**UNIVERSIDAD NACIONAL AUTÓNOMA**

**DE MÉXICO**

**FACULTAD DE CIENCIAS**

# El estudio de Gauss en la Sección VII del libro *Disquisitiones Arithmeticae* sobre la constructibilidad de polígonos regulares.

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE:**

**Matemática**

**P R E S E N T A :**

**Luz Olivia Castillo Pioquinto**

**DIRECTOR DE TESIS:**

**Mat. César Guevara Bravo**

**2016**

Ciudad Universitaria, D. F.

1. Datos del alumno
   Castillo
   Pioquinto
   Luz Olivia
   2224170173
   Universidad Nacional Autónoma de México
   Facultad de Ciencias
   Matemáticas
   410022896

2. Datos del tutor
   Mat.
   Julio César
   Guevara
   Bravo

3. Datos del sinodal 1
   Dr.
   Carlos
   Álvarez
   Jiménez

4. Datos del sinodal 2
   Mat.
   Ernesto
   Mayorga
   Saucedo

5. Datos del sinodal 3
   Mat.
   Emiliano
   Geneyro
   Squarzon

6. Datos del sinodal 4
   M. en F.C.
   María del Pilar
   Piñones
   Contreras

7. Datos de la tesis
   El estudio de Gauss en la Sección VII del libro *Disquisitiones Arithmeticae* sobre la
   constructibilidad de polígonos regulares.
   86 p
   2016

*Los encantos de esta ciencia sublime, las matemáticas, solo se le revelan a aquellos que tienen el valor de profundizar en ella.*

*Carl Friedrich Gauss*

# Agradecimientos

A mis padres. Gracias por el amor, por hacerme su prioridad, por el esfuerzo para darme lo mejor, y por apoyarme en todos los planes que hice. Ustedes siempre serán mi hogar, mi lugar seguro, a donde puedo regresar cuando no me quede nada más. Los amo y siempre los tendré presentes.

A mi profesor, quien a pesar de las circunstancias en las que este trabajo se llevó acabo se ha tomado el tiempo para transmitirme sus conocimientos para finalizar mi tesis con éxito.

A mis sinodales, por el tiempo que dedicaron a la revisión de este trabajo y sus valiosos comentarios.

# Contenido

Introducción ..... IV

CAPITULO I. *Disquisitiones Arithmeticae* ..... 6

1.1 De las congruencias de los números en general. ..... 6
1.2 Sobre las congruencias de primer grado. ..... 8
1.3 Sobre los residuos de potencias ..... 10
1.4 Sobre las congruencias de segundo grado. ..... 14
1.5 Sobre las formas y las ecuaciones indeterminadas de segundo grado. ..... 17
1.6 Aplicaciones varias de las secciones anteriores. ..... 22

CAPITULO II. Sobre la irreductibilidad del polinomio $x^{n-1} + x^{n-2} + \cdots + x + 1$ con $n$ primo ..... 23

CAPITULO III. Descomposición del polinomio $x^{n-1} + x^{n-2} + \cdots + x + 1$ y las soluciones por radicales de sus raíces ..... 33

Períodos Gaussianos ..... 33
Las soluciones del polinomio. ..... 54

Intercapítulo ..... 64

CAPITULO IV. Sobre la construcción de polígonos regulares. ..... 67

División del círculo en $n$ partes. ..... 67
Caso del pentágono construible ..... 71
Caso del polígono de 17 lados ..... 74
Generalización para cualquier entero ..... 77

Conclusión ..... 83

# Introducción

*Johann Carl Friedrich Gauss* nació el 30 de abril de 1777 en Brunswick, Alemania. En 1784, a la edad de 7 años, entró al St. Katharin Volksschule donde recibió la instrucción básica que estuvo a cargo del profesor J. G. Büttner. Dos años después entró a clases de aritmética y fue ahí donde se dice que ocurrió uno de los eventos más sobresalientes del joven Carl. En una ocasión su maestro, Büttner, le dijo a sus alumnos que sumaran los números del 1 al 100, y casi inmediatamente Gauss escribió el resultado en su pequeña pizarra y la dejó en el escritorio del profesor diciendo "¡Ligget se!" (¡Ahí está!). Había escrito un número: 5050, la respuesta correcta. Explicó a su profesor que se había percatado que

$$100 + 1 = 101,$$
$$99 + 2 = 101,$$
$$98 + 3 = 101, \text{ etc.},$$

y que había tantas parejas de estas como números pares entre 1 y 100, entonces, la respuesta era $50 \cdot 101 = 5050$. El profesor Büttner quedó impresionado por el pequeño Gauss, así que en 1788 lo ayudó para que fuera admitido en la escuela secundaria.

El 30 de marzo de 1796, el joven estudiante de 19 años, hizo un descubrimiento que sería determinante en su futuro, probó que era posible construir solo con regla y compás el polígono regular de 17 lados. De hecho, cuando Gauss entró a la Universidad de Gôttinge en 1795, no estaba seguro si debía de estudiar matemáticas o filosofía, pero después del descubrimiento del polígono se animó a estudiar matemáticas.

Alrededor de 1798, se estaban terminando de gestar las *Disquisitiones Arithmeticae*, uno de los más grandes aportes a la matemática, escrito por Carl Friedrich Gauss, pero publicado hasta 1801. En este trabajo, dividido en VII secciones, él recopila una gran cantidad de resultados aritméticos, algunos ya estudiados por otros matemáticos como Lagrange, Euler, Legendre y Fermat, y otros que desarrolló él.[1] Varios de estos resultados corresponden a la teoría de residuos; es decir, a las clases residuales y esto será de gran importancia en el estudio de la sección VII, que es el tema principal en este trabajo.

Los residuos de potencias ya eran estudiados por Euler, de hecho él los usa en su tercera (1755) y cuarta demostración (1758) del *Pequeño Teorema de Fermat*, esta última se en-

[1] Sin embargo, Gauss decide incluir estos resultados en su libro, por un lado, debido a que hasta entonces no había ningún libro que pusiera juntos los trabajos de otros matemáticos y por otro, a que muchos fueron tratados por nuevos métodos, además los resultados de las últimas tres secciones están ligados a los primeros.

cuentra en el artículo "*Theoremata arithmetic nova método demonstrata*".[2] Sin embargo, fue Gauss quien fundamentó esta teoría a la que actualmente se le conoce como aritmética modular y que es una rama importante de la teoría de números.

Otro resultado de gran importancia es el teorema fundamental de la aritmética, y aunque este teorema apareció de manera implícita, por primera vez en los *Elementos* de Euclides –se obtiene a partir de las proposiciones 30 y 31 del libro VII–, fue Gauss quien lo enunció de la forma que actualmente se conoce, y además proporcionó la primera demostración completa. De manera semejante la ley de la reciprocidad cuadrática ya había sido planteada por Euler, y posteriormente enunciada por Legendre –él dio una prueba pero se basaba en argumentos no probados–, pero fue Gauss quien finalmente la demostró en sus *Disquisitiones.*

En esta tesis, en el capítulo I se dará un panorama general acerca de lo que Gauss trata en las primeras seis secciones de las *Disquisitiones Arithmeticae.* Esto se hace con la finalidad de poner en contexto al lector, la intención no es hacer un análisis detallado acerca de estas secciones.

En los capítulos II, III y IV, se pretende analizar detalladamente la sección VII de las *Disquisitiones Arithmeticae*, y esto se debe a que se ha detectado que existen en la literatura matemática múltiples trabajos donde mencionan y retoman algunas partes de esta sección, pero no es fácil encontrar un estudio global de esta parte. La ruta que se seguirá será en tres partes. Primero, en el capítulo II, inicia el estudio sobre la sección VII y específicamente se probará la irreductibilidad de las ecuaciones ciclotómicas de grado primo, $x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$. Segundo, en el capítulo III, con la introducción de los *períodos* formados por las raíces de esta ecuación se mostrarán las posibles descomposiciones de las ecuaciones ciclotómicas y que es posible hallar sus raíces en expresiones con radicales, esto se hará resolviendo ecuaciones de grado menor a las que se llamarán "auxiliares". Por último, en el capítulo IV, se mostrará la conexión entre las raíces $n$-ésimas de la unidad, esto es, entre las raíces de la ecuación $x^n - 1 = 0$ y la construcción de polígonos regulares con regla y compás. Esto consiste en analizar en que casos esas raíces pueden expresarse de tal manera que los únicos radicales que contengan sean cuadráticos, pues se sabe que las raíces cuadradas son construibles. Además, se exhibe la relación entre polígonos construibles y primos de Fermat.

[2] Es el articulo E271, esta clasificación corresponde a la de Gustav Eneström, el archivo completo de los trabajos de Euler se pueden consultar libremente en http://eulerarchive.maa.org

# Capítulo I

## *Disquisitiones Arithmeticae*

### 1.1 De las congruencias de los números en general.

En la primera sección de las *Disquisitiones*, la cual consta de tan solo seis páginas con 12 artículos, Gauss expone algunas nociones básicas de la Aritmética Superior. Él concibe esta subárea como una parte de la Aritmética que abarca todas las propiedades que considera imprescindibles de los números enteros. Los primeros conceptos que menciona son el de congruencia (incongruencia) y el de residuo (no residuo):

> *"Si un número $a$ divide la diferencia de los números $b$ y $c$, se dice que $b$ y $c$ son congruentes según el módulo $a$. Los números $b$ y $c$ son llamados uno residuo del otro."*

En su obra Gauss introduce la notación $a \equiv b (\mathrm{mod}\, c)$ –es el primero que lo hace y es la que se usa actualmente– para referirse a la congruencia de $a$ y $b$ según el módulo $c$. Además, con una nota a pie menciona que elige este símbolo debido a la analogía entre igualdad y congruencia. Cabe mencionar, que durante todo el proceso que le lleva a mostrar las condiciones suficientes para la construcción de polígonos regulares con regla y compás, el concepto de congruencia le será de gran utilidad en la sección VII de sus *Disquisitiones,* así como también lo serán las propiedades que de él se deriven, por ejemplo las clases residuales que se mencionan en el siguiente párrafo.

En el primer teorema [art. 3] de las *Disquisitiones* se muestra que dados $m$ números consecutivos y un entero $n$, este deberá ser congruente a uno y solo uno de aquellos, módulo $m$. De hecho, estos $m$ números consecutivos forman lo que ahora se conoce como un *sistema completo de residuos* módulo $m$. Particularmente a los números consecutivos $0, 1, 2, \ldots, m-1$, y $0, -1, -2, \ldots, -(m-1)$, les llama *residuos mínimos*. Además, exhibe que para cualquier número, este tendrá un residuo mínimo –positivo o negativo– menor que $\frac{m}{2}$, al que se llamará *residuo absolutamente mínimo.*

En los artículos del 5 al 8 analiza algunas propiedades sobre congruencias. Por ejemplo,

I) si el módulo es un número compuesto entonces la congruencia se preserva módulo un factor de dicho número compuesto;

II) las congruencias satisfacen la propiedad transitiva bajo el mismo módulo.

Cabe notar que el lenguaje utilizado por Gauss, en gran medida, se sigue empleando actualmente. De hecho, el contenido de esta sección y la presentación de la misma son muy parecidos al contenido que se puede encontrar en los primeros capítulos de textos actuales sobre teoría de números.

De regreso al libro, algo importante que se menciona en el artículo 8, es que si se tiene que los enteros $a_1, a_2, a_3$ ... son congruentes con $b_1, b_2, b_3$ ... módulo $m$, respectivamente, entonces $a_1a_2a_3 \ldots \equiv b_1b_2b_3\ldots (mod\ m)$. De esto se deduce que las potencias también preservan la congruencia bajo el mismo módulo. Esto último es importante porque ayuda a mostrar en el siguiente artículo que si se tienen dos números congruentes $a$ y $b$, entonces al evaluar dichos números en un cierto polinomio $P(x)$, la congruencia entre $P(a)$ y $P(b)$ se preserva.

Otro resultado interesante respecto a polinomios es que los residuos mínimos módulo $m$ de los valores obtenidos al evaluar números enteros consecutivos en un polinomio son periódicos y tienen periodo $m$.[3]

Posteriormente Gauss da un ejemplo que lo lleva a enunciar un criterio para saber cuándo una congruencia de grado $n$ tiene solución, y lo aborda más, aunque menciona que sería tratado en la sección VIII, sin embargo dicha sección no fue publicada.

Finalmente, en el último artículo, Gauss muestra cómo se puede aplicar la teoría de congruencias para hallar algún criterio acerca de la divisibilidad de un número dado por otro. Algunos de los criterios que enuncia son los siguientes:

1. Un número entero $z = a_n a_{n-1} \ldots a_1 a_0$, donde las $a_i$ son dígitos, es divisible por 3 (o por 9) si y solo si la suma $a_0 + a_1 + a_2 + \ldots + a_n$ es divisible por 3 (o por 9, respectivamente).
2. Un entero $z = a_n a_{n-1} \ldots a_1 a_0$ es divisible por 11 si y solo si la suma $a_0 - a_1 + a_2 - \ldots + (-1)^n a_n$ es divisible por 11.

Es importante decir que en las *Disquisitiones* Gauss no se limitó a exponer solo teoría matemática, con frecuencia proporcionaba ejemplos o aplicación correspondientes a la teoría.

[3] No implica que los residuos cubran todo un sistema completo de residuos módulo $m$

## 1.2 Sobre las congruencias de primer grado.

El tema central de la segunda sección es la resolución de las congruencias de primer grado $ax + b \equiv c(mod\ m)$. Para exponer este tema Gauss primero presenta algunos resultados preliminares, a los que llama "teoremas preparatorios sobre números primos", entre ellos el *Teorema fundamental de la aritmética:*

> *"Cualquier número compuesto puede descomponerse en factores primos de manera única."*

Este teorema ya había sido estudiado por Euclides, quién realizó una prueba constructiva.[4] Gauss completa la demostración de la unicidad de la descomposición.
La descomposición en primos de un número permite conocer cuáles son sus divisores y además permite hallar el *máximo común divisor* y el *mínimo común múltiplo*. Gauss introduce estos dos conceptos brevemente en el artículo 18, de hecho sólo explica cómo hallarlos a partir de la descomposición en primos e ilustra esto con un ejemplo.

En los artículos 19, 20 y 21 presenta una serie de teoremas relativos a números primos, que posteriormente ocupará en la teoría de congruencias. En el artículo 22 retoma los teoremas sobre congruencia y muestra cuando se preserva esta al dividir entre un factor común los residuos, bajo el mismo módulo.

Después, muestra que la expresión $ax + b \equiv c(mod\ m)$, con $a$ y $b$ números dados, tiene solución para $x$, siempre que $a$ y $m$ sean primos relativos. Además, analiza las posibles soluciones de esta congruencia y utilizando artículos previos, llega a la conclusión de que todas las soluciones serán congruentes entre sí y por tanto se considerarán como una sola. Posteriormente exhibe una manera general con la que se puede encontrar la solución y para esta utiliza el algoritmo de Euclides.

Cabe mencionar que el desarrollo de sus cálculos puede sorprender al lector, ya que la manera de tratar este tema es como se realiza actualmente, y esto es algo que sucede a lo largo de todo el libro.

Gauss enseguida analiza el caso para la congruencia $ax + t \equiv u(mod\ m)$ donde $m$ y $a$ no son primos relativos, y en este caso el elemento base para llegar a la solución está en usar el máximo común divisor de $a$ y $m$. Aquí concluye que el conjunto de soluciones está dado por la congruencia $x \equiv v(mod\ f)$, donde $v$ es uno de los valores de $x$ y $f$ es el cociente del módulo $m$ entre el máximo común divisor de $a$ y $m$.

También menciona que para la congruencia $ax \equiv b(mod\ m)$, donde $m$ es un módulo compuesto, en ocasiones es apropiado descomponer dicho módulo en factores, y enseguida se resuelven tantas congruencias como factores se indican en el módulo. Por

[4] Exhibe, en la proposición 32 del libro VII de los elementos que no es posible un proceso infinito en el que se encuentren una cantidad infinita de divisores de un número natural finito. Véase Euclides [1994].

ejemplo, si $m = nn'$, entonces la congruencia original ahora se canaliza a resolver dos congruencias módulo $n'$ y $n$. En caso de que $n'$ y $n$ sean números compuestos se vuelve a hacer este procedimiento; de hecho como bien muestra Gauss en el ejemplo que presenta, esta descomposición del módulo podría ser hasta llegar a los primos si es conveniente.

En los artículos inmediatos Gauss describe varios métodos para hallar los números congruentes a un número dado según un módulo dado, y en cada uno, como siempre, lo clarifica con un ejemplo.

En el artículo 37 aborda las congruencias lineales con varias incógnitas, y en este punto aclara que sólo tratará parcialmente las partes que merezcan la atención, debido a que si se estudia con todo rigor entonces llevaría mucho tiempo y espacio. En la primera observación señala que en el caso de varias incógnitas, así como en las ecuaciones, se deben tener tantas congruencias como incógnitas. Posteriormente utiliza la teoría de las ecuaciones lineales y la teoría desarrollada en los artículos precedentes para hallar la solución del sistema de congruencias, omite algunos detalles formales en los argumentos, pero estos se entenderán a través de ejemplos.

Con lo anterior finaliza la investigación sobre la resolución de congruencias de primer grado, e introduce lo que ahora se conoce como la función $\varphi$ de Euler, la que cuenta el número de enteros positivos que son primos a un número dado y menores que él. Aunque Gauss fue quien introdujo esta notación, fue Euler quien aporto el concepto y derivó la mayoría de sus propiedades en el artículo *"Theoremata arithmetica nova methodo demonstrata"* en 1760.[5] Al respecto Gauss menciona y demuestra algunas propiedades sin dejar de reconocer que ya habían sido probadas por el "ilustre Euler". Una de ellas es que $\varphi$ satisface lo siguiente:

> *Si $A$ es un número que puede descomponerse en factores $a, b, c$, etc. primos entre sí entonces* $\varphi(A) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \cdot \dots$ .

Desde la perspectiva actual decimos que es una función multiplicativa.

En el artículo 39 Gauss modifica ligeramente la definición de $\varphi A$, ahora la define como el número de enteros que son primos con $A$ y menores o iguales a $A$. Este cambio no afecta al cálculo de la función, salvo para $\varphi 1 = 0$ que ahora será $\varphi 1 = 1$.[6]

Con base en esta definición Gauss deriva el siguiente teorema:

> *Si $a, a', a'', \dots$ son todos los divisores de $A$ se tendrá que*
> $\varphi a + \varphi a' + \varphi a'' + \cdots = A.$

[5] Sandifer, Charles (2007), The early mathematics of Leonhard Euler, p. 203.

[6] En la definición original, Euler solo consideraba a los enteros estrictamente menores a $A$, y por ello se tenía que $\varphi 1 = 0$.

En el penúltimo artículo [art. 42] demuestra el siguiente teorema que en álgebra actualmente se conoce como el "lema de Gauss",

*Sean*

$$x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0 \qquad (P)$$
$$x^\mu + b_{\mu-1}x^{\mu-1} + b_{\mu-2}x^{\mu-2} + \cdots + b_0, \qquad (Q)$$

*polinomios cuyos coeficientes son todos racionales* (*no todos enteros*), *entonces* **no** *todos los coeficientes del producto de* $(P)$ *y* $(Q)$ *pueden ser enteros.*

A grandes rasgos la prueba la realiza de la siguiente manera, primero, expresa los coeficientes fraccionarios de $(P)$ y $(Q)$ en su forma reducida, después elige un primo $p$ que divida al menos a uno de los denominadores de $(P)$. A continuación hace notar que al dividir $(Q)$ entre $p$, el polinomio resultante $\frac{(Q)}{p}$ tendrá por lo menos un coeficiente cuyo denominador es un múltiplo de $p$. Luego, de entre todos los coeficientes de $(P)$ que son fracciones elige la fracción –llámese $Gx^g$ al término correspondiente– cuyo denominador tiene como factor una potencia de $p$ que es mayor que el resto de las potencias que aparecen en los denominadores de las otras fracciones, y algo similar hace con $\frac{(Q)}{p}$, en este caso el término será $\Gamma x^\gamma$. Finalmente, muestra que el coeficiente correspondiente al término $x^{g+\gamma}$ en el producto de $(P)$ y $(Q)$ es una fracción, y con esto se ha probado la proposición.

Este resultado se usará en el art. 341 como auxiliar en la prueba de la irreducibilidad del polinomio ciclotómico.

El último teorema que presenta, muestra que el número máximo de raíces que puede tener una congruencia de $m$-ésimo grado

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots + Mx + N \equiv 0 \ (mod\ p),$$

donde $p$ es un primo que no divide al coeficiente principal, es $m$, *i.e.,* no pueden existir más que $m$ raíces incongruentes módulo $p$.

Gauss no fue el primero en demostrar este teorema, Lagrange ya lo había probado en *Mémoires de l'Académie royale de Berlin* y también había sido mostrado por Legendre en *Recherches d'Analyse indéterminée* [*Mémoires in Histoire de l'Académie Royale des Sciences,* p. 465].

## 1.3 Sobre los residuos de potencias.

En esta sección Gauss estudia los números $b$, tal que la congruencia $x^n \equiv b \ (mod\ p)$ es soluble y a estos se les conoce como $n$-ésimo residuo de potencia módulo $p$.

Empieza mostrando cómo son los residuos de los términos en una progresión geométrica, $1, a, a^2, a^3, \ldots$. Siempre habrá un término $a^t$ en la progresión que será congruente con la unidad según un módulo $p$, primo con $a$ y tal que $t < p$. Esta característica de las progresiones de este tipo es la base para la existencia de las raíces primitivas que se definen más adelante.

Para cualquier $a^r$ con $r = mt + k$ ($r$ congruente con $k$ módulo $t$) se tendrá que es congruente con $a^k$ módulo $p$. Esto es,

$$\text{Si } r \equiv k \ (mod\ t), \text{ entonces } a^r \equiv a^k (mod\ p). \qquad \text{[art. 46]}$$

De esto último Gauss obtiene un método para hallar los residuos de cualquier potencia. Por ejemplo, si se busca el residuo de $6^{2207}$ módulo 7, se considera a $k = 2$, y como $2207 \equiv 2(mod\ 3)$, entonces

$$6^{2207} \equiv 6^2 \equiv 1 \ (mod\ 7).$$

Enseguida, Gauss induce [art. 48] que si se asume que $a^t$ es la menor potencia congruente con la unidad[7], entonces los residuos de $1, a, a^2, a^3, \ldots, a^{t-1}$ son diferentes. Así, se puede concluir que si se tiene $a^r$ congruente con $a^k$ módulo $p$, entonces $r$ será congruente con $k$ módulo $t$. Por lo tanto, de los artículos 46 y 48 se deduce que:

Si $(a, p) = 1$ y $t$ es el orden de $a$ módulo $p$, entonces,

$$a^n \equiv 1(mod\ p) \textit{ si y solo si } t|n.$$

En el artículo 49 Gauss empieza a trabajar con módulos primos, en particular en este artículo demuestra que

*si $p$ es un primo que no divide a $a$ y $a^t$ es la mínima potencia de $a$ congruente a la unidad módulo $p$, entonces $t = p - 1$, o un factor de él.*

Este teorema dice que el orden de $a$ módulo $p$ estará entre los divisores de $p - 1$ y será fundamental para la demostración del teorema de Fermat, actualmente conocido como el "pequeño teorema de Fermat",[8]

$$\text{si } p \textit{ es un primo que no divide a } a, \textit{ entonces } a^{p-1} \equiv 1(mod\ p).$$

En el artículo 51 Gauss demuestra el siguiente teorema:

*Si $p$ es un número primo se tendrá que*

$$(a + b + c + \ldots)^p \equiv a^p + b^p + c^p + \ldots (mod\ p),$$

y como caso particular de este se obtiene otra demostración del pequeño teorema de Fermat.

---

[7] En el lenguaje actual a dicha $t$ se le conoce como el orden de $a$ módulo $p$.

[8] Fermat enunció por primera vez este teorema en una carta con fecha del 18 de octubre de 1640 dirigida a su amigo Bernard Frénicle, pero como en otras ocasiones Fermat no incluyó demostración alguna argumentando que era demasiado extensa. El primero en publicar una demostración fue Euler en *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T. VIII.*, y su demostración la hizo por inducción utilizando el método de descenso infinito de Fermat. Euler generalizó el teorema en 1760 introduciendo la función $\varphi(p)$ –recordemos que la notación fue introducida por Gauss–.

En el art. 52 Gauss retoma elementos del art. 49, respecto a que el orden de un número debe estar entre los divisores de $p-1$. Plantea la pregunta de si todos los divisores son exponentes de potencias congruentes a la unidad, es decir, si para cada divisor $d$ de $p-1$ existen números $b$ tales que $b^d \equiv 1\ (mod\ p)$ y en tal caso cuántos de ellos hay. En el proceso de responder a esta interrogante define $\psi(d)$ como el número de enteros menores que $p$ cuyo orden es $d$ módulo $p$ –Gauss utiliza la expresión "*$a$ pertenece al exponente $d$*" para decir que $a$ tiene orden $d$–. Luego demuestra que $\psi(d)$ coincide con la cantidad de números menores que $d$ y primos a él, es decir, con $\varphi(d)$.

Después como caso particular de lo anterior, introduce la noción de *raíz primitiva*, que son aquellos números cuyo orden es $p-1$ módulo $p$, la existencia de estos números la justifica probando los siguientes puntos:

I. Sea $p-1 = a^\alpha\ b^\beta\ c^\gamma$ ... la descomposición en primos de $p-1$. Siempre puede encontrarse números $A, B, C,$ etc. cuyo orden es respectivamente $a^\alpha, b^\beta, c^\gamma,$ etc.

II. El producto de los números $A, B, C,$ etc. tiene orden $p-1$.

Estos números tan peculiares ya habían sido estudiados por Lambert y Euler, sin embargo, el primero de ellos no considero necesaria una prueba de su existencia, y según Gauss la prueba de Euler tenía dos defectos; uno, que asume que $x^n - 1$ tiene $n$ soluciones diferentes, dos que una de las fórmulas que utilizó la demostró solo por inducción.

De acuerdo a la definición, si $g$ es una raíz primitiva se tendrá que los residuos mínimos módulo $p$ de las potencias $g, g^2, g^3, \dots, g^{p-1}$ son diferentes entre sí y por tanto ellos son $1, 2, 3, \dots, p-1$. Cabe destacar que esta noción de raíz primitiva cobrará relevancia en el capítulo III del presente trabajo, especialmente en el art. 343 donde será la base para la distribución de las raíces del polinomio $x^{n-1} + x^{n-2} + \cdots + x + 1$ ($n$ primo) en períodos y estos a su vez serán útiles para hallar soluciones por radicales de dichas raíces.

A continuación, define el índice de un número, esto lo hace como sigue, elige una raíz primitiva $a$ (base) tal que $(a,p) = 1$ y si $a^e \equiv b(mod\ p)$ entonces $e$ será el índice de $b$ y es único debido a que $a, a^2, a^3, \dots, a^{p-1}$ forman un sistema reducido de residuos módulo $p$. Se debe notar que el índice dependerá de la raíz primitiva que se elija y por supuesto también de $a$ y $b$. Con esta definición enuncia algunos teoremas acerca de los índices, estos son análogos a las propiedades que se tienen con los logaritmos.

En lo que sigue utiliza lo visto sobre la resolución de congruencias de primer grado en la sección anterior, así como las nociones de índices, para averiguar en qué caso, y cómo, la congruencia de la forma $x^n \equiv A(mod\ p)$ tiene solución. Resolviendo esto se

sabrá si $A$ es un $n$-ésimo residuo de potencia y de qué potencias.
Primero empieza analizando el caso en el que $A \equiv 1(mod\ p)$ y llega a la conclusión de que las congruencias $x^n \equiv 1(mod\ p)$, pueden reducirse a las de la forma $x^m \equiv 1(mod\ p)$, donde $m$ es un divisor de $p-1$, de hecho $m = (n,\ p-1)$.
Posteriormente generaliza esto para cualquier $A$, y así se enfoca en estudiar las congruencias $x^n \equiv A(mod\ p)$, donde $n$ es un divisor de $p-1$.

En el proceso Gauss obtiene un criterio para saber cuándo un número es o no residuo cuadrático módulo $p$. Esto ya había sido estudiado por Euler y Lagrange, y trata este tema con mayor detalle en la sección III.

Regresando a la solución de las congruencias $x^n \equiv A(mod\ p)$, donde $n$ es divisor de $p-1$, Gauss explica cómo pueden hallarse los valores de esta a partir de un valor conocido y dependiendo también de si $A$ es congruente o incongruente con 1 módulo $p$. En el último caso es necesario conocer las soluciones de $x^n \equiv 1\ (mod\ p)$.
Sin embargo, mostrar los artificios para resolver estas expresiones no fue su objetivo en la segunda sección, así que regresa al estudio de los índices y las raíces primitivas. Lo primero que muestra es que, así como con los logaritmos, si se tiene una tabla de índices en un sistema de base $a$ se puede obtener otra en base $b$, salvo que con los índices se tiene un número finito de sistemas –tantos como raíces primitivas–.

Posteriormente Gauss muestra –de manera teórica y con un ejemplo– un algoritmo más allá del método por tanteo para hallar raíces primitivas, ya habiendo mostrado la existencia de estas en el artículo 55 y usando algunos hechos sobre la solución de $x^n \equiv 1(mod\ m)$. Cabe mencionar que aunque Euler hizo una tabla de todas las raíces primitivas de cada primo $p \leq 41$ en *Opuscula Analytica* Vol. I, él no conocía algún algoritmo para hallarlas.[9]

A continuación presenta el Teorema de Wilson,

> *"el producto de todos los números menores que un número primo dado, sumado a uno, es divisible* por *este primo, esto es,* $(p-1)! \equiv -1\ (mod\ p)$",

como un caso particular de un teorema previo sobre el producto de los términos del período de un número.[10]
La demostración de Gauss se basa en demostrar que los números $2, 3, \ldots, p-2$ son *asociados.* [11]

---

[9] L.E. Dickson, *History of the theory of numbers,* Vol. I, *p.* 181.
[10] El primero en publicar este teorema fue E. Waring en *Meditationes Algebraicae* en 1770, quien se lo atribuyó a John Wilson, uno de sus estudiantes (véase Øystein Ore, *Number Theory and Its History*, p.259.) Pero ninguno dio una demostración hasta 1782 que Waring presentó una en la tercera edición de sus *Meditationes.* Sin embargo, el primero en publicar una prueba de este teorema fue J. L. Lagrange en 1770.
[11] $a$ y $b$ son asociados según el módulo $p$ si su producto es congruente con 1 módulo $p$, además, contémplese que 1 y $p-1$ son asociados de sí mismos.

Después de esto Gauss, sin dar muchos detalles de cómo lo dedujo, presenta una extensión del teorema a un módulo cualquiera:

> *"el producto de todos los números, a la vez menores que cualquier número dado A y primos a él mismo, es congruente, según el módulo A, a la unidad tomada positiva* (si *A es de la forma* $p^m$ *o* $2p^m$, *con* $p$ *un primo diferente de* 2*) o negativamente* (*en otro caso*)*."*

Retomando los teoremas sobre raíces primitivas Gauss muestra los residuos de la suma y producto de aquellas, módulo $p$; también muestra en el art. 79 que el residuo de la serie geométrica $1 + a + a^2 + \cdots + a^t$ es congruente con $0$ módulo $p$ donde $t$ es el mínimo exponente tal que $a^t \equiv 1(mod\ p)$. Este resultado será de gran utilidad en una de las proposiciones de la sección VII.

El artículo 83 contiene una forma general del artículo 49; los artículos 45 a 48 se generalizaron en 55 y 57. En el art. 84 Gauss hace la observación de que los artículos 53 y 54 también son válidos para los módulos que son potencia de un primo. En el artículo siguiente muestra que para módulos de este tipo se puede saber el número de raíces de la congruencia $x^t \equiv 1(mod\ p^n)$. La demostración de esta proposición es algo extensa y Gauss la realiza en tres partes [artículos 86, 87 y 88].

La noción de raíz primitiva se puede extender a módulos que son potencias de un primo impar, si se define así a los números cuyo orden es $p^{n-1}(p-1)$ y todos los resultados mostrados desde al artículo 57 son válidos en este caso. Demuestra que para módulos potencia de 2 no se puede definir la noción de raíz primitiva (salvo para 4), pero sí para los de la forma $2p^n$, con $p$ primo impar.

Concluye esta sección mostrando que para módulos de este tipo existen números cuyo periodo comprenden todos los números primos relativos al módulo.

## 1.4 Sobre las congruencias de segundo grado.

El objetivo de esta sección es dar una prueba formal de la Ley de Reciprocidad cuadrática (L.R.C.), a la que Gauss llamó *Teorema Fundamental*, por ser de gran importancia en la Aritmética Superior. Con el Teorema Fundamental resolverá el problema de determinar si dados dos números uno es o no un residuo cuadrático del otro[12], y por tanto, si una congruencia del tipo anterior tiene solución.

El primero en tratar los temas relacionados con lo que posteriormente sería la reciprocidad cuadrática fue P. Fermat. En una carta dirigida a Marin Mersenne en 1640

[12] Un entero $a$ es un residuo cuadrático de $m$, con $(a, m) = 1$, si la congruencia $x^2 \equiv a(mod\ m)$ tiene solución.

enunció el teorema que sigue:

> ***Tout nombre première, qui surpasse de l'unité un multiple du quaternaire, est une seul fois la somme de deux carrés.***
> (Todo número primo que sea de la forma $4k + 1$, es de manera única la suma de dos cuadrados).

Este resultado está relacionado con la reciprocidad cuadrática pues resulta ser equivalente a:

> *Si $p$ es un primo impar, entonces, $p \equiv 1(mod\ 4)$ sí y sólo sí $-1$ es un residuo cuadrático módulo $p$.*

El primero en desarrollar resultados equivalentes a la L.R.C fue Leonhard Euler alrededor de 1744. Aunque no logró probar muchos de ellos, sí demostró un teorema que actualmente se conoce como el *Criterio de Euler* –lo mencionaremos con mayor detalle más adelante –.

Fue hasta 1797 que André Marie Legendre publicó la L.R.C. en una forma parecida a como se presenta actualmente[13] y dio una demostración parcial. En este mismo ensayo introdujo lo que ahora se conoce como "símbolo de Legendre", que definió como sigue:

Sea $p$ primo impar tal que $p$ no divide a $a$, entonces

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es residuo cuadrático de } p \\ -1 & \text{otro caso} \end{cases}$$

Este símbolo ayuda a la comprensión, así como a la prueba, de algunos teoremas sobre residuos cuadráticos, mismos que Gauss introduce en la sección IV de las *Disquisitiones;* sin embargo, él no lo utiliza.

Fue Gauss, el primero en dar una demostración completa de la L.R.C., la cual se encuentra entre los artículos 135 al 144 de su obra. Como ya se había mencionado esto es precisamente el corazón de la sección IV. Pero antes él debe dar algunos preliminares que le serán de utilidad.

Primero clasifica los residuos mínimos de un módulo $m$ en dos clases. En una estarán los que son congruentes a un cuadrado módulo $m$ –*residuos cuadráticos de* $m$– y en el otro los que no –*residuos no cuadráticos de* $m$–. De hecho, en la demostración concluye implícitamente que para determinar cuáles son los residuos cuadráticos para un módulo dado $m$ basta determinar los residuos módulo $m$ de los cuadrados $0, 1, 4, 9, .., \left(\frac{m}{2}\right)^2$. Para el caso donde el módulo sea un primo impar $p$ (Gauss trabaja con estos en la sección IV) muestra que el número de residuos y no residuos cuadráticos coincide y es $\frac{p-1}{2}$.

Posteriormente, demuestra que: *el producto de dos residuos cuadráticos de un*

[13] Lo publicó en el *Essai sur la Théorie des Nombres*, Paris, 1797.

*número primo* $p$ ($p$ es el módulo) *es un residuo cuadrático; el producto de un residuo con un no-residuo es un no-residuo; y el producto de dos no-residuos es un residuo.* Este teorema se visualiza más claramente con el uso del símbolo de Legendre, pues este satisface,

$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$, donde $p$ es primo que no divide ni $a$ ni a $b$.

Con este teorema el problema de determinar si un número compuesto es o no un residuo de un número primo se reduce a determinar si un número primo es o no residuo de otro primo.

A esto le sigue un análisis de los residuos y los no-residuos cuando el módulo es un número compuesto –potencia de un primo, producto de primos o potencia de primos–, se incluye el caso $p = 2$ (cualquier número será un residuo de 2) y $m = 2^n$. Para el caso en el que $m$ es producto de primos o potencia de ellos, se sabe por propiedades de congruencias que si $n$ es residuo de $m$ también lo será de cada uno de sus factores. Gauss muestra que el inverso también es cierto, esto es, si $n$ es un residuo de cada uno de los factores de $m$ también lo será de $m$ mismo. Con esto, se puede concluir que los casos en los que $m$ es un módulo compuesto se pueden reducir al estudio de los módulos primos.

En el art. 106 Gauss presenta lo que ahora se conoce como *Criterio de Euler* para los residuos cuadráticos, este enuncia lo siguiente:

> *cualquier número* $a$ *no divisible por un primo* $p = 2m + 1$ *es un residuo o no-residuo de* $p$ *según* $a^m \equiv +1 \quad o \quad a^m \equiv -1 \ (mod\ p)$.

Actualmente es presentado como sigue,

> *sea* $p$ *un primo impar. Entonces un entero positivo* $a$ *no divisible por* $p$ *es un residuo cuadrático de* $p$ *si y solo si* $a^{\frac{p-1}{2}} \equiv 1 (mod\ p)$.

Aunque este criterio puede ser de utilidad, no es muy práctico cuándo $a$ o $p$ son números muy grandes.

En los artículos 107 a 124 Gauss realiza una investigación en la que parte de un número dado y explora de qué módulos primos es residuo y de cuáles es un no-residuo. Hace un análisis particular de los residuos +1 y -1; +2 y -2; +3 y -3; +5 y-5; +7 y -7.

Después de algunos preliminares, finalmente en el artículo 131 Gauss presenta el Teorema Fundamental (L.R.C.) y lo hace de la siguiente manera:

> *Si* $p$ *es un número primo de la forma* $4n + 1$, $+p$ *será un residuo o no-residuo de cualquier número primo que tomado positivamente, es un residuo o no-residuo del mismo* $p$. *Si* $p$ *es de la forma* $4n + 3$, $-p$ *tendrá la misma propiedad.*

El teorema muestra la relación que existe entre la solubilidad de las congruencias $x^2 \equiv q(mod\ p)$ y $x^2 \equiv p(mod\ q)$, donde $p$ y $q$ son primos impares; a saber, cuando $p$ es de la forma $4n+1$ la primera es soluble si y solo si lo es la segunda. Si $p$ es de la forma $4n+3$ y $q$ es un residuo de $p$, entonces $p$ será un no residuo de $q$, y viceversa.
Actualmente se estudia a través de la simbología de Legendre, de la siguiente manera:

*Sean $p$ y $q$ distintos primos impares. Entonces* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Antes de proceder con la demostración, muestra algunas consecuencias de suponer válido el Teorema Fundamental (L.R.C.) que le serán de gran utilidad en la prueba.

Gauss se sintió realmente intrigado con este resultado, tanto que realizó otras siete pruebas del teorema –inclusive llegó a llamarle el Teorema Áureo–, seis de ellas publicadas entre 1801 y 1818, y dos más se encontraron en sus diarios sin publicar.[14]
De hecho la L.R.C. es uno de los resultados más estudiado por los matemáticos, se pueden encontrar más de 200 pruebas diferentes. La primera demostración de Gauss es la que presenta en los arts. 135 a 144 de *Disquisitiones*, y lo hace por inducción sobre los primos, en donde surgen 8 diferentes casos. Con esto puede presentar la resolución del problema que se había planteado al principio:

> *Dados dos números cualesquiera $P$ y $Q$ descubrir si uno de ellos es o no un residuo del otro.*

Otra aplicación del Teorema Fundamental que Gauss exhibe es para hallar las formas lineales –fórmula– que contienen a todos los números primos con $A$ –un entero cualquiera–, para los cuales $A$ es un residuo (respectivamente no-residuo). El estudio que Gauss hace sobre este asunto es extenso, abarca seis páginas de sus *Disquisitiones*.

Finalmente, muestra que las congruencias de la forma $ax^2 + bx + c \equiv 0\ (mod\ m)$, a las que llama "congruencias no puras de segundo grado", pueden reducirse a $x^2 \equiv a\ (mod\ m)$. Y con esto concluye su estudio sobre las congruencias de segundo grado.

## 1.5 Sobre las formas y las ecuaciones indeterminadas de segundo grado.

En esta sección de *Disquisitiones,* la cual con 357 páginas abarca más de la mitad del libro, Gauss trata las *formas cuadráticas binarias* –o simplemente *formas cuadráticas*–; es decir, las funciones de dos indeterminadas de la forma:

[14] Franz Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*. p. 9

$$ax^2 + 2bxy + cy^2,$$

donde $a, b, c$ son enteros dados.[15] Gauss proporciona un estudio hecho con base en resolver –encontrar todas las soluciones racionales– las ecuaciones indeterminadas de segundo grado con dos incógnitas, aunque casi toda la sección trata sobre las formas cuadráticas. Estos asuntos ya habían sido estudiados por Fermat, Euler y Lagrange, de hecho, este último fue el primero en resolver el problema de hallar las soluciones de las ecuaciones indeterminadas de segundo grado. Sin embargo, Gauss consideró pertinente retomar todo el argumento sobre estas; primero, para comprender completamente los nuevos resultados acerca de ellos, en especial sobre las formas cuadráticas; segundo, porque la forma de tratarlos –como objetos por sí mismos– se aleja del aspecto Diofantino de sus antecesores. Esto se hace evidente cuando declara lo siguiente:

> *"Cuando no nos conciernen las indeterminadas $x$ e $y$, denotaremos con $(a, b, c)$ a la forma $ax^2 + 2bxy + cy^2$".*

De esta manera Gauss empieza con las investigaciones sobre la representación de los números.[16]

Las primeras investigaciones acerca de la representación de enteros con formas cuadráticas se remontan a Fermat, esta se puede consultar en la correspondencia que mantuvo con Pascal y Mersenne, en ella afirmó haber demostrado las siguientes proposiciones:

1. Cada primo $p$ de la forma $4k + 1$ se puede representar como suma de dos cuadrados.
2. Todo primo de la forma $3k + 1$ se representa como $x^2 + 3y^2$.
3. Todo primo de la forma $8k + 1$ o $8k + 3$ puede ser representado como $x^2 + 2y^2$.

Estos resultados motivaron a Euler y Lagrange a abordar el estudio sobre la representación de enteros a través de formas cuadráticas binarias.

El primer resultado que muestra Gauss (art. 154) es que *si un número $M$ se representa por la forma $(a, b, c)$ entonces $b^2 - ac$ será un residuo cuadrático módulo $M$*. Al número $b^2 - ac$ se le llama el *determinante* de la forma $(a, b, c)$.

Gauss excluye de su estudio a las formas con determinante 0, pues él opina que "perturban la elegancia de los teoremas" ya que requieren un tratamiento particular.

A continuación define en el art. 157 que una forma $F'$ con indeterminadas $x, y$ está contenida en otra forma $F$ con indeterminadas $x', y'$, si esta última puede transformarse en la primera a partir de las sustituciones

$$\begin{aligned} x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y' \end{aligned} \qquad (*)$$

[15] Gauss fue el primero en considerar que la parte mixta de la forma cuadrática fuera par.

[16] Un número dado $M$ se representa con una forma cuadrática si existen enteros $a, b, c, x, y,$ tales que $M = ax^2 + 2bxy + cy^2$.

tal que $\alpha, \beta, \gamma, \delta$ sean enteros. Sí $\alpha\delta - \beta\gamma$ es positivo se llama a $(*)$ transformación *propia* ($F'$está contenido *propiamente* en $F$) e *impropia* si $\alpha\delta - \beta\gamma$ es negativo ($F'$ está contenido *impropiamente* en $F$).

Después de un desarrollo algebraico deduce la identidad $D' = D(\alpha\delta - \beta\gamma)^2$, donde $D$ es el determinante de la forma $F$ y $D'$ es el determinante de la forma $F'$, es decir, cuando $F'$ está contenida en $F$, el determinante de $F$ divide al determinante de $F'$. Luego define que $F$ y $F'$ son formas equivalentes si $F$ está contenida en $F'$ y $F'$ está contenida en $F$. Así, concluye que si dos formas son equivalentes tendrán el mismo determinante y $\alpha\delta - \beta\gamma = \pm 1$. Cuando $F$, así como $F'$, están contenidos *propiamente* (*impropiamente*) el uno en el otro y además son formas equivalentes se dice que son *propiamente* (*impropiamente*) equivalentes.

En lo que sigue, hasta el art. 222, Gauss se dedica al enorme trabajo de clasificar a las formas de acuerdo a su determinante. Antes muestra algunas propiedades acerca de las nociones anteriores, entre ellas, un criterio para hallar las transformaciones entre formas equivalentes:

> *si se tiene una transformación de la forma* $(A, B, C)$ *en la forma* $(a, b, c)$*, y todas las soluciones de la ecuación* $t^2 - Du^2 = m^2$*, donde* $D$ *es el determinante de las formas y* $m$ *el máximo común divisor de sus coeficientes, entonces se puede derivar todas las transformaciones de* $(A, B, C)$ *en* $(a, b, c)$*, las cuáles serán del mismo tipo –propias o impropias– que la transformación dada.*

También trata un poco las *formas ambiguas*, esto es, las formas que son impropiamente equivalentes a ellas mismas; muestra la existencia de estas y de ciertas propiedades que utiliza más adelante. Luego, como aplicación de la teoría de transformaciones, muestra un resultado sobre la representación de los números por formas [art 169].

Gauss divide el estudio de las formas dependiendo de si el determinante es positivo o negativo. Empieza con este último caso y lo primero que muestra [art. 171] es que para toda forma con discriminante negativo se puede encontrar una *forma reducida*[17] (no necesariamente única) propiamente equivalente ella. Enseguida, hace lo propio con las formas de determinante positivo [art. 183].

Después muestra condiciones para que dos formas con determinante negativo sean equivalentes; que el número de formas reducidas que tiene un determinante negativo dado $D$ es finito –relativamente pequeño respecto a $D$–; que todas las formas del mismo

---

[17] Una forma $(A, B, C)$ con determinante $D < 0$ es una *forma reducida* si $2B \leq A \leq \sqrt{-\frac{4}{3}D}$ ; $A \leq C$.
Una forma $(A, B, C)$ con determinante $D > 0$ es *reducida* si $0 \leq B < \sqrt{D}$ ; $\sqrt{D} - B \leq |A| \leq \sqrt{D} + B$.

determinante pueden distribuirse en clases. Resuelve el problema de hallar todas las transformaciones entre dos formas equivalentes. Además aplica la teoría para probar diversos teoremas sobre la representación de números primos por la forma $x^2 + ny^2$.

Sobre las formas con determinante positivo no cuadrado Gauss muestra propiedades de sus formas reducidas y un algoritmo para encontrarlas –también hay un número finito de ellas–. Además proporciona un algoritmo para saber cuándo dos formas que tienen el mismo determinante son equivalentes (propia o impropiamente).

Dada la importancia de conocer todas las soluciones de la ecuación $t^2 - Du^2 = m^2$ (conocida como la *ecuación de Pell)*, ya que su solución provee de todas las transformaciones entre dos formas equivalentes, Gauss dedica los artículos 197 al 202 para explicar cómo hallar la solución fundamental y la solución general de esta ecuación.

Finalmente muestra un algoritmo para hallar todas las representaciones de un entero a través de una forma dada. Para los casos en que el determinante es un cuadrado positivo o cero, Gauss realiza un estudio semejante a los casos anteriores y obtiene resultados análogos.

En los artículos 216 al 220 resuelve el problema de hallar todas las soluciones de la ecuación general de segundo grado con dos incógnitas. Con esto y una breve nota histórica [art.222] finaliza la primera parte de la Sección V.

Los artículos siguientes de la Sección V están dedicados a terminar la investigación de las propiedades de las formas; se introducen los conceptos de *orden, género,* y *composición de formas*. Dos formas $(a, b, c)$ y $(a', b', c')$ están en el mismo *orden* siempre que el máximo común divisor de $a, b, c$ sea igual al máximo común divisor de $a', b', c'$, y lo mismo debe suceder con $a,\ 2b, c$ y $a', 2b', c'$. Los órdenes se clasifican en géneros: dos formas están en el mismo *género* si existe un entero no cero que es representable por ambos. Después de mostrar algunas propiedades generales de estos conceptos, Gauss introduce la operación *composición de formas* [art.235]:

*Si la forma* $F \ldots Ax^2 + 2BXY + CY^2$ *se transforma en el producto de dos formas,*

$f \ldots \ldots ax^2 + 2bXY + cY^2$ y $f' \ldots \ldots a'x^2 + 2b'XY + c'Y^2$

*mediante la sustitución*

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

*de tal manera que los números*

$pq' - qp',\quad pq'' - qp'',\quad pq''' - qp''',\quad p'q'' - q'p'',\quad p'q''' - q'p''',$
$p''q''' - q''p'''$

*no tienen un divisor común, se dice que* $F$ *es la composición de* $f$ y $f'$.

Después indica algunas propiedades sobre la composición de formas, como la asociatividad.

Otros teoremas importantes que muestra son referentes al número de clases en cada género del mismo orden, el número de clases en órdenes distintos, el número de formas ambiguas primitivas, y el art. 261 en el que muestra que al menos la mitad de los posibles caracteres completos no pueden pertenecer a un género, estos le fueron de utilidad en la segunda prueba que hace de su Teorema Fundamental (L.R.C.) en el art. 262. En el art. 263 aplica la teoría y obtiene un método para representar un primo como suma de dos cuadrados.

En la tercer parte de la sección V realiza un breve estudio sobre *formas ternarias de segundo grado*. Las *formas ternarias* son expresiones como estas:

$$Ax^2 + 2Bxy + Cy^2 + 2Dxz + 2Eyz + Fz^2,$$

donde $A, B, C, D, E, F$ son enteros, con determinante igual a

$$ab^2 + a'b'^2 + a''b''^2 - aa'a'' - 2bb'b''.$$

Empieza el estudio de este tema con las propiedades elementales de transformaciones en formas ternarias. En el artículo 278 plantea problemas importantes en la teoría de formas ternarias:

1. Encontrar todas las representaciones de un número dado por una forma ternaria dada.
2. Encontrar todas las representaciones de una forma binaria dada por una forma ternaria dada.
3. Juzgar si dos formas ternarias dadas del mismo determinante son equivalentes, y si lo son, encontrar todas las transformaciones de una en la otra.
4. Juzgar si una forma ternaria dada implica otra forma ternaria dada de determinante mayor, y si lo hace, asignar toda transformación de la primera en la segunda.

Sin embargo, Gauss no aborda estos problemas con todo detalle, sólo muestra que el primer problema se puede reducir al segundo y este al tercero.

En la parte final da algunas aplicaciones de la teoría de formas ternarias a la de formas binarias. Una de ellas es la resolución de la ecuación $ax^2 + by^2 + cz^2$, a la que Gauss llama el teorema fundamental de Legendre:

> *Si los números $a, b, c$ son primos relativos y ninguno igual a cero ni divisibles por un cuadrado, entonces la ecuación $ax^2 + by^2 + cz^2 = 0 \ldots (\Omega)$ no se puede resolver con enteros (excepto cuando $x = y = z = 0$), a menos que $-bc$, $-ac$ y $-ab$ sean residuos cuadráticos de $a$, $b$ y $c$, respectivamente,*

*y estos números tengan signos diferentes; pero cuando estas cuatro condiciones se cumplen,* $(\Omega)$ *se podría resolver con enteros.*

Gauss realiza dos pruebas de este teorema [art.294, 295], y hace un análisis de la prueba de Legendre y muestra por qué su argumento no es completo.

## 1.6 Aplicaciones de las secciones anteriores.

La sección VI está dedicada al estudio de algunas aplicaciones de la teoría vista en las secciones anteriores. En la primera parte (arts. 308-318) Gauss muestra métodos para la descomposición en fracciones parciales, *i.e.*; métodos para descomponer una fracción en una suma de fracciones cuyos denominadores son los factores primos del denominador de la fracción original. Otro tema que aborda es sobre la expansión decimal de una fracción y muestra varios resultados concernientes a esto. Es importante mencionar el art. 310 ya que se requerirá a principios del capítulo IV. En dicho capítulo se verá la conexión entre las soluciones por radicales de las raíces de $x^n - 1$ y la construcción de polígonos regulares, y el artículo 310 proporciona la herramienta para justificar el por qué en los capítulos II y III se enfocó en las raíces de $x^n - 1$ para $n$ primo.

Después Gauss expone un método alterno al que llama *método de exclusión* para la resolución de congruencias de segundo grado, para esto hace uso de la teoría de formas desarrollada en la sección V. Este mismo método le sirve para resolver la ecuación indeterminada $mx^2 + ny^2 = A$. Además, muestra artificios para reducir la operación en ciertos casos.

En la parte final (arts. 329-334) Gauss desarrolla dos criterios para distinguir entre los números primos y los números compuestos, y aborda la descomposición de estos en sus factores primos. El primero de ellos (art. 330) se basa en un hecho expuesto en la sección IV, en el que *todo entero positivo o negativo que es residuo cuadrático del entero* $M$*, también lo es de cualquier divisor de* $M$. El segundo método utiliza los valores de la expresión $x^2 \equiv -D \ (mod\ M)$, bajo ciertas consideraciones, y resultados sobre formas de determinante $-D$.

Con esto finaliza el análisis de las secciones previas a la sección VII del *Disquisitiones Arithmeticae*. Los siguientes capítulos estarán dedicados al estudio de esta última sección.

# Capítulo II

## Sobre la irreductibilidad del polinomio $x^{n-1} + x^{n-2} + \cdots + x + 1$ con $n$ primo.

La sección VII de las *Disquisitiones* pareciera que no está directamente relacionada con las secciones anteriores, pero después de una lectura reflexiva se puede ver que Gauss usa algunas proposiciones que planteó a lo largo de las primeras seis partes.

Se considera que en esta sección del libro existen varios puntos de gran importancia que Gauss planteó, entre ellos los más relevantes son: i) da a conocer la teoría que desarrolló y que ahora se conoce como *períodos gaussianos*, ii) a partir de la teoría de períodos encuentra soluciones por radicales para ciertos polinomios; iii) cuando traslada la teoría del punto anterior a la división del círculo y su conexión con la construcción de polígonos regulares.[18] En su estudio, Gauss, vincula el análisis algebraico de la ecuación $x^n - 1 = 0$ con el problema de construir polígonos regulares de $n$ lados con regla y compás. Con estos temas de los polígonos construibles Gauss da fin a sus *Disquisitiones*, y concluye lo siguiente:

> *Un polígono regular con $n$ lados puede ser construido si $n = 2^k p_1 p_2 \ldots p_t$, donde $k \geq 0$ , y $p_1, p_2, \ldots, p_t$ son primos impares de Fermat.*[19]

Para ejemplificar su proposición muestra que el polígono regular de 17 lados es construible con regla y compás y no es muy diferente de la primera prueba que realizó en 1796. Cabe mencionar que en su época Gauss sabía que esta condición también es necesaria; sin embargo no dejó una prueba formal, esta fue establecida posteriormente por Wantzel en 1837.

A continuación se desarrollará la teoría necesaria para llegar a este resultado que Gauss obtuvo. Concretamente en este capítulo de la tesis se mostrará la irreductibilidad en los racionales de las ecuaciones ciclotómicas, esto es, se mostrará que para $n$ primo, el polinomio

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

[18] El tema de los polígonos construibles surge desde la antigua Grecia. Con ciertas herramientas, y bajo reglas bien definidas ya eran conocidas algunas técnicas para la construcción de algunos polígonos. Pero fue Gauss el primero en dar una caracterización usando matemáticas más allá de la geometría para proponer cuales polígonos son construibles por regla y compás.

[19] Sabemos que los primos de Fermat son de la forma $2^{2^n} + 1$, sin embargo hasta ahora no se conocen explícitamente otros primos de Fermat además de los generados por $n = 0, 1, 2, 3, 4$, y en consecuencia no se sabe si hay una infinidad.

no tiene divisores que tengan todos sus coeficientes racionales. Ahora se da lugar al estudio de los artículos requeridos para poder demostrar este teorema.

**Art. 338.** El teorema que se muestra en este artículo no se requerirá directamente en este trabajo de tesis –Gauss sí lo utilizó en el art. 363 de sus *Disquisitiones*–; sin embargo, debido a que en la prueba se hace uso de un teorema de Newton que sí se requerirá más adelante, se consideró importante mencionarlo.

**Teorema.** Se requiere encontrar una ecuación ($W'$) cuyas raíces son las $\lambda$-ésimas potencias de las raíces de la ecuación

$$z^m + a_1 z^{m-1} + a_2 z^{m-2} + \cdots a_m = 0 \ldots\ldots\ldots\ldots\ldots\ldots (W),$$

donde $\lambda$ es un entero positivo dado.

Para abordar este problema Gauss recurrió al resultado de Newton sobre la suma de potencias de raíces,[20] pero sólo lo menciona y afirma que se puede usar el proceso inverso de Newton para encontrar los coeficientes de la nueva ecuación ($W'$) que él propone. Aquí se tiene el inconveniente que Gauss no desarrolló lo que menciona, supone que el lector lo sabe. En primer lugar veamos cual es el teorema de Newton al que se refiere.

**Teorema (de Newton).** Sea $t^m + p_1 t^{m-1} + p_2 t^{m-2} + \cdots + p_{m-1} t + p_m = 0$ una ecuación con raíces $x_1, x_2, \ldots, x_m$. Para $j = 1, 2, 3, \ldots$ sea $s_j = x_1^j + x_2^j + \cdots + x_m^j$. Sea $p_k = 0$ para $k > m$. Entonces para $j > 0$

$$s_j + p_1 s_{j-1} + p_2 s_{j-2} + \ldots + p_{j-1} s_1 + j p_j = 0.$$

Lo que el teorema está enunciando es que

$$\begin{aligned} s_1 + p_1 &= 0 \\ s_2 + p_1 s_1 + 2p_2 &= 0 \\ s_3 + p_1 s_2 + p_2 s_1 + 3p_3 &= 0 \\ s_4 + p_1 s_3 + p_2 s_2 + p_3 s_1 + 4p_4 &= 0 \end{aligned}$$

o, equivalentemente,

$$\begin{aligned} s_1 &= -p_1 \\ s_2 &= -p_1 s_1 - 2p_2 \\ s_3 &= -p_1 s_2 - p_2 s_1 - 3p_3 \\ s_4 &= -p_1 s_3 - p_2 s_2 - p_3 s_1 - 4p_4. \end{aligned}$$

Newton proporciona con este teorema las sumas de las potencias de las raíces. Pero, si lo que Gauss quiere es encontrar una ecuación que tenga como raíces las $\lambda$-ésimas potencias de las raíces de la ecuación original

$$z^m + a_1 z^{m-1} + a_2 z^{m-2} + \cdots a_m = 0 \qquad (W),$$

[20] Para ver el contexto de este resultado dentro de la obra de Newton véase la *Arithmetica Universalis*, 1707.

entonces, se tienen que conocer los coeficientes de la nueva ecuación $(W')$.

Regresando a la proposición del art. 338, sean $r_1, r_2, \dots, r_m$ las raíces de $(W)$, entonces las raíces de $(W')$ serán ${r_1}^{\lambda}, {r_2}^{\lambda}, \dots, {r_m}^{\lambda}$.
Luego aplicando el teorema anterior a las raíces $r_1, r_2, \dots, r_m$ se pueden hallar las sumas

$$\begin{aligned}
s_1 &= {r_1}^{\lambda} + {r_2}^{\lambda} + \cdots + {r_n}^{\lambda} \\
s_2 &= {r_1}^{2\lambda} + {r_2}^{2\lambda} + \cdots + {r_n}^{2\lambda} \\
&\vdots \\
s_{\lambda} &= {r_1}^{2\lambda} + {r_2}^{2\lambda} + \cdots + {r_n}^{2\lambda} \\
&\vdots \\
s_{2\lambda} &= {r_1}^{2\lambda} + {r_2}^{2\lambda} + \cdots + {r_n}^{2\lambda} \\
&\vdots \\
s_{m\lambda} &= {r_1}^{m\lambda} + {r_2}^{m\lambda} + \cdots + {r_m}^{m\lambda}
\end{aligned}$$

entonces, ya se conocen los valores de

$$s_{\lambda},\ s_{2\lambda}, \dots, s_{m\lambda}.$$

Por otro lado, $s_{j\lambda}$ se puede expresar como

$$s_{j\lambda} = ({r_1}^{\lambda})^j + ({r_2}^{\lambda})^j + \cdots + ({r_m}^{\lambda})^j, \quad 0 < j \leq m.$$

Entonces, aplicando nuevamente el teorema de Newton, donde las raíces que se consideran son ${r_1}^{\lambda}, {r_2}^{\lambda}, \dots, {r_m}^{\lambda}$, se tiene que

$$s_j = -b_1 s_{j-1} - b_2 s_{j-2} - \cdots - b_{j-1} s_1 - j b_j$$

donde $b_1, b_2, \dots, b_{j-1}$ son los coeficientes de la ecuación $(W')$. Pero como ya se conocen los valores $s_j$, entonces se pueden despejar los coeficientes $b_1, b_2, \dots, b_{j-1}, b_j$, y con esto se concluye lo que propuso en el art. 338.

Ahora continúan los artículos que son utilizados directamente para mostrar la irreductibilidad del polinomio ciclotómico. A partir de aquí se supondrá que $n$ es un número primo, salvo que se diga lo contrario.

**Art. 339.** Se mencionarán algunas propiedades de las raíces del polinomio $X = x^{n-1} + x^{n-2} + \cdots + x + 1$ , con $n$ un primo impar; para este caso al conjunto de tales raíces las denota por $\Omega$.

Recuerde que $\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$, entonces si $r$ es una raíz de $\Omega$, se tiene que, para todo entero $k$, $(r^n)^k = 1^k = 1$, esto es, si $\kappa \equiv 0\ (mod\ n)$, entonces $r^{\kappa} = 1$.
Así, se tiene lo siguiente:

- Si $\lambda \equiv \mu\ (mod\ n) \Longrightarrow r^{\lambda - \mu} = 1$ y por tanto $r^{\lambda} = r^{\mu}$.

- Ahora, si $\lambda \not\equiv \mu \ (mod\ n)$, entonces $m.c.d(\lambda - \mu, n) = 1$ y por ello existe $\upsilon$ tal que $(\lambda - \mu)\upsilon \equiv 1 (mod\ n)$, por tanto $r^{(\lambda-\mu)\upsilon} = r \Longrightarrow r^{(\lambda-\mu)\upsilon} \neq 1 \Longrightarrow r^{\lambda} \neq r^{\mu}$.

De lo anterior se concluye que $1,\ r,\ r^2, \dots, r^{n-1}$ son raíces diferentes de la ecuación $x^n - 1 = 0$, y $\Omega = \{r, r^2, \dots, r^{n-1}\} = \{r^e, r^{2e}, \dots, r^{(n-1)e} : e \in \mathbb{Z},\ n \nmid e\}$. Esto último dice que dada una raíz $r \in \Omega$, cualquier raíz de la unidad se puede expresar como una potencia de $r$. Por lo tanto,

$$X = (x - r^e)(x - r^{2e}) \dots (x - r^{e(n-1)})$$

y aunque Gauss no lo menciona, estos elementos de $\Omega$ son raíces primitivas de la unidad.

Otro resultado que exhibe es

$$r^{(n-1)e} + \cdots + r^{3e} + r^{2e} + r^e = -1,$$

esto es, que la suma de las raíces en $\Omega$ es -1.

Por último, Gauss hace un comentario que usará en el artículo 341 y es acerca de las raíces $r$ y $\frac{1}{r}$, a las cuales llama *recíprocas* y estas satisfacen la igualdad

$$(x - r)\left(x - \frac{1}{r}\right) = x^2 - 2xcos\omega + 1, \quad \text{donde } \omega = \frac{2\pi k}{n}, k \in \mathbb{Z}.$$

En general se puede verificar que

$$(x - r^e)\left(x - \frac{1}{r^e}\right) = x^2 - 2xcos\omega + 1$$

usando las formas polares

$$r^e = cos\omega + isen\omega \quad \text{y} \quad \frac{1}{r^e} = cos\omega - isen\omega,$$

donde $\omega = \frac{2\pi k}{n}$, $k = 1, \dots, n-1$.

**Art. 340.** Aquí se probará que al sustituir respectivamente las $k$-ésimas potencias de las raíces de la unidad $(k = 1, 2, \dots, n)$ en un polinomio –que a su vez está formado de polinomios simétricos– de grado $m$ con coeficientes enteros, la cantidad resultante de la suma de las sustituciones mencionadas, será un entero divisible por $n$. Este hecho será de gran utilidad para resolver los planteamientos de artículos posteriores, y como Gauss bien lo menciona, será fundamental en el artículo 341.

Primero obsérvese que si $r$ es raíz de $X$, por el artículo anterior cualquier raíz de $x^n - 1$ se puede expresar como $r^\sigma$ y por tanto un producto de estas raíces también será de la forma $r^\sigma$.

Designando por $\varphi(t_1, t_2, \dots t_m)$ una función entera de las incógnitas $t_1, t_2, \dots, t_m$ que es de la forma

$$ht_1^\alpha t_2^\beta \dots t_m^\upsilon + h't_1^{\alpha'} t_2^{\beta'} \dots t_m^{\upsilon'} + \cdots,$$

donde algunas de las $t_i$ puede no aparecer.

Ahora, si sustituimos las $t_i$ por las raíces $r_1, r_2, .., r_n$ de $x^n - 1$, haciendo $t_i = r_i$, para $i = 1,2, \dots, n$. Entonces,

$$\varphi(t_1, t_2, \dots) = \varphi(r_1, r_2, .., r_n) = hr_1^\alpha r_2^\beta \dots r_n^\rho + h'r_1^{\alpha'} r_2^{\beta'} \dots r_n^{\rho'} + \cdots$$

Pero puesto que cada sumando de la expresión anterior se puede ver como $hr^{\sigma}$, se tiene que $\varphi(r_1, r_2, .., r_n)$ se puede reducir a la forma

$$A + A'r + A''r^2 + \cdots + A^n r^{n-1},$$

donde cada uno de los coeficientes $A', A'', \ldots A^n$ están en términos de algunos de los coeficientes $h, h', \ldots h^v$, e incluso algunos pueden ser igual a cero.

Para las raíces $r_1^2, r_2^2, .., r_n^2$ se tiene

$$\begin{aligned}\varphi(r_1^2, r_2^2, .., r_n^2) &= h(r_1^2)^{\alpha}(r_2^2)^{\beta} \ldots (r_n^2)^{\rho} + h'(r_1^2)^{\alpha'}(r_2^2)^{\beta'} \ldots (r_n^2)^{\rho'} + \cdots \\ &= h(r_1{}^{\alpha} r_2{}^{\beta} \ldots r_n{}^{\rho})^2 + h(r_1{}^{\alpha'} r_2{}^{\beta'} \ldots r_n{}^{\rho'})^2 + \cdots\end{aligned}$$

que se puede expresar como

$$A + A'r^2 + A''r^4 + \cdots + A^n r^{2(n-1)}.$$

En general, se tendrá que $\varphi(r_1^{\lambda}, r_2^{\lambda}, .., r_n^{\lambda})$ se puede expresar como

$$A + A'r^{\lambda} + A''r^{2\lambda} + \cdots + A^n r^{\lambda(n-1)}.$$

Por último,

$$\varphi(r_1^n, r_2^n, .., r_n^n) = A + A'r^n + A''r^{2n} + \cdots + A^n r^{n(n-1)} = A + A' + A'' + \cdots + A^n.$$

Así, la suma

$$\boldsymbol{\psi(r_1, r_2, .., r_n)} = \varphi(r_1, r_2, .., r_n) + \varphi(r_1^2, r_2^2, .., r_n^2) + \cdots + \varphi(r_1^n, r_2^n, .., r_n^n),$$

será

$$\begin{aligned}&= A + A'r + A''r^2 + \cdots + A^n r^{n-1} + A + A'r^2 + A''r^4 + \cdots + A^n r^{2(n-1)} + \cdots \\ &\quad + A + A'r^n + A''r^{4n} + \cdots + A^n r^{n(n-1)} \\ &= nA + A'(1 + r + r^2 + \cdots + r^{n-1}) + A''(1 + r + r^2 + \cdots + r^{n-1}) + \cdots \\ &\quad + A^n(1 + r + r^2 + \cdots + r^{n-1}) \\ &= nA.\end{aligned}$$

Por lo tanto, la suma $\boldsymbol{\psi(r_1, r_2, .., r_n)}$ es divisible por $n$.

## Ejemplo.

Sea $\varphi(t, u, v) = 2tu^2v + tv^3 + 5tuv^2$. Sustituyendo $t, u, v$ por las raíces 1, $r = e^{2\pi i/3}$, $r^2 = e^{4\pi i/3}$ de la ecuación $x^3 - 1$ se tiene que

$\varphi(1, r, r^2) = 2r^2r^2 + r^6 + 5r^5 = 2r^4 + r^6 + 5r^2 = 2r + 1 + 5r^2 = A + A'r + A''r^2$,
donde $A = 1 \quad ; \quad A' = 2 \quad ; \quad A'' = 5.$

Sustituyendo ahora por los cuadrado de las raíces se tiene que

$$\varphi(1, r^2, r^4) = 2r^4r^4 + r^{12} + 5r^2r^8 = 2r^2 + 1 + 5r^4r^6 = A + A'r^2 + A''r^4.$$

y por último,

$$\varphi(1, r^3, r^6) = \varphi(1,1,1) = 2 + 1 + 5 = A + A' + A''.$$

Entonces,

$$\begin{aligned}\varphi(1, r, r^2) + \varphi(1, r^2, r^4) + \varphi(1, r^3, r^6) &= A + A'r + A''r^2 + A + A'r^2 \\ &\quad + A''r^4 + A + A' + A'' \\ &= 3A + A'(1 + r + r^2) + A''(1 + r + r^2)\end{aligned}$$

$$= 3A,$$

y como se puede ver, $n = 3$ divide a la suma anterior.

A continuación se da lugar al resultado que es el elemento central de este capítulo.

**Art. 341.** Trata sobre la demostración de la irreductibilidad de

$$X = x^{n-1} + x^{n-2} + \cdots + x + 1$$

en los racionales y se plantea de la siguiente manera.

**Teorema.** Si la función $X$ es divisible por la función de grado menor

$$P = x^{\lambda} + Ax^{\lambda-1} + Bx^{\lambda-2} + \cdots + Kx + L,$$

entonces los coeficientes $A, B, \ldots, L$ no pueden ser todos racionales.

*Demostración.* Gauss empieza escribiendo a $X$ como $X = PQ$, y aunque no lo menciona está suponiendo que $Q$ es un polinomio no constante. La demostración del teorema se hará en cuatro casos.

Designando al conjunto de las raíces de $P = 0$ por $\mathfrak{P}$; al conjunto de las raíces de $Q = 0$ por $\mathfrak{Q}$; y al conjunto de recíprocos de las raíces en $\mathfrak{P}$ y $\mathfrak{Q}$ por $\mathfrak{R}$ y $\mathfrak{S}$, respectivamente. Es decir, se tiene

$\mathfrak{P}$ = raíces de $P$;

$\mathfrak{R}$ = recíprocos de las raíces de $P$;

$\mathfrak{Q}$ = raíces de $Q$;

$\mathfrak{S}$ = recíprocos de las raíces de $Q$.

Sea $R$ la ecuación cuyas raíces son las contenidas en $\mathfrak{R}$, y $S$ la ecuación de las raíces en $\mathfrak{S}$. Puesto que $X = PQ$, entonces al tomar todas las raíces en $\mathfrak{P}$ y $\mathfrak{Q}$ resulta ser $\Omega$. Además, debido a que $r$ es una raíz de $X$ si y solo si $\frac{1}{r}$ es una raíz de $X$, si se toman todas las raíces en $\mathfrak{R}$ y $\mathfrak{S}$ también se obtiene $\Omega$. Por lo tanto se tiene que

$$RS = X = PQ \quad \text{y} \quad \mathfrak{P} \cup \mathfrak{Q} = \mathfrak{R} \cup \mathfrak{S},$$

de esto se distinguen cuatro casos:

I. $\mathfrak{P} = \mathfrak{R}$

II. $\mathfrak{P} \neq \mathfrak{R}$ y $\mathfrak{P} \cap \mathfrak{R} \neq \emptyset$

III. $\mathfrak{Q} = \mathfrak{S}$ o $\mathfrak{Q} \cap \mathfrak{S} \neq \emptyset$

IV. $\mathfrak{P} \cap \mathfrak{R} = \emptyset$ y $\mathfrak{Q} \cap \mathfrak{S} = \emptyset$.

En cada caso se llegará a un absurdo al suponer que los coeficientes de $P$ son racionales.

I. $\mathfrak{P} = \mathfrak{R}$ ($\mathfrak{P}$ = raíces de $P$ ; $\mathfrak{R}$ = raíces recíprocas de $P$).

Este caso dice que las raíces de $P$ serán las raíces de $R$ – la ecuación cuyas raíces son las contenidas en $\mathfrak{R}$– y viceversa, por ello $P = R$. Así para cada raíz en $\mathfrak{P}$, su recíproco también estará en $\mathfrak{P}$, esto es, $P$ será un producto de $\frac{\lambda}{2}$ factores dobles de la forma

$$(x-r)\left(x-\frac{1}{r}\right)=x^2-2xcos\omega+1=(x-cos\omega)^2+sen^2\omega,$$[21]

de aquí que si $x$ toma un valor real, $P$ tendrá un valor real positivo. Llamemos $P_1,\ P_2,\ P_3,\dots,P_{n-2}$ a los polinomios cuyas raíces serán las potencias cuadradas, cúbicas, cuartas,..., $(n-1)$-ésimas de las raíces de $P$, esto es, si $r_1,\ r_2,\ r_3,\dots,r_\lambda$ son las raíces de $P$, entonces

$$\begin{aligned}
P&=(x-r_1)(x-r_2)(x-r_3)\dots(x-r_\lambda)\\
P_1&=(x-r_1^2)(x-r_2^2)(x-r_3^2)\dots(x-r_\lambda^2)\\
P_2&=(x-r_1^3)(x-r_2^3)(x-r_3^3)\dots(x-r_\lambda^3)\\
&\vdots\\
P_{n-2}&=(x-r_1^{n-1})(x-r_2^{n-1})(x-r_3^{n-1})\dots\left(x-r_\lambda^{n-1}\right).
\end{aligned}$$

Estos también tendrán valores reales positivos si $x$ toma un valor real.[22] Así, si $p,\ p_1,\ p_2,\ p_3,\dots,p_{n-2}$ designan los valores de $P(1),\ P_1(1),P_2(1),\dots,P_{n-2}(1)$ respectivamente, entonces $p,\ p_1,\ p_2,\ p_3,\dots,p_{n-2}$ serán positivos.

En lo que sigue Gauss utiliza el artículo previo –algo que él no menciona–. Designando por $\varphi(t,u,v,\dots)$ la función $(1-t)(1-u)(1-v)$ ..., se tiene que

$$\begin{aligned}
&\varphi(r_1,r_2,r_3,\dots,r_\lambda)=(1-r_1)(1-r_2)(1-r_3)\dots(1-r_\lambda)=p\\
&\varphi(r_1^2,r_2^2,r_3^2\dots,r_\lambda^2)=(1-r_1^2)(1-r_2^2)(1-r_3^2)\dots\left(1-r_\lambda^2\right)=p_1\\
&\qquad\qquad\qquad\qquad\qquad\qquad\vdots\\
&\varphi(r_1^{n-1},r_2^{n-1},r_3^{n-1}\dots,r_\lambda^{n-1})=(1-r_1^{n-1})(1-r_2^{n-1})(1-r_3^{n-1})\dots\left(1-r_\lambda^{n-1}\right)=p_{n-2}\\
&\varphi(r_1^n,r_2^n,r_3^n\dots,r_\lambda^n)=(1-r_1^n)(1-r_2^n)(1-r_3^n)\dots(1-r_\lambda^n)=0.
\end{aligned}$$

Además, obsérvese que por la teoría de las funciones simétricas de las raíces de un polinomio, se tiene que

$$(1-t_1)(1-t_2)(1-t_3)\dots=1+s_1+s_2+\cdots;$$

donde $s_j=(-1)^j\sum_{i_1<i_2<\cdots<i_j}t_{i_1}t_{i_2}\dots t_{i_j}$.

Entonces, $\varphi(t_1,t_2,t_3,\dots)$ se puede ver como la suma de términos de la forma $ht_1^\alpha t_2^\beta,\dots,t_p^\gamma$ y, puesto que $r_1,r_2,\ r_3,\dots,r_\lambda$ también son raíces de $X$ (y por tanto de $x^n-1$), se puede usar la observación hecha al final del art. 340. Así se tiene,

$$\begin{aligned}
p+p_1+\ p_2+\cdots+p_{n-2}&=\varphi(r_1,r_2,r_3,\dots,r_\lambda)+\varphi(r_1^2,r_2^2,r_3^2\dots,r_\lambda^2)+\cdots\\
&\quad+\varphi(r_1^{n-1},r_2^{n-1},r_3^{n-1}\dots,r_\lambda^{n-1})+\varphi(r_1^n,r_2^n,r_3^n\dots,r_\lambda^n)\\
&=nA,
\end{aligned}$$

esto es, $p+p_1+\ p_2+\cdots+p_{n-2}$ será divisible por $n$.

---

[21] Véase art.339

[22] En el art 339 se mencionó la siguiente igualdad,

$$(x-r^e)\left(x-\frac{1}{r^e}\right)=x^2-2xcos\omega+1=(x-cos\omega)^2+sen^2\omega$$

Además,

$$PP_1P_2 \dots P_{n-2} = [(x-r_1)(x-r_2)(x-r_3)\dots(x-r_\lambda)][(x-r_1^2)(x-r_2^2)(x-r_3^2)\dots (x-r_\lambda^2)]\dots[(x-r_1^{n-1})(x-r_2^{n-1})(x-r_3^{n-1})\dots(x-r_\lambda^{n-1})],$$

reordenando y agrupando los factores que tengan las mismas raíces $r_i$ se tiene que

$$PP_1P_2 \dots P_{n-2} = [(x-r_1)(x-r_1^2)\dots(x-r_1^{n-1})][(x-r_2)(x-r_2^2)\dots(x-r_2^{n-1})]\dots \dots [(x-r_\lambda)(x-r_\lambda^2)\dots(x-r_\lambda^{n-1})]$$

y finalmente, como cada factor $[(x-r_i)(x-r_i^2)\dots(x-r_i^{n-1})] = X$, [23] se llega a que $PP_1P_2 \dots P_{n-2} = X^\lambda$.

Así, para obtener el valor de $p \cdot p_1 \cdot p_2 \cdot \dots \cdot p_{n-2}$ basta hacer $x = 1$ en

$$X^\lambda = (x^{n-1} + x^{n-2} + \cdots + x + 1)^\lambda,$$

por tanto $p \cdot p_1 \cdot p_2 \cdot \dots \cdot p_{n-2} = n^\lambda$.

Ahora, Gauss supone que los coeficientes de $P$ son racionales, esto lo llevará a contradecir una de las afirmaciones anteriores.[24] Por el art. 338 si los coeficientes de $P$ son racionales entonces también los de $P_1, P_2, P_3, \dots, P_{n-2}$. Pero, por el artículo 42,[25] puesto que los coeficientes del producto $PP_1P_2 \dots P_{n-2}$ son enteros entonces cada polinomio $P, P_1, P_2, P_3, \dots, P_{n-2}$ debe tener coeficientes enteros, y por tanto, los valores $p$, $p_1$, $p_2$, $p_3 \dots, p_{n-2}$ son enteros. Como el producto $pp_1p_2 \dots p_{n-2} = n^\lambda$, entonces cada $p_j$ debe ser $n$ o una potencia de $n$; pero puesto que hay $n-1$ factores y $\lambda < n-1$, entonces no todos pueden ser de esa forma, esto es, algunos deben ser igual a 1. Digamos que hay una cantidad $g$ de los que son iguales a uno, así se tendrá que

$$p + p_1 + p_2 + \cdots + p_{n-2} = p_{i_1} + p_{i_2} + p_{i_3} + \cdots + p_{i_{n-1-g}} + g \equiv g(mod\ n),$$

con $p_{i_1}, p_{i_2}, p_{i_3}, \dots, p_{i_{n-1-g}} \in \{p, p_1, p_2, p_3 \dots, p_{n-2}\}$,

esto significa que $p + p_1 + p_2 + \cdots + p_{n-2}$ no es divisible por $n$;[26] pero ya se había probado que era divisible por $n$. Esta contradicción vino de suponer que los coeficientes de $P$ son racionales. Así, no todos los coeficientes de $P$ son racionales.

II. $\mathfrak{P} \neq \mathfrak{R}$ y $\mathfrak{P} \cap \mathfrak{R} \neq \emptyset$ ($\mathfrak{P}$ = raíces de $P$ ; $\mathfrak{R}$ = raíces recíprocas de $P$).

Sea $\mathfrak{T} = \mathfrak{P} \cap \mathfrak{R}$ y $T = 0$ la ecuación cuyas raíces son las contenidas en $\mathfrak{T}$. De esto, Gauss afirma que $T$ es el máximo común divisor [27] de los polinomios $P$ y $R$. Se puede notar que $T$ divide a $P$ y a $R$, y que si $T'$ es otro polinomio que también cumple esto,

---

[23] Si $r_i$ es una raíz de $X$, en el art. 339 se vio que $X$ satisface

$$X = [(x-r_i)(x-r_i^2)\dots(x-r_i^{n-1})].$$

[24] Se contrapondrá al hecho de que $p + p_1 + p_2 + \cdots + p_{n-2}$ es divisible por $n$.

[25] Sean $x^m + Ax^{m-1} + Bx^{m-2} + \cdots + N$ y $x^\mu + A'x^{\mu-1} + B'x^{\mu-2} + \cdots + N'$ polinomios con coeficientes racionales. Si los coeficientes de su producto $x^{m+\mu} + \mathfrak{U}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \cdots + \mathfrak{Z}$ son enteros, entonces los coeficientes de cada polinomio deben ser enteros.

[26] Como $p_{i_1} + p_{i_2} + p_{i_3} + \cdots + p_{i_{n-1-g}} + g \equiv g(mod\ n)$ se tiene que $n$ divide a $p_{i_1} + p_{i_2} + p_{i_3} + \cdots + p_{i_{n-1-g}}$ de modo que por la teoría de congruencias si $p + p_1 + p_2 + \cdots + p_{n-2}$ fuera divisible por $n$ se tendría que $n$ divide a $g$, lo cual no es posible pues $g \leq n-1$. Por lo tanto, $n$ **no** divide a $p + p_1 + p_2 + \cdots + p_{n-2}$.

[27] Para la definición véase Galois Theory of Algebraic Equations, Jean Pierre Tignol, p. 55.

entonces sus raíces deben estar contenidas en $\mathfrak{P} \cap \mathfrak{R}$. Así $T'$ debe dividir a $T$ y por lo tanto, $T$ es el máximo común divisor de los polinomios $P$ y $R$.

Ahora, por la definición de $T$ se sabe que sus raíces se encuentran en pares donde una es la recíproca de la otra, es decir, si se encuentra $r$ se encontrará su conjugado, entonces se formarán factores de la forma

$$(x - r)\left(x - \frac{1}{r}\right) = (x - cos\omega)^2 + sen^2\omega.$$

Procediendo análogamente como se hizo con el polinomio $P$ en el caso anterior, se llegará a que $T$ no puede tener todos sus coeficientes racionales. Por otro lado, si se supone que los coeficientes de $P$ –y por tanto los de $R$– son racionales, y puesto que $T$ es un divisor común de ambos, entonces los coeficientes de $T$ deberían ser racionales; sin embargo, esto no es así. Por lo tanto, los coeficientes de $P$ no pueden ser todos racionales.

III. $\mathfrak{Q} = \mathfrak{S}$ o $\mathfrak{Q} \cap \mathfrak{S} \neq \emptyset$ ($\mathfrak{Q}$ = raíces de $Q$ ; $\mathfrak{S}$ = raíces recíprocas de $Q$).

Cuando $\mathfrak{Q}$ y $\mathfrak{S}$ son iguales se prueba que $Q$ no puede tener coeficientes racionales de forma análoga al caso I y si son diferentes pero tienen raíces en común se hará de forma análoga al caso II. Así, como $X = PQ$ y $X$ tiene coeficientes racionales, entonces si los coeficientes de $P$ fueran racionales los de $Q$ también lo serían. Por lo tanto $P$ no puede tener todos sus coeficientes racionales.

IV. $\mathfrak{P} \cap \mathfrak{R} = \emptyset$ y $\mathfrak{Q} \cap \mathfrak{S} = \emptyset$ ($\mathfrak{P}$ = raíces de $P$ ; $\mathfrak{R}$ = raíces recíprocas de $P$; $\mathfrak{Q}$ = raíces de $Q$ ; $\mathfrak{S}$ = raíces recíprocas de $Q$).

Sea $S$ la ecuación cuyas raíces son las contenidas en $\mathfrak{S}$. Entonces, debido a que $\mathfrak{P} \cup \mathfrak{Q} = \Omega = \mathfrak{R} \cup \mathfrak{S}$, se debe tener que el conjunto de las raíces de $P$ tiene que ser igual al conjunto de las raíces de $S$, y el conjunto de raíces de $Q$ igual al conjunto de raíces de $R$. Así, $Q = R$, y por tanto,

$$X = PQ = PR = \left(x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \cdots + Kx + L\right)\left(x^\lambda + \frac{K}{L}x^{\lambda-1} + \cdots + \frac{A}{L}x + \frac{1}{L}\right),$$[28]

Ahora bien, haciendo $x = 1$, resulta

$$X(1) = n = (1 + A + B + \cdots + K + L)\left(1 + \frac{K}{L} + \cdots + \frac{A}{L} + \frac{1}{L}\right),$$

y multiplicando por $L$ se tiene que

$$nL = (1 + A + B + \cdots + K + L)(L + K + \cdots + A + 1) = (1 + A + B + \cdots + K + L)^2.$$

Ahora, si los coeficientes de $P$ y $R$ son racionales, y puesto que los coeficientes del producto $PR = X$ son enteros, entonces, por el artículo 42 los coeficientes de $P$ y $R$ son enteros. Así, $L$ y $\frac{1}{L}$ son enteros, por tanto para que $\frac{1}{L}$ sea entero tiene que pasar que $L = \pm 1$ y como $n = (1 + A + B + \cdots + K + L)^2$, entonces se tendrá un cuadrado mayor que uno, y esto contradice la suposición de que $n$ es primo. Por lo tanto, $P$ no puede tener coeficientes racionales.

[28] De la teoría de polinomios se sabe que la ecuación cuyas raíces son los recíprocos de las raíces de $x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \cdots + Kx + L$ es $x^\lambda + \frac{K}{L}x^{\lambda-1} + \cdots + \frac{A}{L}x + \frac{1}{L}$.

De estos cuatro casos se concluye que $P$ no puede tener todos sus coeficientes racionales. Así, si el polinomio $X = x^{n-1} + x^{n-2} + \cdots + x + 1$, con $n$ primo, es divisible por un polinomio $P$ de grado menor, entonces $P$ no puede tener todos sus coeficientes racionales.

De esta manera se ha llegado al objetivo del capítulo, parte esencial en el análisis sobre la construcción de polígonos regulares con regla y compás.

Recordemos que uno de los objetivos de la sección VII es hallar las raíces del polinomio $X$ y para esto Gauss usará *ecuaciones auxiliares* de menor grado. De hecho, la irreductibilidad del polinomio $X$ se usará para probar que cualquier raíz de una ecuación auxiliar se podrá expresar en términos de otra raíz –de la misma ecuación–. Esto será de utilidad para encontrar una descomposición del polinomio $X$.

# Capítulo III

## Descomposición del polinomio $x^{n-1} + x^{n-2} + \cdots + x + 1$ y las soluciones por radicales de sus raíces.

### Introducción

Después de mostrar la irreductibilidad del polinomio

$$X = x^{n-1} + x^{n-2} + \cdots + x + 1$$

en los racionales, Gauss se propuso desarrollar a $X$ en factores lo más simples posibles. Esto lo muestra en el artículo 352 y para ello previamente definirá una distribución de las raíces de la unidad, distintas de uno, en una modalidad que llama ***períodos*** [art. 343]. Para estos elementos que definió –los períodos- mostrará dos propiedades principales en los artículos 346 y 351.

Para la demostración del artículo 346 Gauss requiere de una propiedad de períodos que muestra a lo largo de los artículos 344 y 345, en estos artículos determinará el producto de una cantidad finita de períodos. Los artículos 348 y 350 serán la base de la demostración del artículo 351.

Posteriormente se darán ejemplos (para $n = 19$ y $n = 17$ en el polinomio $X$) de cómo hallar los factores de la ecuación. Es importante mencionar que, a partir del art. 343, al final de cada propiedad se dará un ejemplo para $n = 19$. Lo anterior se realiza con la finalidad de clarificar el desarrollo de la teoría hasta llegar al objetivo de esta segunda parte para un ejemplo particular. Ha de notarse también, que hasta ese punto no se habla aún sobre la construcción de un polígono.

### Períodos Gaussianos.

Antes de empezar a desarrollar la teoría de Gauss sobre períodos, se debe mencionar que la base de esta distribución de las raíces –en lo que llamaremos períodos– proviene de los ciclos que forman los residuos de las potencias de las clases de residuos módulo $n$. Por ejemplo, para $n = 17$ se tiene la siguiente tabla de residuos:

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 8 | 16 | 15 | 13 | 9 | 1 | 2 | 4 | 8 | 16 | 15 | 13 | 9 | 1 |
| 3 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
| 4 | 4 | 16 | 13 | 1 | 4 | 16 | 13 | 1 | 4 | 16 | 13 | 1 | 4 | 16 | 13 | 1 |
| 5 | 5 | 8 | 6 | 13 | 14 | 2 | 10 | 16 | 12 | 9 | 11 | 4 | 3 | 15 | 7 | 1 |
| 6 | 6 | 2 | 12 | 4 | 7 | 8 | 14 | 16 | 11 | 15 | 5 | 13 | 10 | 9 | 3 | 1 |
| 7 | 7 | 15 | 3 | 4 | 11 | 9 | 12 | 16 | 10 | 2 | 14 | 13 | 6 | 8 | 5 | 1 |
| 8 | 8 | 13 | 2 | 16 | 9 | 4 | 15 | 1 | 8 | 13 | 2 | 16 | 9 | 4 | 15 | 1 |
| 9 | 9 | 13 | 15 | 16 | 8 | 4 | 2 | 1 | 9 | 13 | 15 | 16 | 8 | 4 | 2 | 1 |
| 10 | 10 | 15 | 14 | 4 | 6 | 9 | 5 | 16 | 7 | 2 | 3 | 13 | 11 | 8 | 12 | 1 |
| 11 | 11 | 2 | 5 | 4 | 10 | 8 | 3 | 16 | 6 | 15 | 12 | 13 | 7 | 9 | 14 | 1 |
| 12 | 12 | 8 | 11 | 13 | 3 | 2 | 7 | 16 | 5 | 9 | 6 | 4 | 14 | 15 | 10 | 1 |
| 13 | 13 | 16 | 4 | 1 | 13 | 16 | 4 | 1 | 13 | 16 | 4 | 1 | 13 | 16 | 4 | 1 |
| 14 | 14 | 9 | 7 | 13 | 12 | 15 | 6 | 16 | 3 | 8 | 10 | 4 | 5 | 2 | 11 | 1 |
| 15 | 15 | 4 | 9 | 16 | 2 | 13 | 8 | 1 | 15 | 4 | 9 | 16 | 2 | 13 | 8 | 1 |
| 16 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 | 16 | 1 |

Tabla 1. Residuos de potencias módulo 17. La primera columna representa el elemento de la clase módulo $n$, y el primer reglón a la potencia.

En este caso algunos ejemplos de períodos son
$\{r, r^2, r^4, r^8, r^{16}, r^{15}, r^{13}, r^9\}$, $\{r, r^4, r^{16}, r^{13}\}$, $\{r^2, r^8, r^{15}, r^9\}$ y $\{r, r^{16}\}$,
donde $r$ es una raíz distinta de la unidad de la ecuación $x^{17} - 1 = 0$.
Se podría decir que un período –en el sentido de Gauss– es un conjunto de ciertas raíces $n$-ésimas de la unidad; sin embargo, este no es arbitrario sino que está formado de tal manera que todos los exponentes de la raíz $r$ en ese conjunto conforman un período –en el sentido de congruencias– del número $r$. Es decir, la suma de los exponentes en este conjunto ha de ser congruente con cero módulo $n$.
Por ejemplo, $r, r^2, r^4$ y $r^8$ no se puede considerar un período siguiendo la definición de Gauss, ya que los números 1, 2, 4, 8 no tienen un comportamiento periódico –la suma $1 + 2 + 4 + 8$ no es congruente con cero módulo 17–. Las raíces que corresponden a un período dependerán de los factores de $n - 1$. Esta manera en la que Gauss distribuye las raíces de la unidad, se debe a que podrá relacionar dichas raíces con funciones que tienen solución por radicales, idea que surge a partir de los estudios de Lagrange[29] y Vandermonde.

[29] En 1771 Lagrange publicó en la Academia Prusiana de Ciencias el artículo *Réfléxions sur la Résolution Algébrique des Equations* en el cual analizó los diversos métodos que ya eran conocidos en su época acerca de la resolución de ecuaciones de tercer y cuarto grado, y se percató de que el común denominador en estos métodos era la reducción de las ecuaciones a otras de grado menor llamadas *ecuaciones resolventes*.
Para más detalles ver [Pardo Rego Venancio, *Lagrange: la elegancia matemática*, Nivola Libros y Ediciones, S.L., 2003]

A continuación se desarrolla con detalle la definición de período y las propiedades antes mencionadas. Recordemos que en esta tesis, salvo que se diga lo contrario, $r$ es una raíz $n$–ésima de la unidad.

**Art. 343.** Sea $g$ una raíz primitiva módulo $n$,[30] entonces los números $g, g^2, g^3, \dots, g^{n-2}, g^{n-1}$ forman un sistema reducido de residuos y cada uno de ellos será congruente con uno de los elementos del conjunto $\{1, 2, \dots, n-1\}$ según el módulo $n$;[31] esto es, los números $1,\ g,\ g^2,\ g^3, \dots, g^{n-2}$ son una permutación para $\{1, 2, \dots, n-1\}$. Entonces las raíces $r,\ r^g,\ r^{g^2}, \dots, r^{g^{n-2}}$ forman un nuevo orden para las raíces $r,\ r^2,\ r^3, \dots, r^{n-1}$. Así, se tiene que

$$\left\{r, r^g, r^{g^2}, \dots, r^{g^{n-2}}\right\} = \{r, r^2, r^3, \dots, r^{n-1}\} = \Omega.$$

Si pasa que $n-1 = ef$, donde $e$ y $f$ son enteros positivos, entonces se pueden distribuir las raíces de $\Omega$ en $e$ conjuntos de $f$ términos, para ello Gauss utiliza los exponentes $1, g, g^2, g^3, \dots, g^{n-2}$ y eleva estos números (entre los cuales está $g^f$) a la potencia $e$, pero a partir de $\left(g^f\right)^e$ los residuos se repetirán –esto porque $g$ es raíz primitiva módulo $n$–, y por tanto en el conjunto $\{r,\ r^{g^e}, r^{g^{2e}}, \dots, r^{g^{(n-2)e}}\}$ solo se tendrán $f$ raíces distintas que son

$$r,\ r^{g^e}, r^{g^{2e}}, \dots, r^{g^{(f-1)e}}.$$

Finalmente, estas raíces se elevan a la potencia $\lambda$, un número no divisible por $n$, y se obtienen las $f$ raíces $r^\lambda, r^{\lambda g^e}, r^{\lambda g^{2e}}, \dots, r^{\lambda g^{(f-1)e}}$. Gauss llama *período* $(f, \lambda)$ al conjunto de estas raíces y designa por $(f, \lambda)$ a la suma de estas raíces[32], así, si hacemos $g^e = h$, la suma $(f, \lambda)$ es

$$r^\lambda + r^{\lambda h} + r^{\lambda h^2} + \cdots + r^{\lambda h^{f-1}}.$$

Con esto Gauss divide las raíces contenidas en $\Omega$ de tal manera que cada parte –período– resultará ser la raíz de cierto polinomio, todo esto con el fin de expresar las raíces de $\Omega$ en términos de radicales.

**Ejemplo.** Para $n = 17$, se toman $e = 2$, $f = 8$ y la raíz primitiva $g = 3$.

Así, como se puede ver en la tabla que se muestra arriba los residuos de las potencias de $g = 3$ módulo 17 son

---

[30] $g$ es una raíz primitiva módulo un primo $n$ si las potencias $g^0, g^1, g^2, g^3, \dots, g^{n-2}, g^{n-1}$ forman un ciclo, es decir, si la primera potencia congruente con $g^0 = 1$ módulo $n$ es $g^{n-1}$. En la tabla que se muestra arriba se puede ver que $g = 3$ satisface esta condición para $n = 17$, así 3 es una raíz primitiva módulo 17.

[31] Ya que si $g^m \equiv g^l (mod\ n)$ para $m, l \in \{1, 2, \dots, n-1\}$ y suponiendo sin pérdida de generalidad que $l < m$ se tiene que $g^{m-l} \equiv 1\ (mod\ n)$, pero $m - l < n$, lo cual contradice el hecho de que $n$ es el mínimo entero que satisface esta congruencia, de donde los residuos de los números $1, g, g^2, g^3, \dots, g^{n-2}$ son diferentes, y forman un sistema completo de residuos módulo $n$.

[32] En el *Disquisitiones Arithmeticae* en los artículos posteriores Gauss usa indistintamente la palabra *período* para referirse al conjunto de raíces que forman $(f, \lambda)$ y a la suma de estas raíces. En este trabajo también se usará indistintamente y de ser necesario se harán las aclaraciones apropiadas cuando se pueda dar una confusión.

| $g^{16}$ | $g$ | $g^2$ | $g^3$ | $g^4$ | $g^5$ | $g^6$ | $g^7$ | $g^8$ | $g^9$ | $g^{10}$ | $g^{11}$ | $g^{12}$ | $g^{13}$ | $g^{14}$ | $g^{15}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 |

Luego se eleva a la potencia 2 cada uno de estos residuos y se obtiene

| 1 | $3^2$ | $9^2$ | $10^2$ | $13^2$ | $5^2$ | $15^2$ | $11^2$ | $16^2$ | $14^2$ | $8^2$ | $7^2$ | $4^2$ | $12^2$ | $2^2$ | $6^2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 9 | 13 | 15 | 16 | 8 | 4 | 2 | 1 | 9 | 13 | 15 | 16 | 8 | 4 | 2 |

A partir de estos residuos se podrán generar las raíces de un período de $f$ términos, por ejemplo, si se quieren hallar las $f$ raíces que conforman el período $(8,1)$, se han de multiplicar estos residuos por $\lambda = 1$, de esta manera, el período $(8,1)$ es

$$\{r, r^9, r^{13}, r^{15}, r^{16}, r^8, r^4, r^2\}.$$

Si en cambio estos residuos se multiplican por $\lambda = 3$, se obtienen los residuos $3, 10, 5, 11, 14, 7, 12, 6$, y así se tiene que

$$(8,3) = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6,$$

para $\lambda = 2$, se tiene el período $(8,2) = \{r^2, r, r^9, r^{13}, r^{15}, r^{16}, r^8, r^4\}$,
y cuando $\lambda = 5$ se obtiene el período $\{r^5, r^{11}, r^{14}, r^7, r^{12}, r^6, r^3, r^{10}\}$.
Note que para cualquier $\lambda \neq 1, 3$ no divisible por $n$ se obtendrá el período $(8,1)$ o el período $(8,3)$.
Puesto que $n - 1$ también es igual a $4 \cdot 4$, entonces otra manera de distribuir las raíces de la unidad en $\Omega$ es en 4 períodos de 4 términos. En este caso $e = f = 4$, así en lugar de elevar al cuadrado los residuos de las potencias de $g$, se elevan a la potencia cuarta. De esta forma se obtienen los residuos 1, 13, 16, 4 módulo $n$ y por lo tanto, se tiene que

$$(4,1) = r + r^{13} + r^{16} + r^4, \text{ y}$$
$$(4,2) = r^2 + r^{2\cdot 13} + r^{2.16} + r^{2\cdot 4} = r^2 + r^9 + r^{15} + r^8,$$

como se puede notar $(4,1) + (4,2) = (8,1)$.

Ahora veamos que el concepto de período está bien definido, esto es, que no depende de la raíz primitiva que se escoja.
Primero observe que si $\lambda$ es cualquier entero no divisible por $n$, se tendrá que

$$\left\{r^\lambda, r^{\lambda g}, r^{\lambda g^2}, \dots, r^{\lambda g^{n-2}} : n \nmid \lambda\right\} = \left\{r^\lambda, r^{2\lambda}, r^{3\lambda}, \dots, r^{(n-1)\lambda} : n \nmid \lambda\right\} = \Omega.$$

Debido a que $g^{n-1} \equiv 1 (mod\ n)$ y $\lambda$ es un entero no divisible por $n$, se tiene que, si $\mu \equiv \nu\ (mod\ n-1)$ entonces $\lambda g^\mu \equiv \lambda g^\nu (mod\ n)$ y por lo tanto $r^{\lambda g^\mu} = r^{\lambda g^\nu}$.[33]
Así, si $G$ es otra raíz primitiva, entonces con un análisis semejante a lo realizado al inicio del artículo se tiene que las raíces $r,\ r^G,\ r^{G^2}, \dots, r^{G^{n-2}}$ serán iguales a las raíces $r,\ r^2,\ r^3, \dots, r^{n-2}$ y en consecuencia a las raíces $r,\ r^g,\ r^{g^2}, \dots, r^{g^{n-2}}$, no necesariamente en ese orden. De aquí que las potencias $1,\ G,\ G^2,\ G^3, \dots, G^{n-2}$ sean congruentes a

[33] Si $\mu \equiv \nu\ mod(n-1)$ $(i.e.\ \mu - \nu = (n-1)q)$, entonces $g^{\mu-\nu} = (g^{n-1})^q \equiv 1\ (mod\ n)$, es decir, $g^\mu \equiv g^\nu (mod\ n)$ y por tanto $r^{\lambda g^\mu} = r^{\lambda g^\nu}$.

$1,\ g,\ g^2,\ g^3, \ldots, g^{n-2}$ módulo $n$, aunque no necesariamente en ese orden. Así, los números $1, G^e, G^{2e}, G^{3e}, \ldots, G^{(f-1)e}$ serán congruentes a $1, g^e, g^{2e}, g^{3e}, \ldots, g^{(f-1)e}$, salvo el orden.[34] Si ahora se hace $H = G^e$, entonces los $f$ números $1,\ h,\ h^2,\ h^3, \ldots, h^{f-1}$ (recuerde que $h = g^e$) serán congruentes a $1,\ H,\ H^2,\ H^3, \ldots, H^{f-1}$ según el módulo $n$, salvo el orden. Por lo tanto, las raíces $r,\ r^h,\ r^{h^2}, \ldots, r^{h^{f-1}}$ serán iguales a las raíces $r,\ r^H,\ r^{H^2}, \ldots, r^{H^{f-1}}$, y así también lo serán $r^\lambda,\ r^{\lambda h},\ r^{\lambda h^2}, \ldots, r^{\lambda h^{f-1}}$ y $r^\lambda,\ r^{\lambda H},\ r^{\lambda H^2}, \ldots, r^{\lambda H^{f-1}}$, salvo el orden.

Por lo tanto, las raíces primitivas $g$ y $G$ generan la misma distribución en $e$ períodos de $f$ términos de las raíces en $\Omega$, esto es, que la distribución no depende de la raíz primitiva que se elija.

**Ejemplo.** Para $n = 19$, se tiene que 2 y 3 son raíces primitivas.

Considérese primero $g = 2$, $e = 3$ y $f = 6$, entonces se distribuirán las raíces del polinomio $x^{18} + x^{17} + \cdots + x + 1$ en tres períodos distintos de seis términos.

Para obtener el período $(6,1)$ se calculan los residuos mínimos de $1,\ g^e,\ g^{2e},\ g^{3e}, \ldots, g^{(f-1)e}$:

$$1 \equiv 1(mod\ 19)$$
$$g^e = 2^3 = 8 \equiv 8(mod\ 19)$$
$$g^{2e} = 2^{2\cdot 3} \equiv 7\ (mod\ 19)$$
$$g^{3e} = 2^{3\cdot 3} \equiv 18(mod\ 19)$$
$$g^{4e} = 2^{4\cdot 3} \equiv 11(mod\ 19)$$
$$g^{(f-1)e} = 2^{5\cdot 3} \equiv 12\ (mod\ 19).$$

Así,

$$(6,1) = \{r, r^8, r^7, r^{11}, r^{12}, r^{18}\}.$$

Los residuos mínimos de $2g^e,\ 2g^{2e}, \ldots, 2g^{5e}$ módulo 19 arrojan los exponentes de las raíces que conforman el período $(6,2)$, así

$$(6,2) = \{r^2, r^3, r^5, r^{14}, r^{16}, r^{17}\}.$$

Análogamente se obtienen

$$(6,3) = \{r^3, r^{24}, r^{21}, r^{33}, r^{36}, r^{54}\} = \{r^3, r^5, r^2, r^{14}, r^{17}, r^{16}\} = (6,2)$$

y $$(6,4) = \{r^4, r^{32}, r^{28}, r^{44}.r^{48}, r^{72}\} = \{r^4, r^{13}, r^9, r^6, r^{10}, r^{15}\}.$$

Por otro lado, utilizando la raíz primitiva $g = 3$, se tiene que

$$g^e = 3^3 = 27 \equiv 8\ (mod\ 19)$$
$$g^{2e} = 3^{2\cdot 3} \equiv 7\ (mod\ 19)$$
$$g^{3e} = 3^{3\cdot 3} \equiv 18(mod\ 19)$$
$$g^{4e} = 3^{4\cdot 3} \equiv 11(mod\ 19)$$
$$g^{(f-1)e} = 3^{5\cdot 3} \equiv 12\ (mod\ 19),$$

[34] Arriba se vio que entre los números $1, g^e, g^{2e}, g^{3e}, \ldots, g^{(n-2)e}$ sólo hay $f$ raíces distintas. Lo mismo se verifica para $1, G^e, G^{2e}, G^{3e}, \ldots, G^{(n-2)e}$.

por lo que $(6,1) = \{r, r^7, r^8, r^{11}, r^{12}, r^{18}\}$, resultando ser igual al que se obtuvo con la raíz primitiva $g = 2$. Se puede verificar que también (6,2) y (6,4) son iguales a los que se obtuvieron antes. Así, la distribución de las raíces de Ω en períodos de $f$ términos será la misma independientemente de la raíz primitiva que se elija.

**Art. 344.**- Aquí se muestran diversas propiedades de los períodos que serán de gran utilidad en la resolución del problema principal.

I. Si dos períodos con el mismo número de raíces (a los que Gauss llama *similares*) tienen una raíz en común entonces son iguales, *i.e.*, si $r^{\lambda'}$ es una raíz en $(f,\lambda)$ entonces los períodos $(f,\lambda)$ y $(f,\lambda')$ tendrán exactamente las mismas raíces.

Observe que $\lambda h^f = \lambda g^{ef} = \lambda g^{n-1} \equiv \lambda (mod\ n)$, por tanto se tiene que

$$\lambda h^{f+1} \equiv \lambda h\ (mod\ n)$$
$$\lambda h^{f+2} \equiv \lambda h^2\ (mod\ n)$$
$$\vdots$$

de donde,

$$(f,\lambda h) \overset{\text{def}}{=} \left\{r^{\lambda h}, r^{\lambda h^2}, \dots, r^{\lambda h^f}\right\} = \left\{r^{\lambda h}, r^{\lambda h^2}, \dots, r^{\lambda h^{f-1}}, r^{\lambda}\right\} \overset{\text{def}}{=} (f,\lambda)$$
$$(f,\lambda h^2) \overset{\text{def}}{=} \left\{r^{\lambda h^2}, \dots, r^{\lambda h^f}, r^{\lambda h^{f+1}}\right\} = \left\{r^{\lambda h^2}, \dots, r^{\lambda h^{f-1}}, r^{\lambda}, r^{\lambda h}\right\} \overset{\text{def}}{=} (f,\lambda)$$
$$\vdots$$

En general, se tiene que el período $(f,\lambda)$ es idéntico a los períodos $(f,\lambda)$, $(f,\lambda h^2)$, $(f,\lambda h^3)$, .... Puesto que $r^{\lambda'} \in (f,\lambda)$, entonces $r^{\lambda'} = r^{\lambda h^j}$ p. a. entero $j$ y por lo tanto,

$$(f,\lambda') \overset{\text{def}}{=} \left\{r^{\lambda'}, r^{\lambda' h}, r^{\lambda' h^2}, \dots, r^{\lambda' h^{f-1}}\right\} = \left\{r^{\lambda h^j}, r^{\lambda h^{j+1}}, r^{\lambda h^{j+2}}, \dots, r^{\lambda h^{j+f-1}}\right\}$$
$$\overset{\text{def}}{=} \left(f,\lambda h^j\right) = (f,\lambda).$$

Es decir, sí dos períodos tienen una raíz en común, entonces serán iguales. Además, si $r^{\lambda}$ y $r^{\lambda'} \in (f,\lambda)$ entonces,

$$r^{\lambda'} = r^{\lambda h^j} \text{ p. a. entero } j \quad \text{y} \quad r^{\lambda} = r^{\lambda' h^k} \text{ p. a. entero } k,$$

de donde $\lambda' \equiv \lambda h^v (mod\ n)$.

**Ejemplo.** Previamente se mostró que para el módulo 19 se tiene la siguiente distribución en períodos con seis términos cada uno. Estos son

$$(6,1) = \{r, r^8, r^7, r^{11}, r^{12}, r^{18}\} \qquad (6,2) = \{r^2, r^3, r^5, r^{14}, r^{16}, r^{17}\}$$

$$(6,4) = \{r^4, r^{13}, r^9, r^6, r^{10}, r^{15}\}.$$

Obsérvese que, de acuerdo a la definición el período (6,3) es

$$\{r^3,\ r^{3\cdot 8},\ r^{3\cdot 7},\ r^{3\cdot 11},\ r^{3\cdot 12},\ r^{3\cdot 18}\},$$

pero debido a que se tienen las siguientes congruencias

$$3 \cdot 8 \equiv 5 (mod\ 19)$$
$$3 \cdot 7 \equiv 2 (mod\ 19)$$

$$3 \cdot 11 \equiv 14(mod\ 19)$$
$$3 \cdot 12 \equiv 17(mod\ 19)$$
$$3 \cdot 18 \equiv 16(mod\ 19),$$

el período $(6,3)$ es igual al período $(6,2)$.

Además, puesto que $r^{14}$ es una raíz común de los períodos $(6,2)$ y $(6,14)$, aplicando directamente la propiedad I, se tiene que $(6,2) = (6,14)$. De la misma manera, se puede verificar que los períodos $(6,1)$ y $(6,18)$ son iguales, así como $(6,2) = (6,17)$ y $(6,4) = (6,6) = (6,15)$.
Ahora, como $r^9$ y $r^6$ están en el mismo período, entonces se satisface la congruencia $9 \equiv 6 \cdot (2^3)^4\ mod\ 19$.

II. Los períodos $(f,1)$, $(f,g)$, $(f,g^2), \ldots, (f,g^{e-1})$, considerados como conjunto de raíces, son distintos entre sí y el total de las raíces contenidas en todos los períodos es el conjunto $\Omega$, esto es, $\Omega = (f,1) \cup (f,g) \cup (f,g^2) \cup \ldots \cup (f,g^{e-1})$, excepto cuando $f = n-1$ y $e = 1$, en tal caso $(f,1)$ coincidirá con $\Omega$.

Veamos por qué los periodos mencionados son diferentes. Si los períodos $(f,\lambda)$ y $(f,\lambda')$ con $\lambda,\ \lambda' \in \{1, g, g^2, g^3, \ldots, g^{e-1}\}$ fueran iguales, entonces $r^{\lambda}$ y $r^{\lambda'}$ estarían en un mismo período y por tanto de la última observación en (I) se debería satisfacer la congruencia

$$\lambda' \equiv \lambda g^{ev}(mod\ n) \text{ para algún } v,$$

lo cual es imposible ya que $\frac{\lambda'}{\lambda}$ no puede ser congruente con alguna potencia de $g^e$ módulo $n$. De forma análoga se puede verificar que si $\lambda$ es un entero no divisible por $n$, entonces los períodos $(f,\lambda)$, $(f,\lambda g)$, $(f,\lambda g^2), \ldots, (f,\lambda g^{e-1})$ son distintos entre ellos. Así, los conjuntos $(f,1) \cup (f,g) \cup (f,g^2) \cup \ldots \cup (f,g^{e-1})$ y $(f,\lambda) \cup (f,\lambda g) \cup (f,\lambda g^2) \cup \ldots \cup (f,\lambda g^{e-1})$ están conformados por $n-1$ raíces distintas de la unidad cada uno, entonces,
$(f,1) \cup (f,g) \cup (f,g^2) \cup \ldots \cup (f,g^{e-1}) = \Omega = (f,\lambda) \cup (f,\lambda g) \cup (f,\lambda g^2) \cup \ldots \cup (f,\lambda g^{e-1})$,
y así cualquier otro período de $f$ términos –excepto $f = (f,0) = (f,kn)$–[35] es alguno en $(f,1) \cup (f,g) \cup (f,g^2) \cup \ldots \cup (f,g^{e-1})$.

**Ejemplo.** Para $n = 19$, $f = 6$ y usando la raíz primitiva $g = 2$, en el ejemplo anterior se mostró que raíces conforman los períodos $(6,1), (6,2), (6,2^2)$, entonces se tiene lo siguiente
$(6,1) \cup (6,2) \cup (6,2^2) = \{r, r^8, r^7, r^{11}.r^{12}.r^{18}, r^2, r^3, r^5, r^{14}, r^{16}, r^{17}, r^4, r^{13}, r^9, r^6, r^{10}, r^{15}\}$,
que resulta ser el conjunto $\Omega$ para $n = 19$, esto es, el conjunto de las raíces 19-ésimas de la unidad.

[35] El período $(f,0) = r^0 + r^{0\cdot h} + r^{0\cdot h^2} + \cdots + r^{0\cdot h^{f-1}} = f = r^{kn} + r^{knh} + r^{knh^2} + \cdots + r^{knh^{f-1}} = (f,kn)$.

Además, cualquier otro período de seis términos será igual a (6,1), o a (6,2), o a $(6,2^2)$. Por ejemplo, se puede verificar que los períodos (6,25) y (6,4) tienen en común a la raíz $r^6$, entonces $(6,25) = (6,4)$.

III. Si $n-1 = abc$, con $a, b, c$ enteros positivos, entonces haciendo $f = bc$ y $e = a$ se tendrán $a$ períodos de $bc$ términos, y a su vez cada período de $bc$ términos está compuesto de $b$ períodos de $c$ términos;

$$(bc,\lambda) = \left\{r^{\lambda}, r^{\lambda g^{a}}, r^{\lambda g^{2a}}, \dots, r^{\lambda g^{abc-a}}\right\} = (c,\lambda) \cup (c,\lambda g^{a}) \cup (c,\lambda g^{2a}) \cup \dots \cup \left(c,\lambda g^{ab-a}\right).^{36}$$

**Ejemplo.** Para $n = 19$ se tiene $n-1 = 3\cdot 3\cdot 2$, entonces el período $(6,2) = \{r^2,\ r^3,\ r^5,\ r^{14},\ r^{16},\ r^{17}\}$ se compone a su vez de tres períodos de dos términos cada uno. Así, considerando $\lambda = 2$ y la raíz primitiva $g = 2$, de acuerdo a la propiedad III estos son $(2,2)$, $(2, 2\cdot 2^3)$, $(2, 2\cdot 2^{2\cdot 3})$, los cuales son respectivamente iguales a

$$(2,2) = \{r^2, r^{14}\}, \quad (2,3) = \{r^3, r^{16}\} \quad \text{y} \quad (2,5) = \{r^5, r^{17}\}.$$

**Art. 345.** Ahora se mostrarán algunas características sobre productos de períodos, las cuales serán de gran importancia en el proceso para hallar las *ecuaciones auxiliares* que se mencionaron en la introducción de este capítulo.

A continuación se presenta un ejemplo para establecer la idea de la demostración del teorema correspondiente a este artículo.

**Ejemplo.** Para $n = 19$ se considera $n-1 = 6\cdot 3$ y la raíz primitiva $g = 2$, entonces las raíces 19-ésimas de la unidad se distribuirán en seis períodos de tres términos. Así, de las siguientes congruencias

$$g^e = 2^6 \equiv 7 (mod\ 19)$$
$$g^{2e} = 2^{2\cdot 6} \equiv 11 (mod\ 19)$$

se obtienen los períodos

$$(3,1) = \{r, r^7, r^{11}\}$$
$$(3,2) = \{r^2, r^{14}, r^3\}$$
$$(3,4) = \{r^4, r^9, r^6\}$$
$$(3,8) = \{r^8, r^{18}, r^{12}\}$$
$$(3,16) = \{r^{16}, r^{17}, r^5\}$$
$$(3,13) = \{r^{13}, r^{15}, r^{10}\}.$$

Entonces, el producto de la suma (3,1) por la suma (3,2) es

---

[36] Como se sabe $(bc,\lambda)$ consta de las raíces $r^{\lambda}$, $r^{\lambda g^a}$, $r^{\lambda g^{2a}}$, $r^{\lambda g^{3a}}$, …, $r^{\lambda g^{(b-1)a}}$, …, $r^{\lambda g^{a(bc-1)}}$, y puesto que los coeficientes de las raíces $r^{\lambda}$, $r^{\lambda a}$, $r^{\lambda g^{2a}}$, $r^{\lambda g^{3a}}$, …, $r^{\lambda g^{(b-1)a}}$ satisfacen $\lambda \equiv \lambda g^{av+ab} (mod\ n)$ y $\lambda g^{av'} \not\equiv \lambda g^{av+a\beta} (mod\ n)$, donde $v, v'$ son enteros entre $1, \dots, b-1$, entonces cada una de esas raíces debe de estar en un período distinto, así $(bc,\lambda)$ consta de los $b$ períodos

$$(c,\lambda), (c,\lambda g^a), (c,\lambda g^{2a}), (c,\lambda g^{3a}), \dots, (c,\lambda g^{(b-1)a}).$$

$$(3,1)\cdot(3,2) = rr^2 + rr^{14} + rr^3 + r^7r^2 + r^7r^{14} + r^7r^3 + r^{11}r^2 + r^{11}r^{14} + r^{11}r^3$$
$$= r^3 + r^{15} + r^4 + r^9 + r^2 + r^{10} + r^{13} + r^6 + r^{14}$$
$$= (r^2 + r^{14} + r^3) + (r^4 + r^9 + r^6) + (r^{13} + r^{15} + r^{10})$$
$$= (3,2) + (3,4) + (3,13)$$
$$= (3,3) + (3,4) + (3,15),$$

esta última igualdad se cumple debido a la propiedad presentada en el art. 344.I.

Ahora se hace un producto de tres períodos,

$$(3,1)(3,2)(3,8) = [r^3 + r^{15} + r^4 + r^9 + r^2 + r^{10} + r^{13} + r^6 + r^{14}][r^8 + r^{18} + r^{12}]$$
$$= r^{11} + r^{23} + r^{12} + r^{17} + r^{10} + r^{18} + r^{21} + r^{14} + r^{22} + r^{21} + r^{33} + r^{22}$$
$$+ r^{27} + r^{20} + r^{28} + r^{31} + r^{24} + r^{32} + r^{15} + r^{27} + r^{16} + r^{21} + r^{14} + r^{22}$$
$$+ r^{25} + r^{18} + r^{26}$$
$$= r^{11} + r^4 + 2r^{12} + r^{17} + r^{10} + 2r^{18} + 3r^2 + 3r^{14} + 3r^3 + 2r^8 + r + r^9$$
$$+ r^5 + r^{13} + r^{15} + r^{16} + r^6 + r^7$$
$$= (3,1) + (3,4) + 2(3,8) + (3,16) + (3,13) + 3(3,2).$$

Como se puede apreciar, el producto de dos o más períodos es una combinación lineal de períodos del mismo número de términos. A continuación se mostrará cómo obtener esta expresión.

TEOREMA. Sean $(f,\lambda) = \{r^{\lambda}, r^{\lambda'}, r^{\lambda''}, \ldots\}$ y $(f,\mu)$ dos períodos similares [Ver art. 344 I.], idénticos o diferentes. Entonces, el producto de $(f,\lambda)$ por $(f,\mu)$ será la suma de $f$ períodos similares, a saber,

$$(f,\lambda+\mu) + (f,\lambda'+\mu) + (f,\lambda''+\mu) + \cdots = W.$$

*Demostración.*- Sea $g$ una raíz primitiva para el módulo $n$, $h = g^e$ y $n-1 = ef$. Primero desarrollemos el producto $(f,\lambda)\cdot(f,\mu)$

$$(f,\lambda)\cdot(f,\mu) = (f,\lambda)\cdot\left(r^{\mu} + r^{\mu h} + r^{\mu h^2} + \cdots + r^{\mu h^{f-1}}\right)$$
$$= (f,\lambda)\cdot r^{\mu} + (f,\lambda)\cdot r^{\mu h} + (f,\lambda)\cdot r^{\mu h^2} + \cdots + (f,\lambda)\cdot r^{\mu h^{f-1}}.$$

Por otro lado, del artículo anterior, se sabe que $(f,\lambda) = (f,\lambda h) = (f,\lambda h^2) = (f,\lambda h^3) = \cdots$. Entonces,

$$(f,\lambda)\cdot(f,\mu) = (f,\lambda)\cdot r^{\mu} + (f,\lambda h)\cdot r^{\mu h} + (f,\lambda h^2)\cdot r^{\mu h^2} + \cdots + \left(f,\lambda h^{f-1}\right)\cdot r^{\mu h^{f-1}}.$$

De la definición de los períodos y desarrollando los productos se tiene que

$$(f,\lambda)\cdot(f,\mu) = \left(r^{\lambda+\mu} + r^{\lambda h+\mu} + r^{\lambda h^2+\mu} + \cdots + r^{\lambda h^{f-1}+\mu}\right)$$
$$+ (r^{\lambda h+\mu h} + r^{\lambda h^2+\mu h} + r^{\lambda h^3+\mu h} + \cdots + r^{\lambda h^f+\mu h})$$
$$+ \left(r^{\lambda h^2+\mu h^2} + r^{\lambda h^3+\mu h^2} + r^{\lambda h^4+\mu h^2} + \cdots + r^{\lambda h^{f+1}+uh^2}\right) + \cdots$$
$$+ \left(r^{\lambda h^{f-1}+\mu h^{f-1}} + r^{\lambda h^f+\mu h^{f-1}} + r^{\lambda h^{f+1}+\mu h^{f-1}} + \cdots + r^{\lambda h^{2(f-1)}+\mu h^{f-1}}\right),$$

expresando en residuos mínimos y reordenando,

$$(f,\lambda)\cdot(f,\mu)=\left(r^{\lambda+\mu}+r^{(\lambda+\mu)h}+r^{(\lambda+\mu)h^2}+\cdots+r^{(\lambda+\mu)h^{f-1}}\right)$$
$$+\left(r^{\lambda h+\mu}+r^{(\lambda h+\mu)h}+r^{(\lambda h+\mu)h^2}+\cdots+r^{(\lambda h+\mu)h^{f-1}}\right)+\cdots$$
$$+\left(r^{\lambda h^{f-1}+\mu}+r^{(\lambda h^{f-1}+\mu)h}+r^{(\lambda h^{f-1}+\mu)h^2}+\cdots+r^{(\lambda h^{f-1}+\mu)h^{f-1}}\right)$$
$$=(f,\lambda+\mu)+(f,\lambda h+\mu)+(f,\lambda h^2+\mu)+\cdots+\left(f,\lambda h^{f-1}+\mu\right).$$

Ahora, como $\left\{r^{\lambda},r^{\lambda h},r^{\lambda h^2},\ldots,r^{\lambda h^{f-1}}\right\}=(f,\lambda)=\{r^{\lambda},r^{\lambda'},r^{\lambda''},\ldots\}$, entonces los números $\lambda,\lambda',\lambda'',\ldots$ deben ser congruentes a los números $\lambda,\ \lambda h,\ \lambda h^2,\ldots,\lambda h^{f-1}$ (no necesariamente en ese orden). Así,

$$\lambda+\mu,\ \lambda h+\mu,\ \lambda h^2+\mu,\ldots,\ \lambda h^{f-1}+\mu$$

son congruentes a

$$\lambda+\mu,\quad \lambda'+\mu,\quad \lambda''+\mu,\ldots,$$

de donde,

$$\left\{r^{\lambda+\mu},r^{\lambda h+\mu},r^{\lambda h^2+\mu},\ldots,r^{\lambda h^{f-1}+\mu}\right\}=\{r^{\lambda+\mu},r^{\lambda'+\mu},r^{\lambda''+\mu},\ldots\},$$

y por ello

$$(f,\lambda+\mu)\cup(f,\lambda'+\mu)\cup(f,\lambda''+\mu)\cup\ldots=(f,\lambda+\mu)\cup(f,\lambda h+\mu)\cup(f,\lambda h^2+\mu)\cup\ldots$$
$$\cup\ (f,\lambda h^{f-1}+\mu)$$

Así, $(f,\lambda)\cdot(f,\mu)=(f,\lambda+\mu)+(f,\lambda'+\mu)+(f,\lambda''+\mu)+\cdots=W.$

De este teorema se siguen algunos resultados que serán de gran utilidad para artículos posteriores:

I. Sea $k$ un entero, entonces se tiene

$$(f,\lambda)\cdot(f,\mu)=\left(f,k(\lambda+\mu)\right)+\left(f,k(\lambda'+\mu)\right)+\left(f,k(\lambda''+\mu)\right)+\cdots.$$

Sabemos que los números $\lambda,\ \lambda',\ \lambda'',\ldots$ son congruentes a los números $\lambda,\ \lambda h,\ \lambda h^2,\ldots,\ \lambda h^{f-1}$ (no importa el orden), de donde

$$(f,k\lambda)=\left\{r^{k\lambda},\ r^{k\lambda h},\ r^{k\lambda h^2},\ldots\right\}=\left\{r^{k\lambda},\ r^{k\lambda'},\ r^{k\lambda''},\ldots\right\}.$$

Así, por el teorema anterior,

$$(f,k\lambda)\cdot(f,k\mu)=(f,k\lambda+k\mu)+(f,k\lambda'+k\mu)+(f,k\lambda''+k\mu)+\cdots.$$

II. Si se considera $W$ como en el teorema previo entonces puede reducirse a la forma

$$af+b(f,1)+b'(f,g)+b''(f,g^2)+\cdots+b^e(f,g^{e-1}),$$

donde $a,b,b',b'',\ldots$ son enteros positivos (algunos pueden ser cero).

Esto se debe a que cada uno de los sumandos de $W$ será igual a $(f,kn)=f$ o a alguno de los períodos $(f,1),(f,g),(f,g^2),\ldots,(f,g^{e-1})$ dependiendo de si los números $\lambda+\mu,\ \lambda'+\mu,\ \lambda''+\mu,\ldots$ son o no divisibles por $n$ [art. 344.I].

Además, puesto que los períodos $(f,1),(f,g),(f,g^2),\ldots,(f,g^{e-1})$ coinciden con $(f,\lambda),\ (f,\lambda g),\ (f,\lambda g^2),\ldots,(f,\lambda g^{e-1})$, en algún orden, también se tiene que

$$W=af+c(f,\lambda)+c'(f,\lambda g)+c''(f,\lambda g^2)+\cdots+c^e(f,\lambda g^{e-1}),$$

donde $c, c', c'', \ldots$ son enteros positivos y coinciden con $b, b', b'', \ldots$. (en algún orden). Análogamente se puede concluir que

$$(f, k\lambda) \cdot (f, k\mu) = af + b(f, k) + b'(f, kg) + b''(f, kg^2) + \cdots + b^e(f, kg^{e-1}).$$

III. Sea $k$ un entero, entonces el producto

$$(f, k\lambda) \cdot (f, k\mu) \cdot (f, k\nu) = [af + b(f, k) + b'(f, kg) + \cdots + b^e(f, kg^{e-1})] \cdot (f, k\nu)$$

$$= af \cdot (f, k\nu) + b(f, k) \cdot (f, k\nu) + b'(f, kg) \cdot (f, k\nu) + \cdots + b^e(f, kg^{e-1}) \cdot (f, k\nu),$$

donde cada sumando de esta última expresión se reduce a una expresión similar a $[af + b(f, k) + b'(f, kg) + \cdots + b^e(f, kg^{e-1})]$. Entonces,

$$(f, k\lambda) \cdot (f, k\mu) \cdot (f, k\nu) = cf + d(f, k) + d'(f, kg) + d''(f, kg^2) + \cdots + d^e(f, kg^{e-1}),$$

con los coeficientes $c, d, d', \ldots$ enteros positivos (algunos pueden ser cero).

En general, esto se cumple para cualquier número de períodos que tengan la misma cantidad de términos, y en particular

$$(f, \lambda) \cdot (f, \mu) \cdot (f, \nu) = cf + d(f, 1) + d'(f, g) + d''(f, g^2) + \cdots + d^e(f, g^{e-1}).$$

IV. Sea $F(t, u, v, \ldots)$ una función algebraica racional, se considera que $F$ es una suma de términos de la forma $ht^\alpha u^\beta v^\lambda \ldots$. Entonces, al sustituir las incógnitas $t, u, v$ por los períodos similares $(f, \lambda), (f, \mu), (f, \nu), \ldots$ respectivamente y de los resultados anteriores se tiene que $F$ es una suma de términos de la forma

$$cf + d(f, 1) + d'(f, g) + d''(f, g^2) + \cdots + d^e(f, g^{e-1}),$$

por lo que el valor de $F$ será de la forma

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) + \cdots + B^e(f, g^{e-1}),$$

y los coeficientes $A, B, B'', \ldots$ serán enteros si todos los coeficientes en $F$ son enteros. Pero si sustituimos $t, u, v, \ldots$ por $(f, k\lambda), (f, k\mu), (f, k\nu), \ldots$ respectivamente, el valor de $F$ se reducirá a

$$A + B(f, k) + B'(f, kg) + B''(f, kg^2) + \cdots + B^e(f, kg^{e-1}).^{37}$$

**Ejemplo.** Siguiendo con nuestro caso para $n = 19$, y recordando que el período $(6,2)$ es $\{r^2, r^3, r^5, r^{14}, r^{16}, r^{17}\}$, entonces de acuerdo al teorema se tiene que el producto de la suma $(6,1)$ por la suma $(6,2)$, será

$$(6,1)(6,2) = (6, 1+2) + (6, 1+3) + (6, 1+5) + (6, 1+14)$$
$$+(6, 1+16) + (6, 1+17)$$
$$= (6,3) + (6,4) + (6,6) + (6,15) + (6,17) + (6,18),$$

pero en el ejemplo del art. 344 I. se vio que $(6,6)$ y $(6,15)$ son iguales a $(6,4)$; $(6,17)$ es igual a $(6,2)$; $(6,18)$ igual a $(6,1)$. Así,

$$(6,1)(6,2) = (6,1) + 2(6,2) + 3(6,4).$$

[37] La propiedad IV de hecho proporciona la herramienta que permitirá en el artículo siguiente trabajar con potencias de períodos y así poder expresar algún período como combinación lineal de otro cierto período.

**Art. 346.** El teorema que se muestra en este artículo indica en qué caso se puede expresar un período como combinación lineal de las potencias de otro período similar a él, y provee de un método para hallar tal expresión. Además es importante mencionar que en este artículo se hará uso de la irreductibilidad del polinomio ciclotómico $x^{n-1} + x^{n-2} + \cdots + x + 1$.

TEOREMA. Sean $\lambda, \mu$ dos enteros no divisibles por $n$ y escribiendo $p$ en lugar de $(f, \lambda)$, entonces cualquier otro período $(f, \mu)$ puede ser expresado en la forma

$$\alpha + \beta p + \gamma p^2 + \cdots + \theta p^{e-1},$$

donde los coeficientes $\alpha, \beta, \gamma, \ldots$ son cantidades racionales determinadas.

*Demostración.* Desígnense por $p'$, $p''$, $p'''$, ... a los $e-1$ períodos $(f, \lambda g)$, $(f, \lambda g^2)$, $(f, \lambda g^3), \ldots, (f, \lambda g^{e-1})$. Por lo visto en el art. 344 II, uno de ellos necesariamente coincidirá con $(f, \mu)$. Además satisfacen la ecuación

$$1 + p + p' + p'' + p''' + \cdots = 0. \qquad (1)$$

Ahora, de los corolarios II y III del artículo precedente, al desarrollar las primeras $e-1$-ésimas potencias de $p$ se obtienen las ecuaciones

$$p^2 = (f, \lambda)(f, \lambda) = a_1 f + a_2(f, \lambda) + a_3(f, \lambda g) + a_4(f, \lambda g^2) + a_5(f, \lambda g^3) + \cdots$$

$$p^3 = b_1 f + b_2(f, \lambda) + b_3(f, \lambda g) + b_4(f, \lambda g^2) + b_5(f, \lambda g^3) + \cdots$$

$$p^4 = c_1 f + c_2(f, \lambda) + c_3(f, \lambda g) + c_4(f, \lambda g^2) + c_5(f, \lambda g^3) + \cdots$$

$$\vdots$$

Es decir,

$$0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \cdots \qquad (2)$$

$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \cdots \qquad (3)$$

$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \cdots \qquad (4)$$

$$\vdots$$

Donde, los coeficientes $A, a, a', a'', a''', \ldots, B, b, b', b'', b''', \ldots, C, c, c', c'', c''', \ldots$ son enteros, y no dependen de $\lambda$.[38]

Supóngase que $(f, \mu) = p'$. De las ecuaciones (1), (2), (3),..., que forman un sistema de $(e-1)$ ecuaciones con las $(e-1)$ incógnitas $p'$, $p''$, $p'''$, ..., Gauss obtiene la ecuación,

$$\mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \cdots + \mathfrak{M}p^{e-1} + \mathfrak{N}p' = 0, \qquad (i)$$

con coeficientes $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}, \ldots, \mathfrak{M}$, $\mathfrak{N}$ enteros y no todos cero.
Esto lo hace por el método que ahora se conoce como *eliminación de Gauss.* [39]

[38] Véase art. 344 II.

Ahora, suponiendo que $\mathfrak{N} \neq 0$ entonces se podrá despejar $p'$ de la ecuación anterior, y así obtener $(f, \mu)$ en términos de las potencias de $p$. De forma análoga se procederá en caso de que $(f, \mu) = p'', \acute{o}\ p''', \acute{o}, \ldots$. Entonces, veamos que $\mathfrak{N}$ no puede ser igual a cero.
Si $\mathfrak{N} = 0$, entonces la ecuación (i) sería

$$\mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \cdots + \mathfrak{M}p^{e-1} = 0 \quad , \qquad \text{(ii)}$$

y como es de grado $e - 1$ entonces no puede ser satisfecha por más de $e - 1$ valores distintos. Pero, puesto que $p$ representa a cualquier período de $f$ términos –recordemos que estos y la ecuación (i) no dependen de $\lambda$–, estos satisfacen la ecuación anterior; es decir, $(f, 1)$, $(f, g)$, $(f, g^2)$, $(f, g^3), \ldots, (f, g^{e-1})$ son soluciones de la ecuación (ii). Por lo tanto dos de estos períodos deben tener el mismo valor. Es decir, suponiendo que uno de estos períodos se compone de las raíces $r^{\zeta_1}, r^{\zeta_2}, \ldots, r^{\zeta_f}$ y el otro de las raíces $r^{\eta_1}, r^{\eta_2}, \ldots, r^{\eta_f}$ con $1 \leq \zeta_1, \zeta_2, \ldots, \zeta_f, \eta_1, \eta_2, \ldots, \eta_f \leq n - 1$, entonces se tiene que

$$r^{\zeta_1} + r^{\zeta_2} + \ldots + r^{\zeta_f} = r^{\eta_1} + r^{\eta_2} + \ldots + r^{\eta_f}.$$

Considérese ahora la función $Y = x^{\zeta_1} + x^{\zeta_2} + \ldots + x^{\zeta_f} - x^{\eta_1} - x^{\eta_2} - \ldots - x^{\eta_f}$, si se hace $x = r$ se tiene que $Y = 0$, así $x - r$ es un factor de $Y$. Sin embargo, como ya se sabe, $r$ es una raíz de la ecuación $X = x^{n-1} + x^{n-2} + \ldots + x + 1$, entonces $x - r$ también es un factor de $X$. Por lo tanto, es posible hallar el máximo común divisor de las funciones $X$ y $Y$, el cual tendrá coeficientes racionales y no es de grado $n - 1$, esto último debido a que $(x - 0)$ es un factor de $Y$ pero no de $X$.[40] Así, el máximo común divisor de las funciones $X$ y $Y$ es una función de menor grado que divide a $X$ y que tiene todos sus coeficientes racionales pero esto contradice que $X$ es irreducible [Ver Capítulo II, art. 341]. De esta manera se ha probado que $\mathfrak{N} \neq 0$, y con esto se puede concluir que $(f, \mu) = p'$ se puede expresar como

$$\mathfrak{A}' + \mathfrak{B}'p + \mathfrak{C}'p^2 + \cdots + \mathfrak{M}'p^{e-1}.$$

**Ejemplo.-** Para $n = 19$, $f = 6$, $e = 3$, y raíz primitiva $g = 2$ se expresarán los períodos $p' = (6,2)$ y $p'' = (6,4)$ como una combinación lineal de $p = (6,1)$.
Se sabe que $(6,1) = \{r, r^8, r^7, r^{11}.r^{12}.r^{18}\}$, entonces

$$p^2 = (6,1)(6,1) = (6,2) + (6,9) + (6,8) + (6,12) + (6,13) + (6,19),$$

y reduciendo a períodos equivalentes se tiene

$$p^2 = (6,2) + (6,4) + (6,1) + (6,1) + (6,4) + 6 = 6 + 2(6,1) + (6,2) + 2(6,4),$$

por tanto,

$$p^2 = 6 + 2p + p' + 2p''.$$

---

[39] Véase [Lang Serge, Introduction to Linear Algebra, 2da. edición p. 70]
[40] Note que el grado de $Y$ es menor o igual que $n - 1$. Entonces, si es menor que $n - 1$, el grado del máximo común divisor de $X$ y $Y$ es menor que $n - 1$.
Por otro lado, si el grado de $Y$ es igual a $n - 1$, entonces el grado del máximo común divisor de $X$ y $Y$ es menor o igual que $n - 1$. Si es igual a $n - 1$ implicaría que $X$ y $Y$ tienen las mismas raíces, sin embargo, el cero es una raíz de de $Y$ pero no de de $X$.

Ahora, puesto que $0 = 1 + p + p' + p''$ se tiene

$$p^2 = 6 + 2(p + p'') + p' = 6 + 2(-1 - p') + p' = 4 - p',$$

y $$p^2 = 6 + (p + p' + p'') + p + p'' = 5 + p + p''.$$

Es decir,

$$p' = 4 - p^2,$$
$$p'' = p^2 - 5 - p,$$

de donde,

$$(6,2) = 4 - (6,1)^2 \qquad \text{y} \qquad (6,4) = -5 - (6,1) + (6,1)^2.$$

Ahora, si $(f,\lambda) = p = (6,2);\ p' = (6,4);\ p'' = (6,1)$ y se procede de forma análoga a lo anterior, entonces se tiene que

$$(6,4) = 4 - (6,2)^2\ ; \qquad (6,1) = -5 - (6,2) + (6,2)^2,$$

y si $p = (6,4);\ p' = (6,1); p'' = (6,2)$ entonces

$$(6,1) = 4 - (6,4)^2\ ; \qquad (6,2) = -5 - (6,4) + (6,4)^2.$$

**Art. 347** (TEOREMA). Sea $F = \varphi(t,u,v,\dots)$ una *función algebraica racional invariable*[41] en las incógnitas $t,u,v,\dots$. Sustituyendo estas por las $f$ raíces contenidas en el período $(f,\lambda)$, y por el artículo 340 se tiene que el valor de $F$ se reduce a la forma

$$A + A'r + A''r^2 + \cdots = W.\ ^{42}$$

Entonces, las raíces que pertenecen al mismo período de $f$ términos tendrán coeficientes iguales en esta expresión.

*Demostración.* Sean $r^p$, $r^q$ dos raíces pertenecientes al mismo período de $f$ términos. Supóngase que $p$ y $q$ son enteros positivos menores que $n$. Sean $r^\lambda$, $r^{\lambda'}$, $r^{\lambda''},\dots$ las raíces contenidas en $(f,\lambda)$, donde $\lambda,\ \lambda',\ \lambda'',\dots$ son enteros positivos y menores que $n$. Finalmente sean $\mu,\ \mu',\ \mu'',\dots$ los residuos mínimos positivos de los números $\lambda g^{ve},\ \lambda' g^{ve}, \lambda'' g^{ve},\dots$ módulo $n$.

Se quiere mostrar que $r^p$ y $r^q$ tienen los mismos coeficientes en $W$. Puesto que $r^p$ y $r^q$ están en el mismo período, se puede suponer que $q \equiv pg^{ve}\ (mod\ n)$.

Por el artículo 340 se tiene que

$$\varphi\left(r^{\lambda g^{ve}}, r^{\lambda' g^{ve}}, r^{\lambda'' g^{ve}}, \dots\right) \qquad (I)$$

se puede reducir a la forma

$$A + A' r^{g^{ve}} + A'' r^{2g^{ve}} + \cdots.$$

De aquí se puede ver que el coeficiente de $r^p$ en $(W)$ es el mismo que el de $r^{pg^{ve}}$ en esta última expresión.

Si $\theta, \theta', \dots$ representan los residuos mínimos módulo $n$ de los números $g^{ve}, 2g^{ve}, \dots$, entonces se puede reducir $(I)$ a la expresión

---

[41] Esta función es lo que ahora se conoce como *polinomio simétrico* en $f$ indeterminadas.

[42] Algunos de los coeficientes $A, A', \dots$pueden ser 0.

$$A + A'r^{\theta} + A''r^{\theta'} + \cdots = W'.$$

Así, puesto que uno de los números $\theta, \theta', \ldots$ representa al residuo mínimo de $pg^{ve}$ módulo $n$, el cual es $q$, entonces el coeficiente que tiene $r^q$ en $(W')$ es el mismo que tiene $r^p$ en $(W)$.

Ahora, note que los números $\lambda,\ \lambda',\ \lambda'', \ldots$ son congruentes a $\mu,\ \mu',\ \mu'', \ldots$, salvo el orden, pues cualesquiera dos números $\alpha, \beta$ en $\{\lambda,\ \lambda',\ \lambda'', \ldots\}$ satisfacen la congruencia $\alpha \equiv \beta g^{ve}\ (mod\ n)$. Esto debido a que son exponentes de raíces que están en el mismo período.

Además, se tiene que $\mu \equiv \lambda g^{ve}\ (mod\ n)$ y $\mu' \equiv \lambda' g^{ve} (mod\ n), \ldots$ entonces las raíces $r^{\mu}, r^{\mu'}, r^{\mu''}, \ldots$ son iguales a las raíces $r^{\lambda g^{ve}}, r^{\lambda' g^{ve}}, r^{\lambda'' g^{ve}}, \ldots$. Así, al desarrollar la expresión $(I)$ se obtiene lo mismo que al desarrollar la expresión $\varphi(r^{\mu}, r^{\mu'}, r^{\mu''}, \ldots)$. De hecho

$$W = \varphi\left(r^{\lambda}, r^{\lambda'}, r^{\lambda''}, \ldots\right) = \varphi\left(r^{\mu}, r^{\mu'}, r^{\mu''}, \ldots\right) = (I) = W'$$

pues los números $\mu,\ \mu',\ \mu'', \ldots$ y $\lambda,\ \lambda',\ \lambda'', \ldots$ solo difieren en el orden y $\varphi$ es una función invariable. Por tanto $W'$ es completamente idéntico a $W$ y las raíces $r^p$ y $r^q$ tendrán el mismo coeficiente en $W$.

Como consecuencias inmediatas de este teorema se tienen:

I. $W$ puede ser reducido a la forma
$A + a(f,1) + a'(f,g) + a''(f,g^2) + \cdots + a^e(f,g^{e-1})$,
donde los coeficientes $A, a, \ldots, a^e$ serán cantidades enteras determinadas (alguna puede ser cero), si todos los coeficientes racionales en $F$ lo son.

II. En cambio, si $t, u, v, \ldots$ son sustituidas por las raíces de otro período $(f, k\lambda)$, el valor de F primero se reduce a $A + A'r^k + A''r^{2k} + \cdots = W$ y luego se convertirá en $A + a(f,k) + a'(f,kg) + a''(f,kg^2) + \cdots$.

Estas dos propiedades son el objetivo real del art. 347 y serán usadas en el siguiente artículo para la construcción de las ecuaciones auxiliares, que se requieren en la búsqueda de las raíces del polinomio ciclotómico.

**Ejemplo.** Sea $n = 19,\ g = 2,\ f = 6,\ \lambda = 1$ y la función $\varphi$ designa la suma de los productos dos a dos de las incógnitas, entonces se tiene que

$$\begin{aligned}\varphi(r, r^7, r^8, r^{11}, r^{12}, r^{18}) &= r^8 + r^9 + r^{12} + r^{13} + 1 + r^{15} + r^{18} + 1 + r^6 \\ &\quad +1 + r + r^7 + r^4 + r^{10} + r^{11} \\ &= 3 + (r + r^7 + r^8 + r^{11} + r^{12} + r^{18}) \\ &\quad + (r^4 + r^6 + r^9 + r^{10} + r^{13} + r^{15}) \\ &= 3 + (6,1) + (6,4) = A + a(6,1) + a'(6,2) + a''(6,4),\end{aligned}$$

donde, $A = 3,\ a = 1,\ a'' = 1$ y $a' = 0$.

Si ahora en $\varphi$ se sustituyen las raíces del período $(f, k\lambda) = (6,2)$ se tiene

$$\begin{aligned}\varphi(r^2, r^{14}, r^{16}, r^3, r^5, r^{17}) &= r^5 + r^7 + r^{16} + r^{18} + 1 + r^8 \\ &\quad + r^{17} + 1 + r + 1 + r^2 + r^3 = 3 + (6,1) + (6,2) \\ &= A + a(6,2) + a'(6, 2 \cdot 2) + a''(6, 2 \cdot 2^2).\end{aligned}$$

Como se puede notar, la expresión reducida de $\varphi$ al sustituir sus variables por las raíces del período $(f, k\lambda)$ se puede obtener a partir de la expresión de $\varphi$ para las raíces de $(f, \lambda)$.

A continuación, en el art. 348, se mostrará que $X = x^{n-1} + x^{n-2} + \cdots + 1$ puede descomponerse en $e$ factores de grado $f$, donde cada uno de dichos factores serán polinomios cuyas raíces son aquellas contenidas en un período de $f$ términos –recordemos que $ef = n - 1$ y que no todos los coeficientes de estos factores pueden ser racionales–. La construcción de estos polinomios será útil para hallar las raíces de $X$ en expresiones con radicales, como se verá en el art. 352.

**Art. 348.** Por la teoría de los polinomios simétricos, se sabe que los coeficientes $\alpha,\ \beta,\ \gamma, \ldots$ de la ecuación $x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \ldots = 0$, son los $f$ polinomios simétricos elementales evaluadas en las $f$ raíces –Gauss los llama *funciones invariables*–; esto es, $\alpha$ es la suma de todas las raíces, $\beta$ es la suma de los productos tomados dos a dos, $\gamma$ es la suma de los productos tomados tres a tres a la vez, etc.

Así pues, la ecuación cuyas raíces son aquellas contenidas en el período $(f, \lambda)$ se puede determinar conociendo los valores de sus coeficientes, a saber, el primer coeficiente será $\alpha = (f, \lambda)$. Debido a que el resto de los coeficientes, $\beta, \gamma, \ldots$, son funciones enteras invariables –polinomios simétricos elementales– en las raíces de $(f, \lambda)$, se puede aplicar el artículo 340 a estas funciones y por lo tanto, cada uno se puede reducir a la forma

$$A + A'r + A''r^2 + \cdots = W,$$

y por el art. 347. I. se tiene que cada uno de los coeficientes $\beta, \gamma, \ldots$ puede ser expresado como

$$A + a(f, 1) + a'(f, g) + a''(f, g^2) + \cdots + a^e(f, g^{e-1})$$

donde $A,\ a,\ a',\ a'', \ldots\ , a^e$ son enteros.

En general, por el artículo 347. II, se tendrá que los coeficientes de la ecuación cuyas raíces son las contenidas en cualquier otro período $(f, k\lambda)$ pueden reducirse (derivarse de la anterior) a

$$A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \cdots + a^e(f, kg^{e-1}). \qquad (**)$$

Entonces, los coeficientes de la ecuación cuyas raíces son las contenidas en el período $(f, k\lambda)$ estarán completamente determinados si se conoce el valor de uno de los períodos $(f, 1),\ (f, g),\ (f, g^2),\ \ldots, (f, g^{e-1})$ –basta conocer solo un valor, pues según el artículo 346 el resto puede ser obtenido a partir de este–.

De este modo se pueden obtener las $e$ ecuaciones $z, z', z'', \ldots, z^e$ cuyas raíces son aquellas que están contenidas en $(f, 1),\ (f, g),\ (f, g^2), \ldots, (f, g^{e-1})$, respectivamente. Es decir, las raíces contenidas en $(f, 1)$ junto con las contenidas en los períodos $(f, g),\ (f, g^2), \ldots, (f, g^{e-1})$ son las raíces del producto $zz'z'' \cdots z^e$; sin embargo, también son las raíces del polinomio $X = x^{n-1} + x^{n-2} + \cdots + 1$ [Ver art. 344.II].

Por lo tanto, $X$ es el producto de los $e$ factores $z, z', z'', \ldots, z^e$ y cada uno de ellos es de grado $f$.

**Ejemplo.** Sean $n = 19,\ g = 2,\ e = 3,\ f = 6$ como en los ejemplos previos. En este caso $z, z', z''$ son las ecuaciones cuyas raíces son las contenidas en

$$(6,1) = \{r, r^7, r^8, r^{11}, r^{12}, r^{18}\}, \qquad (6,2) = \{r^2, r^3, r^5, r^{14}, r^{16}, r^{17}\} \text{ y}$$
$$(6,4) = \{r^4, r^6, r^9, r^{10}, r^{13}, r^{15}\},$$

respectivamente.

Primero se hallará la ecuación $z$, cuyas raíces son las contenidas en el período $(6,1)$. Entonces la suma de todas las raíces es $(6,1) = \alpha$, y realizando cálculos algebraicos se verifica que el producto dos a dos de las raíces es $\beta = 3 + (6,1) + (6,4)$; la suma de los productos tomados tres a la vez es $\gamma = 2 + 2(6,1) + (6,2)$ ; la suma de los productos tomados cuatro a la vez es $\delta = 3 + (6,1) + (6,4)$; la suma de los productos tomados cinco a la vez es $\varepsilon = (6,1)$ y finalmente, el producto de todos ellos es igual a uno. Así, la ecuación cuyas raíces son las contenidas en $(6,1)$ es

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x^2 - \varepsilon x + 1 = 0\,.$$

Haciendo $k = g = 2$ y aplicando $(**)$, de los valores $\alpha, \beta, \gamma, \delta, \varepsilon$ se obtienen los coeficientes de $z'$, a saber,

$$\alpha' = (6,2)$$
$$\beta' = 3 + (6,2) + (6,1)$$
$$\gamma' = 2 + 2(6,2) + (6,1)$$
$$\delta' = 3 + (6,2) + (6,1)$$
$$\varepsilon' = (6,2).$$

Así,

$$z' = x^6 - \alpha' x^5 + \beta' x^4 - \gamma' x^3 + \delta' x^2 - \varepsilon' x + 1 = 0.$$

Análogamente para $k = g^2 = 4$, se obtienen los coeficientes de $z''$,

$$\alpha'' = (6,4)$$
$$\beta'' = 3 + (6,4) + (6,2)$$
$$\gamma'' = 2 + 2(6,1) + (6,4)$$
$$\delta' = 3 + (6,1) + (6,4)$$
$$\varepsilon' = (6,1),$$

de donde $z'' = x^6 - \alpha'' x^5 + \beta'' x^4 - \gamma'' x^3 + \delta'' x^2 - \varepsilon'' x + 1 = 0.$

De esta manera se llega a que $X = zz'z''$.

**Art. 349.** Gauss, con base en el teorema de Newton mostrará otra forma de hallar los coeficientes $\alpha, \beta, \gamma, \ldots$ mencionados en el artículo previo. En su opinión este otro método será más conveniente cuando $f$ es un número grande.

Primero note que el periodo $(f, k\lambda) = r^{k\lambda} + r^{k\lambda \mathrm{h}} + r^{k\lambda h^2} + \cdots + r^{k\lambda h^{f-1}}$ es la suma de las potencias $k$-ésimas de las raíces contenidas en $(f, \lambda)$. Así, la suma de los cuadrados de las raíces en $(f, \lambda)$ es $(f, 2\lambda)$, la suma de los cubos es $(f, 3\lambda)$, etc. Entonces si se

designa por $q, q', q'', \ldots$ a los períodos $(f,\lambda)$, $(f,2\lambda)$, $(f,3\lambda)$, ..., respectivamente, por el Teorema de Newton mencionado en el artículo 338, se tendrá

$$\alpha = q, \quad 2\beta = \alpha q - q', \quad 3\gamma = \beta q - \alpha q' + q'', \quad 4\delta = \alpha q'' - \beta q' + \gamma q - q''', \text{ etc.}$$

Al final los coeficientes $\alpha, \beta, \gamma, \ldots$ se reducen a solo sumas de períodos debido al artículo 345.

Sin embargo, si $f$ es par basta con calcular de esta manera solo la mitad de los coeficientes, pues resulta que $\alpha$ es igual al penúltimo, $\beta$ igual al antepenúltimo, etc. Si $f$ es impar, el penúltimo coeficiente resulta de sustituir $(f,\lambda)$ por $(f,-\lambda)$ en $\alpha$, el antepenúltimo resulta de intercambiar en $\beta$ los períodos $(f,\lambda)$, $(f,\lambda g)$, $(f,\lambda g^2)$, ..., por los períodos $(f,-\lambda)$, $(f,-\lambda g)$, $(f,-\lambda g^2)$, respectivamente.

Note que el último coeficiente es igual a uno para cualquier $f$.[43]

Siguiendo con el ejemplo, sean $p, p', p''$ los períodos $(6,1)$, $(6,2)$ y $(6,4)$ respectivamente. Entonces,

$$q = (6,1) = p \qquad q''' = (6,4) = p''$$
$$q' = (6,2) = p' \qquad q'''' = (6,5) = (6,2) = p'$$
$$q'' = (6,3) = (6,2) = p' \qquad q''''' = (6,6) = (6,4) = p'',$$

y por lo tanto[44],

[43] Puesto que los números $\lambda, \lambda h, \lambda h^2, \lambda h^3, \ldots, \lambda h^{f-1}$ forman un sistema reducido de residuos módulo $n$ se tiene que

$$\lambda + \lambda h + \lambda h^2 + \lambda h^3 + \cdots + \lambda h^{f-1} \equiv 0 \ (mod\ n)$$

y por tanto $r^{\lambda} \cdot r^{\lambda h} \cdot r^{\lambda h^2} \cdot r^{\lambda h^3} \cdot \ldots \cdot r^{\lambda h^{f-1}} = 1$. De esto se tiene lo siguiente:

- El *último* coeficiente es igual a 1.
- Si $r_1, r_2, \ldots, r_f$ denotan las $f$ raíces de $(f,\lambda)$, entonces los $\binom{f}{f-1} = f$ sumandos del *penúltimo* coeficiente son de la forma $\frac{r_1 r_2 \ldots r_f}{r_j} = \frac{1}{r_j}$ para $j = 1,2,\ldots,f$ y son distintos entre sí. Además, para $f$ par, si $r_j$ es una raíz de $(f,\lambda)$ su recíproco también lo es. Por tanto el *penúltimo* coeficiente es la suma de las raíces de $(f,\lambda)$, que es igual a $\alpha$.
  Si $f$ es impar $\frac{1}{r_j}$ para $j = 1,2,\ldots,f$ es una raíz en $(f,-\lambda)$ y así el *penúltimo* coeficiente es $= (f,-\lambda)$.
- Los $\binom{f}{f-2} = \frac{f(f-1)}{2}$ términos del *antepenúltimo* coeficiente son de la forma $\frac{r_1 r_2 \ldots r_f}{r_i r_j} = \frac{1}{r_i r_j}$ para $i,j \in \{1,2,\ldots,f\}$. Por otro lado, los $\binom{f}{2} = \frac{f(f-1)}{2}$ términos del coeficiente $\beta$ son de la forma $r_i r_j i,j \in \{1,2,\ldots,f\}, i \neq j$. Como $\frac{1}{r_i r_j} = \frac{1}{r_i} \cdot \frac{1}{r_j}$ y los recíprocos de $r_i$ y $r_j$ están en $(f,\lambda)$ para $f$ par, el recíproco de $r_i r_j$, $\frac{1}{r_i r_j}$, debe ser alguno de los $\binom{f}{2}$ productos $r_i r_j$ que aparecen en $\beta$ – ya que es la suma de productos dos a dos de las raíces en $(f,\lambda)$ –. Por lo tanto, $\beta =$ *antepenúltimo* coeficiente.
  Pero si $f$ es impar $\frac{1}{r_i r_j}$ debe ser alguno de los productos dos a dos de las raíces en $(f,-\lambda)$. Entonces el coeficiente $\beta$ resulta de intercambiar en el *antepenúltimo coeficiente* los períodos $(f,-\lambda),(f,-\lambda g),(f,-\lambda g^2),\ldots$ por los períodos $(f,\lambda),(f,\lambda g),(f,\lambda g^2),\ldots$, respectivamente. O de otra manera, el *antepenúltimo coeficiente* resulta de intercambiar en $\beta$ los períodos $(f,\lambda),(f,\lambda g),(f,\lambda g^2),\ldots$, por los períodos $(f,-\lambda),(f,-\lambda g),(f,-\lambda g^2)$, respectivamente.
- Para el resto de los coeficientes pasa lo mismo que con los coeficientes anteriores y para ver esto se procede también de forma análoga.

$$\alpha = p$$
$$2\beta = 6 + 2p + 2p''$$
$$3\gamma = 6 + 6p + 3p'$$
$$4\delta = 12 + 4p + 4p''$$
etc.

Si se requiere hallar los coeficientes del polinomio cuyas raíces son las sumas de las raíces de un período se realiza un procedimiento similar al anterior. Esto se mencionará en el ejemplo I del art. 351.

**Art. 350** (TEOREMA). Sea $n-1$ el producto de tres enteros positivos $\alpha, \beta, \gamma$ y considere el período $(\beta\gamma, \lambda)$. Sea $F = \varphi(t, u, v, \dots)$ una función de $\beta$ incógnitas y si se sustituyen estas por las $\beta$ sumas $(\gamma, \lambda)$, $(\gamma, \lambda'), (\gamma, \lambda''), \dots, (\gamma, \lambda^{\beta-1})$ de acuerdo al artículo 345.IV el valor de $F$ se reduce a

$$A + a(\gamma, 1) + a'(\gamma, g) + a''(\gamma, g^2) + \cdots + a^{\zeta}\left(\gamma, g^{\alpha(\beta-1)}\right) + \cdots + a^{\theta}\left(\gamma, g^{\alpha\beta-1}\right) = W.$$

Entonces, si $F$ es una función invariable, los períodos en $W$ que están contenidos en el mismo período de $\beta\gamma$ términos[45] tendrán los mismos coeficientes, esto es, los períodos $(\gamma, g^{\theta})$ y $(\gamma, g^{\alpha\vartheta+\theta})$, donde $\vartheta, \theta$ son enteros mayores o iguales que cero, tendrán los mismos coeficientes.

*Demostración.* Primero note que los períodos $(\beta\gamma, \lambda)$ y $(\beta\gamma, \lambda g^{\alpha})$ son iguales[46] y que el segundo consta de los subperíodos[47] $(\gamma, \lambda)$, $(\gamma, \lambda')$, $(\gamma, \lambda'')$, $\dots$, $(\gamma, \lambda^{\beta-1})$,[48] entonces los

---

[44] Recordemos que en artículos previos se mostró que
$$pp' = (6,1) + 2(6,2) + 3(6,4) = p + 2p' + 3p''$$
$$p^2 = 6 + 2p + p' + 2p''.$$
Además,
$$\begin{aligned} p''p' &= (6,6) + (6,7) + (6,9) + (6,18) + (6,20) + (6,21) \\ &= (6,4) + (6,1) + (6,4) + (6,1) + (6,1) + (6,2) \\ &= 3p + p' + 2p'' \\ p''p &= (6,5) + (6,11) + (6,12) + (6,15) + (6,16) + (6,22) \\ &= (6,2) + (6,1) + (6,1) + (6,2) + (6,4) + (6,2) \\ &= 2p + p' + p'', \end{aligned}$$
de donde,
$$\begin{aligned} 2\beta &= p^2 - pp' = 6 + 2p + p' + 2p'' - p' = 6 + 2p + 2p'' \\ 3\gamma &= (3 + p + p'')p - pp' + p' = 3p + p^2 + pp'' - pp' + p' \\ &= 3p + 6 + 2p + p' + p'' + 2p + 3p' + p'' - p - 2p' - 3p'' \\ &= 6 + 6p + 3p' \\ 4\delta &= \alpha q'' - \beta q' + \gamma q - q''' = pp' - 3p' - pp' - p''p' + 2p + 2p^2 + p'p - p'' \\ &= -3p' - 3p - p' - 2p'' + 2p + 12 + 4p + 2p' + 4p'' + p + 2p' + 3p'' - p'' \\ &= 12 + 4p + 4p'' \\ &\text{etc.} \end{aligned}$$

[45] Como se sabe el período $(\beta\gamma, \lambda)$ consta de las raíces $r^{\lambda}$, $r^{\lambda g^{\alpha}}$, $r^{\lambda g^{2\alpha}}$, $r^{\lambda g^{3\alpha}}, \dots, r^{\lambda g^{(\beta-1)\alpha}}, \dots, r^{\lambda g^{\alpha(\beta\gamma-1)}}$, y puesto que los coeficientes de las raíces $r^{\lambda}$, $r^{\lambda g^{\alpha}}$, $r^{\lambda g^{2\alpha}}$, $r^{\lambda g^{3\alpha}}, \dots, r^{\lambda g^{(\beta-1)\alpha}}$ satisfacen $\lambda \not\equiv \lambda g^{\alpha v + \alpha v'} (mod\, n)$ y $\lambda g^{\alpha v'} \not\equiv \lambda g^{\alpha v + \alpha v'} (mod\, n)$, donde $v, v'$ son enteros entre $1, \dots, \beta - 1$, cada una de esas raíces debe estar en un período distinto; así $(\beta\gamma, \lambda)$ consta de los $\beta$ períodos $(\gamma, \lambda)$, $(\gamma, \lambda g^{\alpha})$, $(\gamma, \lambda g^{2\alpha})$, $(\gamma, \lambda g^{3\alpha}), \dots, (\gamma, \lambda g^{(\beta-1)\alpha})$. Esto es, $\lambda' = \lambda g^{\alpha}$, $\lambda'' = \lambda g^{2\alpha}, \dots$.

[46] Debido a que la raíz $r^{\lambda g^{\alpha}}$ está en el período $(\beta\gamma, \lambda)$ y también en $(\beta\gamma, \lambda g^{\alpha})$, entonces por el art. 344.I estos períodos son iguales.

[47] Se nombra subperíodo, a aquellos períodos que están contenidos en otro período con mayor número de términos.

[48] De manera parecida a lo hecho en la nota a pie [45] se puede verificar que $(\beta\gamma, \lambda g^{\alpha})$ consta de los períodos
$$(\gamma, \lambda g^{\alpha}), (\gamma, \lambda g^{2\alpha}), (\gamma, \lambda g^{3\alpha}), \dots, \left(\gamma, \lambda g^{(\beta-1)\alpha}\right), (\gamma, \lambda g^{\beta\alpha}),$$

subperíodos de $(\beta\gamma, \lambda)$ son iguales a los subperíodos de $(\beta\gamma, \lambda g^{\alpha})$. Por lo tanto, $W$ y $W'$ son iguales. Ahora, si se sustituyen los subperíodos del segundo en $F$, entonces por el artículo 345.IV resulta

$$W' = B + b(\gamma, g^{\alpha}) + b'(\gamma, g^{\alpha+1}) + b''(\gamma, g^{\alpha+2}) + \cdots + b^{\zeta}\left(\gamma, g^{\alpha\beta}\right) + \cdots + b^{\theta}\left(\gamma, g^{\alpha\beta+\alpha-1}\right)$$
$$= B + b(\gamma, g^{\alpha}) + b'(\gamma, g^{\alpha+1}) + b''(\gamma, g^{\alpha+2}) + \cdots + b^{\zeta}(\gamma, 1) + \cdots + b^{\theta}\left(\gamma, g^{\alpha\beta}\right).^{49}$$

Sean $(\gamma, \mu)$ y $(\gamma, \mu')$ dos períodos contenidos en el mismo período de $\beta\gamma$ términos, entonces, sin perdida de generalidad, supóngase que $\mu' \equiv \mu g^{\tau\alpha}$, de donde el coeficiente del período que coincide con $(\gamma, \mu')$ en $W'$ es igual al coeficiente del período que coincide con $(\gamma, \mu)$ en $W$. Pero ya que $W$ y $W'$ son iguales, los períodos $(\gamma, \mu)$ y $(\gamma, \mu')$ tendrán los mismos coeficientes en $W$.

Observaciones:

1. Como consecuencia inmediata del teorema previo, $W$ puede ser reducido a la forma
$$C + c(\beta\gamma, 1) + c'(\beta\gamma, g) + \cdots + c^{\epsilon}(\beta\gamma, g^{\alpha-1}),^{50}$$
donde $C, c, c', c''$, etc. son enteros si los coeficientes de $F$ son enteros.

2. Si en lugar de sustituir los períodos contenidos en $(\beta\gamma, \lambda)$ de $F$, se sustituyen los contenidos en cualquier otro período $(\beta\gamma, k\lambda)$ el valor resultante será
$$A + a(\beta\gamma, k) + a'(\beta\gamma, kg) + \cdots + a^{\epsilon}(\beta\gamma, kg^{\alpha-1}).^{51}$$

3. Para el caso particular donde $\alpha = 1$, $W$ es de la forma $A + a(\beta\gamma, 1)$.

**Art. 351.** Con base en la terminología del artículo anterior, considérese la ecuación cuyas raíces son los $\beta$ períodos $(\gamma, \lambda)$, $(\gamma, \lambda')$, $(\gamma, \lambda'')$, …, $(\gamma, \lambda^{\beta-1})$. Los coeficientes de dicha ecuación se pueden expresar de la forma
$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \cdots + a^{\epsilon}(\beta\gamma, g^{\alpha-1}),^{52}$$
donde $A$, $a$, $a'$, $a''$, etc. son enteros.

---

*i.e.*, de los periodos $(\gamma, \lambda g^{\alpha}), (\gamma, \lambda' g^{\alpha}), (\gamma, \lambda'' g^{\alpha}), \ldots, \left(\gamma, \lambda^{\beta-2} g^{\alpha}\right), (\gamma, \lambda^{\beta-1} g^{\alpha})$.

[49] Puesto que $g^{\alpha\beta} \equiv 1 \cdot \left(g^{\alpha\beta}\right)^{\gamma}$; $\alpha\beta = e$, por el artículo 344.I las raíces $r^{g^{\alpha\beta}}$ y $r$ están en el mismo período de $\gamma$ términos y por tanto los períodos $(\gamma, 1)$ y $\left(\gamma, g^{\alpha\beta}\right)$ son iguales. Análogamente se puede ver que los períodos $\left(\gamma, g^{\alpha\beta+\alpha-1}\right)$ y $\left(\gamma, g^{\alpha\beta}\right)$ son iguales.

[50] Observe que los períodos de $\gamma$ términos $(\gamma, 1)$, $(\gamma, g^{\alpha})$, $(\gamma, g^{2\alpha}), \ldots, (\gamma, g^{\alpha(\beta-1)})$ están contenidos en el mismo período de $\beta\gamma$ términos $(\beta\gamma, 1)$, al igual que $(\gamma, g)$, $(\gamma, g^{\alpha+1})$, $(\gamma, g^{\alpha+2}), \ldots, (\gamma, g^{\alpha(\beta-1)+1})$ son los contenidos en $(\beta\gamma, g)$, etc. De donde por el teorema anterior

$$W = A + a(\gamma, 1) + a'(\gamma, g) + a''(\gamma, g^2) + \cdots + a^{\zeta}\left(\gamma, g^{\alpha(\beta-1)}\right) + \cdots + a^{\theta}\left(\gamma, g^{\alpha\beta-1}\right)$$
$$= A + a\left[(\gamma, 1) + (\gamma, g^{\alpha}) + (\gamma, g^{2\alpha}) + \cdots + \left(\gamma, g^{\alpha(\beta-1)}\right)\right] + a'[(\gamma, g) + (\gamma, g^{\alpha+1}) + (\gamma, g^{\alpha+2}) + \cdots + (\gamma, g^{\alpha(\beta-1)+1})]$$
$$+ \cdots + a^{\epsilon}[(\gamma, g^{\alpha-1}) + (\gamma, g^{2\alpha-1}) + \cdots + (\gamma, g^{\alpha\beta-1})]$$
$$= A + a(\beta\gamma, 1) + a'(\beta\gamma, g) + \cdots + a^{\epsilon}(\gamma, g^{\alpha-1}).$$

[51] Esto se muestra de forma análoga como lo fue para el período $(\beta\gamma, \lambda)$, excepto que se aplica el art 345. IV al período $(\beta\gamma, k\lambda)$ .

[52] Los coeficientes de un polinomio mónico se pueden expresar en términos de las raíces de dicho polinomio. Además por el art. 346 el producto de una cantidad finita de períodos de $\gamma$ términos se puede reducir a la forma $A + B(\beta\gamma, 1) + B'(\beta\gamma, g) + \cdots + B^{\epsilon}(\beta\gamma, g^{\alpha-1})$.

Pero si en esta expresión sustituimos el período $(\beta\gamma, \mu)$ por $(\beta\gamma, k\mu)$, entonces se obtienen los coeficientes de la ecuación cuyas raíces son los $\beta$ subperíodos de $\gamma$ términos contenidos en el período $(\beta\gamma, k\lambda)$, así estos estarán determinados por una ecuación de grado $\beta$.

En caso de que $\alpha = 1$, como ya mencionó anteriormente los coeficientes serán de la forma $A + a(\beta\gamma, 1)$ y puesto que $(\beta\gamma, 1) = (n-1, 1) = -1$, estos coeficientes están completamente determinados. Pero si $\alpha > 1$, los coeficientes podrán ser determinados si se conocen los $\alpha$ períodos de $\beta\gamma$ términos.

**Ejemplo I.** Para $n = 19$ se busca la ecuación $x^3 - Ax^2 + Bx - C = 0$ cuyas raíces son los períodos $p = (6,1)$, $p' = (6,2)$ y $p'' = (6,4)$. Como se sabe de la teoría de polinomios simétricos

$$A = p + p' + p'' \qquad B = pp' + pp'' + p'p'' \qquad C = pp'p''.$$

Recordemos que en el art. 349 se mostró que

$$pp' = p + 2p' + 3p'' \quad pp'' = 2p + 3p' + p'' \quad p'p'' = 3p + p' + 2p'',$$

de donde,

$$A = (18,1) = -1 \qquad B = 6(p + p' + p'') = -6$$

$$C \ =^{53} 18 + 11(p + p' + p'') = 18 - 11 = 7$$

Por tanto la ecuación buscada es

$$x^3 + x^2 - 6x - 7 = 0.$$

Usando el teorema de Newton [Ver art. 349]:
Primero recordemos que

$$A = p + p' + p'' = -1$$
$$p^2 = 6 + 2p + p' + 2p''$$
$$p'p' = 6 + 2p + 2p' + p''$$
$$p''p'' = 6 + p + 2p' + 2p'',$$

entonces,

$$p^2 + p'^2 + p''^2 = 18 + 5p + 5p' + 5p'' = 18 + 5(-1) = 13,$$

y

$$p^3 + p'^3 + p''^3 = 36 + 34(-1) = 2.$$

Luego, por el teorema de Newton se tiene

$$2B = A(p + p' + p'') - (p^2 + p'^2 + p''^2) = 1 - 13 = -12$$
$$3C = p^3 + p'^3 + p''^3 - A(p^2 + p'^2 + p''^2) + AB$$
$$= 2 - (-1)(13) + (-1)(-6) = 21,$$

[53] Recuérdese que $p''p'' = 6 + p + 2p' + 2p''$, entonces se tendrá

$$C = (p + 2p' + 3p'')p'' = pp'' + 2p'p'' + 3p''p''$$
$$= 2p + 3p' + p'' + 6p + 2p' + 4p'' + 18 + 3p + 6p' + 6p''$$
$$= 18 + 11p + 11p' + 11p''$$
$$= 18 + 11(p + p' + p'') = 18 - 11 = 7$$

y así se obtiene la misma ecuación que con el método anterior.

**Ejemplo II.** Para $n = 19$ se busca la ecuación cuyas raíces son los períodos $q = (2,1)$, $q' = (2,7)$ y $q'' = (2,8)$, contenidos en el período $(6,1)$.[54]
Así,

$$q + q' + q'' = (6,1) = p$$
$$qq' + qq'' + q'q'' = (6,1) + (6,4) = p + p''$$
$$qq'q'' = 2 + (6,2) = 2 + p',$$[55]

y la ecuación buscada es

$$x^3 - px^2 + (p + p'')x - 2 - p' = 0.$$

La ecuación cuyas raíces son los subperíodos $(2,2)$, $(2,3)$ y $(2,5)$ contenidos en $(6,2)$ puede deducirse a partir de la ecuación anterior sustituyendo $p$, $p'$, $p''$ por $p'$, $p''$, $p$, respectivamente, y si se sustituye por $p''$, $p$, $p'$ se obtiene la ecuación cuyas raíces son $(2,4)$, $(2,6)$ y $(2,9)$.[56]

## Las soluciones del polinomio.

Hasta aquí se han analizado las propiedades de los períodos de Gauss y se ha mostrado que estos se pueden ver como raíces de ciertos polinomios. Sin embargo no se ha visto con claridad cómo lo anterior se aplica a la solución por radicales del polinomio ciclotómico.

Ahora se exhibe lo que se podría llamar un método para hallar las raíces de la unidad en $\Omega$ a través de la solución de las ecuaciones a las que hemos llamado *ecuaciones auxiliares.* Este "método" se aplicará en ejemplos para $n = 17$ y $n = 19$.

**Art. 352.** Sea $g$ una raíz primitiva módulo $n$.

1. Encontrar el residuo mínimo de las potencias $g, g^2, \dots, g^{n-2}$ módulo $n$.

2. Factorizar $n - 1$ (en factores primos), digamos $n - 1 = \alpha\beta\gamma \dots \zeta$. Defínase $\frac{n-1}{\alpha} = \beta\gamma \dots \zeta = a$, $\frac{n-1}{\alpha\beta} = \gamma \dots \zeta = b$, etc.

3. Distribuir las raíces de $\Omega$ en $\alpha$ períodos de $a$ términos, y cada uno de estos en $\beta$ períodos de $b$ términos, y así sucesivamente.

---

[54] Observemos que $n - 1 = 3 \cdot 3 \cdot 2$, así el período $(\beta\gamma, \lambda) = (6,1)$ está conformado por los siguientes tres períodos de dos términos

$$(\gamma, \lambda) = (2,1), \quad (\gamma, \lambda g^{\alpha}) = (2,8) \quad \text{y} \quad (\gamma, \lambda g^{2\alpha}) = (2,7).$$

[55] Notemos que $18 = 9 \cdot 2 \overset{\text{def}}{=} ef$, así

$$q = (2,1) = \{r, r^{\lambda g^e}\} = \{r, r^{18}\}, \quad q' = (2,7) = \{r^7, r^{12}\}, \quad q'' = (2,8) = \{r^8, r^{11}\}.$$

de donde,

$$qq' = (2,8) + (2,13); \quad qq'' = (2,9) + (2,12); \quad q'q'' = (2,15) + (2,18),$$
$$qq'q'' = [(2,8) + (2,13)] \cdot (2,8) = (2,16) + (2,19) + (2,2) + (2,5) = 2 + (6,2).$$

[56] Esto se justifica por el art. 345. II.

4. Determinar, como se mostró en el artículo anterior, una ecuación $(A)$ de grado $\alpha$ cuyas raíces son los $\alpha$ períodos de $a$ términos, así los valores de estos períodos pueden determinarse resolviendo esta ecuación. En este punto es necesario identificar a qué raíz representa cada uno de los períodos $(a,1),\ (a,g),\ldots(a,g^{e-1})$. Ahora bien, como se puede tomar de manera arbitraria una raíz r en $\Omega$ , entonces se puede asumir que $r$ es una de las $a$ raíces de alguno de los periodos arriba mencionados y cuya suma de las raíces –de ese período– a la vez constituyen una raíz de $(A)$. A esta raíz de la ecuación $(A)$ se le puede identificar por el período $(a,1)$; sin embargo, $(a,1)$ no estará completamente determinado hasta que no se escoja la raíz de $(a,1)$ que representa $r$. Así, al determinar a $(a,1)$, por el artículo 346 se pueden hallar el resto de los $\alpha$ períodos de $a$ términos.

Gauss proporciona otro método para distinguir las raíces de la ecuación $(A)$, y consiste en definir $r=\cos\frac{2\pi k}{n}+isen\frac{2\pi k}{n}$ con $k$ un entero no divisible por $n$. Con esto quedarán determinadas las raíces $r^2, r^3,$ etc, y por tanto también los períodos $(a,1)$, $(a,g),\ldots(a,g^{e-1})$. [57]

5. Una vez determinados los $\alpha$ períodos de $a$ términos, se dará lugar a través del método del artículo anterior a la construcción de una ecuación $(B)$ cuyas raíces son los $\beta$ períodos de $b$ términos contenidos en $(a,1)$.[58] En este paso también se necesita saber qué raíz de la ecuación $(B)$ corresponde a qué período de $b$ términos. Puesto que $r$ es una de las raíces que constituyen $(a,1)$, entonces también se puede suponer que es una raíz en $(b,1)$ y así una raíz de la ecuación $(B)$ se representa por el período $(b,1)$. Ya que se ha determinado este período, el resto de los períodos de $b$ términos se pueden hallar de acuerdo con las reglas del artículo 346.

En ocasiones será conveniente hallar y resolver las $\alpha-1$ ecuaciones restantes cuyas raíces son los $\beta$ períodos de $b$ términos contenidos en los períodos

$$(a,g),(a,g^2),\ldots,(a,g^{e-1}),$$

respectivamente, y de esta manera junto con la solución de la ecuación $(B)$ se hallarán todas las raíces de $\Omega$. Finalmente, con la ayuda de tablas de senos, se determina el período al que corresponde cierta raíz. Esto se verá más claro en el siguiente ejemplo.

6. Continuando de esta manera, al final se tendrán todos los $\frac{n-1}{\zeta}$ períodos de $\zeta$ términos. Si se encuentra la ecuación cuyas raíces son las $\zeta$ raíces contenidas en $(\zeta,1)$ con ayuda del art. 348, entonces haciendo $r$ igual a una raíz cualquiera de esta ecuación, mediante las potencias de $r$, se obtendrán todas las raíces de $\Omega$.

También por el artículo 348 se tiene que al resolver la ecuación $(A)$, es decir, al determinar los $\alpha$ períodos de $a$ términos, $X=x^{n-1}+x^{n-2}+\cdots+x+1$ puede descomponerse en $\alpha$ factores de grado $a$. Después al resolver $(B)$, *i.e.*, hallar los $\alpha\beta$ períodos de $b$ tér-

[57] Este método requiere el conocimiento de valores precisos de senos y cosenos.

[58] Los coeficientes de esta ecuación son conocidos, pues resultan ser combinaciones de los períodos $(a,1)$, $(a,g),\ldots$ y estos ya fueron determinados en el paso anterior.

minos, cada uno de estos factores se compone de $\beta$ factores de grado $b$, entonces $X$ se descompone en $\alpha\beta$ factores de grado $b$. Así sucesivamente hasta descomponer a $X$ en $\frac{n-1}{\zeta}$ factores de grado $\zeta$. Estos factores son las *ecuaciones auxiliares.*

A continuación se mostrarán los ejemplos para $n = 17$ y $n = 19$. En el trabajo de Gauss se muestra primero el $n = 19$, pero aquí será al contrario pues se considera que debido a la factorización $17 - 1 = 2 \cdot 2 \cdot 2 \cdot 2$ el proceso para hallar las raíces de $x^{17} - 1 = 0$ es más comprensible que para $x^{19} - 1 = 0$, donde $19 - 1 = 3 \cdot 3 \cdot 2$. Es probable que Gauss dejara al final el ejemplo de $n = 17$ porque después mostraría que es posible construir el polígono regular de 17 lados.

**Ejemplo. I** Para el caso $n = 17$ se tiene que $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, entonces para hallar todas las raíces de $\Omega$ bastará con resolver cuatro ecuaciones cuadráticas (*auxiliares*). Tomando como raíz primitiva $g = 3$, se tienen los siguientes residuos de sus potencias:

| $g^0$ | $g^1$ | $g^2$ | $g^3$ | $g^4$ | $g^5$ | $g^6$ | $g^7$ | $g^8$ | $g^9$ | $g^{10}$ | $g^{11}$ | $g^{12}$ | $g^{13}$ | $g^{14}$ | $g^{15}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 |

De aquí, se obtiene la siguiente distribución de las raíces de $\Omega$, primero en dos períodos de ocho términos, luego cada uno en dos períodos de cuatro términos y finalmente cada uno de estos en dos períodos de dos términos:

$$\Omega = \begin{cases} (8,1) \begin{cases} (4,1) \begin{cases} (2,1) \ \ldots \ r, r^{16} \\ (2,13) \ \ldots \ r^4, r^{13} \end{cases} \\ (4,9) \begin{cases} (2,9) \ \ldots \ r^8, \ r^9 \\ (2,15) \ \ldots \ r^2, r^{15} \end{cases} \end{cases} \\ (8,3) \begin{cases} (4,3) \begin{cases} (2,3) \ \ldots \ r^3, r^{14} \\ (2,5) \ \ldots \ r^5, r^{12} \end{cases} \\ (4,10) \begin{cases} (2,10) \ \ldots \ r^{10}, r^7 \\ (2,11) \ \ldots \ r^{11}, r^6 \end{cases} \end{cases} \end{cases}$$

En lo que sigue, se utilizaran estas notaciones pero se debe tener en cuenta que cada una de estas representa una suma de ciertas raíces de la unidad, esto es,

$$(8,1) = r + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2$$
$$(8,3) = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6$$
$$(4,1) = r + r^{13} + r^{16} + r^4$$
$$(4,9) = r^9 + r^{15} + r^8 + r^2$$
$$(4,3) = r^3 + r^5 + r^{14} + r^{12}$$
$$(4,10) = r^{10} + r^{11} + r^7 + r^6$$
$$(2,1) = r + r^{16}$$

$$(2,13) = r^4 + r^{13}$$
$$(2,9) = r^8 + r^9$$
$$(2,15) = r^2 + r^{15}$$
$$(2,3) = r^3 + r^{14}$$
$$(2,5) = r^5 + r^{12}$$
$$(2,10) = r^{10} + r^7$$
$$(2,11) = r^{11} + r^6.$$

Por las reglas del artículo 351 se encuentra una ecuación $(A)$, $x^2 + x - 4 = 0$,[59] cuyas raíces son las sumas (períodos)

$$(8,1) = r + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2 \quad \text{y}$$
$$(8,3) = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6.$$

Se puede verificar, usando la fórmula de Al-Khwarizmi, que sus raíces son

$$-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1.5615528128 \quad \text{y} \quad -\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2.5615528128.$$

Por lo que se explicó en el art. 352 (paso 3), se puede hacer la primer raíz igual a $(8,1)$ y por ende la otra será igual a $(8,3)$.

Luego, la ecuación $(B)$, cuyas raíces son

$$(4,1) = r + r^{13} + r^{16} + r^4 \quad \text{y} \quad (4,9) = r^9 + r^{15} + r^8 + r^2, \quad \text{es}$$
$$x^2 - (8,1)x - 1 = 0.$$ [60]

Sus raíces son $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)}$. Se toman

$$(4,1) = \frac{1}{2}(8,1) + \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)} = 2.0494811777$$

y

$$(4,9) = \frac{1}{2}(8,1) - \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)} = -0.4879283649.$$

Los períodos restantes, $(4,3)$ y $(4,10)$, contenidos en $(8,3)$, pueden hallarse ya sea resolviendo la ecuación de la que son raíces o por las reglas del art. 346. Primero se hallarán mediante el artículo 346. Designando $(4,1) = p$, se tiene[61],

---

[59] Del esquema que se mostró arriba y las propiedades de períodos, como en el artículo 351 se obtienen los coeficientes de las ecuaciones:

$$(8,1) + (8,3) = (16,1) = -1 \quad \text{y}$$
$$(8,1) \cdot (8,3) = (8,4) + (8,11) + (8,6) + (8,12) + (8,15) + (8,8) + (8,13) + (8,7)$$
$$= (8,1) + (8,3) + (8,3) + (8,3) + (8,1) + (8,1) + (8,1) + (8,3)$$
$$= 4(8,1) + 4(8,3) = 4[(8,1) + (8,3)] = -4.$$

[60] El primer coeficiente es $(4,1) + (4,9) = (8,1)$ y el segundo es $(4,1) \cdot (4,9) = (4,10) + (4,16) + (4,9) + (4,3) = (8,1) + (8,3) = -1$.

[61] Si $p = (4,1)$ se tiene que,

$$p^2 = (4,1) \cdot (4,1) = (4,2) + (4,14) + (4,17) + (4,5) = (4,9) + (4,3) + 4 + (4,3) = 4 + 2(4,3) + (4,9),$$

esto es,

$$(4,9) = p^2 - 4 - 2(4,3)$$

Entonces,

$$p^3 = [4 + 2(4,3) + (4,9)] \cdot (4,1)$$
$$= 4(4,1) + 2(4,4) + 2(4,15) + 2(4,6) + 2(4,13) + (4,10) + (4,16) + (4,9) + (4,3)$$

$$p^2 = 4 + 2(4,3) + (4,9),$$
$$p^3 = 9(4,1) + 3(4,9) + (4,3) + 3(4,10),$$

así,

$$(4,9) = p^2 - 4 - 2(4,3)$$
$$p^3 = 6(4,1) - 2(4,3) + 3[(4,1) + (4,9) + (4,3) + (4,10)] = 6p - 2(4,3) - 3$$

de donde,

$$(4,3) = -\frac{1}{2}p^3 + 3p - \frac{3}{2} = 0.3441507314,$$

y por otro, como

$$p^3 = 9p + 3[p^2 - 4 - 2(4,3)] + (4,3) + 3(4,10) = -\frac{9}{2} - 6p + 3p^2 + \frac{5}{2}p^3 + 3(4,10),$$

de donde,

$$(4,10) = \frac{3}{2} + 2p - p^2 - \frac{1}{2}p^3 = -2.9057035442.$$

La segunda forma se explica en una nota al pie[62] para dar mayor fluidez al proceso.

Ahora, sea $(C)$ la ecuación $x^2 - (4,1)x + (4,3) = 0$,[63] cuyas raíces son los períodos $(2,1) = r + r^{16}$ y $(2,13) = r^4 + r^{13}$, contenidos en $(4,1)$. Puesto que los valores de los coeficientes de $(C)$ son conocidos, se pueden hallar sus raíces que son

$$\frac{1}{2}(4,1) + \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)} = 1.8649444588$$

y

$$\frac{1}{2}(4,1) - \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)} = 0.1845367189$$[64].

La primera de ellas se hace igual a $(2,1)$ y la segunda igual a $(2,13)$.

---

$= 9(4,1) + 3(4,9) + (4,3) + 3(4,10).$

Equivalentemente, $p^3 = 6(4,1) - 2(4,3) + 3[(4,1) + (4,9) + (4,3) + (4,10)] = 6p - 2(4,3) - 3,$

de donde,

$$(4,3) = -\frac{1}{2}p^3 + 3p - \frac{3}{2} = 0.3441507314.$$

Pero $p^3$ también se puede ver como

$$p^3 = 9p + 3[p^2 - 4 - 2(4,3)] + (4,3) + 3(4,10) = -\frac{9}{2} - 6p + 3p^2 + \frac{5}{2}p^3 + 3(4,10),$$

de donde,

$$(4,10) = \frac{3}{2} + 2p - p^2 - \frac{1}{2}p^3 = -2.9057035442.$$

[62] De la segunda forma, hay que resolver la ecuación $x^2 - (8,3)x - 1 = 0$, cuyas raíces son $(4,3)$ y $(4,10)$. Estas raíces son $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$. Para saber cuál de estas representa $(4,3)$ y cuál $(4,10)$ se hará lo siguiente: primero, se calcula el producto $[(4,1) - (4,9)] \cdot [(4,3) - (4,10)] = 2(8,1) - 2(8,3) = +2\sqrt{17}$. De aquí que los factores sean, o ambos positivos o ambos negativos, pero puesto que se conocen los valores de $(4,1)$ y $(4,9)$ es posible calcular $(4,1) - (4,9) = +\sqrt{12 + 3(8,1) + 4(8,3)}$, así el factor $(4,3) - (4,10)$ debe de ser positivo, y por tanto $(4,3) = \frac{1}{2}(8,3) + \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$ y $(4,10) = \frac{1}{2}(8,3) - \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$, que son los mismos valores que se obtuvieron del otro método.

[63] El primer coeficiente es la suma $(2,1) + (2,13) = (4,1)$ y el segundo coeficiente es
$$(2,1) \cdot (2,3) = (2,14) + (2,5) = (2,3) + (2,5) = (4,3).$$

[64] Las raíces de $(C)$ son $\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{(4,1)^2 - 4(4,3)}$. Como ya vimos antes $(4,1)^2 = 4 + 2(4,3) + (4,9)$, de donde $(4,1)^2 - 4(4,3) = 4 + (4,9) - 2(4,3)$. Así las raíces son iguales a $\frac{1}{2}(4,1) \pm \sqrt{4 + (4,9) - 2(4,3)}$.

El resto de los períodos de dos términos se pueden determinar por el art. 346 expresando los períodos $(2,2) = (2,15);\ (2,3);\ (2,5);\ (2,6) = (2,11);\ (2,7) = (2,10);\ (2,8) = (2,9)$ como combinación lineal de potencias de $(2,1)$, tal y como se hizo en el ejemplo previo. Sin embargo, quizá en ocasiones sea más conveniente hallar estos períodos resolviendo ecuaciones cuadráticas, así la ecuación cuyas raíces son los períodos $(2,9)$ y $(2,15)$ es

$$x^2 - (4,9) + (4,10) = 0 \text{ con raíces } \frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}.$$

Para saber a qué período corresponde cada raíz se hace del mismo modo que antes[65], se calcula el producto

$$[(2,1) - (2,13)][(2,9) - (2,15)] = (4,10) + (4,9) - (4,1) - (4,3)$$
$$= -\sqrt{12 + 3(8,1) + 4(8,3)} - \sqrt{12 + 4(8,1) + 3(8,3)},$$

que es negativo y como $(2,1) - (2,13)$ es positivo, $[(2,9) - (2,15)]$ debe ser negativo y por lo tanto se tiene,

$$(2,9) = \frac{1}{2}(4,9) - \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}$$
$$(2,15) = \frac{1}{2}(4,9) + \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}.$$

De manera análoga, se obtiene que,

$$(2,3) = \frac{1}{2}(4,3) + \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)} = 0.8914767116$$
$$(2,5) = \frac{1}{2}(4,3) - \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)} = 0.8914767116$$
$$(2,10) = \frac{1}{2}(4,10) - \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)} = -1.7004342715$$
$$(2,11) = \frac{1}{2}(4,10) + \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)} = -1.2052692728.$$

Finalmente, se hallarán las raíces de $\Omega$. Sea $(D)$ la ecuación $x^2 - (2,1)x + 1$, cuyas raíces son $r$ y $r^{16}$. Las raíces de esta ecuación son

$$\frac{1}{2}(2,1) \pm \frac{1}{2}\sqrt{(2,1)^2 - 4} = \frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{4 - (2,1)^2} = \frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{2 - (2,15)}.$$

Se toma $r = \frac{1}{2}(2,1) + \frac{1}{2}i\sqrt{2 - (2,15)}$ y $r^{16} = \frac{1}{2}(2,1) - \frac{1}{2}i\sqrt{2 - (2,15)}$. El resto de las raíces se obtienen de las potencias de $r$ o resolviendo siete ecuaciones cuadráticas más, donde con cada una de ellas se encuentran dos raíces y se determina el signo del radical que le corresponde a cada raíz de la misma forma que se ha hecho antes. Así, se obtienen los siguientes valores:

$r = 0.9324722294 + 0.3612416662i$ $\quad$ $r^{16} = 0.9324722294 - 0.3612416662i$
$r^2 = 0.7390089172 + 0.6736956436i$ $\quad$ $r^{15} = 0.7390089172 - 0.6736956436i$
$r^3 = 0.4457383558 + 0.8951632914i$ $\quad$ $r^{14} = 0.4457383558 - 0.8951632914i$
$r^4 = 0.0922683595 + 0.9957341763\,i$ $\quad$ $r^{13} = 0.0922683595 - 0.9957341763\,i$
$r^5 = -0.2736629901 + 0.9618256432i$ $\quad$ $r^{12} = -0.2736629901 - 0.9618256432i$

[65] Ver el proceso en la nota a pie 73.

$r^6 = -0.6026346364 + 0.7980172273i$ $\quad$ $r^{11} = -0.6026346364 - 0.7980172273i$
$r^7 = -0.8502171357 + 0.5264321629i$ $\quad$ $r^{10} = -0.8502171357 - 0.5264321629i$
$r^8 = -0.9829730997 + 0.1837495178i$ $\quad$ $r^9 = -0.9829730997 - 0.1837495178i$

Note que estas raíces también pueden ser expresadas con radicales, por ejemplo, se tiene que

$$r = \frac{1}{2}(2,1) + \frac{1}{2}i\sqrt{2 - (2,15)},$$

pero ya se conoce el valor de la suma $(2,1)$ y $(2,15)$, entonces

$$r = \frac{1}{2}\left[\frac{1}{2}(4,1) + \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)}\right] + i\frac{1}{2}\sqrt{2 - \left[\frac{1}{2}(4,9) + \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}\right]}$$

$$= \frac{1}{4}(4,1) + \frac{1}{4}\sqrt{4 + (4,9) - 2(4,3)} + i\frac{1}{2}\sqrt{2 - \frac{1}{2}(4,9) - \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}}.$$

Recordemos que los expresiones con radicales de $(4,1)$, $(4,3)$, $(4,9)$ y $(4,10)$ son

$$(4,1) = \frac{1}{2}(8,1) + \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)}$$
$$(4,9) = \frac{1}{2}(8,1) - \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)}$$
$$(4,3) = \frac{1}{2}(8,3) + \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$$
$$(4,10) = \frac{1}{2}(8,3) - \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)},$$

y que

$$(8,1) = -\frac{1}{2} + \frac{1}{2}\sqrt{17}$$
$$(8,3) = -\frac{1}{2} - \frac{1}{2}\sqrt{17},$$

entonces sustituyendo se tiene que

$$(4,1) = -\frac{1}{4} + \frac{1}{4}\sqrt{17} + \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}}$$
$$(4,9) = -\frac{1}{4} + \frac{1}{4}\sqrt{17} - \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}}$$
$$(4,3) = -\frac{1}{4} - \frac{\sqrt{17}}{4} + \frac{1}{2}\sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}$$
$$(4,10) = -\frac{1}{4} - \frac{\sqrt{17}}{4} - \frac{1}{2}\sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}.$$

Por lo tanto, el valor con radicales de $r$ es

$$r = -\frac{1}{16} + \frac{\sqrt{17}}{16} + \frac{1}{8}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} + \frac{1}{4}\sqrt{\frac{17}{4} + \frac{3\sqrt{17}}{4} - \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} - \frac{1}{2}\sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}}$$
$$+ \boldsymbol{i}\frac{1}{2}\sqrt{\frac{17}{8} - \frac{\sqrt{17}}{8} + \frac{1}{4}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} - \frac{1}{2}\sqrt{\frac{17}{4} + \frac{\sqrt{17}}{4} + \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} + \frac{\sqrt{17}}{2} + \sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}}}.$$

De manera semejante se pueden obtener las expresiones con radicales de las raíces restantes.

**Ejemplo. II** Para $n = 19$ se tiene $n - 1 = 3 \cdot 3 \cdot 2$, entonces para hallar las raíces de $\Omega$ se han de resolver dos ecuaciones cúbicas y una cuadrática.

Puesto que a lo largo de esta segunda parte se ha trabajado con ejemplos para $n = 19$, aquí se reducirán los cálculos y así se desarrollará el ejemplo con mayor fluidez.

**Nota:** El objetivo de este ejemplo es mostrar el camino para hallar las raíces 19–ésimas de la unidad; sin embargo, debido a que involucran radicales cúbicos, que en cierto punto se vuelven inmanejables, y por ello no se usarán estas expresiones con radicales.

Primero obsérvese que tomando como raíz primitiva $g = 2$ se obtienen los siguientes residuos módulo $n$ de las potencias de $g$:

| $g^0$ | $g^1$ | $g^2$ | $g^3$ | $g^4$ | $g^5$ | $g^6$ | $g^7$ | $g^8$ | $g^9$ | $g^{10}$ | $g^{11}$ | $g^{12}$ | $g^{13}$ | $g^{14}$ | $g^{15}$ | $g^{16}$ | $g^{17}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 4 | 8 | 16 | 13 | 7 | 14 | 9 | 18 | 17 | 15 | 11 | 3 | 6 | 12 | 5 | 10 |

Luego, por los artículos 344 y 345, se deduce la siguiente distribución de las raíces de $\Omega^{66}$:

$$\Omega = \begin{cases} (6,1)\begin{cases}(2,1)\ldots\ r, r^{18}\\(2,8)\ldots\ r^8, r^{11}\\(2,7)\ldots\ r^7, r^{12}\end{cases}\\ (6,2)\begin{cases}(2,2)\ldots\ r^2, r^{17}\\(2,16)\ldots r^{16}, r^3\\(2,14)\ldots r^{14}, r^5\end{cases}\\ (6,4)\begin{cases}(2,4)\ldots\ r^4, r^{15}\\(2,13)\ldots r^{13}, r^6\\(2,9)\ldots\ r^9, r^{10}\end{cases}\end{cases}$$

Como ya vimos antes [art. 352 ej. I], la ecuación $(A)$ cuyas raíces son los períodos

$$(6,1) = r + r^8 + r^7 + r^{18} + r^{11} + r^{12},$$
$$(6,2) = r^2 + r^{16} + r^{14} + r^{17} + r^3 + r^5$$
$$(6,4) = r^4 + r^{13} + r^9 + r^{15} + r^6 + r^{10}$$

es

$$x^3 + x^2 - 6x - 7 = 0.$$

Se puede verificar que una de sus raíces es $-1.2218761623$,[67] a la que llamaremos $(6,1)$. Los períodos restantes se hallan a partir de $(6,1)$, lo cual se hizo en el ejemplo del art. 346. Así,

[66] Ver los ejemplos de estos artículos.

[67] Mediante las fórmulas de Cardano-Tartaglia se verifica que las raíces de la ecuación $x^3 + x^2 - 6x - 7 = 0$ son

$$(6,2) = 4 - (6,1)^2 = 2.5070186441$$

$$(6,4) = -5 - (6,1) + (6,1)^2 = -2.2851424818.$$

Ahora, la ecuación $(B)$ cuyas raíces son los períodos $(2,1) = r + r^{18}$, $(2,7) = r^7 + r^{12}$ y $(2,8) = r^8 + r^{11}$ es

$$x^3 - (6,1)x^2 + [(6,1) + (6,4)]x - 2 - (6,2) = 0,$$[68]

o equivalentemente,

$$x^3 + 1.2218761623x^2 - 3.5070186441x - 4.5070186441 = 0.$$

Resolviendo esta ecuación se obtiene la raíz $-1.3545631433$, que se representa con $(2,1) = q$. De manera análoga a lo anterior, se pueden obtener los períodos $(2,2)$, $(2,3)$ y $(2,5)$ a partir de la ecuación

$$x^3 - (6,2)x^2 + [(6,1) + (6,2)]x - 2 - (6,4) = 0.$$

Así mismo, por la ecuación

$$x^3 - (6,4)x^2 + [(6,2) + (6,4)]x - 2 - (6,1) = 0,$$

se obtienen los períodos $(2,4)$, $(2,6)$ y $(2,9)$.

A continuación se hallarán las potencias de $q = (2,1)$ para expresar el resto de los períodos de dos términos como combinación de ellas:

$$q^2 = (2,2) + (2,19) = (2,2) + 2$$
$$q^3 = [(2,2) + 2] \cdot (2,1) = (2,3) + 3(2,1)$$
$$q^4 = [(2,3) + 3q] \cdot q = (2,4) + 4q^2 - 2$$
$$q^5 = [(2,4) + 4q^2 - 2] \cdot q = (2,5) + 5q^3 - 5q$$
$$q^6 = [(2,5) + 5q^3 - 5q] \cdot q = (2,6) + 6q^4 - 9q^2 + 2$$
$$q^7 = [(2,6) + 6q^4 - 9q^2 + 2] \cdot q = (2,7) + 7q^5 - 14q^3 + 7q$$
$$q^8 = [(2,7) + 7q^5 - 14q^3 + 7q] \cdot q = (2,8) + 8q^6 - 20q^4 + 16q^2 - 2$$
$$q^9 = [(2,8) + 8q^6 - 20q^4 + 16q^2 - 2] \cdot q = (2,9) + 9q^7 - 27q^5 + 30q^3 - 9q$$

es decir,

$$(2,2) = q^2 - 2$$
$$(2,3) = q^3 - 3q$$
$$(2,4) = q^4 - 4q^2 + 2$$

---

$$x_1 = \sqrt[3]{\frac{133}{54} - \frac{19i}{6\sqrt{3}}} + \sqrt[3]{\frac{133}{54} + \frac{19i}{6\sqrt{3}}} - \frac{1}{3} = 2.5070$$

$$x_2 = -\frac{1}{2}\left(\sqrt[3]{\frac{133}{54} - \frac{19i}{6\sqrt{3}}} - \sqrt[3]{\frac{133}{54} + \frac{19i}{6\sqrt{3}}}\right) + \frac{1}{2}i\sqrt{3}\left(\sqrt[3]{\frac{133}{54} + \frac{19i}{6\sqrt{3}}} - \sqrt[3]{\frac{133}{54} - \frac{19i}{6\sqrt{3}}}\right) - \frac{1}{3} = -2.2851$$

$$x_3 = -\frac{1}{2}\left(\sqrt[3]{\frac{133}{54} - \frac{19i}{6\sqrt{3}}} - \sqrt[3]{\frac{133}{54} + \frac{19i}{6\sqrt{3}}}\right) - \frac{1}{2}i\sqrt{3}\left(\sqrt[3]{\frac{133}{54} + \frac{19i}{6\sqrt{3}}} - \sqrt[3]{\frac{133}{54} - \frac{19i}{6\sqrt{3}}}\right) - \frac{1}{3} = -1.2218$$

[68] Esto se vio en el art.352 ej. II.

$$(2,5) = q^5 - 5q^3 + 5q$$
$$(2,6) = q^6 - 6q^4 + 9q^2 - 2$$
$$(2,7) = q^7 - 7q^5 + 14q^3 - 7q$$
$$(2,8) = q^8 - 8q^6 + 20q^4 - 16q^2 + 2$$
$$(2,9) = q^9 - 9q^7 + 27q^5 - 30q^3 + 9q.$$

Sustituyendo el valor de $q = (2,1) = -1.3545631433$ en estas expresiones se deducen los siguientes valores numéricos:

$$(2,2) = -0.1651586909$$
$$(2,3) = 1.5782810188$$
$$(2,4) = -1.9727226068$$
$$(2,5) = 1.0938963162$$
$$(2,6) = 0.4909709743$$
$$(2,7) = -1.7589475024$$
$$(2,8) = 1.8916344834$$
$$(2,9) = -0{,}8033908493.$$

Gauss muestra otra forma de obtener estas expresiones que en este trabajo se optó por mencionarlo en nota al pie [69] para no confundir al lector.

Finalmente han de hallarse los valores de las raíces en $\Omega$, así vemos que $r$ y $r^{18}$ son raíces de la ecuación $x^2 - (2,1)x + 1 = 0$,[70] de donde

$$r = \frac{1}{2}(2,1) + i\sqrt{\frac{1}{2} - \frac{1}{4}(2,2)} = -0.6772815716 + 0.7357239107i$$

y $$r^{18} = \frac{1}{2}(2,1) - i\sqrt{\frac{1}{2} - \frac{1}{4}(2,2)} = -0.6772815716 - 0.7357239107i.$$

El resto de las raíces se pueden hallar a través de las potencias de algunas de las dos anteriores, o bien, resolviendo las ocho ecuaciones cuadráticas de la forma

$$x^2 - tx + 1 = 0,$$

---

[69] Sea $r = \cos\left(\frac{2\pi k}{19}\right) + i\text{sen}(\frac{2\pi k}{n})$, entonces

$$r^{18} = \cos\left(\frac{2\cdot 18\pi k}{19}\right) + i\text{sen}\left(\frac{2\cdot 18\pi k}{n}\right) = \cos\left(\frac{2\pi k}{19}\right) - i\text{sen}(\frac{2\pi k}{n}),$$

de donde,

$$(2,1) = 2\cos\left(\frac{2\pi k}{19}\right).$$

Y como en general $r^{\lambda} = \cos\left(\frac{\lambda 2\pi k}{19}\right) + i\text{sen}\left(\frac{\lambda 2\pi k}{19}\right)$, entonces

$$(2,\lambda) = r^{\lambda} + r^{18\lambda} = r^{\lambda} + r^{-\lambda} = 2\cos\left(\frac{\lambda 2\pi k}{19}\right).$$

Por tanto, si $\omega = \frac{2\pi k}{19}$, se tendrá $(2,2) = 2\cos 2\omega$, $(2,3) = 2\cos 3\omega$, .... y de las fórmulas de ángulos múltiples para los cosenos, se derivan las mismas expresiones que antes. Luego, consultando una tabla de cosenos se puede verificar que $(2,1) = 2\cos\left(\frac{7\cdot 2\pi}{19}\right)$, entonces $(2,7) = 2\cos\left(\frac{7\cdot 7\cdot 2\pi}{19}\right) = 2\cos\left(\frac{8\cdot 2\pi}{19}\right)$ y $(2,8) = 2\cos\left(\frac{7\cdot 8\cdot 2\pi}{19}\right) = 2\cos\left(\frac{2\pi}{19}\right)$.

[70] Las raíces de la ecuación $x^2 - (2,1)x + 1 = 0$ son

$$\frac{(2,1)\pm\sqrt{(2,1)^2-4}}{2} = \frac{1}{2}(2,1) \pm i\sqrt{1 - \frac{(2,1)^2}{4}} = \frac{1}{2}(2,1) \pm i\sqrt{1 - \frac{1}{4}[(2,2)+2]} = \frac{1}{2}(2,1) \pm i\sqrt{\frac{1}{2} - \frac{1}{4}(2,2)}.$$

con $t$ variando en $(2,2)$, $(2,3)$, $(2,4)$, $(2,5)$, $(2,6)$, $(2,7)$, $(2,8)$ y $(2,9)$, respectivamente. Y con la ayuda de tabla de cosenos se aclara a que raíz corresponde cada período.
Se hallarán mediante potencias de $r = -0.6772815716 + 0.7357239107i$. Así, al final se obtienen los siguientes valores:

$r = -0.6772815716 + 0.7357239107i$ $\quad$ $r^{18} = -0.6772815716 - 0.7357239107i$
$r^2 = -0.082579345 + 0.9965844930\,i$ $\quad$ $r^{17} = -0.0825793455 - 0.9965844930i$
$r^3 = 0.7891405094 + \ 0.6142127127i$ $\quad$ $r^{16} = 0.7891405094 - 0.6142127127i$
$r^4 = -0.9863613034 + 0.1645945903i$ $\quad$ $r^{15} = -0.9863613034 - 0.1645945903i$
$r^5 = 0.5469481581 + 0.8371664783i$ $\quad$ $r^{14} = 0.5469481581 - 0.8371664783i$
$r^6 = 0.2454854871 + 0.9694002659i$ $\quad$ $r^{13} = 0.2454854871 - 0.9694002659i$
$r^7 = -0.8794737512 + 0.4759473930i$ $\quad$ $r^{12} = -0.8794737512 - 0.4759473930i$
$r^8 = 0.9458172417 + 0.3246994692i$ $\quad$ $r^{11} = 0.9458172417 - 0.3246994692i$
$r^9 = -0.4016954247 + 0{,}9157733267i$ $\quad$ $r^{10} = -0.4016954247 - 0{,}9157733267i$

Este ejemplo también se pudo haber desarrollado primero dividiendo las raíces de Ω en dos períodos de nueve términos, luego cada uno de ellos en tres períodos de tres términos y finalmente hallando las raíces. Pero en este caso los cálculos para hallar los valores de los períodos de tres términos a través de las potencias de uno de ellos se complican. Así que convendría hallarlos de la segunda forma mencionada en párrafos anteriores.
Con esto, se concluye la descripción del método para hallar las raíces de la ecuación $x^n - 1 = 0$ por medio de ecuaciones auxiliares de grado menor.
Recuerde que hasta este punto, no se ha tratado la construcción de polígonos, este es el punto a tratar en el siguiente capítulo.

## Intercapítulo

Los artículos 355-358 de las *Disquisitiones* exponen más características acerca de períodos, pero que en este trabajo solo se mencionará de qué tratan, ya que el objetivo es abordar la constructibilidad de los polígonos con regla y compás.

En el 355 se muestra que el valor de un período con un número par de términos es un número real. Del 356 al 358 se estudian, de manera general las ecuaciones auxiliares que surgen de la distribución de las raíces de Ω –raíces $n$-ésimas de la unidad diferentes de uno con $n$ un número primo–, en dos o tres períodos respectivamente. De hecho, en el art. 356 se exhibe de manera explícita la forma de la ecuación cuadrática cuyas raíces son los dos períodos de $\frac{1}{2}(n-1)$ términos. También en este artículo, Gauss da otra prueba del teorema visto en los arts. 108 y 109 que dice:

$-1$ *es un residuo cuadrático de los números primos de la forma* $4k+1$ *y no residuo de los de la forma* $4k+3$.

Además, casi al final del artículo introduce las siguientes sumas para $n \equiv 1(mod\ 4)$

$$\sum cos\frac{2\pi k\Re P}{n} - \sum cos\frac{2\pi k\Re}{n} = \pm\sqrt{n} \qquad \text{y} \qquad \sum sen\frac{2\pi k\Re}{n} - \sum sen\frac{2\pi k\Re}{n} = 0\,,$$

y para $n \equiv 3(mod\ 4)$ se tienen las sumas

$$\sum cos\frac{2\pi k\Re P}{n} - \sum cos\frac{2\pi k\Re}{n} = 0 \qquad \text{y} \qquad \sum sen\frac{2\pi k\Re}{n} - \sum sen\frac{2\pi k\Re}{n} = \pm\sqrt{n}\,,$$

donde $\Re$ varía sobre los residuos cuadráticos de $n$, menores que $n$, y $\Re$ sobre los no residuos cuadráticos correspondientes. Estas sumas ahora son conocidas como sumas cuadráticas de Gauss.[71] Sin embargo, Gauss no las estudia con detalle en sus *Disquisitiones,* sino hasta el documento *Summatio quarundam serierum singularium* publicado en 1808.

En el artículo 357, Gauss prueba –resultado que mencionó en el art. 124 de la sección IV– que la expresión $\frac{4(x^n-1)}{x-1}$, donde $n$ es un número primo, puede reducirse a algo de la forma,

$$Y^2 + nZ^2 \quad \text{si} \quad n \equiv 3(mod\ 4) \qquad \text{o} \qquad Y^2 - nZ^2 \quad \text{si} \quad n \equiv 1(mod\ 4),$$

con $Y$, $Z$ funciones enteras de $x$. Al final muestra un ejemplo para $n = 17$.

Por último, en el art. 358, analiza la distribución en tres períodos de las raíces en $\Omega$ cuando $n-1$ es de la forma $3k+1$. En dicho artículo, se muestra que la ecuación auxiliar cuyas raíces son estos tres períodos, es de la forma

$$x^3 + x^2 - mx - \left(\frac{1}{9}m + \frac{1}{9}kn\right) = 0, \text{ con } m = \frac{n-1}{3}.$$

En el proceso también se muestra un resultado interesante, que establece que $4n$ puede expresarse de la forma $x^2 + 27y^2$, esto puede obtenerse también de la teoría de formas cuadráticas de la sección V de las *Disquisitiones.*

A continuación se da una visión general de lo que tratan los artículos 359 a 365 y aunque estos se relacionan con la constructibilidad de polígonos regulares, en el capítulo IV, se desarrollarán solo algunos de ellos.

En el art. 359, Gauss presenta algunas observaciones acerca de las raíces de la ecuación $x^e - 1 = 0$, donde $e$ puede ser un entero primo o compuesto:

I. Se sabe que estas raíces están dadas por $\cos\frac{2\pi k}{e} + i\text{sen}\frac{2\pi k}{e}$, donde $k \equiv 0, 1, \ldots, e-1\ (mod\ e)$. Además, para cualquier $k \equiv 0\ (mod\ e)$ la raíz será igual a uno y en cualquier otro caso distinta de uno.

[71] Carlos Ivorra Castillo, *Teoría de números* pág. 303.

II. Si $R$ es una raíz que corresponde a un valor de $k$ que es primo relativo con $e$, entonces las $e$ cantidades $1,\ R,\ R^2, R^3, \ldots,\ R^{e-1}$ son distintas y son todas las raíces de la ecuación $x^e - 1 = 0$. [72]

III. Sea $R$ como en el inciso anterior, entonces se tiene que

$$1 + R^\lambda + R^{2\lambda} + R^{3\lambda} + \ \ldots + R^{\lambda(e-1)} = 0,$$

donde $\lambda$ es cualquier entero no divisible por $e$. Cuando $\lambda$ es divisible por $e$, la suma es igual a $e$.

En el art. 360, muestra que para un primo $n$, con $n - 1 = \alpha\beta\gamma$, estas ecuaciones pueden admitir soluciones por radicales. Sin embargo, no lo hace con todo detalle sino que presenta solo los principios que él considera más importantes. Para ello Gauss utiliza la resolvente de Lagrange [73]

$$t = (\gamma, 1) + (\gamma, g^\alpha)R + (\gamma, g^{2\alpha})R^2 + \cdots + \left(\gamma, g^{\alpha\beta-\alpha}\right)R^{\beta-1},$$

donde $R$ es una raíz $\beta$-ésima de la unidad.

En los artículos 361 a 364 analiza la relación entre las raíces de la ecuación $x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$ y las funciones trigonométricas.

Finalmente, en el art. 365 –el objetivo de esta sección– da una caracterización de los polígonos que pueden construirse solo con regla y compás. Además, concluye el ejemplo para $n = 17$ y verifica que es posible construir de esta manera el polígono regular de 17 lados.

---

[72] Puesto que $(\cos\frac{2\pi k}{e} + i sen\frac{2\pi k}{e})^\lambda = \cos\frac{\lambda 2\pi k}{e} + i sen\frac{\lambda 2\pi k}{e}$, la $e$-ésima potencia de $R$ será igual a $\cos 2\pi k + i sen 2\pi k = 1$ y como $k$ no es divisible por $e$, las potencias anteriores son distintas de 1 y por tanto diferentes entre sí. Además como $R^e = 1$, las $e$ cantidades $1,\ R,\ R^2, R^3, \ldots,\ R^{e-1}$ satisfacen $x^e - 1$.

[73] Se refiere al tipo de ecuaciones que originalmente Lagrange llamó *resolvente*. [Véase *Lagrange. La elegancia matemática*, p. 135 ]

# Capítulo IV

## Sobre la construcción de polígonos regulares.

### Introducción

Este capítulo se centra en la conexión entre las soluciones por radicales de la ecuación $x^n - 1 = 0$ y la constructibilidad de polígonos regulares de $n$ lados.

Ahora, se mencionan algunos hechos sobre la construcción de ciertos objetos geométricos que sí se pueden construir únicamente con regla y compás, y que son la base de la teoría que a continuación se abordará sobre la construcción de polígonos.

1) Dados dos puntos A y B, se pueden construir nuevos puntos, mediante una sucesión finita de operaciones de los siguientes tipos:
   i. Dibujar una línea que pase por dos puntos dados,
   ii. Dibujar un círculo cuyo centro es un punto dado y con radio la distancia entre dos puntos dados.

   A estos puntos obtenidos se les llama *puntos construibles.*
2) Un punto B sobre el plano puede construirse con regla y compás a partir de A y 0 (origen del plano) si y solo si cada una de sus coordenadas (OA, OB) pueden obtenerse de 0 y 1 mediante una sucesión finita de operaciones:
   i. Operaciones racionales (suma, resta, multiplicación, división).
   ii. Extracción de raíces cuadradas. [74]

A continuación se desarrolla la teoría que Gauss expuso en el artículo 336 de las *Disquisitiones* y que en este trabajo se decidió reubicar debido a la conexión que guarda con los asuntos vinculados con la partición del círculo, que es el tema a tratar en este capítulo.

### División del círculo en $n$ partes.

La división del círculo en $n$ partes iguales[75] al caso particular donde $n$ es un número primo, y para ello se usará el art. 310 de la sección VI, en el que aparece el siguiente lema.

[74] Para la demostración de esta proposición véase *Galois Theory of Algebraic Equations*, por Jean-Pierre Tignol.
[75] $n$ es entero y en consecuencia se podrá realizar la construcción de un polígono regular de $n$ lados.

**Lema 1.** Sea $\frac{m}{n}$ una fracción cuyo denominador $n$ es el producto de factores $a, b, c, d, \ldots$, que son primos entre sí, entonces $\frac{m}{n}$ se puede expresar como

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \cdots.$$

Los numeradores $\alpha, \beta, \gamma, \delta, \ldots$ se pueden tomar positivos y menores que sus denominadores, salvo el último, el cual queda determinado con la selección de los anteriores.
[Para la demostración véase *Disquisitiones Arithmeticae*, p. 388]

Considérese que $A = \frac{m2\pi}{n}$, con $m$ y $n$ enteros, note que esto representa $m$ de las $n$ partes en las que se divide al círculo. Sean $a, b, c, d,$ etc., los factores de la descomposición en primos (o potencias de primos) de $n$, entonces por el lema anterior se tiene que $A = (\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \cdots)2\pi$. Así, las funciones trigonométricas de este ángulo se pueden hallar a partir de $\frac{\alpha 2\pi}{a}$, $\frac{\beta 2\pi}{b}, \ldots$ por las propiedades de estas funciones. Entonces, basta considerar la división del círculo en partes cuyo número es primo o potencia de un primo. Pero, debido a que las funciones trigonométricas circulares del ángulo $\frac{m2\pi}{p^{\lambda}}$ pueden deducirse de las funciones trigonométricas circulares del ángulo $\frac{m2\pi}{p^{\lambda-1}}$, entonces es suficiente realizar el estudio de la división del círculo solo para $n$ primo.

Enseguida, Gauss exhibe que los arcos iguales de la división del círculo se pueden expresar a través de funciones trigonométricas. De esta manera, él muestra en el art. 337 que a partir de las raíces de la unidad se puede encontrar el valor de ciertas funciones trigonométricas que tienen términos del tipo

$$\operatorname{sen}\left(\frac{2\pi k}{p}\right),\ \cos\left(\frac{2\pi k}{p}\right)\ \text{y}\ \tan\left(\frac{2\pi k}{p}\right),$$

donde $k = 0,1,2, \ldots p-1$.

Por ejemplo, para las raíces del polinomio $x^6 - 1 = 0$, sabemos que la forma polar de estas es:

$$\cos\left(\frac{2\pi\cdot 0}{6}\right) + i\operatorname{sen}\left(\frac{2\pi\cdot 0}{6}\right)$$
$$\cos\left(\frac{2\pi}{6}\right) + i\operatorname{sen}\left(\frac{2\pi}{6}\right)$$
$$\cos\left(\frac{4\pi}{6}\right) + i\operatorname{sen}\left(\frac{4\pi}{6}\right)$$
$$\cos\left(\frac{6\pi}{6}\right) + i\operatorname{sen}\left(\frac{6\pi}{6}\right)$$
$$\cos\left(\frac{8\pi}{6}\right) + i\operatorname{sen}\left(\frac{8\pi}{6}\right)$$
$$\cos\left(\frac{10\pi}{6}\right) + i\operatorname{sen}\left(\frac{10\pi}{6}\right),$$

entonces se obtienen los términos

$$\cos\left(\frac{2\pi\cdot 0}{6}\right), \cos\left(\frac{2\pi}{6}\right),\ \cos\left(\frac{4\pi}{6}\right),\ \cos\left(\frac{6\pi}{6}\right), \cos\left(\frac{8\pi}{6}\right), \cos\left(\frac{10\pi}{6}\right),$$

y también

$$\operatorname{sen}\left(\frac{2\pi\cdot 0}{6}\right),\ \operatorname{sen}\left(\frac{2\pi}{6}\right),\ \operatorname{sen}\left(\frac{4\pi}{6}\right),\ \operatorname{sen}\left(\frac{6\pi}{6}\right),\ \operatorname{sen}\left(\frac{8\pi}{6}\right),\ \operatorname{sen}\left(\frac{10\pi}{6}\right),$$

que están asociados a las raíces, pero lo más importante es que las parejas de términos asociados de la forma $\cos\left(\frac{2\pi k}{6}\right)+i\operatorname{sen}\left(\frac{2\pi k}{6}\right)$ representan a los vértices del polígono de seis lados inscrito en la circunferencia unitaria. De esta manera se llega al primer paso para dividir el círculo en partes iguales, y ahora se tienen "funciones trigonométricas de arcos iguales que son partes de la circunferencia completa". En otras palabras, si se logra dividir al círculo en $n$ partes iguales, entonces es posible construir un polígono regular también con $n$ lados iguales. Sin embargo, no es suficiente con las expresiones polares de las raíces $n$-ésimas de la unidad, ya que se debe verificar que sean construibles, o dicho de otra manera, que sean expresables por radicales.

**Art. 361.-** Hasta ahora no se ha detallado la relación que existe entre el conjunto de raíces $\Omega$ de la ecuación $X=x^{n-1}+x^{n-2}+\cdots x+1$ y las funciones trigonométricas de los ángulos $\frac{2\pi}{n},\frac{2\cdot 2\pi}{n},\frac{3\cdot 2\pi}{n},\ldots,\frac{(n-1)2\pi}{2n},\frac{(n+1)2\pi}{2n},\ldots,\frac{(n-1)2\pi}{n}$.

En el método usado en el art. 352 para encontrar las raíces de la unidad en $\Omega$ –salvo que se consulten tablas de senos, aunque esto es menos directo–, queda incierto qué raíz es $\left[\cos\left(\frac{2\pi}{n}\right)+i\operatorname{sen}\left(\frac{2\pi}{n}\right)\right]$, cuál es $\left[\cos\left(\frac{2\cdot 2\pi}{n}\right)+i\operatorname{sen}\left(\frac{2\cdot 2\pi}{n}\right)\right]$, etc. Recuerde que en los artículos previos, las raíces de X se encontraban a través de la construcción de polinomios cuyos coeficientes dependían de los llamados períodos gaussianos, y de esta forma no se recurría a las formas trigonométricas. Ahora es cuando se presenta la duda señalada, pero esta se puede abordar observando que los cosenos de los ángulos $\frac{2\pi}{n}$, $\frac{2\cdot 2\pi}{n}$, $\frac{3\cdot 2\pi}{n},\ldots,\frac{(n-1)2\pi}{2n}$ decrecen continuamente y que los senos son positivos.[76]

Por otro lado, los $\frac{n-1}{2}$ ángulos restantes tomados de manera descendente, $\frac{(n-1)2\pi}{n}$, $\frac{(n-2)2\pi}{n}$, $\frac{(n-3)2\pi}{n},\ldots,\frac{(n+1)2\pi}{2n}$, tienen los mismos cosenos que los ángulos anteriores, respectivamente, esto es, $\cos\frac{2\pi}{n}=\cos\frac{(n-1)2\pi}{n}$; sin embargo, los valores de los senos son negativos, aunque tienen los mismos valores absolutos.

A modo de ejemplo, se analiza esta relación entre las raíces y las funciones trigonométricas en el ejemplo para $n=17$. Aquí los ángulos a considerar son

$$\frac{2\pi}{17},\ \frac{4\pi}{17},\ \frac{6\pi}{17},\ldots,\frac{16\pi}{17},\ \frac{18\pi}{17},\ldots,\frac{30\pi}{17},\ \frac{32\pi}{17}.$$

[76] Debido a que $\frac{(n-1)2\pi}{2n}<\pi$, entonces los ángulos $\frac{2\pi}{n}$, $\frac{2\cdot 2\pi}{n}$, $\frac{3\cdot 2\pi}{n},\ldots,\frac{(n-1)2\pi}{2n}$ se encuentran en el intervalo $(0,\pi)$, en dicho intervalo el coseno es decreciente y el seno toma solo valores positivos.

Primero observe que los cosenos de los $\frac{n-1}{2}$ ángulos $\frac{2\pi}{17}, \frac{4\pi}{17}, \frac{6\pi}{17}, \ldots, \frac{16\pi}{17}$ están en el intervalo $(0, \pi)$, donde la función coseno es decreciente, y por lo tanto

$$\cos\frac{2\pi}{17} > \cos\frac{4\pi}{17} > \cdots > \cos\frac{16\pi}{17}.$$

En ese mismo intervalo el seno toma valores positivos, entonces $\operatorname{sen}\frac{2\pi}{17}, \operatorname{sen}\frac{4\pi}{17}, \ldots, \operatorname{sen}\frac{16\pi}{17}$ son positivos. Además, puesto que los ángulos restantes $\frac{32\pi}{17}, \frac{30\pi}{17}, \ldots, \frac{18\pi}{17}$ son conjugados (suman $2\pi$) con los ángulos $\frac{2\pi}{17}, \frac{4\pi}{17}, \frac{6\pi}{17}, \ldots, \frac{16\pi}{17}$, respectivamente, se tiene que $\cos\frac{32\pi}{17} = \cos\frac{2\pi}{17}$, $\cos\frac{30\pi}{17} = \cos\frac{4\pi}{17}$, ... , $\cos\frac{18\pi}{17} = \cos\frac{16\pi}{17}$. Pero como puede verse los senos de dichos ángulos son negativos.

Recordemos ahora a las raíces de $x^{16} + x^{15} + \cdots + x + 1 = 0$ que fueron obtenidas anteriormente en el ejemplo I del artículo 352:

$r = 0.9324722294 + 0.3612416662i$ $\qquad$ $r^{16} = 0.9324722294 - 0.3612416662i$

$r^2 = 0.7390089172 + 0.6736956436i$ $\qquad$ $r^{15} = 0.7390089172 - 0.6736956436i$

$r^3 = 0.4457383558 + 0.8951632914i$ $\qquad$ $r^{14} = 0.4457383558 - 0.8951632914i$

$r^4 = 0.0922683595 + 0.9957341763\,i$ $\qquad$ $r^{13} = 0.0922683595 - 0.9957341763\,i$

$r^5 = -0.2736629901 + 0.9618256432i$ $\qquad$ $r^{12} = -0.2736629901 - 0.9618256432i$

$r^6 = -0.6026346364 + 0.7980172273i$ $\qquad$ $r^{11} = -0.6026346364 - 0.7980172273i$

$r^7 = -0.8502171357 + 0.5264321629i$ $\qquad$ $r^{10} = -0.8502171357 - 0.5264321629i$

$r^8 = -0.9829730997 + 0.1837495178i$ $\qquad$ $r^9 = -0.9829730997 - 0.1837495178i$

Así, como $\cos\frac{2\pi}{17} = \cos\frac{32\pi}{17}$ es el mayor valor de todos, debe corresponder a la mayor de las partes reales de las raíces anteriores, que es igual a $0.9324722294$. De la misma forma, el valor positivo $0.3612416662i$ corresponde al $\operatorname{sen}\frac{2\pi}{17}$, así como $-0.3612416662$ a $\operatorname{sen}\frac{32\pi}{17}$. Por lo tanto, se tendrá que

$$r = \cos\frac{2\pi}{17} + i\operatorname{sen}\frac{2\pi}{17}$$

$$r^2 = \cos\frac{32\pi}{17} + i\operatorname{sen}\frac{32\pi}{17}.$$

Entonces, como se muestra en este ejemplo, de las raíces $\Omega$ las dos que tienen la mayor parte real (iguales entre sí) corresponden a los ángulos $\frac{2\pi}{n}, \frac{(n-1)2\pi}{n}$. La primera tiene el coeficiente de $i$ positivo y la segunda lo tiene negativo.

De las $n-3$ raíces restantes, las que tienen la mayor parte real corresponderán a los ángulos $\frac{2\cdot 2\pi}{n}, \frac{(n-2)2\pi}{n}$, y así sucesivamente. Además, si se conoce la raíz correspondiente

al ángulo $\frac{2\pi}{n}$, las correspondientes a los ángulos restantes se pueden determinar a partir de ella, ya que si se supone que es $r^{\lambda}$, las raíces $r^{2\lambda}$, $r^{3\lambda}$, $r^{4\lambda}$, ..., $r^{(n-1)\lambda}$ corresponderán respectivamente a los ángulos $\frac{2\cdot 2\pi}{n}$, $\frac{3\cdot 2\pi}{n}$, $\frac{4\cdot 2\pi}{n}$, ..., $\frac{(n-1)2\pi}{n}$, etc. De esta manera los cosenos y senos de los ángulos $\frac{2\pi}{n}$, $\frac{2\cdot 2\pi}{n}$, ..., estarán completamente determinados.

Continuando con el ejemplo previo, se tiene que la raíz $r$ corresponde al ángulo $\frac{2\pi}{17}$, entonces $r^2$, $r^3$, $r^4$, $r^5$, etc. corresponderán a los ángulos $\frac{2\cdot 2\pi}{17}$, $\frac{3\cdot 2\pi}{17}$, $\frac{4\cdot 2\pi}{17}$, $\frac{5\cdot 2\pi}{17}$, etc., respectivamente.

En el ejemplo II del artículo 352, la mayor parte real es la de las raíces $r^{11}$ y $r^{8}$, la primera tiene parte imaginaria positiva y la segunda negativa. Entonces $r^{11}$ corresponde al ángulo $\frac{2\pi}{19}$ (*i.e.* $r^{11} = \cos\frac{2\pi}{19} + i\,\mathrm{sen}\,\frac{2\pi}{19}$) y $r^{8}$ al ángulo $\frac{18\cdot 2\pi}{19}$.
Por lo tanto, las raíces $r^{2\cdot 11}$, $r^{3\cdot 11}$, $r^{4\cdot 11}$, ..., $r^{18\cdot 11}$, esto es, $r^{3}$, $r^{14}$, $r^{6}$, ..., $r^{8}$ corresponderán a los ángulos $\frac{2\cdot 2\pi}{19}$, $\frac{3\cdot 2\pi}{19}$, $\frac{4\cdot 2\pi}{19}$, ..., $\frac{18\cdot 2\pi}{19}$.

Cabe resaltar que debido a que las raíces de la ecuación $x^n - 1 = 0$ tienen el mismo módulo, entonces geométricamente en el plano complejo se ubican en la circunferencia unitaria. Además el ángulo formado entre cualesquiera dos raíces consecutivas es el mismo. Por estas razones, las raíces representan los vértices de un polígono regular inscrito en un círculo de radio uno. De esta manera, si los cosenos de las raíces de la unidad se pueden construir con regla y compás, entonces los vértices también se pueden construir y de esta manera el polígono de $n$ lados será construible.

Veamos esto de manera más concreta, mostrando los casos para la construcción del pentágono y para el de 17 lados. En ambos casos se hará explícito que lo requerido es que sea posible construir con regla y compás el $\cos\frac{2\pi}{5}$ y $\cos\frac{2\pi}{17}$, para que así sea posible construir los respectivos polígonos.

## Caso del pentágono construible

Se tiene el pentágono regular inscrito con centro en $0$, radio la unidad y un vértice en el punto $(1, 0)$, al que se representa por A.

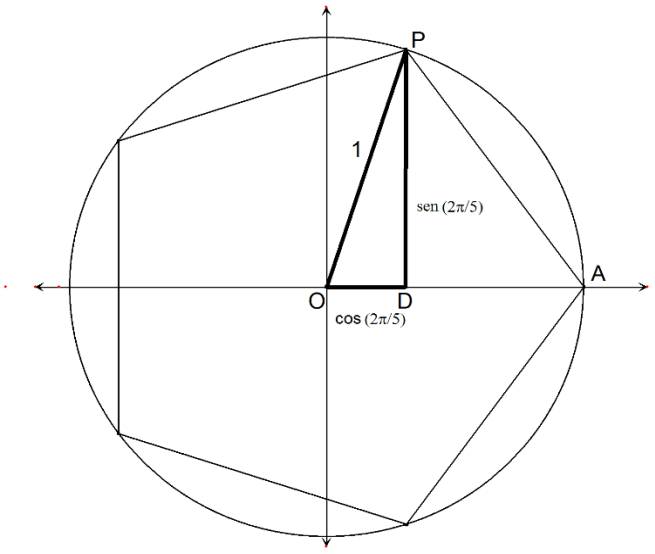



Figura 1.

Ahora se puede ubicar a las coordenadas del vértice P de la forma $(\cos\frac{2\pi}{5}, \text{sen}\frac{2\pi}{5})$. Visto desde la perspectiva de los números complejos se tiene

$$r = \cos\frac{2\pi}{5} + i\text{sen}\frac{2\pi}{5},$$

y como $r^5 = \cos(\frac{5\cdot 2\pi}{5}) + i\text{sen}(\frac{5\cdot 2\pi}{5}) = \cos 2\pi + i\text{sen}2\pi = 1$, entonces se puede decir que $r$ es una raíz del polinomio $r^5 - 1 = 0$.

Por otro lado, como $r^5 - 1 = (r-1)(r^4 + r^3 + r^2 + r + 1) = 0$ y además $r \neq 1$, entonces $r$ es raíz de $r^4 + r^3 + r^2 + r + 1 = 0$. Pero si a partir de esta igualdad se factoriza $r^2$, entonces se tiene que

$$r^2\,(r^2 + r^1 + 1 + r^{-1} + r^{-2}) = 0. \qquad \text{(I)}$$

Nótese que como

$$r = \cos\frac{2\pi}{5} + i\text{sen}\frac{2\pi}{5},$$

entonces,

$$r^{-1} = \cos\frac{2\pi}{5} - i\text{sen}\frac{2\pi}{5},$$

y así la suma de las raíces arroja

$$r + r^{-1} = 2\cos\frac{2\pi}{5},$$

por lo tanto, $$\cos\frac{2\pi}{5} = \frac{r + r^{-1}}{2}. \qquad \text{(II)}$$

Ahora bien, la última igualdad para el coseno es precisamente la distancia OD en la figura. Esto significa que si se puede construir con regla y compás a OD, entonces se podrá trazar también con regla y compás la distancia ortogonal que definirá al punto P, que es el vértice del pentágono.

Retomando el factor de la derecha de la igualdad (I), se tiene que

$$(r^2 + r^1 + 1 + r^{-1} + r^{-2}) = 0 = (r + r^{-1})^2 + (r + r^{-1}) - 1$$

y de (II) ya se sabe que $r + r^{-1} = 2\cos\frac{2\pi}{5}$.

Entonces, si se hace $r + r^{-1} = y$, se tiene que $(r + r^{-1})^2 + (r + r^{-1}) - 1$ toma la forma $y^2 + y - 1 = 0$. Las soluciones de esta ecuación cuadrática son $y = \frac{-1 \pm \sqrt{5}}{2}$. Tomando la raíz positiva $y = \frac{-1+\sqrt{5}}{2}$, y dado que $y = 2\cos\frac{2\pi}{5}$, se tiene que

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

Sin embargo, el coseno de este ángulo es precisamente la distancia OD que se busca, y además el números $\frac{-1+\sqrt{5}}{4}$ sí es construible ya que solo involucra raíces cuadráticas. Ya que se conoce el ángulo en O entonces por la ley de cosenos se puede calcular el segmento entre el punto P y A. Este ángulo es igual a $\sqrt{\frac{5+\sqrt{5}}{2}}$ [Fig. 2], y es uno de los lados del pentágono; pero lo más importante es que este también puede ser construible, pues solo depende de raíces cuadráticas. Ahora, que ya se conoce uno de los lados y que este es una cuerda del círculo unitario, se puede construir todo el pentágono solo con regla y compás.

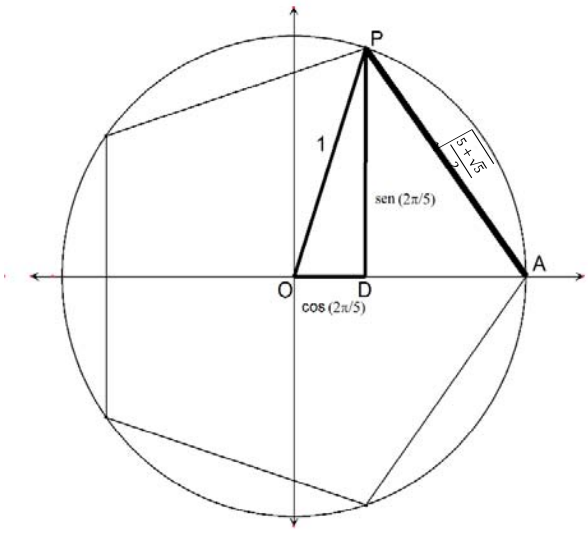



Figura 2.

Si bien este ejemplo del pentágono aclara la idea de lo que es un polígono construible, no muestra cómo se está aplicando el trabajo de los artículos anteriores de Gauss. El siguiente ejemplo es una vía para entender los procedimientos planteados por Gauss.

## Caso del polígono de 17 lados.

Lo que se propone Gauss en este problema es poder construir solo con regla y compás un polígono de 17 lados, y lo hace a través de dividir el círculo en 17 partes. Para esto recurre a la representación compleja de las raíces del polinomio $x^{17} - 1 = 0$, donde los ángulos que subtienden cada lado miden $\left(\frac{2\pi}{17}\right)$. En la figura 3, OD es la base del triángulo ODB, o de manera equivalente $\text{OD} = \cos\left(\frac{2\pi}{17}\right)$, entonces el objetivo es poder expresar con radicales a OD, lo que lleva a que sea construible, y por tanto a que también lo sea DB. De esta manera se obtiene el vértice en B.

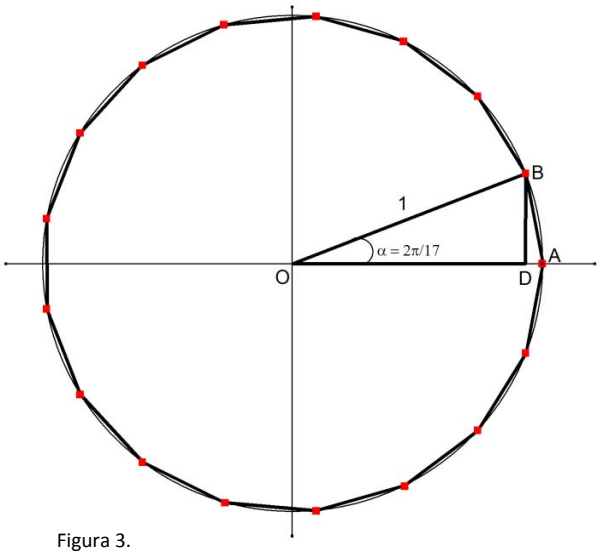


Figura 3.

Recuerde que en el art. 361 se mostró la relación entre las raíces y las funciones trigonométricas, y se llegó, en general, a que $\cos\frac{2\pi}{n} = \cos\frac{2(n-1)\pi}{n}$ representa a la mayor de las partes reales[77] correspondientes a las raíces de $X = x^{n-1} + x^{n-2} + \cdots + x + 1$. Además

[77] Desde el punto de vista geométrico estas partes reales corresponden a los catetos adyacentes de mayor longitud y sobre el eje real positivo, y son los que darán la posibilidad de construir, a la vez, los vértices más cercanos al eje.

de que $\operatorname{sen}\frac{2\pi}{n}$ es positivo y $\operatorname{sen}\frac{2(n-1)\pi}{n}$ es negativo. Particularmente para $n = 17$ se concluyó lo siguiente,

$$r = \cos\frac{2\pi}{17} + i\operatorname{sen}\frac{2\pi}{17}$$
$$r^{16} = \cos\frac{2\pi}{17} - i\operatorname{sen}\frac{2\pi}{17},$$

entonces puesto que el período $(2,1)$ es igual a $r + r^{16}$ se tiene

$$(2,1) = \left[\cos\left(\frac{2\pi}{17}\right) + i\operatorname{sen}\left(\frac{2\pi}{17}\right)\right] + \left[\cos\left(\frac{2\pi}{17}\right) - i\operatorname{sen}\left(\frac{2\pi}{17}\right)\right] = 2\cos\left(\frac{2\pi}{17}\right),$$

así, se tiene que

$$(2,1) = 2\cos\left(\frac{2\pi}{17}\right).$$

Por lo tanto, para hallar $\cos\left(\frac{2\pi}{17}\right)$, primero debemos conocer la expresión con radicales de $(2,1)$. Para ello recordemos que en la parte final del capítulo anterior de este trabajo, se hallaron las raíces de $x^{16} + x^{15} + \cdots + x + 1 = 0$. Estas raíces se obtuvieron mediante la resolución sucesiva de ecuaciones cuadráticas.

Para poder decir que las raíces son construibles se requiere regresar al proceso de cómo se hallaron las raíces mencionadas.

Primero, del total de raíces $r,\ r^2, \ldots, r^{16}$ se crearon dos períodos, que son

$$(8,1) = r + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2 \quad \text{y}$$
$$(8,3) = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6,$$

y al considerarlos raíces de una cuadrática, se llegó a la ecuación

$$x^2 + x - 4 = 0, \qquad \text{(III)}$$

la cual se obtuvo debido a las propiedades de sus coeficientes respecto de sus raíces; a saber, $(8,1) + (8,3) = -1$ y $(8,1)(8,3) = -4$.

Por otro lado, se sabe que las raíces de (III) son $-\frac{1}{2} + \frac{1}{2}\sqrt{17}$ y $-\frac{1}{2} - \frac{1}{2}\sqrt{17}$, y como en el capítulo anterior se toman como sigue

$$(8,1) = -\frac{1}{2} + \frac{1}{2}\sqrt{17} \quad \text{y} \quad (8,3) = -\frac{1}{2} - \frac{1}{2}\sqrt{17}.$$

Ahora, del período $(8,1)$ se tienen los períodos

$$(4,1) = r + r^{13} + r^{16} + r^4 \quad \text{y} \quad (4,9) = r^9 + r^{15} + r^8 + r^2,$$

que se consideran raíces de una cuadrática, y de esta manera se obtiene la ecuación

$$x^2 - \left[-\frac{1}{2} + \frac{1}{2}\sqrt{17}\right]x - 1 = 0,$$ [78]

cuyas raíces son

$$-\frac{1}{4} + \frac{1}{4}\sqrt{17} + \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} \qquad \text{y} \qquad -\frac{1}{4} + \frac{1}{4}\sqrt{17} - \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}}.$$

[78] Recuerde que la suma $(4,1) + (4,9)$ es igual al coeficiente del término lineal de la ecuación cuyas raíces son precisamente $(4,1)$ y $(4,9)$, y que el producto $(4,1)(4,9)$ es igual a término constante. Es así como se obtienen los coeficientes

$$(4,1) + (4,9) = -\frac{1}{2} + \frac{1}{2}\sqrt{17}$$
$$(4,1)(4,9) = -1.$$

Se toma

$$(4,1) = -\frac{1}{4} + \frac{1}{4}\sqrt{17} + \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}},$$

entonces, se tendrá

$$(4,9) = -\frac{1}{4} + \frac{1}{4}\sqrt{17} - \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}}.$$

Luego, por el art. 346, el resto de los períodos de cuatro términos –del período (8,3) se obtienen a su vez dos períodos de cuatro términos que son (4,3) y (4,10)– se pueden obtener mediante la combinación lineal de las potencias de alguno de los períodos ya conocidos y así se tiene que

$$(4,3) = -\frac{1}{4} - \frac{1}{4}\sqrt{17} + \frac{1}{2}\sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}$$

$$(4,10) = -\frac{1}{4} + \frac{1}{4}\sqrt{17} - \frac{1}{2}\sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}.$$

Finalmente, partiendo el período $(4,1)$ en dos subperíodos de dos términos, $(2,1)$ y $(2,13)$, se obtiene la ecuación $x^2 - (4,1)x + (4,3) = 0$, cuyas raíces son precisamente estos períodos de dos términos. Así, al resolver esta ecuación y considerando los valores de $(4,1)$ y $(4,3)$ con radicales, que se muestran arriba, se obtienen las dos raíces también con radicales para $(2,1)$ y $(2,13)$ y en particular

$$(2,1) = -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{4}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} + \frac{1}{2}\sqrt{\frac{17}{4} + \frac{3\sqrt{17}}{4} - \frac{1}{2}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} - \sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}}.$$

Ahora que ya se conoce el valor de $(2,1)$, se puede hallar $\cos\left(\frac{2\pi}{17}\right)$, a partir de la relación $2\cos\left(\frac{2\pi}{17}\right) = (2,1)$, obtenida anteriormente. Entonces, se tiene que

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{8}\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - 2\sqrt{\frac{17}{2} - \frac{\sqrt{17}}{2}} - 4\sqrt{\frac{17}{2} + \frac{\sqrt{17}}{2}}}$$

$$= -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\ .$$

Recordemos que $\cos\left(\frac{2\pi}{17}\right)$ representa la distancia OD, y que si se puede construir este segmento, entonces se puede construir una ortogonal que defina el primer vértice y en consecuencia el primer lado del polígono. Finalmente, se tiene que OPD es construible y así también la perpendicular BD. De esta manera, Gauss muestra que sí se pueden construir los vértices del polígono de 17 lados.[79]

[79] Es importante mencionar que no solo podrían construirse polígonos inscritos en una circunferencia unitaria sino que también de cualquier radio y esto se puede justificar mediante el Teorema de Thales.

## Generalización para cualquier entero.

De las discusiones anteriores (art. 352 y 361), para el caso en el que $n$ es un número primo, el problema de dividir el círculo en $n$ partes se ha trasladado a la solución de tantas ecuaciones *auxiliares* como factores tenga $n-1$, y el grado de cada una de estas ecuaciones a su vez depende del tamaño de los factores. Así, siempre que $n-1$ sea una potencia del número 2, la división del círculo se reduce a resolver ecuaciones cuadráticas únicamente, y las raíces podrán expresarse en términos de raíces cuadradas. Esto último es importante, ya que como se mencionó a principio del capítulo, un punto es construible en el plano si cada una de sus coordenadas –que en este caso son senos y cosenos– se pueden expresar mediante las operaciones suma, resta, multiplicación, división y extracción de raíces cuadradas.

Además, si $\sqrt{a}$ es construible entonces $\sqrt{\sqrt{a}} = \sqrt[4]{a}$ es construible y así mismo $\sqrt{\sqrt{\sqrt{a}}} = \sqrt[8]{a}$. En general $\sqrt[2^k]{a}$ será construible.

Por tanto, para estos casos la división del círculo o la inscripción de un polígono regular de $n$ lados se puede realizar geométricamente.

Cabe mencionar que aunque para ciertos primos $n$, es posible hallar las raíces $n$-ésimas de la unidad en términos de radicales –tal como Gauss mostró en el art. 360 del *Disquisitiones Arithmeticae*–, si los radicales no corresponden a raíces cuadradas entonces no es posible la construcción mediante regla y compás, por ejemplo para $n = 19$ , en las raíces se involucran radicales cúbicos y estos ya no son construibles.

Hasta ahora solo se ha tratado la construcción de polígonos con un número primo de lados pero por lo mencionado en el art. 336, aunado a la descomposición en primos de un entero, se puede generalizar el análisis para cualquier entero $N$, y de esta manera determinar la cantidad de lados que puede tener un polígono para ser construible.

Note que las raíces de $x^4 - 1$ son $\pm 1$ y $\pm i$, las cuales son construibles y en el plano complejo se representan por las coordenadas $(1,0), (-1,0)$, $(0, i)$, $(0, -i)$, que son los vértices de un polígono de cuatro lados inscrito en la circunferencia unitaria. Así, el polígono de $2^2$ lados es construible [Figura 4].

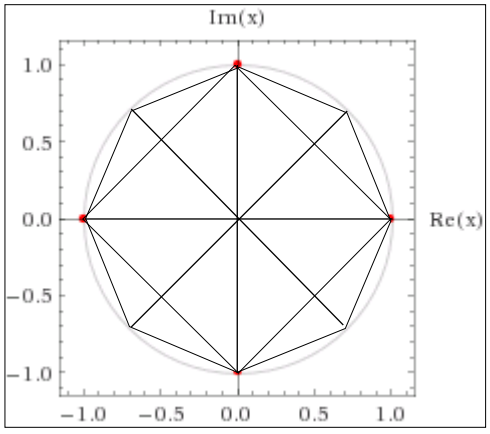



Figura 4.

Además, se sabe que la bisección de un ángulo se puede realizar con regla y compás, y por tanto se tendrán los vértices de un polígono de $2 \cdot 2^2$ lados. Se puede seguir con este proceso de partir en dos los ángulos formados entre dos vértices consecutivos de cada nuevo polígono y de esta manera construir un polígono de $2^{\mu} \cdot 2^2$ lados. Entonces, los polígonos de $2^n$ lados son construibles. Lo anterior se puede aplicar a cualquier polígono construible de $l$ lados, por lo tanto, se puede concluir que si un polígono de $l$ lados es construible, el polígono de $2^n l$ también será construible.

La construcción del polígono de $z$ lados, donde $z$ es un número primo impar es posible si $z$ es de la forma $2^m + 1$ –recordemos que para dividir al círculo en $n$ partes, basta que $n - 1$ sea una potencia de 2–, pero como $z$ es primo resulta que $m$ debe de ser una potencia de 2. Esto porque si $m$ no es potencia de 2 entonces debe tener un factor impar, así $m$ sería de la forma

$$m = t \cdot r \ , \qquad \text{con } t \text{ impar}$$

de donde,

$$2^m + 1 = 2^{t \cdot r} + 1 = (2^r)^t + 1^t,$$

entonces $2^m + 1$ tiene como divisor a $2^r + 1$,[80] y por lo tanto es un número compuesto. Entonces $m$ debe ser una potencia de 2.

Así, se tiene que el polígono con un número primo $z$ de lados será construible si $z$ es de la forma $2^{2^k} + 1$. [81]

[80] Recuerde que si $t$ es un número impar, entonces del teorema del binomio se puede ver que $a + b$ divide a $a^t + b^t$.

[81] Los números de la forma $2^{2^k} + 1$ donde $k$ es un número natural son conocidos como ***números de Fermat*** en honor a Pierre de Fermat, quien fue el primero en estudiar estos números. Al observar que los primeros cinco números de esta forma son primos, Fermat conjeturó que todo entero de la forma $2^{2^k} + 1$ es primo. Sin embargo, esto no es así y fue probado por Leonhard Euler en 1732. Hasta ahora no se sabe si los únicos primos de Fermat son aquellos cinco o si existen infinitos primos de la forma $2^{2^k} + 1$.

Por lo tanto, por lo anterior ya se sabe que es posible construir un polígono de $2z$ lados, y a la vez uno de $2^2z$ lados y así sucesivamente uno de $2^nz$ lados. Con esto se obtiene un conjunto infinito de polígonos construibles, y lo mismo se puede hacer con los otros primos de Fermat.

Ahora veamos el caso de cualquier compuesto $N = ab$, donde $a$ y $b$ representan respectivamente el números de lados de polígonos construibles. Supóngase además que $(a, b) = 1$, entonces por las propiedades del máximo común divisor se tiene que uno es combinación lineal de $a$ y $b$, es decir, existen enteros $x$ y $y$ tales que

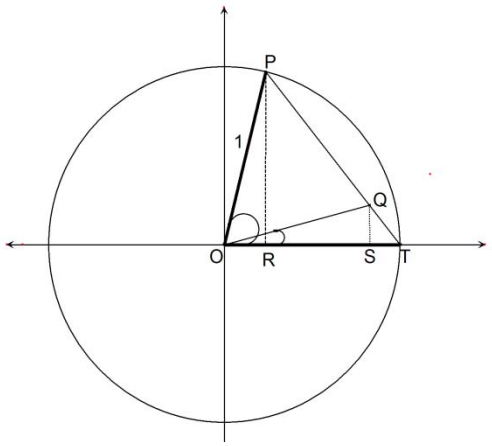
$$ax + by = 1$$

de donde,

$$\frac{1}{ab} = \frac{x}{b} + \frac{y}{a},$$

y así,

$$\frac{2\pi m}{ab} = \frac{2\pi mx}{b} + \frac{2\pi my}{a}.$$




$\Gamma$ = PT = $a$
QT = $b$
$\angle POT = \frac{2\pi}{a}$
$\angle QOS = \frac{2\pi}{a}$
OR = $\cos\left(\frac{2\pi}{a}\right)$
PR = $\operatorname{sen}\left(\frac{2\pi}{a}\right)$
OS = $\cos\left(\frac{2\pi}{ab}\right)$
SQ = $\operatorname{sen}\left(\frac{2\pi}{ab}\right)$

Figura 5.

Entonces, el ángulo correspondiente al polígono de $N = a \cdot b$ lados se puede expresar en términos de múltiplos de los ángulos correspondientes a los polígonos construibles de $a$ y $b$ lados respectivamente. Con base en lo anterior se pueden hallar el seno y el coseno del ángulo $\left(\frac{2\pi}{ab}\right)$ correspondiente al polígono de $N$ lados, a partir de que se conocen el seno y el coseno de los ángulos $\frac{2\pi m}{a}$ y $\frac{2\pi m}{b}$ correspondientes a los polígonos de $a$ y $b$ lados, respectivamente Lo más importante es que $\frac{2\pi m}{a}$ y $\frac{2\pi m}{b}$ son construibles. Así,

como $\cos(\frac{2\pi m}{ab})$ y $\text{sen}(\frac{2\pi m}{ab})$ son construibles, es decir, se pueden expresar por radicales, entonces es posible hallar la cuerda $\Gamma$ mediante la ley de cosenos y verificar que esta también es construible:

$$\Gamma^2 = 1^2 + 1^2 - 2\cos(\frac{2\pi m}{ab}).$$

También se puede visualizar de la siguiente manera. Puesto que en el plano complejo las coordenadas $\left(\cos\left(\frac{2\pi m}{ab}\right), \text{sen}\left(\frac{2\pi m}{ab}\right)\right)$ con $0 \leq m \leq ab - 1$ representan los vértices del polígono de $N = a \cdot b$ lados, entonces para ver que este es construible, basta con mostrar que los puntos $\left(\cos\left(\frac{2\pi m}{ab}\right), \text{sen}\left(\frac{2\pi m}{ab}\right)\right)$ son construibles. Lo señalado es posible si $\cos(\frac{2\pi m}{ab})$ y $\text{sen}(\frac{2\pi m}{ab})$ son construibles. Así al ser construibles los puntos $\left(\cos\left(\frac{2\pi m}{ab}\right), \text{sen}\left(\frac{2\pi m}{ab}\right)\right)$ con $0 \leq m \leq ab - 1$, es posible trazar las rectas que los unen y de esta manera el polígono de $N$ lados es construible.

Con lo anterior se muestra la forma en la que se pueden construir polígonos cuyo número de lados se representa como un producto de dos factores donde cada uno a la vez representa la cantidad de lados de un polígono también construible. A continuación se generaliza este resultado al caso donde $N$ se puede expresar como producto de más factores que tienen las mismas características que el caso anterior.

Así, sea $N = a \cdot b \cdot c \ldots$, donde $a, b, c, \ldots$ son el número de lados de polígonos construibles respectivamente y además primos relativos entre sí. Por el lema mencionado en el art. 336 se sabe que el ángulo $\frac{2\pi q}{N}$ se puede expresar como

$$\frac{2\pi\alpha}{a} + \frac{2\pi\beta}{b} + \frac{2\pi\gamma}{c} + \cdots.$$

De esta manera, puesto que el seno y el coseno de $\frac{2\pi q}{N}$ correspondiente al polígono de $N$ lados se pueden obtener a partir de los ya conocidos senos y cosenos de los ángulos $\frac{2\pi\alpha}{a}$, $\frac{2\pi\beta}{b}$, $\frac{2\pi\gamma}{c}$ ..., entonces es posible la construcción de los vértices y por tanto los lados del polígono de $N$ lados.

Entonces, si $N$ es un primo de la forma $2^{2^k} + 1$ –primo de Fermat– se tiene que $(2^n, N) = 1$ y así es posible la construcción de polígonos de $2^n \cdot (2^{2^k} + 1)$ lados. También es posible la construcción de productos de distintos primos de Fermat. No se incluyen las potencias ya que es importante que los factores sean primos relativos.

En conclusión, si $N$ es una potencia de 2, o un primo de la forma $2^{2^k} + 1$, o un producto de primos distintos de esta forma, o un producto de primos distintos de esta forma por una potencia de 2. Es decir, si los factores primos de $N$ son de la forma $2^{2^k} + 1$

y $N$ no incluye potencias de primos de esta forma entonces el polígono de $N$ lados es construible.

Los siguientes son algunos valores de $N$ para los que el polígono de $N$ lados es construible:

$$3 = 2^{2^0} + 1$$
$$4 = 2^2$$
$$5 = 2^{2^1} + 1$$
$$6 = 2(2^{2^0} + 1)$$
$$8 = 2^3$$
$$10 = 2(2^{2^1} + 1)$$
$$12 = 2^2(2^{2^0} + 1)$$
$$15 = (2^{2^0} + 1)(2^{2^1} + 1)$$
$$17 = 2^{2^2} + 1$$
$$256 = 2^{2^3} + 1$$
$$65537 = 2^{2^4} + 1.$$

El polígono de 7 lados no es construible debido que su único factor primo impar, qu es él mismo, debería ser de la forma $2^{2^k} + 1$ y no lo es. Además, al tratar de hallar las raíces séptimas de la unidad por el método de Gauss, se tendría que resolver al menos una ecuación de grado 3 y una de grado 2 y entonces las raíces quedarían expresadas en términos de raíces cuadradas y cúbicas, pero estas últimas no son construibles.

En sus *Disquisitiones Arithmeticae* Gauss menciona los valores de $N < 300$ para los que el polígono de $N$ lados es construible:

$$2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80,$$
$$85, 96, 102, 120,128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.$$

Como se puede apreciar hasta ahora, solo se han dado las condiciones suficientes para la construcción de un polígono pero resulta que estas condiciones también son necesarias. Sin embargo, en sus *Disquisitiones* Gauss no mostró de manera rigurosa este último hecho, su razonamiento se basó en que las raíces cuadradas son los únicos radicales construibles, o equivalentemente que todo número construible se puede expresar en término de raíces cuadradas. Pero esto último no fue probado sino hasta 1837 por Pierre Wantzel.

# Conclusión

El objetivo de esta tesis era hacer un estudio de la sección VII del *Disquisitiones Arithmeticae* de Gauss, particularmente los resultados relacionados con la constructibilidad de polígonos regulares con regla y compás. Después de estudiar la sección VII se concluyó que una vía para hacer el análisis era la de partir el contenido en la forma siguiente:

I. Mostrar la irreductibilidad del polinomio ciclotómico.
II. Dar a conocer la teoría que desarrolló y que ahora se conoce como *períodos gaussianos*, que a la vez estos proporcionan ecuaciones auxiliares para encontrar soluciones por radicales de las raíces de la ecuación $x^n - 1 = 0$.
III. Trasladar la teoría del punto anterior a la división del círculo y mostrar la conexión con la construcción de polígonos regulares.

Ahora se puede decir que en esta ruta de estudio, los *periodos gaussianos* son la parte más creativa de Gauss, creemos que es donde más aporta a la teoría de ecuaciones ciclotómicas. Es importante notar que desarrolla ampliamente la teoría de periodos, y actualmente no es fácil encontrar el fundamento de esto, generalmente lo mencionan y lo usan pero no exponen como se gesta la teoría, por esto se piensa que sí es importante leer a Gauss directamente en sus *Disquisitiones*.

Se espera que con este trabajo se haya logrado construir una vía para poder adentrarse directamente a la obra original de Gauss, en particular el capítulo VII.

La lectura de las *Disquisitiones* no fue fácil, sin embargo, ha sido una aventura adentrarse al trabajo de uno de los matemáticos más importantes de la historia. Los trabajos de Gauss siguen dando lugar a futuras investigaciones. Un proyecto interesante también sería completar el análisis del trabajo de Gauss acerca de la construcción de polígonos y realizado por Pierre Wantzel.

# BIBLIOGRAFIA


Bühler, W. K. (1981). *Gauss A biographical Study,* Springer-Verlag, New York.

Dickson, L.E. (1919). *History of the theory of numbers,* Vol. I: Divisibility and primality, Carnegie Institution of Washington.

Dickson, L.E. (1920). *History of the theory of numbers,* Vol. II: Diophantine Analysis, Carnegie Institution of Washington.

Dunnington, G. W. (2004). *Carl Friedrich Gauss Titan of Science,* The Mathematical Association of America, New York.

Euclides (1994). Elementos, Libros V-IX. Traducción de María Luisa Puertas Castaños, Editorial Grados.

Gauss, Carl Friedrich (1995) [1801] (versión en español). *Disquisitiones arithmeticae*, traducido por Hugo Barrantes, Michael Joseph y Ángel Ruiz, San José, Costa Rica: Centro de Investigaciones Matemáticas y Meta-Matemáticas (CIMM), Universidad de Costa Rica.

Gauss, Carl Friedrich (1986) [1801] (versión en inglés). *Disquisitiones arithmeticae*, traducido por Arthur A. Clarke, Springer-Verlag.

Goldstein, C., Schappacher, N. y Schwerme, J. (2007). *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, Springer.

Göksel Agargün, A. y Özkan, E. Mehmet (2001). "A Historical Survey of the Fundamental Theorem of Arithmetic" en *Historia Mathematica* vol. 28 (2001), pp. 207-214, Department of Mathematics, Yıldız Technical University, Davutpaşa Yerleşim Birimi, 34210 Esenler, İstanbul, Turkey.

Ivorra Castillo, Carlos. Universidad de Valencia. *Teoría de números.*
<http://www.uv.es/ivorra/Libros/Numeros.pdf>.

Lang, S. (1987). *Introduction to Linear Algebra, Springer-Verlag.*

Lemmermeyer, Franz (2000). *Reciprocity Laws: From Euler to Eisenstein*, Springer.

Ore, Øystein *(1*948). *Number Theory and Its History,* Edit. Dover.

Pérez Sanz, A. (2008). "Gauss y el polígono regular de 17 lados" en *Revista Suma,* edición 58, pp. 101-105.

Pardo Rego, V. (2003). *Lagrange. La elegancia matemática,* Nivola Libros y Ediciones, S.L.

Sandifer, Charles (2007). *The early mathematics of Leonhard Euler*, The Mathematical Association of America.

Tignol, Jean-Pierre (2002). *Galois Theory of Algebraic Equations*, World Scientific Publishing Co. Pte. Ltd.

Wantzel, Pierre (1837). Recherche sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas. *Journal de Mathématiques Pures et Appliquées.* [Paris], pp. 366-372.