosophical remarks on new theorems analogous to the Fundamental Theorem of Arithmetic. *Notre Dame Journal of Formal Logic* VI, No. 3, 218-222.

Rashed, R. 1982. Matériauxpourl'histoire des nombres amiables. *Journal for the History of Arabic Science* 6, 209-278.

Tabla de ilustraciones

Ilustración 1: Euclides 11
Ilustración 2: al-Farisi 12
Ilustración 3: Leonhard Paul Euler 13
Ilustración 4: Adrien-Marie Legendre 14
Ilustración 5: Johann Carl Friederich Gauss 15
Ilustración 6: Proposiciones y definiciones relacionadas en la demostración de la proposición VII.30 18
Ilustración 7: Diagrama de las proposiciones utilizadas para demostrar la proposición 9 32

Bibliografía

Agargün, A., & Fletcher, C. (1994). al-Farisi and the Fundamental Theorem of Aritmetic. *Historia Mathematica, 21*, 162-173.

Agargün, A., &Özkan, E. (2001). A Historical Survey of the Fundamental Theorem of Arithmetic. *Historia Mathematica* , 207-214.

Chadid, I. C. (1996). *El más prolífico en la historia de las Matemáticas Leonhard Euler.* México, D.F.: Grupo Editorial Iberoamérica, S.A.

Duran, A. J. (2002). La matemática y sus elementos: de Euclides a Bourbaki. *LA GACETA DE LA RSME, Vol 5.3* , 649-672.

Euler, L. (1770). *Vollständige Einleitung zur Algebra.*(J. Hewlett, Trans.) St Petersburg.

Gauss, C. F. (1801). *Disquisitiones Arithmeticae.* (H. Barrantes, M. Josephy, & A. Ruiz, Trans.)

Goldstein, C. (1992). On a Seventeenth Century Version of the "Fundamental Theorem of Aritmetic". *Historia Matematica, 19* (2), 125-231.

Guacaneme, E. A. (2011). *La historia de las Matemáticas en la educación de un profesor: razones e intenciones.* XIII CONFERENCIA INTERAMERICANA DE EDUCAÇAO MATEMATICA.

Guacaneme, E. A. (2007). *Una aproximación a la relación Historia de las Matemáticas - Conocimiento del profesor de matemáticas.* Tercer encuentro de programas de formación inicial de profesores de matemáticas.

Heath, T. (1908). *The Thirteen Books Of Euclid's Elements.*Cambridge.

Hernández, P. G. (2006, Diciembre). CARL FRIEDRICH GAUSS, ESTUDIO DE SU OBRA “DISQUISITIONES ARITHMETICAE” Y CONSTRUCCIÓN DE POLÍGONOS REGULARES CON REGLA Y COMPÁS. Madrid.

Hogendijk, J.P.1975Thabit ibn Qurra and the pair of amicable numbers 17296, 18416.*Historia Mathematica12*3269-273

León, E. (2009). La Gema de la Reina: Una breve revisión histórica de la ley de reciprocidad cuadrática. *Lecturas Matemáticas, 30*, 17-27.

MEN. (1998). *Lineamientos curriculares de matemáticas.* Bogotá, D.C.: Ministerio de Educación Nacional.

Pettofrezzo, A., & Byrkit, D. (1972). *Introducción a la Teoría de Números.* (R. Pomareda, Trans.) Chile: Pretice/Hall International.

Rico, L. Marín, A. Lupiañez, J. Gomez, P. (2008). Planificación de las matemáticas escolares en secundaria. El caso de los números naturales. *Suma* , 7-23.