Sección Sétima

ECUACIONES QUE DEFINEN SECCIONES DE UN CIRCULO.

335.

Dentro de los espléndidos desarrollos, contribución de los matemáticos modernos, la teoría de las funciones circulares sin duda ocupa uno de los lugares más importantes. A menudo tenemos ocasión, en una variedad de contextos, de referirnos a este notable tipo de cantidad, y no hay parte de la matemática general que no dependa de ella en alguna forma. Ya que los más brillantes matemáticos modernos por su industria y sagacidad la han erigido en una extensiva disciplina, se esperaría firmemente que cualquier parte de la teoría, por no hablar de una parte elemental, debería haber sido significativamente desarrollada. Me refiero a la teoría de funciones trigonométricas correspondientes a arcos que son conmesurables con la circunferencia, i.e., la teoría de polígonos regulares. Solamente una pequeña parte de esta teoría ha sido desarrollada hasta ahora, como la siguiente sección aclarará. Los lectores podrían sorprenderse de encontrar una discusión de este tema en el presente trabajo, el cual trata con una disciplina aparentemente tan diferente; pero el tratamiento mismo hará abundantemente claro que hay una conexión íntima entre este tema y la Aritmética Superior.

Los principios de la teoría que vamos a explicar de hecho se extienden mucho más allá de lo que indicaremos. Por ello, pueden ser aplicados no solamente a funciones circulares sino también a otras funciones trascedentales, e.g., a aquéllas que dependen de la integral $\int \frac{dx}{\sqrt{1-x^4}}$ y también a varios tipos de congruencias. Ya que, sin embargo, estamos preparando un gran trabajo sobre esas funciones trascendentales

y puesto que trataremos congruencias extensamente en la continuación de estas *Disquisitiones*, hemos decidido considerar aquí solamente funciones circulares. Y aún cuando es posible discutirlas en toda su generalidad, la reduciremos al caso más simple en el artículo siguiente, tanto por motivos de brevedad como porque los nuevos principios de esta teoría puedan ser más fácilmente comprendidos.

La discusión se reduce al caso más simple, donde el número de partes en las cuales se corta el círculo es un número primo.

336.

Designando la circunferencia del círculo o cuatro ángulos rectos por P y suponiendo que m y n son enteros y n un producto de los factores relativamente primos a, b, c, etc., el ángulo $A = \frac{mP}{n}$ puede ser reducido por los métodos del artículo 310 a la forma $A = (\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{ etc.})P$, y las funciones trigonométricas correspondientes a él pueden ser encontradas por métodos conocidos a partir de los de las partes $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$, etc. De esta forma, ya que se pueden tomar a, b, c, etc. como números primos o potencias de números primos, es suficiente considerar la división del círculo en partes cuyo número es un primo o una potencia de un primo y se obtendrá inmediatamente un polígono de n lados a partir de los polígonos de a, b, c, etc. lados. Sin embargo, restringiremos nuestra discusión al caso en que el círculo es dividido en un número primo (impar) de partes, especialmente por la siguiente razón. Es claro que las funciones circulares correspondientes al ángulo $\frac{mP}{p^2}$ son deducidas de las funciones pertenecientes a $\frac{mP}{p}$ mediante la solución de una ecuación de grado p. Y de éste, por una ecuación del mismo grado podemos derivar las funciones correspondientes a $\frac{mP}{p^3}$ etc. De esta forma, si ya se tiene un polígono de p lados, para determinar un polígono de p^λ lados necesariamente se requerirá la solución de $\lambda - 1$ ecuaciones de grado p. Aún cuando la siguiente teoría puede ser extendida también a este caso, no obstante no podremos evitar tantas ecuaciones de grado p, y no existe manera de reducir su grado si p es primo. Así, e.g., se mostrará abajo que un polígono de 17 lados puede ser contruido geométricamente; pero para obtener un polígono de 289 lados no hay manera de eludir el resolver una ecuación de grado 17.

Ecuaciones para funciones trigonométricas de arcos que son una parte o partes de la circunferencia completa,
reducción de las funciones trigonométricas a las raíces de la ecuación $x^n - 1 = 0$.

337.

Es bien conocido que las funciones trigonométricas de todos los ángulos $\frac{kP}{n}$ donde la k denota en general todos los números 0, 1, 2, ... $n-1$, son expresadas por las raíces de ecuaciones de grado n. Los *senos* son las raíces de la ecuación (I):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{ etc.} \pm \frac{1}{2^{n-1}}nx = 0$$

los *cosenos* son las raíces de la ecuación (II):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0$$

y las *tangentes* son las raíces de la ecuación (III):

$$x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{n-4} - \text{ etc. } \pm nx = 0$$

Estas ecuaciones (que son todas verdaderas para cualquier valor impar de n, y la ecuación II es cierta también para cualquier valor par), poniendo $n = 2m+1$, pueden ser fácilmente reducidas a grado m. Para I y III esto justamente requiere dividir a la izquierda por x y sustituir x^2 por y. De todas formas la ecuación II incluye la raíz $x = 1$ $(= \cos 0)$ y todas las otras son iguales en pares ($\cos\frac{P}{n} = \cos\frac{(n-1)P}{n}$, $\cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$, etc.); así el lado izquierdo es divisible por $x-1$ y el cociente será un cuadrado. Si extraemos la raíz cuadrada, la ecuación II se reduce a la siguiente:

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3} + \frac{1}{16}\frac{(m-2)(m-3)}{1\cdot 2}x^{m-4} + \frac{1}{32}\frac{(m-3)(m-4)}{1\cdot 2}x^{m-5} - \text{ etc.} = 0$$

Sus raíces serán los cosenos de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, ... $\frac{mP}{n}$. Hasta ahora no se ha hecho ninguna reducción más allá de estas ecuaciones para el caso en que n es un número primo.

No obstante, ninguna de estas ecuaciones es tan tratable y tan conveniente para nuestros propósitos como $x^n - 1 = 0$. Sus raíces están íntimamente relacionadas

con las raíces de las anteriores. Esto es, escribiendo por brevedad i para la cantidad imaginaria $\sqrt{-1}$, las raíces de la ecuación $x^n - 1 = 0$ serán

$$\cos\frac{kP}{n} + i\,\mathrm{sen}\,\frac{kP}{n} = r$$

donde para k se debe tomar todos los números 0, 1, 2, $\ldots n-1$. De esta forma, ya que $\frac{1}{r} = \cos\frac{kP}{n} - i\,\mathrm{sen}\,\frac{kP}{n}$, las raíces de la ecuación I serán $\frac{1}{2i}(r - \frac{1}{r})$ o $i\frac{1-r^2}{2r}$; las raíces de la ecuación II, $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+r^2}{2r}$; finalmente las raíces de la ecuación III, $\frac{i(1-r^2)}{1+r^2}$. Por esta razón construiremos nuestra investigación sobre una consideración de la ecuación $x^n - 1 = 0$, asumiendo que n es un número primo impar. Con el fin de no interrumpir el orden de la investigación, consideraremos primero el siguiente lema.

338.

PROBLEMA. *Dada la ecuación*

$$(W)\ldots z^m + Az^{m-1} + \text{ etc.} = 0$$

encontrar la ecuación (W') *cuyas raíces son las* λ*-ésimas potencias de las raíces de la ecuación* (W)*, donde* λ *es un exponente entero positivo dado.*

Solución. Si designamos las raíces de la ecuación W por a, b, c, etc., las raíces de la ecuación W' serán a^λ, b^λ, c^λ, etc. Por un teorema de Newton muy conocido, de los coeficientes de la ecuación W se puede encontrar la suma de cualquier potencia de las raíces a, b, c, etc. Por consiguiente, se buscan las sumas

$$a^\lambda + b^\lambda + c^\lambda + \text{ etc.}, \quad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} + \text{ etc. etc.} \quad \text{hasta} \quad a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{ etc.}$$

y por un procedimiento inverso, de acuerdo con el mismo teorema, pueden ser deducidos los coeficientes de la ecuación W', *Q. E. F.* Al mismo tiempo, es claro que si todos los coeficientes de W son racionales, todos los de W' también lo serán. Por otro método se puede probar que si todos los primeros son enteros, los últimos también serán enteros. No gastaremos más tiempo sobre este teorema aquí, puesto que no es necesario para nuestro propósito.

339.

La ecuación $x^n - 1 = 0$ (siempre con la suposición que n es un número primo impar) tiene solamente una raíz real, $x = 1$; las restantes $n-1$ raíces que están dadas por la ecuación

$$x^{n-1} + x^{n-2} + \text{ etc.} + x + 1 = 0$$

son todas imaginarias ; denotaremos su conjunto por Ω y la función

$$x^{n-1} + x^{n-2} + \text{ etc.} + x + 1 \quad \text{por} \quad X$$

Si por consiguiente r es cualquier raíz en Ω, resulta $1 = r^n = r^{2n}$ etc. y en general $r^{en} = 1$ para cualquier valor entero positivo o negativo de e. Así, si λ y μ son enteros congruentes según n, tendremos $r^\lambda = r^\mu$. Pero si λ y μ son no congruentes según n, entonces r^λ y r^μ serán diferentes, pues en este caso se puede encontrar un entero ν tal que $(\lambda - \mu)\nu \equiv 1 \pmod{n}$, así $r^{(\lambda-\mu)\nu} = r$ y ciertamente $r^{\lambda-\mu}$ no es $= 1$. Es claro que cualquier potencia de r es también una raíz de la ecuación $x^n - 1 = 0$. Por lo tanto, ya que las cantidades $1(= r^0)$, r, r^2, $\ldots r^{n-1}$ son todas diferentes, ellas nos darán todas las raíces de la ecuación $x^n - 1 = 0$ y así los números r, r^2, r^3, $\ldots r^{n-1}$ coincidirán con Ω. Más generalmente, entonces, Ω coincidirá con r^e, r^{2e}, r^{3e}, $\ldots r^{(n-1)e}$, si e es cualquier entero positivo o negativo no divisible por n. Tenemos por lo tanto

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e})$$

y de esto

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

y

$$1 + r^e + r^{2e} + \ldots + r^{(n-1)e} = 0$$

Si tenemos dos raíces como r y $\frac{1}{r}$ $(= r^{n-1})$ o en general r^e y r^{-e}, las llamaremos raíces *recíprocas*. Evidentemente el producto de dos factores simples $x - r$ y $x - \frac{1}{r}$ es real y es $= x^2 - 2x\cos\omega + 1$, donde el ángulo ω es igual al ángulo $\frac{P}{n}$ o a algún múltiplo de él.

340.

Por eso, representando una raíz en Ω por r, todas las raíces de la ecuación $x^n - 1 = 0$ se expresan mediante potencias de r y el producto de varias raíces de esta

ecuación puede ser expresado por r^λ de manera que λ es 0 o positivo y $< n$. Por lo tanto, si $\varphi(t, u, v, \ldots)$ designa una función algebraica racional entera de las incógnitas t, u, v, etc., que es una suma de términos de la forma $ht^\alpha u^\beta v^\gamma \ldots$, evidentemente si sustituimos t, u, v, etc. por las raíces de la ecuación $x^n - 1 = 0$, digamos $t = a$, $u = b$, $v = c$, etc., entonces $\varphi(a, b, c, \ldots)$ puede ser reducido a la forma

$$A + A'r + A''r^2 + A'''r^3 + \cdots + A^v r^{n-1}$$

de tal manera que los coeficientes A, A', etc. (algunos de ellos pueden no aparecer y por lo tanto son $= 0$) son cantidades determinadas. Y todos estos coeficientes serán enteros si todos los coeficientes en $\varphi(t, u, v, \ldots)$, i.e., todos los h, son enteros. Si después de esto sustituimos t, u, v ..., por a^2, b^2, c^2, ..., respectivamente, cada término $ht^\alpha u^\beta v^\gamma \ldots$ que ha sido reducido a r^σ se hace ahora $r^{2\sigma}$ y así:

$$\varphi(a^2, b^2, c^2, \ldots) = A + A'r^2 + A''r^4 + A'''r^6 + \cdots + A^v r^{2n-2}$$

y en general para cualquier valor entero de λ,

$$\varphi(a^\lambda, b^\lambda, c^\lambda, \ldots) = A + A'r^\lambda + A''r^{2\lambda} + \cdots + A^v r^{(n-1)\lambda}$$

Esta proposición es muy importante y es fundamental para la discusión siguiente. También se sigue de ello que

$$\varphi(1, 1, 1, \ldots) = \varphi(a^n, b^n, c^n, \ldots) = A + A' + A'' + \cdots + A^v$$

y

$$\varphi(a, b, c, \ldots) + \varphi(a^2, b^2, c^2, \ldots) + \varphi(a^3, b^3, c^3, \ldots) + \ldots + \varphi(a^n, b^n, c^n, \ldots) = nA$$

De aquí, esta suma es entera y divisible por n cuando todos los coeficientes en $\varphi(t, u, v, \ldots)$ son enteros.

Teoria de las raíces de la ecuación $x^n - 1 = 0$ (donde n es primo).
Omitiendo la raíz 1, las restantes (Ω) están en $X = x^{n-1} + x^{n-2} +$ etc. $+x + 1 = 0$.
La funcion X no se puede descomponer en factores con coeficientes racionales.

341.

TEOREMA. *Si la función X es divisible por la función de grado más pequeño*

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

los coeficientes A, B, ... L no pueden ser todos racionales.

Demostración. Sea $X = PQ$ y $\mathfrak{P}$ el conjunto de las raíces de la ecuación $P = 0$, $\mathfrak{Q}$ el conjunto de las raíces de la ecuación $Q = 0$, así que Ω consiste de $\mathfrak{P}$ y $\mathfrak{Q}$ tomados juntos. Además, sea $\mathfrak{R}$ el conjunto de raíces recíprocas de $\mathfrak{P}$, $\mathfrak{S}$ el conjunto de raíces recíprocas de $\mathfrak{Q}$ y sean las raíces que están contenidas en $\mathfrak{R}$, raíces de la ecuación $R = 0$ (esto se convierte en $x^\lambda + \frac{K}{L}x^{\lambda-1} +$ etc. $+ \frac{A}{L}x + \frac{1}{L} = 0$) y sean aquéllas que están contenidas en $\mathfrak{S}$, raíces de la ecuación $S = 0$. Evidentemente si tomamos las raíces $\mathfrak{R}$ y $\mathfrak{S}$ juntas obtenemos el conjunto Ω y $RS = X$. Ahora, distinguimos cuatro casos.

I. Cuando $\mathfrak{P}$ coincide con $\mathfrak{R}$ y consecuentemente $P = R$. En este caso obviamente pares de raíces en $\mathfrak{P}$ serán siempre recíprocas y así P será el producto de $\frac{1}{2}\lambda$ factores dobles de la forma $x^2 - 2x\cos\omega + 1$. Como este factor $= (x - \cos\omega)^2 + \operatorname{sen}\omega^2$, es claro que para cualquier valor real de x, P tiene necesariamente un valor real positivo. Sean $P' = 0$, $P'' = 0$, $P''' = 0$, $\ldots P^\nu = 0$ las ecuaciones cuyas raíces son las potencias cuadradas, cúbicas, cuartas, $\ldots (n-1)$-ésimas de las raíces de $\mathfrak{P}$ respectivamente, y sean p, p', p'', $\ldots p^\nu$ los valores de las funciones P, P', P'', $\ldots P^\nu$, respectivamente, que se obtienen al hacer $x = 1$. Entonces, por lo que se dijo antes, p será una cantidad positiva, y por una razón similar también serán positivos p', p'', etc. Ya que, por consiguiente, p es el valor de la función $(1-t)(1-u)(1-v)$ etc., que es obtenida sustituyendo t, u, v, etc. por las raíces contenidas en $\mathfrak{P}$; p' es el valor de la misma función obtenida al sustituir t, u, v, etc., por los cuadrados de esas raíces; y 0 es su valor cuando $t = 1$, $u = 1$, $v = 1$, etc.: la suma $p + p' + p'' \cdots + p^\nu$ será un entero divisible por n. Además es fácil ver que el producto $PP'P'' \ldots$ será $= X^\lambda$ y así $pp'p'' \ldots = n^\lambda$.

Ahora, si todos los coeficientes en P fueran racionales, todos aquéllos en P', P'', etc. también lo serían, por el artículo 338. Sin embargo, por el artículo 42, todos esos coeficientes tendrían que ser enteros. Así p, p', p'', etc. también deberán ser enteros; como su producto es n^λ y su número es $n - 1 > \lambda$, algunos de ellos (al menos $n - 1 - \lambda$) deben ser $= 1$, y los otros iguales a n o a una potencia de n. Y si g de ellos son $= 1$, la suma $p + p' +$ etc. será $\equiv g \pmod{n}$ y así, de seguro, no divisible por n. Así, nuestra suposición es inconsistente.

II. Cuando $\mathfrak{P}$ y $\mathfrak{R}$ no coinciden pero contienen algunas raíces comunes, sea $\mathfrak{T}$ este conjunto y $T = 0$, la ecuación de la cual ellos son las raíces. Entonces T será el máximo común divisor de las funciones P y R (como es claro de la teoría de las ecuaciones). Sin embargo, pares de raíces en $\mathfrak{T}$ serán recíprocas y como fue demostrado antes, no todos los coeficientes en T pueden ser racionales. Pero esto de seguro sucedería si todos los de P, y así también los de R, fueran racionales, como

resulta de la naturaleza de la operación por medio de la cual encontramos el máximo común divisor. Así, nuestra suposición es absurda.

III. Cuando $\mathfrak{Q}$ y $\mathfrak{S}$ coinciden o tienen raíces comunes, se prueba, exactamente de la misma forma, que no todos los coeficientes de Q son racionales; pero ellos serían racionales si todos los de P fueran racionales, y esto es imposible.

IV. Si $\mathfrak{P}$ no tiene raíces en común con $\mathfrak{R}$ y $\mathfrak{Q}$ ninguna en común con $\mathfrak{S}$, todas las raíces $\mathfrak{P}$ deberían encontrarse necesariamente en $\mathfrak{S}$, y todas las raíces $\mathfrak{Q}$ en $\mathfrak{R}$. Por lo tanto $P = S$ y $Q = R$, y así $X = PQ$ será el producto de P por R; i.e.,

$$\text{de} \qquad x^\lambda + Ax^{\lambda-1} \cdots + Kx + L \qquad \text{por} \qquad x^\lambda + \frac{K}{L}x^{\lambda-1} \cdots + \frac{A}{L}x + \frac{1}{L}$$

Así, haciendo $x = 1$, resulta

$$nL = (1 + A \ldots + K + L)^2$$

Ahora, si todos los coeficientes en P fueran racionales, y así por el artículo 42 también enteros, L, el cual debe dividir al último coeficiente en X, i.e., la unidad, será necesariamente $= \pm 1$ y así $\pm n$ sería un cuadrado. Pero ya que esto es contrario a la hipótesis, la suposición es inconsistente.

Entonces, por este teorema es claro que no importa como se factorice X, algunos de los coeficientes, al menos, serán irracionales, y así, no se pueden determinar excepto mediante una ecuación de grado mayor que la unidad.

Declaración del propósito de las investigaciones siguientes.

342.

No será inútil declarar en pocas palabras el propósito de las investigaciones siguientes. Es resolver *gradualmente* la X en más y más factores, de manera que sus coeficientes sean determinados por ecuaciones de un orden tan pequeño como sea posible, hasta llegar finalmente a factores simples o sea a las raíces Ω. Probaremos que si el número $n - 1$ es resuelto de alguna manera en factores enteros α, β, γ, etc. (se puede asumir cada uno de ellos primo), X se puede resolver en α factores de grado $\frac{n-1}{\alpha}$ con coeficientes determinados por una ecuación de grado α; cada uno de éstos será resuelto en otros β de grado $\frac{n-1}{\alpha\beta}$ con la ayuda de una ecuación de grado β etc. Así, si ν designa el número de factores α, β, γ, etc., la determinación de las raíces Ω se reduce a la solución de ν ecuaciones de grados α, β, γ, etc. Por ejemplo, para

$n = 17$, donde $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, habrá que resolver cuatro ecuaciones cuadráticas; para $n = 73$, tres ecuaciones cuadráticas y dos cúbicas.

En lo que sigue a menudo hay que considerar potencias de la raíz r cuyos exponentes son también potencias: expresiones de esta clase son muy difíciles de imprimir. Por lo tanto, para facilitar la tipografía utilizaremos la siguiente abreviación. Para r, r^2, r^3, etc. escribiremos [1], [2], [3], etc. y en general para r^λ, donde λ es cualquier entero, escribiremos $[\lambda]$. Tales expresiones no están completamente determinadas, pero lo estarán tan pronto como tomemos una raíz específica de Ω para r o sea para [1]. En general $[\lambda]$ y $[\mu]$ serán iguales o diferentes de acuerdo con que λ y μ sean congruentes o no congruentes según el módulo n. Además $[0] = 1$; $[\lambda] \cdot [\mu] = [\lambda + \mu]$; $[\lambda]^v = [\lambda v]$; la suma $[0] + [\lambda] + [2\lambda] \ldots + [(n-1)\lambda]$ es 0 o n de acuerdo con que λ sea no divisible o divisible por n.

Todas las raíces de Ω se distribuyen en ciertas clases (períodos).

343.

Si, para el módulo n, g es ese tipo de número que en la sección III llamamos una raíz primitiva, los $n-1$ números 1, g, g^2, $\ldots g^{n-2}$ serán congruentes a los números 1, 2, 3, $\ldots n-1$ según el módulo n. El orden será diferente, pero todo número en una serie será congruente a alguno en la otra. De esto se sigue inmediatamente que las raíces [1], [g], [g^2], $\ldots$ [g^{n-2}] coinciden con Ω. Por un argumento similar las raíces

$$[\lambda],\ [\lambda g],\ [\lambda g^2],\ \ldots\ [\lambda g^{n-2}]$$

coincidirán con Ω cuando λ es cualquier entero no divisible por n. Además, ya que $g^{n-1} \equiv 1 \pmod{n}$, es fácil ver que las dos raíces $[\lambda g^\mu]$ y $[\lambda g^\nu]$ serán identicas o diferentes de acuerdo con que μ y ν sean congruentes o no congruentes según $n - 1$.

Si por lo tanto G es otra raíz primitiva, las raíces [1], [g], $\ldots$ [g^{n-2}] también coincidirán con [1], [G], $\ldots$ [G^{n-2}], exceptuando el orden. Además, si e es un divisor de $n - 1$, y se pone $n - 1 = ef$, $g^e = h$, $G^e = H$, entonces los f números 1, h, h^2, $\ldots h^{f-1}$ serán congruentes a 1, H, H^2, $\ldots H^{f-1}$ según n (sin considerar el orden). Supongamos que $G \equiv g^\omega \pmod{n}$, que μ es un número positivo arbitrario $< f$ y que ν es el residuo más pequeño de $\mu\omega \pmod{f}$. Entonces resultará $\nu e \equiv \mu\omega e \pmod{n-1}$ y así $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$ o $H^\mu \equiv h^\nu$; i.e., cualquier número en la segunda serie 1, H, H^2, etc. será congruente a un número en la serie 1, h, h^2, $\ldots$

y viceversa. Así, las f raíces [1], [h], [h^2], ... [h^{f-1}] serán idénticas con [1], [H], [H^2], ... [H^{f-1}]. De la misma manera, es fácil ver que las series más generales

$$[\lambda], [\lambda h], [\lambda h^2], \ldots [\lambda h^{f-1}] \quad \text{y} \quad [\lambda], [\lambda H], [\lambda H^2], \ldots [\lambda H^{f-1}]$$

coinciden. Designaremos la *suma* de tales f raíces, $[\lambda] + [\lambda h] +$ etc. $+ [\lambda h^{f-1}]$ por (f, λ). Puesto que ella no cambia al tomar una raíz primitiva diferente g, debe ser considerada como independiente de g. Llamaremos al *conjunto* de las mismas raíces el *período* (f, λ) y olvidaremos el orden de las raíces *). Para exhibir un tal período será conveniente reducir cada raíz a su expresión más simple, esto es, sustituir los números λ, λh, λh^2, etc. por sus residuos más pequeños según el módulo n. Se podrían ordenar los términos de acuerdo con los tamaños de estos residuos.

Por ejemplo, para $n = 19$, 2 es una raíz primitiva y su período (6,1) consiste de las raíces [1], [8], [64], [512], [4096] y [32768] o sea [1], [7], [8], [11], [12] y [18]. Similarmente, el período (6,2) consiste de las raíces [2], [3], [5], [14], [16] y [17]. El período (6,3) es idéntico con el precedente. El período (6,4) contiene las raíces [4], [6], [9], [10], [13] y [15].

Varios teoremas concernientes a estos períodos.

344.

Se ofrecen inmediatamente las siguientes observaciones acerca de períodos de este tipo.

I. Ya que $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$, etc. (mod. n), es claro que (f, λ), $(f, \lambda h)$, $(f, \lambda h^2)$, etc. están compuestos por las mismas raíces. En general, por consiguiente, si designamos por $[\lambda']$ cualquier raíz en (f, λ), este período será completamente idéntico a (f, λ'). Si por lo tanto dos períodos que tienen el mismo número de raíces (los llamaremos *similares*) tienen una raíz en común, ellos serán idénticos. Por lo tanto no puede ocurrir que dos raíces estén contenidas juntas en un período y solamente una de ellas se encuentre en otro período similar. Además, si dos raíces $[\lambda]$ y $[\lambda']$ pertenecen al mismo período de f términos, el valor de la expresión $\frac{\lambda'}{\lambda}$ (mod. n) es congruente a alguna potencia de h; esto es, podemos asumir que $\lambda' \equiv \lambda g^{\nu e}$ (mod. n).

II. Si $f = n - 1$, $e = 1$, el período $(f, 1)$ coincidirá con Ω. En los casos restantes Ω estará compuesto por los períodos $(f, 1)$, (f, g), (f, g^2), ... (f, g^{e-1}). Por

*) En lo que sigue también es posible llamar a la suma el valor numérico del período, o simplemente el período, cuando no haya ambigüedad.

lo tanto estos períodos serán completamente diferentes unos de otros y es claro que cualquier otro período similar (f, λ) coincidirá con uno de éstos si $[\lambda]$ pertenece a Ω, i.e., si λ no es divisible por n. El período $(f, 0)$ o (f, kn) está evidentemente compuesto de f unidades. También es claro que si λ es cualquier número no divisible por n, el conjunto de e períodos (f, λ), $(f, \lambda g)$, $(f, \lambda g^2)$, $\ldots (f, \lambda g^{e-1})$ también coincidirá con Ω. Así, e.g., para $n = 19$, $f = 6$, Ω consistirá de los tres períodos (6,1), (6,2) y (6,4). Cualquiera otro período similar, excepto (6,0), puede ser reducido a uno de éstos.

III. Si $n - 1$ es el producto de tres números positivos a, b y c, es evidente que cualquier período de bc términos está compuesto de b períodos de c términos; por ejemplo (bc, λ) está compuesto por (c, λ), $(c, \lambda g^a)$, $(c, \lambda g^{2a}) \ldots (c, \lambda g^{ab-a})$. Estos últimos se dicen estar contenidos en los primeros. Así para $n = 19$ el período (6,1) consiste de los tres períodos (2,1), (2,8) y (2,7). El primero contiene las raíces r y r^{18}; el segundo r^8 y r^{11}; el tercero r^7 y r^{12}.

345.

Teorema. *Sean (f, λ) y (f, μ) dos períodos similares, idénticos o diferentes, (f, λ) consistiendo de las raíces $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc. Entonces el producto de (f, λ) por (f, μ) será la suma de f períodos similares, a saber*

$$= (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \text{ etc.} = W$$

Demostración. Sea como antes $n - 1 = ef$; g una raíz primitiva para el módulo n y $h = g^e$. De lo que hemos dicho antes, tenemos $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2)$ etc. El producto buscado será

$$= [\mu] \cdot (f, \lambda) + [\mu h] \cdot (f, \lambda h) + [\mu h^2] \cdot (f, \lambda h^2) + \text{ etc.}$$

y así

$$\begin{array}{llll} = [\lambda + \mu] & +[\lambda h + \mu] & \cdots & +[\lambda h^{f-1} + \mu] \\ +[\lambda h + \mu h] & +[\lambda h^2 + \mu h] & \cdots & +[\lambda h^f + \mu h] \\ +[\lambda h^2 + \mu h^2] & +[\lambda h^3 + \mu h^2] & \cdots & +[\lambda h^{f+1} + \mu h^2] \text{ etc.} \end{array}$$

una expresión que contendrá en conjunto f^2 raíces. Y si se suman las columnas verticales juntas, resulta

$$(f, \lambda + \mu) + (f, \lambda h + \mu) + \cdots + (f, \lambda h^{f-1} + \mu)$$

una expresión que coincide con W, porque por hipótesis los números λ, λ', λ'', etc. son congruentes a λ, λh, λh^2, $\ldots \lambda h^{f-1}$ según el módulo n (aquí no estamos interesados en el orden) y así también

$$\lambda + \mu, \quad \lambda' + \mu, \quad \lambda'' + \mu, \quad \text{etc.}$$

serán congruentes a

$$\lambda + \mu, \quad \lambda h + \mu, \quad \lambda h^2 + \mu, \quad \ldots \ \lambda h^{f-1} + \mu \quad \textit{Q. E. D.}$$

Agregamos los siguientes corolarios a este teorema:

I. Si k designa cualquier entero, el producto de $(f, k\lambda)$ por $(f, k\mu)$ será

$$= (f, k(\lambda + \mu)) + (f, k(\lambda' + \mu)) + (f, k(\lambda'' + \mu)) + \text{ etc.}$$

II. Ya que los términos particulares de W coinciden con la suma $(f, 0)$ la cual $= f$, o con una de las sumas $(f, 1)$, (f, g), $(f, g^2) \ldots (f, g^{e-1})$, W puede ser reducido a la siguiente forma

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

donde los coeficientes a, b, b', etc. son enteros positivos (o alguno puede aún ser $= 0$). Es también claro que el producto de $(f, k\lambda)$ por $(f, k\mu)$ entonces se convertirá en

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

Así, e.g., para $n = 19$ el producto de la suma $(6, 1)$ por ella misma, o sea el cuadrado de esta suma, será $= (6, 2) + (6, 8) + (6, 9) + (6, 12) + (6, 13) + (6, 19) = 6 + 2(6, 1) + (6, 2) + 2(6, 4)$.

III. Puesto que el producto de los términos individuales de W por un período similar (f, ν) puede ser reducido a una forma análoga, es evidente que el producto de tres períodos $(f, \lambda) \cdot (f, \mu) \cdot (f, \nu)$ puede ser representado por $cf + d(f, 1) \ldots + d^{\varepsilon}(f, g^{e-1})$ y los coeficientes c, d, etc. serán enteros y positivos (o $= 0$) y para cualquier valor entero de k tenemos

$$(f, k\lambda) \cdot (f, k\mu) \cdot (f, k\nu) = cf + d(f, k) + d'(f, kg) + \text{ etc.}$$

Este teorema puede ser extendido al producto de cualquier número de períodos similares, y no importa si estos períodos son todos diferentes o parcialmente o totalmente idénticos.

IV. Se sigue de esto que si en cualquier función algebraica racional entera $F = \varphi(t, u, v, \ldots)$ sustituimos las incógnitas t, u, v, etc. por los períodos similares (f, λ), (f, μ), (f, ν), etc. respectivamente, su valor será reducible a la forma

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

y los coeficientes A, B, B', etc. serán enteros si todos los coeficientes en F son enteros. Pero si después sustituimos t, u, v, etc. por $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$, etc. respectivamente, el valor de F será reducido a $A + B(f, k) + B'(f, kg) +$ etc.

346.

TEOREMA. *Suponiendo que λ es un número no divisible por n, y escribiendo por brevedad p en lugar de (f, λ), cualquier otro período similar (f, μ), en el cual μ no es divisible por n, puede ser reducido a la forma*

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

donde los coeficientes α, β, etc. son cantidades racionales determinadas.

Demostración. Desígnense por p', p'', p''', etc. los períodos $(f, \lambda g)$, $(f, \lambda g^2)$, $(f, \lambda g^3)$, etc. hasta $(f, \lambda g^{e-1})$. Su número será $e - 1$ y uno de ellos necesariamente coincidirá con (f, μ). Inmediatamente resulta la ecuación

$$0 = 1 + p + p' + p'' + p''' + \text{ etc.} \qquad (I)$$

Ahora, si de acuerdo con las reglas del artículo precedente se desarrollan las potencias de p hasta la $e - 1$-ésima, se extenderán otras $e - 2$ ecuaciones

$$0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \text{ etc.} \qquad (II)$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{ etc.} \qquad (III)$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{ etc.} \qquad (IV)$$
$$\text{etc.}$$

Todos los coeficientes A, a, a', etc.; B, b, b', etc.; etc. serán enteros y, como sigue inmediatamente del artículo precedente, completamente independientes de λ; esto es, se obtienen las mismas ecuaciones no importa cual sea el valor que demos a λ. Esta observación puede ser extendida a la ecuación I en tanto que λ no sea divisible por n. Supongamos que $(f, \mu) = p'$; por ello es fácil ver que si (f, μ) coincide con cualquiera de los otros períodos p'', p''', etc. la siguiente línea de argumento puede ser usada de modo completamente análogo. Ya que el número de ecuaciones I, II, III, etc. es $e-1$, las cantidades p'', p''', etc. cuyo número es $= e-2$, pueden ser eliminadas de ellas por métodos conocidos. La ecuación resultante (Z) estará libre de ellas:

$$0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \text{ etc.} + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

Esto se puede hacer de manera tal que todos los coeficientes $\mathfrak{A}$, $\mathfrak{B}$, $\ldots\,\mathfrak{N}$ sean enteros y de seguro no todos $= 0$. Ahora, si no tenemos $\mathfrak{N} = 0$, se sigue que p' puede ser determinado como lo demanda el teorema. Queda por lo tanto probar que no puede hacerse $\mathfrak{N} = 0$.

Suponiendo que $\mathfrak{N} = 0$, la ecuación Z se convierte en $\mathfrak{M}p^{e-1} + \text{etc.} + \mathfrak{B}p + \mathfrak{A} = 0$. Ya que ella no puede tener grado mayor que $e-1$, no es satisfecha por más que $e-1$ valores diferentes de p. Pero ya que las ecuaciones de las cuales se deduce Z son independientes de λ, se sigue que Z no depende de λ y así ella tendrá lugar, no importa qué entero no divisible por n tomemos para λ. Por consiguiente esta ecuación Z será satisfecha por cualquiera de las sumas $(f, 1)$, (f, g), (f, g^2), $\ldots\,(f, g^{e-1})$, y se sigue inmediatamente que no todas estas sumas pueden ser diferentes sino que al menos dos de ellas deben ser iguales. Suponga que una de estas dos sumas iguales contiene las raíces $[\zeta]$, $[\zeta']$, $[\zeta'']$, etc. y la otra las raíces $[\eta]$, $[\eta']$, $[\eta'']$, etc. Supondremos (esto es legítimo) que todos los números ζ, ζ', ζ'', etc., η, η', η'', etc. son positivos y $< n$. Evidentemente todos serán diferentes y ninguno de ellos $= 0$. Designaremos por Y la función

$$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + \text{ etc.} - x^{\eta} - x^{\eta'} - x^{\eta''} - \text{ etc.}$$

Su término mayor no puede exceder a x^{n-1} y $Y = 0$ si se pone $x = [1]$. Así Y tendrá un factor $x - [1]$ en *común* con la función denotada por X en lo que precede y es fácil probar que esto sería absurdo. En efecto, si Y y X tienen un factor común, el máximo común divisor de las funciones X e Y (no puede tener grado $n-1$ porque Y es divisible por x) tendría todos sus coeficientes racionales. Esto seguiría de la

naturaleza de las operaciones involucradas en encontrar el máximo común divisor de dos funciones cuyos coeficientes son todos racionales. Pero en el artículo 341 probamos que X no puede tener un factor con coeficientes racionales de grado menor que $n-1$. Por lo tanto la suposición $\mathfrak{N} = 0$ no puede ser consistente.

Ejemplo. Para $n = 19$, $f = 6$ resulta $p^2 = 6 + 2p + p' + 2p''$. Ya que $0 = 1 + p + p' + p''$, deducimos que $p' = 4 - p^2$, $\quad p'' = -5 - p + p^2$. Por consiguiente

$$\begin{aligned} (6,2) &= 4 - (6,1)^2, \qquad & (6,4) &= -5 - (6,1) + (6,1)^2 \\ (6,4) &= 4 - (6,2)^2, \qquad & (6,1) &= -5 - (6,2) + (6,2)^2 \\ (6,1) &= 4 - (6,4)^2, \qquad & (6,2) &= -5 - (6,4) + (6,4)^2 \end{aligned}$$

347.

TEOREMA. *Sea* $F = \varphi(t, u, v, \ldots)$ *una función algebraica racional entera invariable**) en las incógnitas t, u, v, etc. Sustituyendo éstas por las f raíces contenidas en el período (f, λ), por las reglas del artículo 340 el valor de F es reducido a la forma

$$A + A'[1] + A''[2] + \text{ etc.} = W\,.$$

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

Demostración. Sean $[p]$ y $[q]$ dos raíces pertenecientes al mismo período y suponga que p y q son positivas y menores que n. Hay que mostrar que $[p]$ y $[q]$ tienen el mismo coeficiente en W. Sea $q \equiv pg^{\nu e} \pmod{n}$; y sean $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc. las raíces contenidas en (f, λ), donde suponemos que λ, λ', λ'', etc. son positivos y menores que n; finalmente sean μ, μ', μ'', etc. los menores residuos positivos de los números $\lambda g^{\nu e}$, $\lambda' g^{\nu e}$, $\lambda'' g^{\nu e}$, etc. según el módulo n. Evidentemente éstos serán idénticos con los números λ, λ', λ'', etc., aunque el orden puede estar transpuesto. Del artículo 340 es claro que

$$\varphi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}], \ldots) = (I)$$

---

*) Funciones invariables son aquéllas en las que todas las incógnitas están contenidas del mismo modo, o, más claramente, funciones que no cambian no importa la forma en que se presenten las incógnitas; tales son por ejemplo, la suma de las incógnitas, su producto, la suma de productos de pares de ellas, etc.

es reducido a

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{ etc.} \quad \text{o a} \quad A + A'[\theta] + A''[\theta'] + \text{ etc.} = (W')$$

Aquí, θ, θ', etc. designan los residuos mínimos de los números $g^{\nu e}$, $2g^{\nu e}$, etc. según el módulo n y así vemos que el coeficiente que tiene $[q]$ en (W') es el mismo que tiene $[p]$ en (W). Si desarrollamos la expresión (I) obtendremos lo mismo que obtenemos de desarrollar la expresión $\varphi([\mu], [\mu'], [\mu'']$, etc.) porque $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$, etc. (mod. n). De hecho, esta última expresión produce el mismo resultado que $\varphi([\lambda], [\lambda'], [\lambda'']$, etc.), ya que los números μ, μ', μ'', etc. difieren de los números λ, λ', λ'', etc. solamente en el orden y esto no tiene importancia en una función invariable. Así, W' es completamente idéntico con W y por eso la raíz $[q]$ tendrá el mismo coeficiente que $[p]$ en W. *Q. E. D.*

Entonces es claro que W puede ser reducido a la forma

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

y los coeficientes A, a, $\ldots a^{\varepsilon}$ serán cantidades determinadas y enteras si todos los coeficientes racionales en F son enteros. Así, e.g., si $n = 19$, $f = 6$, $\lambda = 1$ y la función φ designa la suma de los productos de las incógnitas tomadas dos a dos, su valor es reducido a $3 + (6, 1) + (6, 4)$.

Si después de esto t, u, v, etc. son sustituidas por las raíces de otro período $(f, k\lambda)$, el valor de F se convertirá en

$$A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \text{ etc.}$$

348.

En cualquier ecuación

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \cdots = 0$$

los coeficientes α, β, γ, etc. son funciones invariables de las raíces; esto es, α es la suma de todas ellas, β es la suma de sus productos tomados dos a la vez, γ es la suma de sus productos tomados tres a la vez, etc. Por lo tanto en la ecuación cuyas

raíces son aquéllas contenidas en el período (f, λ), el primer coeficiente será $= (f, \lambda)$ y cada uno de los otros puede ser reducido a la forma

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

con todos los A, a, a', etc. enteros. Es luego evidente que la ecuación cuyas raíces son las raíces contenidas en cualquiera otro período $(f, k\lambda)$ puede ser derivada de la anterior sustituyendo $(f, 1)$ por (f, k) en cada uno de los coeficientes, (f, g) por (f, kg), y en general (f, p) por (f, kp). De esta forma por lo tanto, se pueden especificar e ecuaciones $z = 0$, $z' = 0$, $z'' = 0$, etc., cuyas raíces serán las raíces contenidas en $(f, 1)$, (f, g), (f, g^2), etc., tan pronto como encontremos las e sumas $(f, 1)$, (f, g), (f, g^2), etc. o mejor dicho tan pronto como encontremos *una* cualquiera de ellas. Esto es cierto porque, por el artículo 346, todas las restantes pueden ser deducidas racionalmente de una de ellas. Hecho esto, la función X será resuelta en e factores de grado f, pues evidentemente el producto de las funciones z, z', z'', etc. será $= X$.

Ejemplo. Para $n = 19$ la suma de todas las raíces en el período $(6, 1)$ es $(6, 1) = \alpha$; la suma de sus productos tomados dos a la vez $= 3 + (6, 1) + (6, 4) = \beta$; similarmente, la suma de los productos tomados tres a la vez $= 2+2(6, 1)+(6, 2) = \gamma$; la suma de los productos tomados cuatro a la vez $= 3 + (6, 1) + (6, 4) = \delta$; la suma de los productos tomados cinco a la vez $= (6, 1) = \varepsilon$; el producto de todos ellos $= 1$. Así la ecuación

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

contendrá todas las raíces incluidas en $(6, 1)$. Y si sustituimos $(6, 1)$, $(6, 2)$ y $(6, 4)$ por $(6, 2)$, $(6, 4)$ y $(6, 1)$ respectivamente en los coeficientes α, β, γ, etc., resultará la ecuación $z' = 0$, la cual contendrá las raíces de $(6, 2)$. Si la misma permutación se aplica de nuevo, tendremos la ecuación $z'' = 0$ conteniendo las raíces de $(6, 4)$, y el producto $zz'z'' = X$.

349.

A menudo es más conveniente, en especial cuando f es un número grande, deducir los coeficientes β, γ, etc. de las sumas de las potencias de las raíces, por el teorema de Newton. Así la suma de los cuadrados de las raíces contenidas en (f, λ)

es $= (f, 2\lambda)$, la suma de los cubos es $= (f, 3\lambda)$, etc. Si escribimos q, q', q'', etc. por (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$, etc. tendremos

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

donde, por el artículo 345, el producto de dos períodos ha de ser convertido inmediatamente en una suma de períodos. Así, en nuestro ejemplo, escribiendo p, p' y p'' por $(6, 1)$, $(6, 2)$ y $(6, 4)$ respectivamente, tendremos q, q', q'', q''', q'''' y q''''' respectivamente $= p$, p', p', p'', p' y p''. Luego

$$\alpha = p, \qquad 2\beta = p^2 - pp' = 6 + 2p + 2p''$$
$$3\gamma = (3 + p + p'')p - pp' + p' = 6 + 6p + 3p'$$
$$4\delta = (2 + 2p + p')p - (3 + p + p'')p' + pp' - p'' = 12 + 4p + 4p'', \text{ etc.}$$

Sin embargo, es suficiente computar la mitad de los coeficientes de esta manera, porque no es difícil probar que los últimos son iguales a los primeros en orden inverso; esto es, el último $= 1$, el penúltimo $= \alpha$, el antepenúltimo $= \beta$, etc.; o, de otra manera, el último puede ser derivado del primero sustituyendo $(f, 1)$, (f, g), etc. por los períodos $(f, -1)$, $(f, -g)$, etc. o sea $(f, n-1)$, $(f, n-g)$, etc. Los primeros casos se tienen cuando f es impar. El último coeficiente, sin embargo, siempre será $= 1$. La base para esto es establecida por el teorema del artículo 79, pero por razones de brevedad no nos dilataremos en el argumento.

350.

Teorema. *Sea $n-1$ el producto de los tres enteros positivos α, β y γ y considere el período $(\beta\gamma, \lambda)$ de $\beta\gamma$ términos compuesto de los β períodos menores de γ términos, (γ, λ), (γ, λ'), (γ, λ''), etc. Supongamos luego que en una función de β incógnitas tal como en el artículo* 347, *esto es en $F = \varphi(t, u, v, \ldots)$, se sustituyen las incógnitas t, u, v, etc. por las sumas (γ, λ), (γ, λ'), (γ, λ''), etc. respectivamente y de acuerdo con las reglas del artículo* 345.IV *su valor es reducido a*

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

Entonces digo que si F es una función invariable, los períodos en W que están contenidos en el mismo período de $\beta\gamma$ términos (i.e. en general los períodos (γ, g^{μ}) y $(\gamma, g^{\alpha\nu+\mu})$ donde ν es cualquier entero), tendrán los mismos coeficientes.

Demostración. Ya que el período $(\beta\gamma, \lambda g^\alpha)$ es idéntico a $(\beta\gamma, \lambda)$, los períodos menores $(\gamma, \lambda g^\alpha)$, $(\gamma, \lambda' g^\alpha)$, $(\gamma, \lambda'' g^\alpha)$, etc. los cuales comprenden al primero, necesariamente coinciden con aquéllos que comprenden al último, aunque en un orden diferente. Si se supone que F será transformado en W' sustituyendo t, u, v, etc. por las primeras cantidades, respectivamente, W' coincidirá con W. Pero por el artículo 347 resulta

$$\begin{aligned} W' &= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \cdots + a^\zeta(\gamma, g^{\alpha\beta}) \cdots + a^\theta(\gamma, g^{\alpha\beta+\alpha-1}) \\ &= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \cdots + a^\zeta(\gamma, 1) \cdots + a^\theta(\gamma, g^{\alpha-1}) \end{aligned}$$

así esta expresión debe coincidir con W y el primero, segundo, tercero, etc. coeficientes en W (comenzando con a) deben coincidir con el $\alpha+1$-ésimo, el $\alpha+2$-ésimo, el $\alpha+3$-ésimo, etc. Concluimos en general que los coeficientes de los períodos (γ, g^μ), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu})$, $\ldots (\gamma, g^{\nu\alpha+\mu})$, los cuales son el $\mu-1$-ésimo, el $\alpha+\mu+1$-ésimo, el $2\alpha+\mu+1$-ésimo, $\ldots \nu\alpha+\mu+1$-ésimo $\ldots$ deben coincidir con alguno otro. *Q. E. D.*

Así, es claro que W puede ser reducido a la forma

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \cdots + a^\varepsilon(\beta\gamma, g^{\alpha-1})$$

con todos los coeficientes A, a, etc. enteros, si todos los coeficientes en F son enteros. Suponga después de esto que sustituimos las incógnitas en F por los β períodos de γ términos que constituyen otro período de $\beta\gamma$ términos, por ejemplo, aquéllos contenidos en $(\beta\gamma, \lambda k)$ que son $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$, etc. Entonces el valor resultante será $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \cdots + a^\varepsilon(\beta\gamma, g^{\alpha-1}k)$.

Es obvio que el teorema puede ser extendido al caso donde $\alpha = 1$ o $\beta\gamma = n-1$. En este caso *todos* los coeficientes en W serán iguales, y W será reducido a la forma $A + a(\beta\gamma, 1)$.

351.

Ahora, reteniendo la terminología del artículo precedente, es claro que los coeficientes individuales de la ecuación cuyas raíces son las β sumas (γ, λ), (γ, λ'), (γ, λ''), etc. pueden ser reducidos a una forma como

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \cdots + a^\varepsilon(\beta\gamma, g^{\alpha-1})$$

y los números A, a etc. serán todos enteros. Se deriva de esto la ecuación cuyas raíces son los β períodos de γ términos contenidos en otro período $(\beta\gamma, k\lambda)$ si en todos los

coeficientes sustituimos todos los períodos $(\beta\gamma, \mu)$ por $(\beta\gamma, k\mu)$. Si por consiguiente $\alpha = 1$, todos los β períodos de γ términos estarán determinados por una ecuación de grado β, y cada uno de los coeficientes será de la forma $A + a(\beta\gamma, 1)$. Como resultado, *todos ellos serán cantidades conocidas* porque $(\beta\gamma, 1) = (n-1, 1) = -1$. Si $\alpha > 1$, los coeficientes de la ecuación cuyas raíces son todos los períodos de γ términos contenidos en un período dado de $\beta\gamma$ términos, serán cantidades conocidas en tanto que todos los valores numéricos de todos los α períodos de $\beta\gamma$ términos sean conocidos. El cálculo de los coeficientes de estas ecuaciones será a menudo más fácil, especialmente cuando β no es muy pequeño, si primero se calculan las sumas de las potencias de las raíces y se deducen de éstas los coeficientes por el teorema de Newton, como arriba en el artículo 349.

Ejemplo. I. Para $n = 19$ se busca la ecuación cuyas raíces son las sumas $(6, 1)$, $(6, 2)$ y $(6, 4)$. Designando estas raíces por p, p', p'', etc. respectivamente y la ecuación buscada por

$$x^3 - Ax^2 + Bx - C = 0$$

tenemos

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

Entonces

$$A = (18, 1) = -1$$

y

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

así

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

y finalmente

$$C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7$$

por lo tanto la ecuación buscada es

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

Usando el otro método, tenemos

$$p + p' + p'' = -1$$

$$p^2 = 6 + 2p + p' + 2p'', \qquad p'^2 = 6 + 2p' + p'' + 2p, \qquad p''^2 = 6 + 2p'' + p + 2p'$$

de donde

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

y similarmente

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

De esto y del teorema de Newton derivamos la misma ecuación que antes.

II. Para $n = 19$ se busca la ecuación cuyas raíces son las sumas $(2, 1)$, $(2, 7)$ y $(2, 8)$. Si las designamos por q, q' y q'' encontramos

$$q + q' + q'' = (6, 1), \qquad qq' + qq'' + q'q'' = (6, 1) + (6, 4), \qquad qq'q'' = 2 + (6, 2)$$

y así, reteniendo la misma notación que en lo precedente, la ecuación buscada será

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

La ecuación cuyas raíces son las sumas $(2, 2)$, $(2, 3)$ y $(2, 5)$ contenidas en $(6, 2)$ puede ser deducida de lo anterior sustituyendo p, p' y p'' por p', p'' y p, respectivamente, y si hacemos la misma sustitución nuevamente, se obtiene la ecuación cuyas raíces son las sumas $(2, 4)$, $(2, 6)$ y $(2, 9)$ contenidas en $(6, 4)$.

La solución de la ecuación $X = 0$ según se desarrolla de la investigación precedente.

352.

El teorema anterior junto con sus corolarios contiene los principios básicos de la teoría completa, y el método de hallazgo de los valores de las raíces Ω puede ser tratado ahora en unas pocas palabras.

Primero hay que tomar un número g que sea una raíz primitiva para el módulo n y encontrar el residuo mínimo de las potencias de g hasta g^{n-2} según el módulo n. Resuelva $n - 1$ en factores, y de hecho en factores primos si es conveniente reducir el problema a ecuaciones del menor grado posible. Estos se llaman (el orden es arbitrario) α, β, γ, $\ldots\zeta$ y defina

$$\frac{n-1}{\alpha} = \beta\gamma\ldots\zeta = a, \qquad \frac{n-1}{\alpha\beta} = \gamma\ldots\zeta = b, \quad \text{etc.}$$

Distribuya todas la raíces Ω en α períodos de a términos, y de nuevo cada uno de éstos en β períodos de b términos, y nuevamente cada uno de éstos en γ períodos, etc.

Determine como en el artículo precedente la ecuación (A) de grado α, cuyas raíces son las α sumas de a términos; sus valores pueden ser determinados resolviendo esta ecuación.

Pero aquí surge una dificultad porque parece incierto qué sumas deben hacerse iguales a qué raíces de la ecuación (A); esto es, cuál raíz debe ser denotada por $(a,1)$, cuál por (a,g), etc. Podemos resolver esta dificultad de la siguiente forma. Designamos con $(a,1)$ una raíz cualquiera de la ecuación (A); en efecto, como cualquier raíz de esta ecuación es la suma de a raíces de Ω, y es completamente arbitrario cual raíz de Ω se denota por [1], es posible asumir que [1] expresa una de las raíces que constituyen una raíz dada de la ecuación (A), y de aquí esta raíz de la ecuación (A) será $(a,1)$. Aún así la raíz [1] no estará completamente determinada; todavía permanece completamente arbitrario o indefinido cuál de las raíces que componen $(a,1)$ escogemos para adoptar como [1]. Tan pronto como $(a,1)$ sea determinada, todas las sumas restantes de a términos pueden ser racionalmente deducidas de ella (art. 346). Así, es claro que es necesario resolver para una sola raíz de la ecuación. También se puede usar el siguiente método, menos directo, para el mismo propósito. Tome para [1] una raíz definida; i.e. sea $[1] = \cos\frac{kP}{n} + i\,\mathrm{sen}\,\frac{kP}{n}$ con el entero k tomado arbitrariamente pero de tal manera que no sea divisible por n. Cuando se hace esto, también [2], [3], etc. determinarán raíces definidas, y las sumas $(a,1)$, (a,g), etc. designarán cantidades definidas. Ahora, si estas cantidades son calculadas de una tabla de senos con precisión tal que se pueda decidir cuáles son las más grandes y cuáles las más pequeñas, ésta será dejada como la manera de distinguir sin duda las raíces individuales de la ecuación (A).

Cuando de esta forma se han encontrado todas las α sumas de a términos, determínese por los métodos del artículo precedente la ecuación (B) de grado β, cuyas raíces son las β sumas de b términos contenidas en $(a,1)$; todos los coeficientes de esta ecuación serán cantidades conocidas. Ya que en esta etapa es arbitrario cual de los $a = \beta b$ raíces contenidas en $(a,1)$ es denotada por [1], cualquier raíz dada de la ecuación (B) puede ser expresada por $(b,1)$ porque es lícito suponer que una de las b raíces de las cuales está compuesta es denotada por [1]. Determínese por lo tanto una raíz cualquiera de la ecuación (B) por una solución de ésta. Sea ella $= (b,1)$ y derive de ésta por el artículo 346 todas las restantes sumas de b términos. De esta manera tenemos al mismo tiempo un método de corroboración de los cálculos, puesto que el total de todas las sumas de b términos que pertenecen a un período cualquiera de a términos es conocido. En algunos casos es igualmente fácil formar otras $\alpha - 1$ ecuaciones de grado β, cuyas raíces sean respectivamente las β sumas individuales

de b términos contenidas en los restantes períodos de a términos (a, g), (a, g^2), etc. y determinar *todas* las raíces mediante la solución tanto de estas ecuaciones como de la ecuación B. Entonces, de la misma manera que antes, con la ayuda de una tabla de senos, podemos decidir cuáles son los períodos de b términos para los cuales las raíces individuales encontradas de esta manera son iguales. Pero para ayudar en esta decisión pueden ser usados varios otros mecanismos que no se pueden explicar plenamente aquí. Uno de ellos, sin embargo, el caso donde $\beta = 2$, es especialmente útil y puede ser explicado más brevemente por ilustración que por reglas. Lo utilizaremos en los siguientes ejemplos.

Después de encontrar los valores de todos las $\alpha\beta$ sumas de b términos de esta forma, se puede utilizar un método similar para determinar por ecuaciones de grado γ todas las $\alpha\beta\gamma$ sumas de c términos. Esto es, se puede *o* encontrar *una* ecuación de grado γ de acuerdo con el artículo 350, cuyas raíces son las γ sumas de c términos contenidos en $(b, 1)$, y resolviendo ésta encontrar una raíz que se llama $(c, 1)$ y finalmente de esto por los métodos del artículo 346 deducir todas las sumas restantes; *o* de manera similar encontrar las $\alpha\beta$ ecuaciones de grado γ cuyas raíces son respectivamente las γ sumas de c términos contenidas en los períodos individuales de b términos. Se puede resolver todas estas ecuaciones para todas sus raíces y determinar el orden de las raíces con la ayuda de una tabla de senos como hicimos antes. Sin embargo, para $\gamma = 2$ se puede usar el mecanismo que mostraremos más abajo.

Continuando de esta manera finalmente habrá todas las $\frac{n-1}{\zeta}$ sumas de ζ términos; y si se encuentra por los métodos del artículo 348 la ecuación de grado ζ cuyas raíces son las ζ raíces de Ω contenidas en $(\zeta, 1)$, todos sus coeficientes serán cantidades conocidas. Y si resolvemos para una raíz cualquiera, se puede hacerla $= [1]$, y sus potencias darán todas las otras raíces Ω. Si nos gusta más, podemos resolver para *todas* las raíces de esa ecuación. Entonces mediante la solución de las otras $\frac{n-1}{\zeta} - 1$ ecuaciones de grado ζ, las cuales contienen respectivamente todas las ζ raíces en cada uno de los restantes períodos de ζ términos, se puede encontrar todas las restantes raíces Ω.

Es claro, sin embargo, que en tanto que la primera ecuación (A) sea resuelta, o en tanto que se tengan los valores de todas las α sumas de a términos, tendremos también la resolución de X en α factores de grado a, por el artículo 348. Luego, después de resolver la ecuación (B) o después de encontrar los valores de todas las $\alpha\beta$ sumas de b términos, cada uno de esos factores será resuelto asimismo en β factores, y así X será resuelto en $\alpha\beta$ factores de grado b, etc.

Ejemplo para $n = 19$ donde la operación se reduce a resolver dos ecuaciones cúbicas y una cuadrática.

353.

Primer ejemplo para $n = 19$. Ya que aquí $n - 1 = 3 \cdot 3 \cdot 2$, la búsqueda de las raíces Ω se reduce a la solución de dos ecuaciones cúbicas y una cuadrática. Este ejemplo es entendido más fácilmente porque para la mayor parte las operaciones necesarias ya han sido discutidas antes. Tomando el número 2 como la raíz primitiva g, los residuos mínimos de sus potencias producirán lo siguiente (los exponentes de las potencias están escritos en la primera línea y los residuos en la segunda):

$$\begin{array}{c} 0.\ 1.\ 2.\ 3.\ \ 4.\ \ 5.\ 6.\ \ 7.\ 8.\ \ 9.\ 10.\ 11.\ 12.\ 13.\ 14.\ 15.\ 16.\ 17 \\ 1.\ 2.\ 4.\ 8.\ 16.\ 13.\ 7.\ 14.\ 9.\ 18.\ 17.\ 15.\ 11.\ \ 3.\ \ 6.\ 12.\ \ 5.\ 10 \end{array}$$

De esto, por los artículos 344 y 345, se deduce fácilmente la siguiente distribución de todas las raíces Ω en tres períodos de seis términos y de cada uno de ellos en tres períodos de dos términos:

$$\Omega = \quad (18,1) \left\{ \begin{array}{lll} (6,1) \left\{ \begin{array}{lll} (2,\ 1) & \ldots & [1],\ [18] \\ (2,\ 8) & \ldots & [8],\ [11] \\ (2,\ 7) & \ldots & [7],\ [12] \end{array} \right. \\ (6,2) \left\{ \begin{array}{lll} (2,\ 2) & \ldots & [2],\ [17] \\ (2{,}16) & \ldots & [3],\ [16] \\ (2{,}14) & \ldots & [5],\ [14] \end{array} \right. \\ (6,4) \left\{ \begin{array}{lll} (2,\ 4) & \ldots & [4],\ [15] \\ (2{,}13) & \ldots & [6],\ [13] \\ (2,\ 9) & \ldots & [9],\ [10] \end{array} \right. \end{array} \right.$$

La ecuación (A), cuyas raíces son las sumas $(6,1)$, $(6,2)$ y $(6,4)$, resulta ser $x^3 + x^2 - 6x - 7 = 0$ y una de las raíces es $-1{,}2218761623$. Expresando en términos de $(6,1)$, tenemos

$$(6,2) = 4 - (6,1)^2 = 2{,}5070186441$$
$$(6,4) = -5 - (6,1) + (6,1)^2 = -2{,}2851424818$$

Así X se resuelve en tres factores de grado 6, si estos valores son sustituidos en las fórmulas del artículo 348.

La ecuación (B), cuyas raíces son las sumas $(2,1)$, $(2,7)$ y $(2,8)$, resulta ser

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

o

$$x^3 + 1{,}2218761623x^2 - 3{,}5070186441x - 4{,}5070186441 = 0$$

Una raíz es $-1{,}3545631433$ que llamaremos $(2,1)$. Por el método del artículo 346 se encuentran las siguientes ecuaciones donde, por brevedad, se escribe q en vez de $(2,1)$:

$$\begin{aligned}
(2,2) &= q^2 - 2 \\
(2,3) &= q^3 - 3q \\
(2,4) &= q^4 - 4q^2 + 2 \\
(2,5) &= q^5 - 5q^3 + 5q \\
(2,6) &= q^6 - 6q^4 + 9q^2 - 2 \\
(2,7) &= q^7 - 7q^5 + 14q^3 - 7q \\
(2,8) &= q^8 - 8q^6 + 20q^4 - 16q^2 + 2 \\
(2,9) &= q^9 - 9q^7 + 27q^5 - 30q^3 + 9q
\end{aligned}$$

En el presente caso estas ecuaciones pueden ser encontradas más fácilmente del modo siguiente que por los métodos del artículo 346. Suponiendo

$$[1] = \cos\frac{kP}{19} + i\,\mathrm{sen}\,\frac{kP}{19}$$

tenemos

$$[18] = \cos\frac{18kP}{19} + i\,\mathrm{sen}\,\frac{18kP}{19} = \cos\frac{kP}{19} - i\,\mathrm{sen}\,\frac{kP}{19}$$

y así

$$(2,1) = 2\cos\frac{kP}{19}$$

y en general

$$[\lambda] = \cos\frac{\lambda kP}{19} + i\,\mathrm{sen}\,\frac{\lambda kP}{19}, \quad \text{y así} \quad (2,\lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$$

Por lo tanto si $\frac{1}{2}q = \cos\omega$, resultará $(2,2) = 2\cos 2\omega$, $(2,3) = 2\cos 3\omega$, etc., y las mismas fórmulas de antes serán derivadas del conocimiento de ecuaciones para los

cosenos de ángulos múltiples. Ahora, de estas fórmulas se derivan los siguientes valores numéricos:

$$\begin{array}{l|l} (2,2) = -0{,}1651586909 & (2,6) = \quad 0{,}4909709743 \\ (2,3) = \quad 1{,}5782810188 & (2,7) = -1{,}7589475024 \\ (2,4) = -1{,}9727226068 & (2,8) = \quad 1{,}8916344834 \\ (2,5) = \quad 1{,}0938963162 & (2,9) = -0{,}8033908493 \end{array}$$

Los valores de $(2,7)$ y $(2,8)$ pueden encontrarse de la ecuación (B) donde son las dos raíces restantes. La duda sobre *cual* de estas raíces es $(2,7)$ y cual es $(2,8)$ puede eliminarse por un cálculo aproximado de acuerdo con las fórmulas dadas antes o por medio de tablas de senos. Una rápida consulta nos muestra que $(2,1) = 2\cos\omega$ haciendo $\omega = \frac{7}{19}P$ y así tenemos

$$(2,7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P, \quad \text{y} \quad (2,8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P$$

Similarmente podemos encontrar las sumas $(2,2)$, $(2,3)$ y $(2,5)$ también por la ecuación

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

cuyas raíces son ellas, y la incertidumbre sobre qué raíces corresponden a qué sumas se puede eliminar exactamente de la misma manera que antes. Finalmente, las sumas $(2,4)$, $(2,6)$ y $(2,9)$ se pueden encontrar por la ecuación

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

[1] y [18] son las raíces de la ecuación $x^2 - (2,1)x + 1 = 0$. Una de ellas será

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

y la otra

$$= \frac{1}{2}(2,1) - i\sqrt{\frac{1}{2} - \frac{1}{4}(2,2)}$$

y los valores numéricos serán $= -0{,}6772815716 \pm 0{,}7357239107\,i$. Las dieciseis raíces restantes pueden ser encontradas de las potencias de una u otra de estas raíces o resolviendo las otras ocho ecuaciones similares. Para decidir, en el segundo método

cual raíz tiene el signo positivo para su parte imaginaria y cual el negativo, podemos usar tablas de senos o el artificio que explicamos en el siguiente ejemplo. De esta manera encontraremos los siguientes valores, con el signo superior correspondiendo a la primera raíz y el signo inferior a la segunda raíz:

$$\begin{aligned}
[1] \text{ y } [18] &= -0{,}6772815716 \pm 0{,}7357239107\, i \\
[2] \text{ y } [17] &= -0{,}0825793455 \mp 0{,}9965844930\, i \\
[3] \text{ y } [16] &= 0{,}7891405094 \pm 0{,}6142127127\, i \\
[4] \text{ y } [15] &= -0{,}9863613034 \pm 0{,}1645945903\, i \\
[5] \text{ y } [14] &= 0{,}5469481581 \mp 0{,}8371664783\, i \\
[6] \text{ y } [13] &= 0{,}2454854871 \pm 0{,}9694002659\, i \\
[7] \text{ y } [12] &= -0{,}8794737512 \mp 0{,}4759473930\, i \\
[8] \text{ y } [11] &= 0{,}9458172417 \mp 0{,}3246994692\, i \\
[9] \text{ y } [10] &= -0{,}4016954247 \pm 0{,}9157733267\, i
\end{aligned}$$

Ejemplo para $n = 17$ donde la operación se reduce a resolver cuatro ecuaciones cuadráticas.

354.

Segundo ejemplo para $n = 17$. Aquí $n-1 = 2\cdot 2\cdot 2\cdot 2$, así el cálculo se reducirá a cuatro ecuaciones cuadráticas. Para la raíz primitiva tomaremos el número 3, cuyas potencias tienen residuos mínimos según el módulo 17 que son

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15
1.	3.	9.	10.	13.	5.	15.	11.	16.	14.	8.	7.	4.	12.	2.	6

De esto derivamos la siguiente distribución del conjunto Ω en dos períodos de ocho términos, cuatro de cuatro términos, ocho de dos términos:

$$\Omega = (16,1)\left\{\begin{array}{l}
(8,1)\left\{\begin{array}{l}
(4,\ 1)\left\{\begin{array}{lll} (2,\ 1) & \ldots & [1],\ [16] \\ (2{,}13) & \ldots & [4],\ [13] \end{array}\right. \\
(4,\ 9)\left\{\begin{array}{lll} (2,\ 9) & \ldots & [8],\ [9] \\ (2{,}15) & \ldots & [2],\ [15] \end{array}\right.
\end{array}\right. \\
(8,3)\left\{\begin{array}{l}
(4,\ 3)\left\{\begin{array}{lll} (2,\ 3) & \ldots & [3],\ [14] \\ (2,\ 5) & \ldots & [5],\ [12] \end{array}\right. \\
(4,10)\left\{\begin{array}{lll} (2{,}10) & \ldots & [7],\ [10] \\ (2{,}11) & \ldots & [6],\ [11] \end{array}\right.
\end{array}\right.
\end{array}\right.$$

Se encuentra por las reglas del artículo 351 que la ecuación (A), cuyas raíces son las sumas $(8,1)$ y $(8,3)$, es $x^2 + x - 4 = 0$. Sus raíces son $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1{,}5615528128$ y $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2{,}5615528128$. Haremos la primera $= (8,1)$ y así necesariamente la última $= (8,3)$.

La ecuación (B), cuyas raíces son las sumas $(4,1)$ y $(4,9)$, es $x^2 - (8,1)x - 1 = 0$. Sus raíces son $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{4 + (8,1)^2} = \frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)}$. Haremos $(4,1)$ igual a la cantidad que tenga el signo radical positivo y cuyo valor numérico es $2{,}0494811777$. Así la cantidad con el signo del radical negativo y cuyo valor numérico es $-0{,}4879283649$ será expresada por $(4,9)$. Las sumas restantes de cuatro términos, a saber $(4,3)$ y $(4,10)$, pueden ser calculadas de dos maneras. *Primera,* por el método del artículo 346, que da las siguientes fórmulas cuando abreviamos $(4,1)$ con la letra p:

$$(4,3) = -\frac{3}{2} + 3p - \frac{1}{2}p^3 = 0{,}3441507314$$
$$(4,10) = \frac{3}{2} + 2p - p^2 - \frac{1}{2}p^3 = -2{,}9057035442$$

El mismo método da la fórmula $(4,9) = -1 - 6p + p^2 + p^3$ y de ésta obtenemos el mismo valor que antes. El *segundo* método permite determinar las sumas $(4,3)$ y $(4,10)$ resolviendo la ecuación $x^2 - (8,3)x - 1 = 0$ de la que ellas son las raíces. Estas raíces son $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{4 + (8,3)^2}$, o sea

$$\frac{1}{2}(8,3) + \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)} \quad \text{y} \quad \frac{1}{2}(8,3) - \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$$

Se puede remover la duda de *cual* raíz debe ser expresada por $(4,3)$ y cual por $(4,10)$ mediante el siguiente artificio que mencionamos en el artículo 352. Calcule el producto de $(4,1) - (4,9)$ por $(4,3) - (4,10)$ que es $= 2(8,1) - 2(8,3)$ *). Ahora el valor de esta expresión es positivo $= +2\sqrt{17}$ y, ya que el primer factor del producto, $(4,1) - (4,9) = +\sqrt{12 + 3(8,1) + 4(8,3)}$, es positivo, el otro factor $(4,3) - (4,10)$, deberá ser también positivo. Por lo tanto $(4,3)$ es igual a la primera raíz que tiene el signo positivo enfrente del radical, y $(4,10)$ es igual a la segunda raíz. De esto resultarán los mismos valores numéricos que antes.

Habiendo encontrado todas las sumas de cuatro términos, procedemos a las sumas de dos términos. La ecuación (C), cuyas raíces son $(2,1)$ y $(2,13)$ y está

*) La base real de este artificio es el hecho, fácil de prever, que el producto no contiene sumas de cuatro términos sino únicamente sumas de ocho términos. El matemático entrenado puede comprender fácilmente la razón de esto. Por brevedad la omitiremos aquí.

contenida en $(4,1)$, será $x^2 - (4,1)x + (4,3) = 0$. Sus raíces son

$$\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{-4(4,3) + (4,1)^2} \quad \text{o sea} \quad \frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)}$$

Cuando tomamos la cantidad radical positiva, obtenemos el valor 1,8649444588, la que hacemos $= (2,1)$ y así $(2,13)$ será igual a la otra cuyo valor es $= 0{,}1845367189$. Si las sumas restantes de dos términos han de ser encontradas por el método del artículo 346, se pueden usar las mismas fórmulas para $(2,2)$, $(2,3)$, $(2,4)$, $(2,5)$, $(2,6)$, $(2,7)$ y $(2,8)$ como lo hicimos en el ejemplo precedente para cantidades similares, es decir, $(2,2)$ (o $(2,15)$) $= (2,1)^2 - 2$ etc. Pero si parece preferible encontrarlas en pares resolviendo una ecuación cuadrática, para $(2,9)$ y $(2,15)$ obtenemos la ecuación $x^2 - (4,9)x + (4,10) = 0$ cuyas raíces son $\frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}$. Se puede determinar que signo usar del mismo modo que antes. Calculando el producto de $(2,1) - (2,13)$ por $(2,9) - (2,15)$ resulta $-(4,1) + (4,9) - (4,3) + (4,10)$. Ya que éste es negativo y el factor $(2,1) - (2,13)$ es positivo, $(2,9) - (2,15)$ deberá ser negativo y es necesario usar el signo superior positivo para $(2,15)$ y el signo inferior negativo para $(2,9)$. De esto se computa que $(2,9) = -1{,}9659461994$ y $(2,15) = 1{,}4780178344$. Entonces, ya que calculando el producto de $(2,1) - (2,13)$ por $(2,3) - (2,5)$ resulta la cantidad positiva $(4,9) - (4,10)$, el factor $(2,3) - (2,5)$ debe ser positivo. Y por un cálculo parecido al anterior se encuentra

$$(2,3) = \frac{1}{2}(4,3) + \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)} = \quad 0{,}8914767116$$
$$(2,5) = \frac{1}{2}(4,3) - \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)} = -0{,}5473259801$$

Finalmente, mediante operaciones completamente análogas se descubre

$$(2,10) = \frac{1}{2}(4,10) - \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)} = -1{,}7004342715$$
$$(2,11) = \frac{1}{2}(4,10) + \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)} = -1{,}2052692728$$

Resta ahora descender a las raíces Ω mismas. La ecuación (D) cuyas raíces son $[1]$ y $[16]$ nos da $x^2 - (2,1)x + 1 = 0$. Las raíces de ella son $\frac{1}{2}(2,1) \pm \frac{1}{2}\sqrt{(2,1)^2 - 4}$ o mejor dicho

$$\frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{4 - (2,1)^2} \quad \text{o sea} \quad \frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{2 - (2,15)}$$

Tomaremos los signos superiores para [1], los inferiores para [16]. Se deducen las catorce raíces restantes de las potencias de [1] o por la solución de siete ecuaciones cuadráticas, cada una de las cuales nos dará dos raíces, y la incertidumbre acerca de los signos de las cantidades radicales puede ser removida mediante el mismo mecanismo usado antes. Así [4] y [13] son las raíces de la ecuación $x^2-(2,13)x+1=0$ y así igual a $\frac{1}{2}(2,13) \pm \frac{1}{2}i\sqrt{2-(2,9)}$. Calculando el producto de $[1]-[16]$ por $[4]-[13]$ sin embargo obtenemos $(2,5)-(2,3)$, una cantidad real negativa. Por lo tanto, puesto que $[1]-[16]$ es $+i\sqrt{2-(2,15)}$, i.e. el producto imaginario i por una cantidad real *positiva,* $[4]-[13]$ debe también ser el producto de i por una cantidad real *positiva*, porque $i^2 = -1$. Como conclusión tomaremos el signo superior para [4] y el signo inferior para [13]. Similarmente para las raíces [8] y [9] encontramos $\frac{1}{2}(2,9) \pm \frac{1}{2}i\sqrt{2-(2,1)}$ así, ya que el producto de $[1]-[16]$ por $[8]-[9]$ es $(2,9)-(2,10)$ y negativo, debemos tomar el signo superior para [8] y el signo inferior para [9]. Si computamos entonces las restantes raíces obtendremos los siguientes valores numéricos, donde el signo superior ha de ser tomado para la primera raíz y el signo inferior para la segunda:

$$
\begin{aligned}
[1],[16]\ldots &\quad 0{,}9324722294 \pm 0{,}3612416662\,i \\
[2],[15]\ldots &\quad 0{,}7390089172 \pm 0{,}6736956436\,i \\
[3],[14]\ldots &\quad 0{,}4457383558 \pm 0{,}8951632914\,i \\
[4],[13]\ldots &\quad 0{,}0922683595 \pm 0{,}9957341763\,i \\
[5],[12]\ldots &-0{,}2736629901 \pm 0{,}9618256432\,i \\
[6],[11]\ldots &-0{,}6026346364 \pm 0{,}7980172273\,i \\
[7],[10]\ldots &-0{,}8502171357 \pm 0{,}5264321629\,i \\
[8],[\ 9]\ldots &-0{,}9829730997 \pm 0{,}1837495178\,i
\end{aligned}
$$

Lo que precede puede bastar para resolver la ecuación $x^n - 1 = 0$ y así también para encontrar las funciones trigonométricas correspondientes a los arcos que son conmesurables con la circunferencia. Pero esta materia es tan importante que no podemos concluir sin indicar algunas de las observaciones que arrojan luz sobre el tema, lo mismo que ejemplos relacionados con él o que dependen de él. Entre éstos seleccionaremos específicamente aquéllos que pueden ser resueltos sin una gran cantidad de aparato que depende de otras investigaciones y los consideramos solamente como *ejemplos* de esta inmensa teoría que deberá ser considerada detalladamente en una ocasión posterior.

Investigaciones adicionales sobre los períodos de raíces.
Sumas con un número par de términos son cantidades reales.

355.

Ya que siempre n se supone impar, 2 estará entre los factores de $n-1$, y el conjunto Ω estará compuesto de $\frac{1}{2}(n-1)$ períodos de dos términos. Un tal período $(2,\lambda)$ consistirá de las raíces $[\lambda]$ y $[\lambda g^{\frac{1}{2}(n-1)}]$, denotando, como antes, g como cualquier raíz primitiva para el módulo n. Pero $g^{\frac{1}{2}(n-1)} \equiv -1 \pmod{n}$ y así $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (ver art. 62) y $[\lambda g^{\frac{1}{2}(n-1)}] = [-\lambda]$. Por lo tanto, suponiendo que $[\lambda] = \cos\frac{kP}{n} + i\,\mathrm{sen}\,\frac{hP}{n}$ y $[-\lambda] = \cos\frac{kP}{n} - i\,\mathrm{sen}\,\frac{kP}{n}$, resulta la suma $(2,\lambda) = 2\cos\frac{kP}{n}$. Hasta este punto únicamente deducimos la conclusión de que el valor de cualquier suma de dos términos es una cantidad real. Puesto que cualquier período que tenga un número par de términos $= 2a$ se puede descomponer en a períodos de dos términos, en general es claro que el valor de cualquier suma que tenga un número par de términos es siempre una cantidad real. Por lo tanto, si en el artículo 352 entre los factores α, β, γ, etc., se reservan dos hasta el final, todas las operaciones serán hechas sobre cantidades reales hasta que lleguemos a una suma de dos términos, y los imaginarios serán introducidos cuando pasamos de estas sumas a las raíces mismas.

De la ecuación que define la distribución de las raíces Ω en dos períodos.

356.

Merecen atención especial las ecuaciones auxiliares mediante las cuales se determinan para cualquier valor de n las sumas que forman el conjunto Ω. Ellas están conectadas de una manera sorprendente con las propiedades más recónditas del número n. Aquí nos restringiremos al estudio de los dos casos siguientes. *Primero,* la ecuación cuadrática cuyas raíces son sumas de $\frac{1}{2}(n-1)$ términos, *segundo,* en caso de que $n-1$ tenga el factor 3, consideraremos la ecuación cúbica cuyas raíces son sumas de $\frac{1}{3}(n-1)$ términos.

Escribiendo por brevedad m en lugar de $\frac{1}{2}(n-1)$ y designando por g alguna raíz primitiva para el módulo n, el conjunto Ω consistirá de dos períodos $(m,1)$ y (m,g). El primero contendrá las raíces $[1]$, $[g^2]$, $[g^4]$, $\ldots$ $[g^{n-3}]$, el último las raíces $[g]$, $[g^3]$, $[g^5]$, $\ldots$ $[g^{n-2}]$. Suponiendo que los residuos mínimos positivos de los números g^2, g^4,$\ldots$ g^{n-3} según el módulo n son, en orden arbitrario, R, R', R'', etc. y los residuos de g, g^3, g^5, $\ldots$ g^{n-2} son N, N', N'', etc., entonces las raíces de las que consiste $(m,1)$, coinciden con $[1]$, $[R]$, $[R']$, $[R'']$, etc. y las raíces del período (m,g) con $[N]$, $[N']$, $[N'']$, etc. Es claro que todos los números 1, R, R', R'', etc. son *residuos*

cuadráticos del número n. Puesto que todos ellos son diferentes y menores que n, y ya que su número es $= \frac{1}{2}(n-1)$ y así igual al número de todos los residuos positivos de n que son menores que n, estos residuos coincidirán completamente con aquellos números. Igualmente, todos los números N, N', N'', etc. son diferentes uno del otro y de los números 1, R, R', etc. y junto con éstos agotan todos los números 1, 2, 3, $\ldots n-1$. Se sigue que los números N, N', N'', etc. deben coincidir con todos los *no residuos cuadráticos* positivos de n que son menores que n. Ahora, si se supone que la ecuación cuyas raíces son las sumas $(m,1)$ y (m,g) es

$$x^2 - Ax + B = 0$$

resulta

$$A = (m,1) + (m,g) = -1, \qquad B = (m,1) \cdot (m,g)$$

El producto de $(m,1)$ por (m,g) es, por el artículo 345,

$$= (m, N+1) + (m, N'+1) + (m, N''+1) + \text{ etc.} = W$$

y de ese modo se reducirá a una forma $\alpha(m,0) + \beta(m,1) + \gamma(m,g)$. Para determinar los coeficientes α, β y γ observamos *primero* que $\alpha+\beta+\gamma = m$ (porque el número de sumas en $W = m$); *segundo,* que $\beta = \gamma$ (esto sigue del artículo 350 pues el producto $(m,1) \cdot (m,g)$ es una función invariable de las sumas $(m,1)$ y (m,g) de las que se compone la suma más grande $(n-1,1)$); *tercero,* puesto que todos los números $N+1$, $N'+1$, $N''+1$, etc. están contenidos entre las cotas 2 y $n+1$, es claro que *o* ninguna suma en W puede ser reducida a $(m,0)$ y así $\alpha = 0$ cuando el número $n-1$ no se halla entre los números N, N', N'', etc. *o* que una suma, digamos (m,n) puede ser reducida a $(m,0)$ y así $\alpha = 1$ cuando $n-1$ no se halla entre los números N, N', N'', etc. En el primer caso por lo tanto se infiere $\alpha = 0$, $\beta = \gamma = \frac{1}{2}m$, en el último $\alpha = 1$, $\beta = \gamma = \frac{1}{2}(m-1)$. Ya que los números β y γ deben ser enteros, se sigue que se tendrá el primer caso, esto es, $n-1$ (o lo que es lo mismo, -1) no se encontrará entre los no residuos de n cuando m es par o n es de la forma $4k+1$. El último caso se tendrá, esto es, $n-1$ o sea -1 será un no residuo de n, siempre que m sea impar o n sea de la forma $4k+3$ *). Ahora, ya que $(m,0) = m$, $(m,1) + (m,g) = -1$, el

*) De esta forma damos una nueva demostración del teorema que dice que -1 es un residuo de todos los números primos de la forma $4k+1$ y un no residuo de todos los de la forma $4k+3$. Antes (art. 108, 109 y 262) probamos esto de varias maneras diferentes. Si es preferible asumir este teorema, no habrá necesidad de distinguir entre los dos casos porque β y γ ya serán enteros.

producto buscado será $= -\frac{1}{2}m$ en el primer caso y será $= \frac{1}{2}(m+1)$ en el último. Así la ecuación en el primer caso será $x^2 + x - \frac{1}{4}(n-1) = 0$ con raíces $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$, en el último $x^2 + x + \frac{1}{4}(n+1)$ con raíces $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$.

Sea $\mathfrak{R}$ el conjunto de todos los residuos cuadráticos positivos de n que son menores que n y sea $\mathfrak{N}$ el conjunto de todos los no residuos correspondientes. Entonces, no importa cuál raíz de Ω sea escogida por [1], la diferencia entre las sumas $\sum[\mathfrak{R}]$ y $\sum[\mathfrak{N}]$ será $= \pm\sqrt{n}$ para $n \equiv 1$ e $= \pm i\sqrt{n}$ para $n \equiv 3 \pmod 4$. Se sigue que si k es cualquier entero no divisible por n

$$\sum \cos\frac{k\mathfrak{R}P}{n} - \sum \cos\frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \quad \text{y} \quad \sum \operatorname{sen}\frac{k\mathfrak{R}P}{n} - \sum \operatorname{sen}\frac{k\mathfrak{N}P}{n} = 0$$

para $n \equiv 1 \pmod 4$. Por otra parte para $n \equiv 3 \pmod 4$ la primera diferencia será $= 0$ y la segunda $= \pm\sqrt{n}$. Estos teoremas son tan elegantes que merecen una distinción especial. Observamos que los signos superiores siempre se mantienen cuando en vez de k se toma la unidad o un residuo cuadrático de n y los inferiores cuando k es un no residuo. Estos teoremas mantienen la misma o aún mayor elegancia cuando son extendidos a valores compuestos de n. Pero estas materias están en un nivel superior de investigación y reservaremos sus consideraciones para otra ocasión.

Demostración de un teorema mencionado en Sección IV.

357.

Sea

$$z = x^m - ax^{m-1} + bx^{m-2} - \text{ etc.} = 0$$

la ecuación de grado m cuyas raíces son las m raíces contenidas en el período $(m, 1)$. Aquí $a = (m, 1)$ y cada uno de los coeficientes restantes b, etc. serán de la forma $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ con $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$, enteros (art.348). Denotando por z' la función en la que se transforma z cuando se sustituyen $(m, 1)$ por (m, g) en todas partes y (m, g) por (m, g^2), o lo que es la misma cosa $(m, 1)$, entonces las raíces de la ecuación $z' = 0$ serán las raíces contenidas en (m, g) y el producto

$$zz' = \frac{x^n - 1}{x - 1} = X$$

Por lo tanto z puede ser reducida a la forma $R + S(m, 1) + T(m, g)$ donde R, S y T serán funciones enteras de x con todos sus coeficientes enteros. Hecho esto, resulta

$$z' = R + S(m, g) + T(m, 1)$$

Y si por brevedad escribimos p y q por $(m,1)$ y (m,g) respectivamente

$$2z = 2R + (S+T)(p+q) - (T-S)(p-q) = 2R - S - T - (T-S)(p-q)$$

y similarmente

$$2z' = 2R - S - T + (T-S)(p-q)$$

así, poniendo

$$2R - S - T = Y, \qquad T - S = Z$$

resulta $4X = Y^2 - (p-q)^2 Z^2$ y ya que $(p-q)^2 = \pm n$

$$4X = Y^2 \mp nZ^2$$

El signo superior vale cuando n es de la forma $4k+1$, el inferior cuando n es de la forma $4k+3$. Este es el teorema que prometimos probar (art. 124). Es fácil ver que los dos términos de mayor grado en la función Y siempre serán $2x^m + x^{m-1}$ y el mayor en la función Z, x^{m-1}. Todos los coeficientes restantes serán enteros, variarán de acuerdo con la naturaleza del número n y no se puede dar una fórmula analítica general.

Ejemplo. Para $n = 17$, por las reglas del artículo 348, la ecuación cuyas raíces son las ocho raíces contenidas en (8,1) será

$$x^8 - px^7 + (4+p+2q)x^6 - (4p+3q)x^5 + (6+3p+5q)x^4 \\ -(4p+3q)x^3 + (4+p+2q)x^2 - px + 1 = 0$$

por lo tanto

$$R = x^8 + 4x^6 + 6x^4 + 4x^2 + 1$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + x^2 - x$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2x^2$$

y

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5x^2 + x + 2$$
$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + x$$

He aquí algunos otros ejemplos

n	Y	Z
3	$2x+1$	1
5	$2x^2+x+2$	x
7	$2x^3+x^2-x-2$	x^2+x
11	$2x^5+x^4-2x^3+2x^2-x-2$	x^4+x
13	$2x^6+x^5+4x^4-x^3+4x^2+x+2$	x^5+x^3+x
19	$2x^9+x^8-4x^7+3x^6+5x^5-5x^4$ $-3x^3+4x^2-x-2$	$x^8-x^6+x^5+x^4-x^3+x$
23	$2x^{11}+x^{10}-5x^9-8x^8-7x^7-4x^6$ $+4x^5+7x^4+8x^3+5x^2-x-2$	$x^{10}+x^9-x^7-2x^6-2x^5$ $-x^4+x^2+x$

De la ecuación que distribuye las raíces Ω en tres períodos.

358.

Procedemos ahora a la consideración de las ecuaciones cúbicas que determinan las tres sumas de $\frac{1}{3}(n-1)$ términos que componen el conjunto Ω, para el caso en que n es de la forma $3k+1$. Sea g cualquier raíz primitiva para el módulo n y $\frac{1}{3}(n-1)=m$ que será un entero par. Entonces las tres sumas que componen Ω serán $(m,1)$, (m,g) y (m,g^2), por las cuales escribimos p, p' y p'' respectivamente. Es claro que la primera contiene las raíces $[1]$, $[g^3]$, $[g^6]$, $\ldots [g^{n-4}]$, la segunda las raíces $[g]$, $[g^4]$, $\ldots [g^{n-3}]$, y la tercera las raíces $[g^2]$, $[g^5]$, $\ldots [g^{n-2}]$. Suponiendo que la ecuación buscada es

$$x^3 - Ax^2 + Bx - C = 0$$

resulta

$$A = p+p'+p'', \quad B = pp'+p'p''+pp'', \quad C = pp'p''$$

y directamente $A=-1$. Sean $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., los residuos positivos mínimos de los números g^3, g^6, $\ldots g^{n-4}$ según el módulo n, en orden arbitrario, y sea $\mathfrak{K}$ el conjunto de ellos y el número 1. Similarmente sean $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, etc. los residuos mínimos de los números g, g^4, g^7, $\ldots g^{n-3}$ y $\mathfrak{K}'$ su conjunto; finalmente sean $\mathfrak{A}''$, $\mathfrak{B}''$, $\mathfrak{C}''$, etc. los residuos mínimos de g^2, g^5, g^8, $\ldots g^{n-2}$ y $\mathfrak{K}''$ su conjunto. Así todos los números en $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$ serán diferentes y coincidirán con 1, 2, 3, $\ldots n-1$. Primero que todo, debemos observar aquí que el número $n-1$ debe estar en $\mathfrak{K}$, pues es fácil ver que es un residuo de $g^{\frac{3m}{2}}$. También sigue de esto que los dos números h, $n-h$ se encontrarán siempre en uno *mismo* de los tres conjuntos $\mathfrak{K}$, $\mathfrak{K}'$ y $\mathfrak{K}''$, porque si

uno de ellos es un residuo de la potencia g^λ, el otro será un residuo de la potencia $g^{\lambda+\frac{3m}{2}}$ o de $g^{\lambda-\frac{3m}{2}}$ si $\lambda > \frac{3m}{2}$. Denotaremos por $(\mathfrak{K}\mathfrak{K})$ el número de enteros en la serie 1, 2, 3, $\ldots n-1$ que pertenencen a $\mathfrak{K}$ por sí mismos y cuando son aumentados en una unidad; similarmente $(\mathfrak{K}\mathfrak{K}')$ será el número de enteros en la misma serie, que están ellos mismos contenidos en $\mathfrak{K}$ pero están en $\mathfrak{K}'$ cuando son aumentados en una unidad. Será inmediatamente obvio cual es el significado de las notaciones $(\mathfrak{K}\mathfrak{K}'')$, $(\mathfrak{K}'\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}')$, $(\mathfrak{K}'\mathfrak{K}'')$, $(\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}''\mathfrak{K}')$ y $(\mathfrak{K}''\mathfrak{K}'')$. Hecho esto, digo *primero* que $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$. En efecto, suponiendo que h, h', h'', etc. son todos los números de la serie 1, 2, 3, $\ldots n-1$ que están ellos mismos en $\mathfrak{K}$ pero con los próximos números mayores $h+1$, $h'+1$, $h''+1$, etc. en $\mathfrak{K}'$, de modo que por definición el número de ellos es $(\mathfrak{K}\mathfrak{K}')$, entonces es claro que todos los números $n-h-1$, $n-h'-1$, $n-h''-1$, etc. están contenidos en $\mathfrak{K}'$ y los próximos números mayores $n-h$, $n-h'$, etc. en $\mathfrak{K}$; y ya que existen $(\mathfrak{K}'\mathfrak{K})$ de tales números en total, de seguro no podemos tener $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$. Se demuestra similarmente que no es posible tener $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$, así estos números son necesariamente iguales. Exactamente de la misma manera se prueba que $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$ y $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$. *Segundo,* ya que cualquier número en $\mathfrak{K}$, con excepción del más grande, $n-1$, debe ser seguido por el siguiente mayor en $\mathfrak{K}$ o en $\mathfrak{K}'$ o en $\mathfrak{K}''$, la suma $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$ debe ser igual al número de todos los números en $\mathfrak{K}$ disminuido en una unidad, esto es $= m-1$. Por una razón similar

$$(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m$$

Con estos preliminares, por las reglas del artículo 345 desarrollaremos el producto pp' en $(m, \mathfrak{A}'+1) + (m, \mathfrak{B}'+1) + (m, \mathfrak{C}'+1) +$ etc. Esta expresión se reduce fácilmente a $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$. Por el artículo 345 se obtiene de esto el producto $p'p''$ sustituyendo $(m,1)$, (m,g) y (m,g^2) por las cantidades (m,g), (m,g^2) y (m,g^3) respectivamente, i.e., p, p' y p'' por p', p'' y p respectivamente . Así tenemos $p'p'' = (\mathfrak{K}'\mathfrak{K})p' + (\mathfrak{K}'\mathfrak{K}')p'' + (\mathfrak{K}'\mathfrak{K}'')p$ y similarmente $p''p = (\mathfrak{K}'\mathfrak{K})p'' + (\mathfrak{K}'\mathfrak{K}')p + (\mathfrak{K}'\mathfrak{K}'')p'$. De esto obtenemos *primero*

$$B = m(p + p' + p'') = -m$$

y *segundo* de una manera similar a aquélla por la cual fue desarrollado pp', se reduce también pp'' a $(\mathfrak{K}''\mathfrak{K})p + (\mathfrak{K}''\mathfrak{K}')p' + (\mathfrak{K}''\mathfrak{K}'')p''$. Y ya que esta expresión debe ser idéntica a la precedente, es necesario que $(\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}'\mathfrak{K}')$ y $(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K})$. Ahora, poniendo

$$(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}') = a$$

$$(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}') = b$$
$$(\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}'') = c$$

resulta $m-1 = (\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}\mathfrak{K}) + b + c$. Y ya que $a+b+c = m$, $(\mathfrak{K}\mathfrak{K}) = a-1$. Así las nueve cantidades desconocidas se reducen a tres a, b y c o mejor, ya que $a+b+c = m$, a dos. Finalmente, es claro que el cuadrado p^2 se convierte en $(m, 1+1) + (m, \mathfrak{A}+1) + (m, \mathfrak{B}+1) + (m, \mathfrak{C}+1) +$ etc. Entre los términos de esta expresión tenemos (m, n) que se reduce a $(m, 0)$ o sea a m, y los restantes términos se reducen a $(\mathfrak{K}\mathfrak{K})p + (\mathfrak{K}\mathfrak{K}')p' + (\mathfrak{K}\mathfrak{K}'')p''$, así $p^2 = m + (a-1)p + bp' + cp''$.

Como un resultado de las investigaciones anteriores tenemos las siguientes reducciones:

$$\begin{aligned} p^2 &= m + (a-1)p + bp' + cp'' \\ pp' &= bp + cp' + ap'' \\ pp'' &= cp + ap' + bp'' \\ p'p'' &= ap + bp' + cp'' \end{aligned}$$

donde las tres incógnitas satisfacen la ecuación condicional

$$a+b+c = m \qquad (I)$$

y por otra parte es cierto que estos números son enteros. Como una consecuencia tenemos

$$\begin{aligned} C = p \cdot p'p'' &= ap^2 + bpp' + cpp'' \\ &= am + (a^2+b^2+c^2-a)p + (ab+bc+ac)p' + (ab+bc+ac)p'' \end{aligned}$$

Pero ya que $pp'p''$ es una función invariable de p, p' y p'', los coeficientes por los que ellos son multiplicados en la expresión precedente son necesariamente iguales (art. 350) y hay una nueva ecuación

$$a^2+b^2+c^2-a = ab+bc+ac \qquad (II)$$

y de ésta $C = am + (ab+bc+ac)(p+p'+p'')$ o (causa de (I) y por el hecho que $p+p'+p'' = -1$)

$$C = a^2 - bc \qquad (III)$$

Ahora, aún cuando C depende de tres incógnitas y existen solamente dos ecuaciones, no obstante con la ayuda de la condición de que a, b y c son enteros, ellos serán

suficientes para determinar C completamente. Para demostrar esto, expresamos la ecuación (II) como

$$12a + 12b + 12c + 4 = 36a^2 + 36b^2 + 36c^2 - 36ab - 36ac - 36bc - 24a + 12b + 12c + 4$$

Por (I), el lado izquierdo se convierte en $= 12m + 4 = 4n$. El lado derecho se reduce a

$$(6a - 3b - 3c - 2)^2 + 27(b - c)^2$$

o, escribiendo k en vez de $2a - b - c$, a $(3k-2)^2 + 27(b-c)^2$. Así el número $4n$ (i.e. el cuádruple de cualquier número primo de la forma $3m+1$) puede ser representado por la forma $x^2 + 27y^2$. Esto puede, por supuesto, deducirse sin ninguna dificultad de la teoría general de formas binarias, pero es notable que tal descomposición está ligada a los valores de a, b y c. Ahora, el número $4n$ siempre puede ser descompuesto de una única manera en la suma de un cuadrado y 27 veces otro cuadrado. Demostraremos esto como sigue *). Si se supone que

$$4n = t^2 + 27u^2 = t'^2 + 27u'^2$$

tenemos *primero*

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16n^2$$

segundo

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16n^2$$

tercero

$$(tu' + t'u)(tu' - t'u) = 4n(u'^2 - u^2)$$

De esta tercera ecuación se sigue que n, por ser un número primo, divide uno de los números $tu' + t'u$, $tu' - t'u$. De la primera y segunda, sin embargo, es claro que cada uno de estos números es menor que n, así al que n divide es necesariamente $= 0$. Por lo tanto $u'^2 - u^2 = 0$ y $u'^2 = u^2$ y $t'^2 = t^2$; i.e. las dos descomposiciones no son diferentes. Supongamos ahora que se conoce la descomposición de $4n$ en un cuadrado más 27 veces un cuadrado (esto se puede hacer por el método directo de la sección V o por el método indirecto de los art. 323 y 324). Si $4n = M^2 + 27N^2$, los cuadrados $(3k-2)^2$ y $(b-c)^2$ estarán determinados y tendremos dos ecuaciones

*) Esta proposición puede probarse mucho más directamente a partir de los principios de la sección V.

en lugar de la ecuación (II). Pero claramente no solo estará determinado el cuadrado $(3k-2)^2$ sino también su raíz $3k-2$. Porque debe ser $= +M$ o $= -M$, la ambigüedad es fácilmente eliminada, pues ya que k debe ser un entero, resulta $3k-2 = +M$ o $= -M$ de acuerdo con que M sea de la forma $3z+1$ o $3z+2$ *). Ahora, puesto que $k = 2a-b-c = 3a-m$, resulta $a = \frac{1}{3}(m+k)$, $b+c = m-a = \frac{1}{3}(2m-k)$ y así

$$\begin{aligned} C = a^2 - bc &= a^2 - \frac{1}{4}(b+c)^2 + \frac{1}{4}(b-c)^2 \\ &= \frac{1}{9}(m+k)^2 - \frac{1}{36}(2m-k)^2 + \frac{1}{4}N^2 = \frac{1}{12}k^2 + \frac{1}{3}km + \frac{1}{4}N^2 \end{aligned}$$

y entonces se han encontrado todos los coeficientes de la ecuación. *Q. E. F.* Esta fórmula será mucho más simple si sustituimos N^2 por sus valores de la ecuación $(3k-2)^2 + 27N^2 = 4n = 12m+4$. Después del cálculo obtenemos

$$C = \frac{1}{9}(m+k+3km) = \frac{1}{9}(m+kn)$$

El mismo valor puede ser reducido a $(3k-2)N^2 + k^3 - 2k^2 + k - km + m$. Aunque esta expresión es menos útil, muestra inmediatamente que C resulta ser un entero, como debería.

Ejemplo. Para $n = 19$ tenemos $4n = 49 + 27$, así $3k-2 = +7$, $k = 3$, $C = \frac{1}{9}(6+57) = 7$ y la ecuación buscada es $x^3 + x^2 - 6x - 7 = 0$, como antes (art. 351). Similarmente, para $n = 7$, 13, 31, 37, 43, 61 y 67 el valor de k es respectivamente 1, -1, 2, -3, -2, 1, -1 y $C = 1$, -1, 8, -11, -8, 9, -5.

Aunque el problema que hemos resuelto en este artículo es bastante intrincado, no hemos querido omitirlo a causa de la elegancia de la solución y porque da ocasión para usar varios artificios que son fructíferos también en otras discusiones †).

---

*) Evidentemente M no puede ser de la forma $3z$ por que, de lo contrario, sería divisible por 3. Con respecto a la ambigüedad de si $b-c$ debe ser $= N$ o $= -N$, es innecesario considerar la cuestión aquí, y por la naturaleza del caso no se puede determinar porque depende de la elección de la raíz primitiva g. Para algunas raíces primitivas la diferencia $b-c$ será positiva y para otras será negativa.

†) Corolario. Sea ε una raíz de la ecuación $x^3 - 1 = 0$. Tendremos $(p + \varepsilon p' + \varepsilon^2 p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$. Sean $\frac{M}{\sqrt{4n}} = \cos\varphi$ y $\frac{N\sqrt{27}}{\sqrt{4n}} = \operatorname{sen}\varphi$ y como resultado

$$p = -\frac{1}{3} + \frac{2}{3}\cos\frac{1}{3}\varphi\sqrt{n} \quad ; \quad M \equiv +1 \pmod 3 \quad ; \quad 1 \equiv M(1\cdot 2\cdot 3\ldots m)^3 \pmod n$$

Si se hace $3x+1 = y$, entonces resulta $y^3 - 3ny - Mn = 0$.