Sección Tercera

SOBRE

RESIDUOS DE LAS POTENCIAS

Los residuos de los términos de una progresión geométrica que comienza desde la unidad constituyen una serie periódica.

45.

TEOREMA. *En toda progresión geométrica 1, a, a^2, a^3, etc., aparte del primer término, se da además otro término a^t, congruente a la unidad, según el módulo p, que es primo a a, cuyo exponente es $t < p$.*

Demostración. Puesto que el módulo p es primo a a, y por lo tanto es primo a cualquier potencia de a, ningún término de la progresión será $\equiv 0 \pmod{p}$, sino que cada uno será congruente a uno de los números 1, 2, 3, $\ldots p-1$. De éstos, hay $p-1$, pues, es evidente que si se considerasen más que $p-1$ términos de la progresión, no todos pueden tener diferentes residuos mínimos. Entonces, entre los términos 1, a, a^2, a^3, $\ldots a^{p-1}$, se encontrarán al menos dos congruentes a un residuo mínimo. Sea pues, $a^m \equiv a^n$ y $m > n$, y al dividir por a^n, resultará $a^{m-n} \equiv 1$ (art. 22), donde $m - n < p$, y > 0. *Q. E. D.*

Ejemplo. En la progresión 2, 4, 8, etc., el primer término que es congruente a la unidad, según el módulo 13, resulta ser $2^{12} = 4096$. Pero, según el módulo 23, en esta progresión es $2^{11} = 2048 \equiv 1$. Igualmente, 15625, la sexta potencia del número 5, es congruente a la unidad, según el módulo 7, la quinta de ella, 3125, según el módulo 11. Por tanto, en unos casos la potencia congruente a la unidad resulta menor que $p - 1$. Pero, en otros, es necesario ascender hasta la $(p-1)$-ésima potencia.

46.

Cuando se continúa una progresión más allá de un término que es congruente a la unidad, se producen nuevamente los mismos residuos que se tienen al principio. Es claro que si $a^t \equiv 1$, se tendrá $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$, etc., hasta que se encuentre el término a^{2t} cuyo residuo menor otra vez será $\equiv 1$, y el período de los residuos comenzará de nuevo. Se tiene, pues, un período que comprende t residuos, que en cuanto finaliza se vuelve a repetir desde el comienzo; y ningún otro residuo, salvo aquéllos contenidos en este período, puede aparecer en toda la progresión.

En general, será $a^{mt} \equiv 1$, y $a^{mt+n} \equiv a^n$, lo cual en nuestra notación se presenta así:

Si $r \equiv \rho \pmod{t}$, *será* $a^r \equiv a^\rho \pmod{p}$.

47.

De este teorema, se gana un método para encontrar muy fácilmente los residuos de potencias, tan grandes como sean sus exponentes, una vez que se encuentra una potencia congruente a la unidad. Si, por ejemplo, se busca el residuo resultante de la división de la potencia 3^{1000} por 13, será $3^3 \equiv 1 \pmod{13}$, $t = 3$; como $1000 \equiv 1 \pmod{3}$, será $3^{1000} \equiv 3 \pmod{13}$.

48.

Cuando a^t es la menor potencia congruente a la unidad (excepto $a^0 = 1$, tal caso no será tratado aquí), los t términos que constituyen un período de residuos serán todos diferentes, como se puede ver con facilidad de la demostración del art. 45. Entonces, también la proposición del art. 46 puede invertirse; esto es, si $a^m \equiv a^n \pmod{p}$, será $m \equiv n \pmod{t}$. Pues, si m y n fueran incongruentes según el módulo t, sus residuos mínimos μ, ν serían diferentes. Pero, $a^\mu \equiv a^m$ y $a^\nu \equiv a^n$, así pues $a^\mu \equiv a^\nu$, i.e., no todas las potencias menores que a^t son incongruentes, contra la hipótesis.

Si $a^k \equiv 1 \pmod{p}$, entonces será $k \equiv 0 \pmod{t}$, i.e., k será divisible por t.

Hasta aquí hemos hablado de módulos cualesquiera, primos a a. Ahora, trataremos por aparte los módulos que son números absolutamente primos y luego desarrollaremos una investigación más general con esta base.

Se consideran primero los módulos que son números primos.

49.

TEOREMA. *Si p es un número primo que no divide a a, y si a^t es la menor potencia de a congruente a la unidad, según el módulo p, el exponente t será $= p-1$, o será un factor de este número.*

Consúltese los ejemplos del art. 45.

Demostración. Puesto que ya hemos demostrado que t es $= p-1$ o $< p-1$, falta que, en el segundo caso, se demuestre que t siempre es un factor de $p-1$.

I. Reúnanse los menores residuos positivos de todos estos términos 1, a, a^2, $\ldots a^{t-1}$, que se denotarán por α, α', α'', etc., de modo que sea $\alpha = 1$, $\alpha' \equiv a$, $\alpha'' \equiv a^2$, etc. Se ha visto que todos son diferentes; pues, si dos términos a^m y a^n tuvieran el mismo residuo, (al suponer $m > n$) sería $a^{m-n} \equiv 1$, no obstante que $m - n < t$. Q.E.A., puesto que ninguna potencia inferior a a^t es congruente a la unidad (por hipótesis). Además, todos los α, α', α'', etc. están contenidos en la sucesión de números 1, 2, 3, $\ldots p-1$ que, sin embargo, no se agotan pues $t < p-1$. Denotaremos el conjunto de todos α, α', α'', etc. con (A). Por tanto, (A) contiene t términos.

II. Tómese un número cualquiera β entre 1, 2, 3, $\ldots p-1$ que falte en (A) . Multiplíquese β por todos los α, α', α'', etc. Sean β, β', β'', etc. los residuos menores originados de allí cuyo número será t. Pero estos residuos serán diferentes entre sí y además diferentes de α, α', α'', etc. Si la primera aserción fuera falsa, se tendría $\beta a^m \equiv \beta a^n$, dividiendo por β, $a^m \equiv a^n$, contra lo que hemos demostrado. Si la segunda fuera falsa, se tendría $\beta a^m \equiv a^n$. Por tanto, cuando $m < n$, $\beta \equiv a^{n-m}$, i.e., β sería congruente con uno de éstos α, α', α'', etc. contra la hipótesis; cuando vale $m > n$, al multiplicar por a^{t-m}, $\beta a^t \equiv a^{t+n-m}$, o por medio de $a^t \equiv 1$, $\beta \equiv a^{t+n-m}$, lo cual es un absurdo. Denótese el conjunto de todos los β, β', β'', etc., cuyo número $= t$ con (B) y se tiene ya $2t$ números de 1, 2, 3, $\ldots p-1$. Por tanto, y si (A) y (B) comprenden todos estos números, se tiene $\frac{p-1}{2} = t$. Así el teorema se ha demostrado.

III. Si todavía quedan algunos, sea γ uno de ellos. Multiplíquense por él todos α, α', α'', etc. y sean γ, γ', γ'', etc. los residuos mínimos de los productos y denótese el conjunto de todos ellos con (C). Por tanto, (C) comprende t números de 1, 2, 3, $\ldots p-1$, que son todos diferentes entre sí, y diferentes de los contenidos en (A) y (B). Las primeras aserciones se demuestran de igual modo como en el II, la tercera como sigue: si fuera $\gamma a^m \equiv \beta a^n$, sería $\gamma \equiv \beta a^{n-m}$, ó $\equiv \beta a^{t+n-m}$ según que $m < n$ ó $> n$, y en cualquier caso γ sería congruente a un número de (B) contra

la hipótesis. Por tanto, se tienen $3t$ números de 1, 2, 3, $\ldots p-1$ y si no faltan más resulta $t = \frac{p-1}{3}$ y así el teorema quedará demostrado.

IV. Si faltan todavía otros, del mismo se habrá de proceder a un cuarto conjunto (D) de números, etc. Pero, es evidente, puesto que el número de enteros 1, 2, 3, $\ldots p-1$ es finito, que al fin se habrán de agotar todos ellos, y que será un múltiplo de t: por eso t será algún factor del número $p-1$. *Q. E. D.*

El teorema de Fermat.

50.

Así, puesto que $\frac{p-1}{t}$ es un entero, resulta al elevarse ambas partes de la congruencia $a^t \equiv 1$ a la potencia $\frac{p-1}{t}$, $a^{p-1} \equiv 1$ *ó sea* $a^{p-1} - 1$ *siempre es divisible por* p*, cuando* p *es un primo que no divide a* a*.*

Este teorema, el cual ya sea por su elegancia o por su gran utilidad es digno de toda atención, suele llamarse el *teorema de Fermat,* por su inventor. (Véase Fermat, *Opera Matem.*, Toulouse 1679, p. 163). El inventor no presentó una demostración, sin embargo afirmó tener una en su poder. El gran Euler fue el primero que publicó una demostración, en su disertación titulada *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T.* VIII.*) Se basa ésta en el desarrollo de la potencia $(a+1)^p$, donde se deduce fácilmente de la forma de los coeficientes, que $(a+1)^p - a^p - 1$ siempre será divisible por p cuando $a^p - a$ es divisible por p. Ahora, como $1^p - 1$ siempre es divisible por p, también $2^p - 2$ lo será siempre, por tanto también $3^p - 3$, y en general $a^p - a$. Y si p no divide a a, tampoco $a^{p-1} - 1$ será divisible por p. Esto basta para aclarar la idea del método. El gran Lambert presentó una demostración parecida en *Actis Erudit,* 1769, p. 109. Porque se veía que el desarrollo de una potencia binomia era bastante ajeno de la teoría de los números, el gran Euler buscó otra demostración que aparece en *Comment. nov. Petr. T.* VII p. 70, y que está en armonía con lo que expusimos en el artículo anterior. Además, en lo siguiente, se nos ofrecerán otras demostraciones. En este lugar, se permite añadir otra más, la cual se basa en principios semejantes a los de la primera del gran Euler.

*) En un comentario anterior, el gran hombre todavía no había logrado su propósito. *Comm. Petr. T.* VI p. 106.— En una controversia famosa entre Maupertuis y König, surgida sobre el principio de la acción mínima, aunque muy pronto llevó a una variedad de cosas, König afirmó tener en su poder una carta de Leibniz, en la cual está contenida una demostración de este teorema que concuerda con la primera de Euler. *Appel au public.* p. 106. No queremos negar la veracidad de este testimonio, ciertamente Leibniz nunca publicó su hallazgo. Vea *Hist. de l'Ac. de Prusse,* 1750 p. 530.

La siguiente proposición, de la cual un caso especial es nuestro teorema, también será útil para otras investigaciones.

51.

La p-ésima potencia del polinomio $a + b + c +$ etc. es

$$\equiv a^p + b^p + c^p + \text{ etc.}$$

según el módulo p siempre que p sea un número primo.

Demostración. Es evidente que la p-ésima potencia del polinomio $a + b + c +$ etc. está compuesta de términos de la forma $\chi a^\alpha b^\beta c^\gamma$ etc., donde $\alpha + \beta + \gamma +$ etc. $= p$, y χ denota en cuántas maneras p objetos pueden permutarse cuando α, β, γ, etc. de ellas son respectivamente iguales a a, b, c, etc. Pero, antes, en el artículo 41, mostramos que este número siempre es divisible por p, si todos los objetos no son iguales, i.e., si no es que uno de los números α, β, γ, etc. $= p$ y los demás $= 0$. De esto se sigue que todos los términos de $(a + b + c +$ etc.$)^p$, excepto a^p, b^p, c^p, etc., son divisibles por p; por tanto, cuando se trata la congruencia según el módulo p, pueden omitirse todos ellos, y será

$$(a + b + c + \text{ etc.})^p \equiv a^p + b^p + c^p + \text{ etc.} \qquad \text{Q.E.D}$$

Ahora si se ponen todas las cantidades a, b, c, etc. $= 1$ y el número de ellas es $= k$, tendremos $k^p \equiv k$, como en el artículo anterior.

Cuantos números corresponden a un período,
en el cual el número de términos es un divisor dado del número $p - 1$.

52.

Dado que otros números, que no sean divisores del número $p - 1$, no pueden ser los exponentes de las potencias menores congruentes a la unidad, se plantea el problema de si todos los divisores de $p - 1$ disfrutan de esta propiedad, y cuando se clasifican todos estos números no divisibles por p, según el exponente de su potencia menor congruente a la unidad, ¿cuántos de ellos se encuentran para cada uno de los exponentes? Primero conviene observar que basta considerar todos los números positivos de 1 hasta $p - 1$; pues, es evidente que los números congruentes deben

elevarse a una misma potencia para que sean congruentes a la unidad, y por tanto, un número cualquiera debe referirse al mismo exponente al que su residuo menor se refiere. Por consiguiente, tenemos que dedicarnos a hallar cómo, con respecto a esto, se han distribuido los números 1, 2, 3, $\dots p-1$ entre los factores individuales del número $p-1$. Por brevedad, si d es uno de los divisores del número $p-1$ (entre los que también se incluyen 1 y $p-1$) por medio de ψd denotaremos el número de enteros positivos menores que p mismo, cuya d-ésima potencia es la menor congruente a la unidad.

53.

Para que esta investigación pueda entenderse fácilmente, agregamos un ejemplo. Para $p = 19$, los números 1, 2, 3, $\dots 18$ se distribuirán entre los divisores del número 18, de este modo

1	1
2	18
3	7, 11
6	8, 12
9	4, 5, 6, 9, 16, 17
18	2, 3, 10, 13, 14, 15

Por tanto, en este caso, $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, y $\psi 18 = 6$. Un poco de atención enseña que tantos números pertenecen a cualquier exponente como tantos se dan no mayores que él y primos a él, o que en este caso particular, usando la notación del art. 39, $\psi d = \varphi d$. Ahora demostraremos que esta observación es verdadera en general.

I. Si se tiene algún número a *perteneciente* al exponente d (i.e., cuya d-ésima potencia es congruente a la unidad y todas sus potencias inferiores son incongruentes), todas sus potencias a^2, a^3, a^4, $\dots a^d$, o los menores restos de ellas, poseerán también la primera propiedad (la d-ésima potencia de ellas es congruente a la unidad) y puesto que esto puede expresarse diciendo que todos los residuos mínimos de los números a, a^2, a^3, $\dots a^d$ (que son todos diferentes) son raíces de la congruencia $x^d \equiv 1$ y como ésta no puede tener más que d raíces diferentes, es evidente que, excepto los residuos mínimos de los números a, a^2, a^3, $\dots a^d$, no se presenta ningún otro entre los números de 1 a $p-1$ inclusive, cuya d-ésima potencia sea congruente a la unidad. De donde,

es claro que todos los números pertenecientes al exponente d se encuentran entre los residuos mínimos de los números a, a^2, a^3, $\ldots a^d$. Cuáles son y cuántos son ellos, se encontrará como sigue. Si k es un número primo a d, todas las potencias de a^k, cuyos exponentes son $< d$, no serán congruentes a la unidad; pues, sea $\frac{1}{k} \pmod{d} \equiv m$ (ver art. 31), será $a^{km} \equiv a$, por tanto, si la e-ésima potencia de a^k fuera congruente a la unidad y $e < d$, entonces, resultaría $a^{kme} \equiv 1$, y de aquí $a^e \equiv 1$, contrario a la hipótesis. Por eso, es claro que el residuo mínimo de a^k pertenece al exponente d. Si k tiene algún divisor δ común con d, el residuo mínimo de a^k no pertenecerá al exponente d, pues, además la $\frac{d}{\delta}$-ésima potencia es congruente a la unidad (pues, $\frac{kd}{\delta}$ sería divisible por d, o sea $\equiv 0 \pmod{d}$ y por ende $a^{\frac{k\delta}{d}} \equiv 1$). Por consiguiente, se reúnen tantos números pertenecientes al exponente d como números de 1, 2, 3, $\ldots d$ que sean primos a d. Pero, debe recordarse que esta conclusión está basada en la suposición de que ya se tiene un número a perteneciente al exponente d. Por lo cual queda la duda de si es posible que ningún número pertenezca del todo a algún exponente y la conclusión se limita a que ψd sea $= 0$ ó $= \varphi d$.

54.

II. Ahora sean d, d', d'', etc. todos los divisores del número $p-1$: como todos los números 1, 2, 3, $\ldots p-1$ están distribuidos entre éstos,

$$\psi d + \psi d' + \psi d'' + \text{ etc.} = p - 1$$

Pero, en el art. 40, hemos demostrado que

$$\varphi d + \varphi d' + \varphi d'' + \text{ etc.} = p - 1$$

y del artículo anterior, se sigue que ψd es igual o menor que φd, pero no puede ser mayor; de modo semejante para $\psi d'$ y $\varphi d'$, etc., por lo tanto, si algún término (o varios) de ψd, $\psi d'$, $\psi d''$, etc., fuera menor que el término correspondiente de φd, $\varphi d'$, $\varphi d''$, la suma de aquéllos no podría ser igual a la suma de éstos. De esto concluimos que ψd *siempre es igual a* φd, y por eso no depende de la magnitud de $p - 1$.

55.

Un caso particular del artículo anterior merece muchísima atención, a saber, *siempre se presentan números de los cuales ninguna potencia menor que la* $(p-1)$*-ésima es congruente a la unidad,* y hay tantos de ellos entre 1 y $p-1$ como números

menores que $p-1$ y primos a $p-1$. Puesto que la demostración de este teorema no es tan obvia como puede parecer a primera vista, y por la importancia del propio teorema, se puede añadir aquí otra bastante diferente de la anterior; ya que una diversidad de métodos suele ayudar mucho a esclarecer asuntos bastante dudosos. Resuélvase $p-1$ en sus factores primos, de modo que $p-1 = a^\alpha b^\beta c^\gamma$ etc., donde a, b, c, etc. denotan números primos diferentes. Entonces, complementaremos la demostración de este teorema por medio de lo siguiente:

I. Siempre puede encontrarse un número A (o varios) pertenecientes al exponente a^α, e igualmente números B, C, etc., pertenecientes respectivamente a los exponentes b^β, c^γ, etc.

II. El producto de todos los números A, B, C, etc. (o el producto de sus residuos mínimos) pertenece al exponente $p-1$. Esto lo demostramos así:

I. Sea g algún número de 1, 2, 3, $\ldots p-1$ que *no* satisface la congruencia $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$. Como es de grado $< p-1$, todos estos números no pueden satisfacerla. Entonces, digo que si se pone $= h$ la $\frac{p-1}{a^\alpha}$-ésima potencia de g, este número o su residuo mínimo pertenecerá al exponente a^α.

Pues, es evidente que la potencia a^α-ésima de h será congruente a la $(p-1)$-ésima de g, i.e., a la unidad. Pero, la $a^{\alpha-1}$-ésima potencia de h será congruente a la $\frac{p-1}{a}$-ésima potencia de g, i.e., será no congruente a la unidad, y mucho menos las $a^{\alpha-2}$, $a^{\alpha-3}$, etc. potencias de h pueden ser congruentes a la unidad. Pero, el exponente de la potencia menor de h congruente a la unidad, o el exponente al cual pertenece h debe dividir al número a^α (art. 48). Por lo tanto, puesto que a^α no es divisible por ningún otro número más que por sí mismo y por las potencias menores de a, necesariamente a^α será el exponente al cual pertenece h. *Q. E. D.* Con un método similar se demuestra que existen números que pertenecen a los exponentes b^β, c^γ, etc.

II. Si suponemos que el producto de todos los A, B, C, etc. no pertenece al exponente $p-1$, sino a uno menor t , $p-1$ se dividirá por t (artículo 48), es decir, $\frac{p-1}{t}$ será un entero mayor que la unidad. Sin embargo, con facilidad se ve que este coeficiente o es uno de los números primos a, b, c, etc., o al menos es divisible por uno de ellos (artículo 17), e.g., por a. Con respecto a los otros, la demostración es igual. Así, t dividirá a $\frac{p-1}{a}$; por tanto, el producto ABC etc., elevado a la $\frac{p-1}{a}$-ésima potencia será congruente a la unidad (artículo 46). Pero, es claro que cada uno de los B, C, etc. (excepto A) elevados a la $\frac{p-1}{a}$-ésima potencia serán congruentes a la unidad, cuando los exponentes b^β, c^γ, etc. a los cuales pertenecen dividan a $\frac{p-1}{a}$. Por

eso se tendrá

$$A^{\frac{p-1}{a}} B^{\frac{p-1}{a}} C^{\frac{p-1}{a}} \text{ etc.} \equiv A^{\frac{p-1}{a}} \equiv 1$$

De donde sigue que el exponente, al cual pertenece A, debe dividir a $\frac{p-1}{a}$ (art. 48), i.e., $\frac{p-1}{a^{\alpha+1}}$ es entero; pero $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \text{ etc.}}{a}$ no puede ser un número entero (art. 15). Finalmente, hay que concluir que nuestra suposición no puede afirmarse, i.e., el producto ABC etc., en realidad, pertenece al exponente $p-1$. *Q. E. D.*

La segunda demostración parece algo más larga que la primera, pero la primera resulta menos directa que ésta.

56.

Este teorema suministra un ejemplo notable sobre cuánta circunspección se requiere siempre en la teoría de los números, para que no supongamos como cierto lo que no es. El célebre Lambert en su disertación citada arriba, *Acta Erudit.* 1769, p. 127, hace mención a esta proposición, pero no atestigua necesidad alguna de una demostración. Nadie ha intentado una demostración excepto Euler, *Comment. nov. Ac. Petrop. T.* XVIII, 1773, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* p. 85 y siguientes. Véase en particular su artículo 37 donde habló bastante sobre la necesidad de una demostración. Pero, la demostración que el docto hombre presentó tiene dos defectos. Uno: en su art. 31, tácitamente supone que la congruencia $x^n \equiv 1$ (traducidos sus argumentos usando nuestra notación) en realidad tiene n raíces diferentes, aunque, sólo había demostrado anteriormente que no puede tener más que n raíces. Otro: dedujo la fórmula de su artículo 34 sólo por inducción.

Raíces primitivas, bases e índices.

57.

Como el ilustre Euler, llamaremos *raíces primitivas* a los números pertenecientes al exponente $p-1$. Por lo tanto, si a es una raíz primitiva, los residuos mínimos de las potencias a, a^2, a^3, $\ldots a^{p-1}$ serán todos diferentes, de donde se deduce fácilmente que entre éstos deben aparecer todos los números 1, 2, 3, $\ldots p-1$, ya que el número de éstos es igual al número de residuos mínimos, i.e., cualquier número no divisible por p es congruente a alguna potencia de a. Esta propiedad notable es de gran utilidad y puede simplificar bastante las operaciones aritméticas respecto a las

congruencias, casi de igual modo como la introducción de los logaritmos simplifica las operaciones de la aritmética común. Elegiremos libremente alguna raíz primitiva como *base,* a la cual referiremos todos los números no divisibles por p, y si $a^e \equiv b \pmod{p}$, llamaremos a e el *índice* de b. Por ejemplo, si para el módulo 19 se toma la raíz primitiva 2 como base, corresponderán

números	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18.
índices	0. 1. 13. 2. 16. 14. 6. 3. 8. 17. 12. 15. 5. 7. 11. 4. 10. 9.

Es claro, además, al mantener la base constante, que a cada número corresponden varios índices, pero todos ellos serán congruentes según el módulo $p-1$. Por lo que, cuando hay una discusión sobre los índices, aquéllos que son congruentes según el módulo $p-1$ se considerarán equivalentes de la misma manera como los números se consideran equivalentes cuando son congruentes según el módulo p.

Algoritmos de los índices.

58.

Los teoremas que tratan sobre los índices son completamente análogos a los que se refieren a los logaritmos.

El índice del producto compuesto de cualquier número de factores es congruente, según el módulo $p-1$, a la suma de los índices de los factores individuales.

El índice de la potencia de un número cualquiera es congruente, según el módulo $p-1$, al producto del índice del número dado por el exponente de la potencia.

Hemos omitido las demostraciones por su facilidad.

De esto se percibe que si deseamos construir una tabla de la cual se puedan sacar los índices de todos los números según módulos diferentes, de ésta se pueden omitir tanto todos los números mayores al módulo como todos los compuestos. Se ha agregado un ejemplo de este tipo de tabla al final de esta obra, *Tab. I,* donde en la primera columna vertical se colocan los números primos y las potencias de números primos de 3 hasta 97, los cuales se deben considerar como módulos. A la par de éstos están los números tomados como base. Luego siguen los índices de los números primos sucesivos que siempre están arreglados en pequeños bloques de cinco. Arriba los números primos están dispuestos en el mismo orden; de modo que un índice que corresponda a un número primo dado, según un módulo dado, pueda encontrarse fácilmente.

Así por ejemplo si $p = 67$; el índice del número 60, tomado 12 como base, será

$$\equiv 2\,\text{Ind.}\,2 + \text{Ind.}\,3 + \text{Ind.}\,5 \pmod{66} \equiv 58 + 9 + 39 \equiv 40.$$

59.

El índice de un valor cualquiera de la expresión $\frac{a}{b} \pmod{p}$, *(art. 31) es congruente, según el módulo* $p-1$, *a la diferencia de los índices del numerador* a *y del denominador* b, *si es que* a *y* b *no son divisibles por* p.

Sea c, pues, un valor cualquiera; tenemos $bc \equiv a \pmod{p}$ y por lo tanto

$$\text{Ind.}\,b + \text{Ind.}\,c \equiv \text{Ind.}\,a \pmod{p-1}$$

y así

$$\text{Ind.}\,c \equiv \text{Ind.}\,a - \text{Ind.}\,b$$

Entonces, si se tiene una tabla con el índice que corresponde a cualquier número, según cualquier módulo primo, y otra de la cual pueda derivarse el número que corresponda a un índice dado, todas las congruencias de primer grado podrán resolverse muy fácilmente; puesto que todas pueden reducirse a aquéllas cuyo módulo es un primo (art. 30). E.g., la congruenca propuesta

$$29x + 7 \equiv 0 \pmod{47} \qquad \text{será} \qquad x \equiv \frac{-7}{29} \pmod{47}$$

De donde $\text{Ind.}\,x \equiv \text{Ind.}\,-7 - \text{Ind.}\,29 \equiv \text{Ind.}\,40 - \text{Ind.}\,29 \equiv 15 - 43 \equiv 18 \pmod{46}$

Pero, se encuentra el número 3 cuyo índice es 18. Así, $x \equiv 3 \pmod{47}$. No hemos adjuntado la segunda tabla; pero, a cambio de esto, podrá servir otra en su lugar, como mostraremos en la Sección VI.

Sobre las raíces de la congruencia $x^n \equiv A$.

60.

De una manera semejante a como hemos designado en el art. 31 las raíces de las congruencias del primer grado, así, en lo siguiente, presentaremos las raíces de las congruencias puras de grados mayores con un símbolo. Como $\sqrt[n]{A}$ no puede significar más que una raíz de la ecuación $x^n = A$, así al adjuntarse el módulo con el símbolo $\sqrt[n]{A} \pmod{p}$ se denotará cualquier raíz B de la congruencia $x^n \equiv A \pmod{p}$. Decimos que esta expresión $\sqrt[n]{A} \pmod{p}$ tiene tantos valores como

raíces incongruentes mód. p, puesto que todos los que son congruentes según el módulo p se consideran como equivalentes (art. 26). Además, es claro que si A y B son congruentes, según el módulo p las expresiones $\sqrt[n]{A}$ y $\sqrt[n]{B}$ (mod. p) serán equivalentes.

Ahora, si se pone $\sqrt[n]{A} \equiv x \pmod{p}$, será $n \operatorname{Ind}. x \equiv \operatorname{Ind}. A \pmod{p-1}$. De esta congruencia, se deducen, según las reglas de la sección anterior, los valores de $\operatorname{Ind}. x$, y de éstos, los valores correspondientes de x. Fácilmente, se percibe que x tiene tantos valores como raíces de la congruencia $n \operatorname{Ind}. x \equiv \operatorname{Ind}. A \pmod{p-1}$. Es claro, pues, que $\sqrt[n]{A}$ tendrá un único valor, cuando n es primo a $p-1$; sin embargo, cuando los números n y $p-1$ tienen un máximo común divisor δ, $\operatorname{Ind}. x$ tendrá δ valores incongruentes según el módulo $p-1$, y $\sqrt[n]{A}$ tantos valores incongrentes, según p, siempre que $\operatorname{Ind}. A$ sea divisible por δ. Al faltar esta condición, $\sqrt[n]{A}$ no tendrá ningún valor real.

Ejemplo. Búsquense los valores de la expresión $\sqrt[15]{11}$ (mod. 19). Así, debe resolverse la congruencia $15 \operatorname{Ind}. x \equiv \operatorname{Ind}. 11 \equiv 6 \pmod{18}$ y se encontrarán tres valores de $\operatorname{Ind}. x \equiv 4,\ 10,\ 16 \pmod{18}$. Los valores correspondientes de x son 6, 9 y 4.

61.

Por más fácil que este método sea, cuando están adjuntadas las tablas necesarias, no debemos olvidarnos de que éste es indirecto. Por lo tanto, vale la pena investigar cuán poderosos son los métodos directos; trataremos aquí lo que pueda resultar de lo anterior; otros que requieren consideraciones más profundas están reservados para la sección VIII. Iniciamos con el caso más sencillo, donde $A = 1$, es decir, donde se buscan las raíces de la congruencia $x^n \equiv 1 \pmod{p}$. Aquí, por tanto, tomando cualquier raíz primitiva como base, debe resultar $n \operatorname{Ind}. x \equiv 0 \pmod{p-1}$. Esta congruencia, cuando n es primo a $p-1$, tendrá una sola raíz; es decir, $\operatorname{Ind}. x \equiv 0 \pmod{p-1}$. *En este caso* $\sqrt[n]{1} \pmod{p}$ tendrá un único valor, o sea $\equiv 1$. Sin embargo, cuando los números n y $p-1$ tengan máximo común divisor δ, la solución completa de la congruencia $n \operatorname{Ind}. x \equiv 0 \pmod{p-1}$ será $\operatorname{Ind}. x \equiv 0 \pmod{\frac{p-1}{\delta}}$ (ver art. 29): i.e., $\operatorname{Ind}. x$, según el módulo $p-1$, deberá ser congruente a alguno de estos números

$$0, \quad \frac{p-1}{\delta}, \quad \frac{2(p-1)}{\delta}, \quad \frac{3(p-1)}{\delta}, \quad \ldots \frac{(\delta-1)(p-1)}{\delta}$$

o tendrá δ valores incongruentes según el módulo $p-1$, por tanto, también en este caso, x tendrá δ valores diferentes (incongruentes según el módulo p). De donde se percibe que la expresión $\sqrt[\delta]{1}$ también tiene δ valores diferentes, cuyos índices coinciden completamente con los anteriores. Por eso, la expresión $\sqrt[\delta]{1} \pmod p$ equivale totalmente a $\sqrt[n]{1} \pmod p$; i.e., la congruencia $x^\delta \equiv 1 \pmod p$ tiene las mismas raíces que ésta, $x^n \equiv 1 \pmod p$. La anterior, sin embargo, será de grado inferior, si δ y n no son iguales.

Ejemplo. $\sqrt[15]{1} \pmod{19}$ tiene tres valores, pues 3 es el máximo divisor común de los números 15 y 18 y, a la vez, éstos serán valores de la expresión $\sqrt[3]{1}$ (mod. 19). Estos son 1, 7 y 11.

62.

Por medio de esta reducción, no logramos resolver ninguna otra congruencia sino las de la forma $x^n \equiv 1$, donde n es un divisor del número $p-1$. Más adelante, mostraremos que las congruencias de esta forma siempre pueden reducirse, pero lo anterior no basta. Podemos aquí tratar un solo caso, o sea, donde $n = 2$. Es claro que los valores de la expresión $\sqrt[2]{1}$ serán $+1$ y -1, pues, no puede tener más que dos y $+1$ y -1 siempre son incongruentes a menos que el módulo sea $= 2$, en cuyo caso $\sqrt[2]{1}$ puede tener un solo valor, como se puede ver. De donde, por consiguiente, sigue que $+1$ y -1 serán también los valores de la expresión $\sqrt[2m]{1}$ cuando m es primo a $\frac{p-1}{2}$. Esto siempre sucede cuando el módulo es de esta clase, con tal que sea un número absolutamente primo (a menos que $p-1 = 2m$, en tal caso todos los números 1, 2, 3, $\ldots p-1$ son raíces), e.g., cuando $p = 3, 5, 7, 11, 23, 47, 59, 83, 107$ etc. Se adjuntará aquí como corolario que el índice de -1 siempre es $\equiv \frac{p-1}{2} \pmod{p-1}$ cualquiera que sea la raíz primitiva tomada como base. Pues, $2\,\mathrm{Ind.}\,(-1) \equiv 0 \pmod{p-1}$. Así, $\mathrm{Ind.}\,(-1)$ será $\equiv 0$, ó $\equiv \frac{p-1}{2} \pmod{p-1}$. Pero, 0 siempre es el índice de $+1$, y $+1$ y -1 siempre deben tener diferentes índices (excepto el caso $p = 2$, al que no vale la pena referirse aquí).

63.

Hemos mostrado, en el art. 60, que la expresión $\sqrt[n]{A} \pmod p$ tiene δ valores diferentes, o no tiene ninguno, si δ es el máximo común divisor de los números n y $p-1$. Ahora, del mismo modo como mostramos que $\sqrt[n]{A}$ y $\sqrt[\delta]{A}$ son equivalentes si $A \equiv 1$, demostramos más generalmente que la expresión $\sqrt[n]{A}$ siempre puede reducirse

a la otra $\sqrt[\delta]{B}$, a la cual equivalga. Pues, denotado un valor cualquiera de éstos por x, será $x^n \equiv A$; ahora, sea t un valor cualquiera de la expresión $\frac{\delta}{n} \pmod{p-1}$, la cual tiene valores reales como se percibe en el art. 31, será $x^{tn} \equiv A^t$, pero $x^{tn} \equiv x^\delta$, puesto que $tn \equiv \delta \pmod{p-1}$. Por tanto, $x^\delta \equiv A^t$ y cualquier valor de $\sqrt[n]{A}$ será también un valor de $\sqrt[\delta]{A^t}$. Por lo tanto, cuando $\sqrt[n]{A}$ tiene valores reales, será totalmente equivalente a la expresión $\sqrt[\delta]{A^t}$, puesto que aquélla ni tiene otros valores diferentes a la anterior, ni tiene menos. Es posible que $\sqrt[n]{A}$ no tenga ningún valor real aún cuando $\sqrt[\delta]{A^t}$ tenga valores reales.

Ejemplo. Si se buscan los valores de la expresión $\sqrt[21]{2} \pmod{31}$, el máximo común divisor de los números 21 y 30 será 3, y éste es un valor de la expresión $\frac{3}{21} \pmod{30}$; por tanto, si $\sqrt[21]{2}$ tiene valores reales, equivaldrá a la expresión $\sqrt[3]{2^3}$ o sea $\sqrt[3]{8}$, se encontrará en verdad que los valores de la expresión posterior, que son 2, 10, 19, también satisfacen la anterior.

64.

Para no intentar realizar en vano esta operación, conviene investigar una regla por medio de la cual pueda deducirse de inmediato si $\sqrt[n]{A}$ admite valores reales o no. Si se tiene una tabla de índices, el asunto es claro, pues, es claro, en el art. 60, que se tendrán valores reales si el índice de A, tomando cualquier raíz primitiva como base, es divisible por δ; pero si no lo es, no se tendrán. No obstante, esto puede hallarse sin esa tabla. Pues, al poner el índice de $A = k$, si es divisible por δ, será $\frac{k(p-1)}{\delta}$ divisible por $p-1$ y vice-versa. Pero, el índice del número $A^{\frac{p-1}{\delta}}$ será $\frac{k(p-1)}{\delta}$. Por lo cual, si $\sqrt[n]{A} \pmod{p}$ tiene valores reales, $A^{\frac{p-1}{\delta}}$ será congruente a la unidad; en caso contrario, será incongruente. Así, en el ejemplo del artículo anterior, se tiene $2^{10} = 1024 \equiv 1 \pmod{31}$, de donde se concluye que $\sqrt[21]{2} \pmod{31}$ tiene valores reales. De modo semejante, resulta cierto que $\sqrt[2]{-1} \pmod{p}$ siempre tiene dos valores reales cuando p es de la forma $4m+1$, pero ninguno cuando p es de la forma $4m+3$, puesto que $(-1)^{2m} = 1$ y $(-1)^{2m+1} = -1$. Este elegante teorema se enuncia ordinariamente así: *si p es número primo de la forma $4m+1$, se puede encontrar un cuadrado a^2, de modo que a^2+1 sea divisible por p, pero si al contrario, p es de la forma $4m-1$, no se puede encontrar tal cuadrado.* De esta forma fue demostrado por el ilustre Euler, en *Comm. nov. Acad. Petrop.* XVIII, p. 112 del año 1773. El ya había presentado otra demostración mucho antes en 1760, *Comm. nov.* V, p. 5. En una disertación anterior, *Comm. nov.* IV, p. 25, todavía no la había perfeccionado. Luego, el ilustre Lagrange

presentó una demostración del teorema, *Nouveaux Mém. de l'Ac. de Berlín,* 1775, p. 342. Presentaremos otra demostración, en la siguiente sección, específicamente dedicada a este argumento.

65.

Después de que hemos hablado de reducir todas las expresiones $\sqrt[n]{A} \pmod{p}$ a otras, donde n es divisor del número $p-1$, y hemos encontrado un criterio de si admite o no valores reales, consideraremos más precisamente tales expresiones $\sqrt[n]{A} \pmod{p}$, donde n es divisor de $p-1$. Primero mostraremos qué relación tienen los valores individuales de la expresión entre sí; luego indicaremos unos artificios, con cuya ayuda muchas veces puede encontrarse un valor de la expresión.

Primero. Cuando $A \equiv 1$ y r es alguno de los n valores de la expresión $\sqrt[n]{1} \pmod{p}$, ó $r^n \equiv 1 \pmod{p}$, también todas las potencias de este r serán valores de esta expresión; pero de ellos, tantos serán diferentes como unidades tenga el exponente al cual r pertenece (art. 48). Si, por lo tanto, r es el valor que pertenece al exponente n, estas potencias r, r^2, r^3, $\ldots r^n$ de este mismo r (donde en el lugar de la última puede sustituirse la unidad) involucrarán todos los valores de la expresión $\sqrt[n]{1} \pmod{p}$. En la sección VIII explicaremos bastante cuáles métodos existen para encontrar aquellos valores que pertenecen al exponente n.

Segundo. Cuando A es incongruente a la unidad, y conocemos un valor de la expresión $\sqrt[n]{A} \pmod{p}$, digamos z, los restantes pueden deducirse del siguiente modo. Sean los valores de la expresión $\sqrt[n]{1}$

$$1,\ r,\ r^2,\ \ldots r^{n-1}$$

(como mostramos arriba). Entonces todos los valores de la expresión $\sqrt[n]{A}$ serán

$$z,\ zr,\ zr^2,\ \ldots zr^{n-1}.$$

Está claro, pues, que todos éstos satisfacen la congruencia $x^n \equiv A$: pongamos cualquiera de ellos $\equiv zr^k$, la n-esima potencia de ella, $z^n r^{nk}$, por ser $r^n \equiv 1$ y $z^n \equiv A$, será congruente a A. Todos son diferentes como se deduce fácilmente del art. 23; pero la expresión $\sqrt[n]{A}$ no puede tener más que estos n valores. Así, por ejemplo, si un valor de una expresión $\sqrt[2]{A}$ es z, el otro será $-z$. Finalmente, de esto se debe concluir que no se pueden encontrar todos los valores de la expresión $\sqrt[n]{A}$ si no se conocen igualmente todos los valores de la expresión $\sqrt[n]{1}$.

66.

Lo segundo que nos habíamos propuesto mostrar era en cuál caso un valor de la expresión $\sqrt[n]{A} \pmod{p}$ puede encontrarse directamente (donde se supone que n es un divisor de $p-1$). Esto resulta cuando algún valor es congruente a alguna potencia de A, lo cual no es tan raro, y no será superfluo detenernos en ello. Sea tal valor z, *si existe*, o sea $z \equiv A^k$ y $A \equiv z^n \pmod{p}$. De esto se deduce que $A \equiv A^{kn}$; por lo tanto, si se tiene un número k, de modo que $A \equiv A^{kn}$, A^k será el valor buscado. Pero esto equivaldrá aquí a la condición siguiente, $1 \equiv kn \pmod{t}$, denotando a t el exponente al cual pertenece A (art. 46, 48). Para que esta congruencia sea posible, se requiere que n sea primo a t. En este caso será $k \equiv \frac{1}{n} \pmod{t}$, pero si t y n tienen un divisor común, ningún valor z puede ser congruente a alguna potencia de A.

67.

No obstante, como conviene conocer a t para esta solución, veamos cómo podemos proceder si desconocemos este número. Primero, se percibe fácilmente que t debe dividir a $\frac{p-1}{n}$, si es que $\sqrt[n]{A} \pmod{p}$ tiene valores reales, como siempre lo hemos supuesto aquí. Sea pues y una solución cualquiera, entonces tendremos $y^{p-1} \equiv 1$ y $y^n \equiv A \pmod{p}$; por lo cual elevando las partes de la última congruencia a la $\frac{p-1}{n}$-ésima potencia resultará $A^{\frac{p-1}{n}} \equiv 1$; de tal modo $\frac{p-1}{n}$ es divisible por t (art. 48). Ahora, si $\frac{p-1}{n}$ es primo a n, la congruencia del artículo anterior, $kn \equiv 1$, no sólo podrá resolverse según el módulo $\frac{p-1}{n}$, sino claramente el valor de k que satisface a esta congruencia según este módulo también la satisfará según el módulo t, el cual divide a $\frac{p-1}{n}$ (art. 5). Por tanto, se ha encontrado lo buscado. Sin embargo, si $\frac{p-1}{n}$ no es primo a n, se eliminarán todos los factores primos de $\frac{p-1}{n}$, que a la vez dividen a n. Por eso, encontraremos un número $\frac{p-1}{nq}$, primo a n, donde q denota el producto de todos los factores primos que hemos eliminado. Ahora, si la condición que logramos en el artículo anterior, que t sea primo a n, tiene lugar, t no sólo será primo a q sino también dividirá a $\frac{p-1}{nq}$. Por eso, si se resuelve la congruencia $kn \equiv 1 \pmod{\frac{p-1}{nq}}$ (lo que puede ser, puesto que n es primo a $\frac{p-1}{nq}$), el valor k también satisfará la congruencia, según el módulo t; lo cual se buscaba. Todo este artificio consiste en hallar un número que pueda funcionar en vez de t, el cual no conocemos. Aunque siempre conviene recordar: hemos supuesto que, cuando $\frac{p-1}{n}$ no es primo a n, cabe la condición del artículo anterior, pero si no es cierta, todas las conclusiones serían erróneas. Sin embargo, si aún siguiendo las reglas dadas, se encuentra un valor

para z, cuya n-ésima potencia es incongruente a A, esto sería una muestra de que la condición no puede satisfacerse y que el método no puede emplearse del todo.

68.

Pero, en este caso también puede ser ventajoso haber realizado este trabajo y vale la pena investigar cómo este valor falso se relaciona con los verdaderos. Así, supongamos que los números k y z están bien determinados, pero que z^n no es $\equiv A \pmod{p}$. Entonces, si sólo pueden determinarse valores de la expresión $\sqrt[n]{\frac{A}{z^n}} \pmod{p}$, multiplicando cada uno de estos valores por z, obtendremos los valores de $\sqrt[n]{A}$. Pues si v es algún valor de $\sqrt[n]{\frac{A}{z^n}}$: será $(vz)^n \equiv A$. Pero la expresión $\sqrt[n]{\frac{A}{z^n}}$ es más simple que $\sqrt[n]{A}$, puesto que $\frac{A}{z^n} \pmod{p}$ con frecuencia pertenece a un exponente menor que A. Es decir, si d es el máximo común divisor de los números t y q, $\frac{A}{z^n} \pmod{p}$ pertenecerá al exponente d, como se demostrará ahora. Sustituyendo por el valor z, será $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \pmod{p}$. Pero, $kn-1$ es divisible por $\frac{p-1}{nq}$ (artículo anterior), $\frac{p-1}{n}$ por t (ibid.) o sea $\frac{p-1}{nd}$ por $\frac{t}{d}$. Ahora bien $\frac{t}{d}$ es primo a $\frac{q}{d}$ (hip.), así $\frac{p-1}{nd}$ será divisible por $\frac{tq}{d^2}$ o bien $\frac{p-1}{nq}$ por $\frac{t}{d}$. También $kn-1$ será divisible por $\frac{t}{d}$ y $(kn-1)d$ por t. Por lo tanto, $A^{(kn-1)d} \equiv 1 \pmod{p}$. De donde se deduce fácilmente que $\frac{A}{z^n}$, elevada a la d-ésima potencia, será congruente a la unidad. El que $\frac{A}{z^n}$ no pueda pertenecer a un exponente menor que d, puede demostrarse fácilmente; pero, ya que no se requiere para nuestros fines, no nos detendremos en esto. Podemos estar seguros que $\frac{A}{z^n} \pmod{p}$ siempre pertenecerá a un exponente menor que A, excepto en un caso único, cuando t divide a q; de donde $d = t$.

Pero, ¿de qué sirve que $\frac{A}{z^n}$ pertenezca a un exponente menor que A? Se presenta mayor cantidad de números que pueden ser A que los que pueden ser $\frac{A}{z^n}$, y cuando haya ocasión de desarrollar varias expresiones $\sqrt[n]{A}$ según un mismo módulo, tendremos la ventaja de derivar varios resultados de una misma fuente. Así, por ejemplo, siempre será posible determinar al menos un valor de la expresión $\sqrt[2]{A}$ (mod. 29), si sólo se conocen los valores de la expresión $\sqrt[2]{-1}$ (que son ± 12). Del artículo anterior se conoce fácilmente que un valor de esta expresión siempre puede determinarse directamente, ya sea cuando t es impar y $d = 2$ o cuando t es par. Excepto para -1, ningún otro número pertenece al exponente 2.

Ejemplos. Búsquese $\sqrt[3]{31} \pmod{37}$. Aquí, $p-1 = 36$, $n = 3$, $\frac{p-1}{3} = 12$, y así $q = 3$. Por lo tanto, debe ser $3k \equiv 1 \pmod{4}$, lo cual se obtiene poniendo $k = 3$. Aquí $z \equiv 31^3 \pmod{37} \equiv 6$, se halla realmente $6^3 \equiv 31 \pmod{37}$. Si los

valores de la expresión $\sqrt[3]{1} \pmod{37}$ son conocidos, también los restantes valores de la expresión $\sqrt[3]{6}$ pueden determinarse. Los valores de $\sqrt[3]{1} \pmod{37}$ son 1, 10 y 26. Al multiplicarlos por 6, se producen los restantes $\equiv 23$ y 8.

Sin embargo, si se busca el valor de la expresión $\sqrt[2]{3} \pmod{37}$, será $n = 2$, $\frac{p-1}{n} = 18$, y de aquí $q = 2$. Por tanto, debe ser $2k \equiv 1 \pmod{9}$, de donde resulta $k \equiv 5 \pmod{9}$. Por consiguiente, $z \equiv 3^5 \equiv 21 \pmod{37}$; pero 21^2 no es $\equiv 3$, sino $\equiv 34$. Así, $\frac{3}{34} \pmod{37} \equiv -1$, y $\sqrt[2]{-1} \pmod{37} \equiv \pm 6$; de donde se obtendrán los valores verdaderos $\pm 6 \cdot 21 \equiv \pm 15$.

Esto es casi todo lo que se puede decir acerca del desarrollo de tales expresiones. Es evidente que los métodos directos con frecuencia resultan bastante largos; pero esto es cierto para casi todos los métodos directos en la teoría de los números; por esto, consideramos que debemos demostrarlo. También, conviene observar que no es de nuestro interés explicar los artificios particulares que se presentan aquí.

La conexión entre los indices en sistemas diferentes.

69.

Volvemos ahora a las raíces que llamamos primitivas. Hemos mostrado, al tomar una raíz primitiva cualquiera como base, que todos los números, cuyos índices son primos a $p-1$, también serán raíces primitivas, y ninguno aparte de éstos. A la vez se conoce el número de raíces primitivas. Véase art. 53. En general, queda a nuestro arbitrio saber cuál raíz primitiva escogeremos como base. De esto se percibe, también aquí, como en el cálculo logarítmico, que pueden presentarse diferentes sistemas*). Veamos las relaciones que los conectan. Sean a y b dos raíces primitivas, sea m otro número. Cuando se toma a a como base, el índice del número $b \equiv \beta$, pero el índice del número $m \equiv \mu \pmod{p-1}$; cuando se toma b como base, el índice del número $a \equiv \alpha$, el índice de b sin embargo $\equiv \nu \pmod{p-1}$. Entonces será $\alpha\beta \equiv 1 \pmod{p-1}$; puesto que $a^\beta \equiv b$, de donde $a^{\alpha\beta} \equiv b^\alpha \equiv a \pmod{p}$ (por hipótesis), por lo tanto $\alpha\beta \equiv 1 \pmod{p-1}$. Mediante un razonamiento similar, se descubre que $\nu \equiv \alpha\mu$, por eso $\mu \equiv \beta\nu \pmod{p-1}$. Por lo tanto, si se ha construido una tabla de índices para la base a, fácilmente puede convertirse en otra, donde la base es b. Pues si para la base a el índice de b es $\equiv \beta$, para la base b el índice de a será

*) Difieren en esto: en los logaritmos el número de sistemas es infinito; aquí hay tantos como el número de raíces primitivas. Obviamente, bases congruentes producen los mismos sistemas.

$\equiv \frac{1}{\beta} \pmod{p-1}$, y multiplicando todos los índices de la tabla por este número, se tendrán todos los índices para la base b.

70.

Aunque un número dado puede tener varios índices, tomadas unas u otras raíces primitivas como base, todas concuerdan en esto: todos tendrán el mismo máximo común divisor con $p-1$. Pues, si por la base a, el índice del número dado es m, pero por la base b es n, y si los máximos comunes divisores μ y ν con $p-1$ se suponen diferentes, uno de ellos será mayor, por ejemplo $\mu > \nu$, y por eso n no dividirá a μ. Pero, denotado el índice de a por α, cuando se toma a b como base, será (artículo anterior) $n \equiv \alpha m \pmod{p-1}$, de donde μ dividirá a n. *Q. E. A.*

Se percibe también que este máximo común divisor de los índices de un número dado y de $p-1$ no depende de la base porque es igual a $\frac{p-1}{t}$, donde t denota el exponente al cual pertenece el número sobre cuyos índices se trata. Pues si el índice para una base cualquiera es k, t será el número menor que, multiplicado por k, resultará un múltiplo de $p-1$ (excepto cero) (véanse artículos 48 y 58), o sea, el valor menor de la expresión $\frac{0}{k} \pmod{p-1}$ excepto cero. No obstante, que esto es igual al máximo común divisor de los números k y $p-1$, se obtiene del artículo 29 sin dificultad.

71.

Además se demuestra fácilmente que la base siempre puede tomarse de modo que un número que pertenece al exponente t tiene cualquier índice dado cuyo máximo común divisor con $p-1$ es $= \frac{p-1}{t}$. Por brevedad, designaremos éste por d, si el índice propuesto es $\equiv dm$, y el índice del número propuesto $\equiv dn$, cuando se toma cualquier raíz primitiva como base, entonces m y n serán primos a $\frac{p-1}{d}$, o sea a t. Entonces, si ε es el valor de la expresión $\frac{dn}{dm} \pmod{p-1}$ y a la vez es primo a $p-1$, a^{ε} será una raíz primitiva. Tomada ésta como base, el número propuesto producirá el índice dm (pues será $a^{\varepsilon dm} \equiv a^{dn} \equiv$ número propuesto). Pero, del modo siguiente se demuestra que la expresión $\frac{dn}{dm} \pmod{p-1}$ admite valores primos a $p-1$. Esta expresión equivaldrá a: $\frac{n}{m} \pmod{\frac{p-1}{d}}$ o sea $\frac{n}{m} \pmod{t}$ (véase art. 31, 2). Todos sus valores serán primos a t; ya que, si algún valor e tuviera un divisor común con t, este divisor también debería dividir a me, por tanto, también me es congruente a n según t, contrariamente a la hipótesis de que n es primo a t. Por lo tanto, cuando todos los

divisores primos de $p-1$ también dividen a t, todos los valores de la expresión $\frac{n}{m}$ (mod. t) serán primos a $p-1$, y el número de ellos $= d$. Sin embargo, cuando $p-1$ involucra otros divisores primos f, g, h, etc., que no dividen a t, se toma cualquier valor de la expresión $\frac{n}{m}$ (mod. t) $\equiv e$. Entonces, puesto que t, f, g, h, etc., son primos entre sí, puede hallarse un número ε que es congruente a e según el módulo t, pero según f, g, h, etc. es congruente a números cualesquiera primos a éstos respectivamente (art. 32). Por eso tal número no será divisible por ningún factor primo de $p-1$, por lo tanto será primo a $p-1$, tal como se esperaba. Finalmente, sin dificultad alguna, se deduce de la teoría de las combinaciones que el número de tales valores será $= \frac{p-1}{t} \cdot \frac{f-1}{f} \cdot \frac{g-1}{g} \cdot \frac{h-1}{h} \cdot$ etc.; pero para que no se extienda mucho esta disgresión, hemos omitido la demostración, puesto que no nos concierne.

Bases adaptadas para usos especiales.

72.

Aunque generalmente sea muy arbitrario cuál raíz primitiva se tomará como base, a veces ciertas bases pueden presentar algunas conveniencias especiales. En la tabla I, siempre hemos tomado el número 10 como la base cuando éste era raíz primitiva; de otra manera hemos determinado la base de modo que el índice del número 10 sea el menor posible, i.e., $= \frac{p-1}{t}$, donde t denota el exponente al cual perteneció 10. Pero, lo que ganamos con esto, lo presentaremos en la Sección VI, donde la misma tabla se aplicará para otros fines. Sin embargo, puesto que aquí esto todavía puede permanecer un poco arbitrario, como aparece en el artículo anterior: para establecer algo fijo, de todas las raíces primitivas, eligimos siempre como base la *menor*. Así, para $p = 73$, donde $t = 8$ y $d = 9$, a^{ε} tiene $\frac{72 \cdot 2}{8 \cdot 3}$, i.e., 6 valores que son 5, 14, 20, 28, 39, 40. Por esto, tomamos el mínimo, 5, como base.

Método para la determinación de las raíces primitivas.

73.

Los métodos para encontrar las raíces primitivas se basan en su mayoría en el tanteo. Si se reune lo que hemos aprendido en el artículo 55, con lo que diremos adelante sobre las soluciones de la congruencia $x^n \equiv 1$, se tendrá casi todo lo que puede lograrse con los métodos directos. El ilustre Euler reconoce (*Opuscula Analytica, T.* I, *p.* 152) que parece extremadamente difícil encontrar estos números, y se refiere a su naturaleza como uno de los misterios más grandes de los números. Pero,

pueden determinarse bastante rápidamente al intentarlo de la siguiente manera. Un conocedor sabrá evitar operaciones prolijas por medio de varios artificios particulares: pero esto se aprende mas rápidamente con práctica que con preceptos.

1^o. Tómese libremente un número a, primo a p (siempre designamos el módulo con esta letra) (casi siempre lleva a los cálculos cortos si escogemos el menor posible, e.g., el número 2); luego determínese su período (art. 46), i.e., los residuos mínimos de sus potencias, hasta encontrar la potencia a^t cuyo residuo mínimo sea 1*). Ahora, si $t = p - 1$, a es una raíz primitiva.

2^o. Pero, si $t < p-1$, se toma otro número b que no está en el período de a, y de modo semejante se investigará su período. Al designar por u el exponente al cual pertenece b, se percibe fácilmente que u ni puede ser igual a t, ni a un factor de t; de hecho en los dos casos sería $b^t \equiv 1$; lo cual no puede ser, puesto que el período de a contiene todos los números cuya t-ésima potencia es congruente a la unidad (art. 53). Ahora si u es $= p - 1$, b será una raíz primitiva; pero si u no es $= p - 1$, sino un múltiplo de t, hemos logrado esto: que conocemos un número perteneciente a un exponente mayor, de modo que nuestro propósito, encontrar el número perteneciente al exponente *máximo,* está próximo. Pero si u no es $= p-1$, ni a un múltiplo de t, no obstante, podemos encontrar un número u que pertenece a un exponente mayor que t, a saber, al exponente igual al mínimo común múltiplo de los números t y u. Sea éste $= y$, así resuélvase y en dos factores primos entre sí, m y n, de modo que uno divide a t, y el otro a u†). Entonces, la $\frac{t}{m}$-ésima potencia de a será $\equiv A$, la $\frac{u}{n}$-ésima potencia de b será $\equiv B \pmod{p}$, y el producto AB será un número perteneciente al exponente y. Es fácil percibir que A pertenece al exponente m, y B al exponente n, de modo que el producto AB pertenecerá a mn, puesto que m y n son primos entre sí. Esto podrá demostrarse prácticamente del mismo modo como en el art. 55, II.

3^o. Ahora, si $y = p-1$, AB será una raíz primitiva. Si no es el caso, entonces de igual manera que antes se deberá tomar otro número que no aparece en el período de AB. Esto, o bien, será una raíz primitiva, o pertenecerá a un exponente mayor que y, o por medio de él (como antes) podrá encontrarse un número que pertenece a un exponente mayor que y. Por tanto, como los números que resultan de repeticiones

*) Se percibe con facilidad que no es necesario conocer estas potencias, puesto que el residuo mínimo puede obtenerse fácilmente de un residuo mínimo de la potencia anterior.

†) Del art. 18 se deriva cómo se puede hacer sin dificultad. Resuélvase y en factores que son o bien números primos diferentes, o bien potencias de números primos diferentes. Cada uno de ellos dividirá a t o a u (o a ambos). Asígnense cada uno o a t o a u según el cual él divida por él: cuando alguno divide a ambos, se le puede asignar arbitrariamente. Sea m el producto de los asignados a t, el de los otros $= n$. Está claro que m divide a t, n divide a u, y $mn = y$.

de esta operación pertenecen a exponentes continuamente crecientes; es claro que, finalmente, se debe encontrar un número que pertenezca al exponente mayor, i.e., una raíz primitiva. *Q. E. F.*

74.

Estas reglas anteriores serán más claras mediante un ejemplo. Sea $p = 73$ para el cual se busca una raíz primitiva. Intentaremos primero con el número 2, cuyo período es el siguiente:

1.2.4.8.16.32.64.55.37.1 etc.
0.1.2.3. 4. 5. 6. 7. 8.9 etc.

Puesto que ya la potencia del exponente 9 es congruente a la unidad, 2 no es una raíz primitiva. Pruébese con otro número que no aparece en el período de 2, por ejemplo 3, cuyo período es éste:

1.3.9.27.8.24.72.70.64.46.65.49. 1 etc.
0.1.2. 3.4. 5. 6. 7. 8. 9.10.11.12 etc.

Por lo tanto, 3 tampoco es una raíz primitiva. En cambio, el mínimo común múltiplo de los exponentes a los cuales pertenecen 2 y 3 (i.e., los números 9 y 12) es 36, el cual se resuelve en los factores 9 y 4 según los preceptos del artículo anterior. Así que al elevarse 2 a la potencia $\frac{9}{9}$, i.e., reteniendo el número 2; y 3 a la potencia 3: el producto de éstos es 54, que por tanto pertenecerá al exponente 36. Si finalmente se calcula el período de 54, y se intenta con un número no contenido en él, por ejemplo, el número 5, se descubrirá que es una raíz primitiva.

Varios teoremas sobre los períodos y las raíces primitivas.

75.

Antes de dejar este argumento, presentaremos algunas proposiciones, a las que por su simplicidad conviene prestarles atención.

El producto de todos los términos del período de un número cualquiera es $\equiv 1$*, cuando el número de ellos o el exponente al cual pertenece el número es impar, y* $\equiv -1$ *cuando este exponente es par.*

Ejemplo. Para el módulo 13 el período del número 5 consta de estos términos 1, 5, 12, 8, cuyo producto $480 \equiv -1 \pmod{13}$.

Según el mismo módulo, el período del número 3 consta de los términos 1, 3, 9, cuyo producto $27 \equiv 1 \pmod{13}$.

Demostración. Sea t el exponente al cual pertenece un número, y $\frac{p-1}{t}$ el índice del número, lo cual siempre puede ser si se determina debidamente la base (art. 71). Entonces, el índice del producto de todos los términos del período será

$$\equiv (1+2+3+ \text{ etc.} + t-1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2}$$

i.e., $\equiv 0 \pmod{p-1}$ cuando t es impar, y $\equiv \frac{p-1}{2}$ cuando t es par; por tanto, en el primer caso este producto $\equiv 1 \pmod{p}$; en el último $\equiv -1 \pmod{p}$, (art. 62). *Q. E. D.*

76.

Si ese número en el teorema precedente es una raíz primitiva, su período comprenderá todos los números 1, 2, 3, $\ldots p-1$, cuyo producto siempre $\equiv -1$ (pues $p-1$ es siempre par, excepto un caso, $p=2$, en el cual -1 y $+1$ son equivalentes). Este elegante teorema suele enunciarse así: *el producto de todos los números menores que un número primo dado, sumado a uno, es divisible por este primo.* Fue publicado primero por el célebre Waring, y adscrito a Wilson, (*Meditt. algebr.*, tercera edición, *p.* 380). Pero ninguno pudo demostrarlo, y el célebre Waring confesó que la demostración parecía más difícil porque ninguna *notación* puede confeccionarse para expresar un número primo. Pero a nuestro juicio tales verdades debían percibirse por medio de las nociones más que por las notaciones. Después, el ilustre Lagrange presentó una demostración (*Nouv. Mém. de l'Ac. Berlin,* 1771). Se basa en la consideración de los coeficientes originados en el desarrollo del producto

$$(x+1)(x+2)(x+3)\ldots(x+p-1).$$

De hecho, con poner este producto

$$\equiv x^{p-1} + Ax^{p-2} + Bx^{p-3} + \text{ etc.} + Mx + N$$

los coeficientes A, B, etc., M serán divisibles por p, y N será $= 1\cdot 2\cdot 3\cdot \ldots \cdot p-1$. Ahora, para $x=1$, el producto será divisible por p; entonces será $\equiv 1+N \pmod{p}$, de donde necesariamente $1+N$ podrá dividirse por p.

Finalmente, el ilustre Euler ha presentado una demostración en *Opusc. analyt. T.* I. *p.* 329 que concuerda con la expuesta por nosotros. Pero si tan distinguidos matemáticos no han considerado sin mérito a este teorema para sus meditaciones, esperamos no ser censurados si adjuntamos todavía otra demostración.

77.

Cuando según el módulo p, el producto de dos números a y b es congruente a la unidad, llamaremos a los números a y b *asociados,* tal como lo hizo Euler. Entonces, según la sección anterior, cualquier número positivo menor que p tendrá un único asociado positivo menor que p. Puede demostrarse fácilmente que de los números 1, 2, 3,... $p-1$, los únicos asociados de sí mismos son 1 y $p-1$: pues los números asociados de sí mismos serán raíces de la congruencia $x^2 \equiv 1$; que es de segundo grado, por tanto no puede tener más que dos raíces, i.e., ninguna otra más que 1 y $p-1$. Excluidos éstos de los números restantes, 2, 3, $\ldots p-2$ estarán asociados siempre en pares; por tanto el producto de ellos será $\equiv 1$, de donde el producto de todos 1, 2, 3, $\ldots p-1$, será $\equiv p-1$ o sea $\equiv -1$. *Q. E. D.*

Por ejemplo, para $p = 13$, se asocian los números 2, 3, 4, $\ldots 11$ así: 2 con 7; 3 con 9; 4 con 10; 5 con 8; 6 con 11; entonces $2 \cdot 7 \equiv 1$; $3 \cdot 9 \equiv 1$ etc. Por tanto $2 \cdot 3 \cdot 4 \cdot \ldots 11 \equiv 1$, y $1 \cdot 2 \cdot 3 \ldots 12 \equiv -1$.

78.

El teorema de Wilson puede exponerse más generalmente así: *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 o negativamente.* Se debe tomar la unidad negativamente cuando A es de la forma p^m, o bien $2p^m$, donde p denota un número primo diferente de 2, y además cuando $A = 4$; se toma positivamente en todos los casos restantes. El teorema, como fue presentado por el célebre Wilson, está contenido bajo el primer caso. Por ejemplo, para $A = 15$, el producto de los números 1, 2, 4, 7, 8, 11, 13, 14 es $\equiv 1 \pmod{15}$. Por brevedad no adjuntamos la demostración: observamos solamente que puede completarse de modo semejante al del artículo anterior, excepto que la congruencia $x^2 \equiv 1$ puede tener más de dos raíces, las cuales exigen ciertas consideraciones peculiares. También la demostración puede derivarse de la consideración de los índices, similarmente como en el artículo 75, si se agrega lo que pronto expondremos sobre los módulos compuestos.

79.

Volvemos a la enumeración de otras proposiciones (art. 75).

La suma de todos los términos del período de un número cualquiera es $\equiv 0$, como en el ejemplo del artículo 75, $1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}$.

Demostración. Sea a el número de cuyo período se trata, y t el exponente al cual pertenece. La suma de todos los términos del período será:

$$\equiv 1 + a + a^2 + a^3 + \text{ etc.} + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}$$

Pero, $a^t - 1 \equiv 0$: por tanto esta suma siempre será $\equiv 0$ (art. 22), a menos que por casualidad $a-1$ sea divisible por p, o sea $a \equiv 1$; por lo tanto, este caso debe excluirse si deseamos llamar *período* a un solo término.

80.

El producto de todas las raíces primitivas es $\equiv 1$, excepto el caso único $p = 3$; pues en este se presenta una sola raíz primitiva, 2.

Demostración. Si se toma una raíz primitiva cualquiera como base, los índices de todas las raíces primitivas serán números primos a $p-1$ y a la vez menores que él. Pero la suma de estos números, i.e., el índice del producto de todas las raíces primitivas, es $\equiv 0 \pmod{p-1}$, de donde el producto $\equiv 1 \pmod{p}$. En efecto se percibe fácilmente que si k es un número primo a $p-1$, también $p-1-k$ será primo a $p-1$, y por lo tanto la suma de los números primos a $p-1$ se compone de pares cuya suma es divisible por $p-1$ (aunque k nunca puede ser igual a $p-1-k$ excepto en el caso $p-1=2$, o sea $p=3$, el cual excluimos; pues es claro, en todos los casos restantes que $\frac{p-1}{2}$ no es primo a $p-1$).

81.

La suma de todas las raíces primitivas es o bien $\equiv 0$ (cuando $p-1$ es divisible por algún *cuadrado*), *o bien* $\equiv \pm 1 \pmod{p}$ (cuando $p-1$ es un producto de números primos diferentes; si el número de ellos es par, se toma el signo positivo, pero si es impar, se toma el negativo.)

Ejemplo. 1^o. Para $p = 13$, se tienen las raíces primitivas 2, 6, 7, 11, cuya suma $26 \equiv 0 \pmod{13}$.

2^o. Para $p = 11$, las raíces primitivas son 2, 6, 7, 8, cuya suma $23 \equiv +1$ (mod. 11).

3^o. Para $p = 31$, las raíces primitivas son 3, 11, 12, 13, 17, 21, 22, 24 cuya suma $123 \equiv -1 \pmod{31}$.

Demostración. Arriba hemos demostrado (art. 55, II), que si $p-1$ es $= a^\alpha b^\beta c^\gamma$ etc. (donde a, b, c, etc. designan números primos diferentes), y A, B, C, etc. son números cualesquiera pertenecientes a los exponentes a^α, b^β, c^γ, etc., respectivamente, entonces todos los productos ABC etc. representarán raíces primitivas. También puede demostrarse fácilmente que cualquier raíz primitiva puede representarse por tal tipo de producto, y de hecho de manera única*).

De esto sigue que estos productos pueden tomarse en lugar de las raíces primitivas mismas. Pero, puesto que en estos productos conviene combinar todos los valores de A con todos los de B, etc., la suma de todos estos productos es un producto de la suma de todos los valores de A, multiplicada por la suma de todos los valores de B, multiplicada por la suma de todos los valores de C, etc., como es conocido de la teoría de combinaciones. Denótense todos los valores de A; B etc., por A, A', A", etc.; B, B', B", etc. etc., entonces la suma de todas las raíces primitivas será:

$$\equiv (A + A' + \text{ etc.})(B + B' + \text{ etc.}) \text{ etc.}$$

Ahora digo que si el exponente α es $= 1$, la suma $A + A' + A$" $+$ etc. será $\equiv -1 \pmod{p}$, pero si α es > 1, esta suma será $\equiv 0$, y de manera similar para los restantes β, γ, etc. Tan pronto como esto sea demostrado, la verdad de nuestro teorema será manifiesta. De hecho, cuando $p-1$ es divisible por algún cuadrado, alguno de los exponentes α, β, γ, etc. superará a la unidad, de donde alguno de los factores cuyo producto es congruente a la suma de todas las raíces primitivas será $\equiv 0$, y por eso también lo será el producto mismo. Pero cuando $p-1$ no puede dividirse por ningún cuadrado, todos los exponentes α, β, γ, etc. serán $= 1$, de donde la suma de todas las raíces primitivas será congruente al producto de tantos factores, cada uno de los cuales es $\equiv -1$, como cantidad de números a, b, c, etc. se tenga. Por eso la suma será $\equiv \pm 1$, según que el número de éstos sea par o impar. Ello se demuestra como sigue.

1^o. Cuando $\alpha = 1$ y A es un número perteneciente al exponente a, los restantes números que pertenecen a este exponente serán A^2, A^3, $\ldots A^{a-1}$. Pero

$$1 + A + A^2 + A^3 + \ldots + A^{a-1}$$

*) Claramente determínense los números $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc. de manera que $\mathfrak{a} \equiv 1 \pmod{a^\alpha}$ y $\equiv 0 \pmod{b^\beta c^\gamma}$ etc.); $\mathfrak{b} \equiv 1 \pmod{b^\beta}$ y $\equiv 0 \pmod{a^\alpha c^\gamma}$ etc.) etc. (véase art. 32), de donde será $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} +$ etc. $\equiv 1 \pmod{p-1}$, (art. 19). Ahora, si cualquier raíz primitiva r se representa por el producto ABC etc., se tomará $A \equiv r^{\mathfrak{a}}$, $B \equiv r^{\mathfrak{b}}$, $C \equiv r^{\mathfrak{c}}$, etc., luego A pertenecerá al exponente a^α, B al exponente b^β, etc.; el producto de todos los números A, B, C, etc., será $\equiv r \pmod{p}$. Finalmente se ve con facilidad que A, B, C, etc., no pueden determinarse de ninguna otra manera.

es la suma de un período completo, de donde $\equiv 0$ (art. 79), por lo cual

$$A + A^2 + A^3 + \ldots + A^{a-1} \equiv -1$$

2^o. Sin embargo, cuando $\alpha > 1$ y A es un número perteneciente al exponente a^α, se tendrán los restantes números que pertenecen a este exponente, si de A^2, A^3, A^4, $\ldots A^{a^\alpha - 1}$ se suprimen A^a, A^{2a}, A^{3a}, etc., (véase art. 53). Entonces la suma de ellos será

$$\equiv 1 + A + A^2 + \ldots + A^{a^\alpha - 1} - (1 + A + A^{2a} + \ldots + A^{a^\alpha - a})$$

i.e., congruente a la diferencia de dos períodos, y por eso $\equiv 0$. *Q. E. D.*

Sobre los módulos que son potencias de números primos.

82.

Todo lo que hasta ahora hemos expuesto se ha basado en la suposición de que el módulo es un número primo. Nos queda considerar el caso donde se toma un número compuesto como módulo. Pero como aquí ni se presentan propiedades tan elegantes como en el caso anterior, ni es necesario buscar artificios sutiles para éstas, sino más bien casi todo puede extraerse por medio de una aplicación de los principios anteriores, sería superfluo y tedioso discutir todos los detalles aquí. Así que expondremos brevemente cuáles casos son comunes al caso anterior y cuales son propios.

83.

Las proposiciones de los artículos 45–48 ya fueron demostradas en general. Pero la proposición del art. 49 tiene que cambiarse como sigue:

Si f denota cuántos números son primos a m y, a la vez, menores que m, i.e., si $f = \varphi m$ (art. 38), entonces el exponente t de la potencia menor de un número dado a primo a m que es congruente a la unidad según el módulo m, será $= f$, o bien un factor de este número.

La demostración de la proposición del artículo 49 también puede valer para este caso, si se sustituyen p por m, $p-1$ por f, y los números 1, 2, 3, $\ldots p-1$, por los números a la vez menores que y primos a m. Dejamos esta tarea al lector.

Además las restantes demostraciones de las cuales hemos hablado allí (art. 50, 51) no pueden aplicarse a este caso sin mucha ambigüedad. Con respecto a las proposiciones de los artículos 52 y siguientes, nace una gran diferencia entre los módulos que son potencias de números primos y los que pueden dividirse por muchos números primos. Por lo tanto, consideraremos los módulos del género anterior por separado.

84.

Si el módulo $m = p^n$, donde p es un número primo, será $f = p^{n-1}(p-1)$ (art. 38). Ahora, si a este caso se aplican las investigaciones contenidas en los artículos 53 y 54, hechos los cambios necesarios como prescribimos en el artículo anterior, se descubrirá que todo lo que se demostró allí valdrá también en este caso, si se demostrara antes que una congruencia de la forma $x^t - 1 \equiv 0 \pmod{p^n}$ no puede tener más que t raíces diferentes. Para un módulo primo dedujimos esta verdad de las proposiciones más generales del art. 43, las cuales valen en su mayor generalidad solamente para módulos que son números primos, y por eso no debe aplicarse a este caso. No obstante demostraremos utilizando un método especial, que esta proposición es verdadera en este caso particular. Luego (sección VIII) aprenderemos a encontrarla más fácilmente.

85.

Nos proponemos demostrar este teorema:

Si e es el máximo común divisor de los números t y $p^{n-1}(p-1)$, la congruencia $x^t \equiv 1 \pmod{p^n}$ tendrá e raíces diferentes.

Sea $e = kp^\nu$ tal que k no involucre el factor p, de modo que divida al número $p-1$. Entonces la congruencia $x^t \equiv 1$, según el módulo p, tendrá k raíces diferentes denotadas A, B, C, etc., y cualquier raíz de la misma congruencia según el módulo p^n, debe ser congruente, según el módulo p, a alguno de los números A, B, C, etc. Ahora demostraremos que la congruencia $x^t \equiv 1 \pmod{p^n}$ tiene p^ν raíces congruentes a A, otras tantas a B etc., todas según el módulo p. Por esto, el número de todas las raíces será kp^ν o sea e, como hemos dicho. Para llevar a cabo esta demostración,demostraremos *primero*, que si α es una raíz congruente a A según el módulo p, también

$$\alpha + p^{n-\nu}, \quad \alpha + 2p^{n-\nu}, \quad \alpha + 3p^{n-\nu}, \quad \ldots \alpha + (p^\nu - 1)p^{n-\nu}$$

serán raíces; *segundo*, que los números congruentes a A según el módulo p diferentes de los que estén comprendidos en la forma $\alpha + hp^{n-\nu}$ (donde h denota cualquier entero) no pueden ser raíces. De donde es claro que se tendrán p^ν raíces diferentes, y no más: lo mismo tendrá que valer también para las raíces que son congruentes a cada uno de los números B, C, etc. *Tercero*, mostraremos como se puede siempre encontrar una raíz congruente a A según p.

86.

TEOREMA. *Si, como en el artículo anterior, t es un número divisible por p^ν pero no por $p^{\nu+1}$, tendremos:*

$$(\alpha + hp^\mu)^t - \alpha^t \equiv 0 \pmod{p^{\mu+\nu}}, \quad \text{y} \quad \equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\nu+1}}$$

La última parte del teorema no tiene lugar cuando $p = 2$ y a la vez $\mu = 1$.

La demostración de este teorema puede hacerse mediante el desarrollo de la potencia de un binomio, si se muestra que todos los términos después del segundo son divisibles por $p^{\mu+\nu+1}$. Sin embargo, puesto que la consideración de los denominadores de los coeficientes resulta un poco ambigua, preferimos el siguiente método.

Si suponemos *primero* $\mu > 1$ y $\nu = 1$, puesto que

$$x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \text{ etc.} + y^{t-1})$$

se tendrá $$(\alpha + hp^\mu)^t - \alpha^t = hp^\mu((\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2}\alpha + \text{ etc.} + \alpha^{t-1})$$

Pero $$\alpha + hp^\mu \equiv \alpha \pmod{p^2}$$

por lo que cada término $(\alpha+hp^\mu)^{t-1}$, $(\alpha+hp^\mu)^{t-2}\alpha$, etc. será $\equiv \alpha^{t-1} \pmod{p^2}$, y por tanto la suma de todos será $\equiv t\alpha^{t-1} \pmod{p^2}$ o sea, será de la forma $t\alpha^{t-1} + Vp^2$, donde V denota un número cualquiera. Por eso, $(\alpha + hp^\mu)^t - \alpha^t$ será de la forma

$$\alpha^{t-1}hp^\mu t + Vhp^{\mu+2}, \quad \text{i.e.,} \quad \equiv \alpha^{t-1}hp^\mu t \pmod{p^{\mu+2}} \quad \text{y} \quad \equiv 0 \pmod{p^{\mu+1}}$$

Por lo tanto el teorema está demostrado para este caso.

Ahora, si el teorema no fuera válido para otros valores de ν, manteniendo todavía $\mu > 1$, necesariamente se presentará algún límite abajo del cual el teorema sea válido, pero más allá falso. Sea φ el menor valor de ν para el cual es falso, de donde se ve fácilmente , que si t es divisible por $p^{\varphi-1}$ pero no divisible por p^φ, el

teorema será verdadero hasta aquí, pero falso si se sustituye t por tp. Por lo tanto tenemos

$$(\alpha + hp^\mu)^t \equiv \alpha^t + \alpha^{t-1}hp^\mu t \pmod{p^{\mu+\varphi}} \quad \text{o sea} \quad = \alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\varphi}$$

donde u denota algún número entero. Pero ya que el teorema está demostrado para $\nu = 1$, se tendrá:

$$(\alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-t}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$$

y por lo tanto también

$$(\alpha + hp^\mu)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^\mu tp \pmod{p^{\mu+\varphi+1}}$$

i.e., el teorema también es válido si se sustituye t por tp, i.e., también para $\nu = \varphi$ contra la hipótesis. De donde es claro que el teorema será válido para todos los valores de ν.

87.

Falta el caso donde $\mu = 1$. Por medio de un método enteramente similar al que hemos aplicado en el artículo anterior, puede demostrarse sin usar el teorema binomial que

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}\\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp\\ \alpha^2(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp\end{aligned}$$

etc.

de donde su suma (puesto que el número de términos $= t$) será

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}$$

Sin embargo, puesto que t es divisible por p, también $\frac{(t-1)t}{2}$ será divisible por p en todos los casos, excepto en aquél donde $p = 2$, sobre el cual ya hemos informado en el artículo anterior. Pero, en los casos restantes será $\frac{(t-1)t}{2}\alpha^{t-2}hp \equiv 0 \pmod{p^2}$,

y por tanto también la suma $\equiv t\alpha^{t-1} \pmod{p^2}$ como en el artículo anterior. El resto de la demostración procede aquí del mismo modo.

Por lo tanto, concluimos en general, excepto en el único caso $p = 2$, que

$$(\alpha + hp^{\mu})^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$$

y $(\alpha + hp^{\mu})^t$ *no* $\equiv \alpha^t$ para cualquier módulo que sea una potencia de p mayor que $p^{\mu+\nu}$, siempre que h no sea divisible por p, y que p^{ν} sea la potencia mayor de p que divide al número t.

De aquí, se derivan directamente las proposiciones 1 y 2, que nos habíamos propuesto demostrar: a saber,

primero, si $\alpha^t \equiv 1$, será también $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$;

segundo, si algún número α' es congruente, según el módulo p, a A, y luego también a α, pero no congruente a α según el módulo $p^{n-\nu}$, y si satisface la congruencia $x^t \equiv 1 \pmod{p^n}$. Suponemos α' es $= \alpha + lp^{\lambda}$ de modo que l no es divisible por p, entonces será $\lambda < n - \nu$, pero entonces $(\alpha + lp^{\lambda})^t$ será congruente a α^t según el módulo $p^{\lambda+\nu}$, pero no según el módulo p^n que es una potencia mayor, por lo que α' no es una raíz de la congruencia $x^t \equiv 1$.

88.

Tercero, se debe buscar alguna raíz de la congruencia $x^t \equiv 1 \pmod{p^n}$ que sea congruente a A. Mostraremos aquí solamente cómo puede hacerse esto si ya se conoce una raíz de esta misma congruencia según el módulo p^{n-1}. Es claro que esto es suficiente, ya que podemos ir del módulo p para el cual A es una raíz, al módulo p^2 y de este a todas las potencias siguientes.

Así, sea α una raíz de la congruencia $x^t \equiv 1 \pmod{p^{n-1}}$, búsquese una raíz de la misma congruencia, según el módulo p^n. Póngase ésta $= \alpha + hp^{n-\nu-1}$, la cual debe tener esta forma según el artículo anterior (consideraremos por separado el caso donde $\nu = n - 1$ pues ν no puede ser mayor que $n - 1$). Por lo tanto, tendremos

$$(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^{n-1}}$$

Pero

$$(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$$

Así, por consiguiente, si h se determina de modo que $1 \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$; o sea (puesto que por hipótesis $1 \equiv \alpha^t \pmod{p^{n-1}}$ y t es divisible por

p^ν) $\frac{\alpha^t-1}{p^{n-1}} + \alpha^{t-1}h\frac{t}{p^\nu}$ es divisible por p, tendremos la raíz buscada. Que esto se puede hacer es claro a partir de la sección anterior, puesto que hemos supuesto que aquí t no puede dividirse por una potencia de p mayor que p^ν, por lo tanto $\alpha^{t-1}\frac{t}{p^\nu}$ es primo a p.

Pero si $\nu = n-1$, i.e., t es divisible por p^{n-1} o sea también por una potencia mayor de p, cualquier valor de A que satisface a la congruencia $x^t \equiv 1$ según el módulo p, también satisfará a la misma según el módulo p^n. Pues si $t = p^{n-1}\tau$, será $t \equiv \tau \pmod{p-1}$: de donde, puesto que $A^t \equiv 1 \pmod{p}$, será también $A^\tau \equiv 1 \pmod{p}$. Ahora sea $A^\tau = 1 + hp$, tendremos $A^t = (1+hp)^{p^{n-1}} \equiv 1 \pmod{p^n}$ (art. 87).

89.

Todo lo derivado en el artículo 57 y siguientes con la ayuda del teorema que establece que la congruencia $x^t \equiv 1$ no puede tener más que t raíces diferentes, también vale para un módulo que es una potencia de un número primo. Si se les llama *raíces primitivas* a los números que pertenecen al exponente $p^{n-1}(p-1)$, es decir, en cuyos períodos aparecen todos los números no divisibles por p, entonces aquí también habrá raíces primitivas. Todo lo que antes presentamos sobre los índices y su aplicación a la resolución de la congruencia $x^t \equiv 1$, también puede aplicarse a este caso. Puesto que esto no ha presentado ninguna dificultad, sería superfluo repetir todo aquí. Además hemos mostrado cómo las raíces de la congruencia $x^t \equiv 1$, según el módulo p^n, pueden derivarse de las raíces de la misma congruencia según el módulo p. Pero todavía hay que agregar algo al caso donde una potencia del número 2 es módulo, puesto que fue excluído anteriormente.

Módulos que son potencias de 2.

90.

Si se toma alguna potencia del número 2, mayor que la segunda, como módulo, por ejemplo 2^n, la potencia 2^{n-2} de cualquier número impar es congruente a la unidad.

Por ejemplo $3^8 = 6561 \equiv 1 \pmod{32}$.

De hecho, cualquier número impar o está comprendido en la forma $1+4h$ o bien en $-1+4h$: de donde la proposición sigue directamente (teorema art. 86).

Puesto que el exponente al cual pertenece cualquier número impar, según el módulo 2^n, debe ser divisor de 2^{n-2}, pertenecerá a alguno de los números 1, 2, 4, 8, $\ldots 2^{n-2}$, entonces es fácil juzgar a cuál de ellos pertenece. Si el número propuesto $= 4h \pm 1$, y la mayor potencia de 2 que divide a h es $= m$ (que también puede ser $= 0$, cuando h es impar); entonces el exponente al cual pertenece el número propuesto será $= 2^{n-m-2}$ si $n > m+2$. Pero, si $n = 0$ o $< m+2$, el número propuesto es $\equiv \pm 1$ y pertenecerá o al exponente 1 o al exponente 2. Es claro que un número de la forma $\pm 1 + (2^{m+2}k)$ (la cual equivale a $4h \pm 1$) elevado a la potencia 2^{n-m-2}, será congruente a la unidad según el módulo 2^n, pero incongruente si es elevado a una potencia inferior del número 2, como se deduce del art. 86 con facilidad. Por lo tanto, cualquier número de la forma $8k+3$ o $8k+5$ pertenecerá al exponente 2^{n-2}.

91.

Se sigue de aquí que no se presentan *raíces primitivas* en el sentido aceptado antes por nosotros para esta expresión. Esto es, no hay números cuyos períodos comprenden todos los números menores que el módulo y primos a él. Sin embargo, se percibe fácilmente que aquí existe una analogía. De hecho, se encuentra que una potencia impar de un número de la forma $8k+3$ siempre tiene la forma $8k+3$; mientras que una potencia par siempre es de la forma $8k+1$. Por tanto, ninguna potencia puede ser de la forma $8k+5$ u $8k+7$. Puesto que el período de un número de la forma $8k+3$ consta de 2^{n-2} términos diferentes, cada uno de los cuales es o de la forma $8k+3$ o de la forma $8k+1$, y como no se dan más que 2^{n-2} números menores que el módulo, evidentemente cada número de la forma $8k+1$ u $8k+3$ es congruente, según el módulo 2^n, a alguna potencia de un número cualquiera de la forma $8k+3$. De modo similar puede demostrarse que el período de un número de la forma $8k+5$ consta de todos los números de la forma $8k+1$ y $8k+5$. Si, por lo tanto, se toma como base un número de la forma $8k+5$, se obtendrán índices reales de todos los números de la forma $8k+1$ y $8k+5$ tomados positivamente y de todos los de la forma $8k+3$ y $8k+7$ tomados negativamente. Aquí se consideran equivalentes dos índices congruentes según 2^{n-2}. De este modo, se debe interpretar nuestra Tabla I donde siempre tomamos el número 5 como base para los módulos 16, 32 y 64 (puesto que para el módulo 8 ninguna tabla es necesaria). Por ejemplo, al número 19, que es de la forma $8n+3$, y por lo tanto está tomado negativamente, le corresponde el índice 7 para el módulo 64, esto es $5^7 \equiv -19 \pmod{64}$. Pero al tomar números de las formas $8n+1$, $8n+5$ negativamente, y los números de las formas $8n+3$, $8n+7$ positivamente,

ciertos índices tendrán que considerarse imaginarios. Con la introducción de esto, el cálculo de índices puede reducirse a un algoritmo bastante simple. Pero, puesto que, si deseamos exponer esto con todo rigor, nos llevará mucho tiempo, reservamos este trabajo para otra ocasión cuando quizás intentemos profundizar la teoría de las cantidades imaginarias, la cual, a nuestro juicio, nadie ha reducido a nociones claras. Los expertos pueden encontrar este algoritmo con facilidad; los menos hábiles, sin embargo, pueden usar esta tabla si han comprendido los principios presentados arriba, de la misma manera como quienes no saben nada sobre las investigaciones modernas sobre *logaritmos* imaginarios aún usan logaritmos.

Módulos compuestos de varios primos.

92.

Según un módulo compuesto de varios primos, casi todo lo que pertenece a los residuos de las potencias puede deducirse de la teoría general de las congruencias. Pero, puesto que después enseñaremos en detalle a reducir cualquier congruencia, según un módulo compuesto de varios primos, a congruencias, de las cuales el módulo es o primo o una potencia de un primo, no nos detendremos más en esto. Solamente observamos que la bellísima propiedad que vale para los otros módulos, a saber que siempre existen números cuyo período comprende todos los números primos al módulo, aquí no vale, excepto en un único caso, cuando el módulo es el doble de un número primo, o de una potencia de un número primo. De hecho si el módulo m se reduce a la forma $A^aB^bC^c$ etc., donde A, B, C, etc. denotan números primos diferentes, y si además se denota $A^{a-1}(A-1)$ por α, $B^{b-1}(B-1)$ por β, etc., y luego z es un número primo a m; será $z^\alpha \equiv 1 \pmod{A^a}$, $z^\beta \equiv 1 \pmod{B^b}$, etc. Por tanto, si μ es el mínimo común múltiplo de los números α, β, γ, etc., será $z^\mu \equiv 1$ según todos los módulos A^a, B^b, etc., de donde también según m, que es igual al producto de aquéllos. Pero, excepto el caso donde m es el doble de un número primo o de una potencia de un número primo, el mínimo común múltiplo de los números α, β, γ, etc. es menor que su producto (puesto que los números α, β, γ, etc. no pueden ser primos entre sí, sino que tienen el divisor común 2). Por tanto, ningún período puede comprender tantos términos como números menores y primos al módulo, puesto que el número de éstos es igual al producto de α, β, γ, etc. Así, por ejemplo, para $m = 1001$ la potencia 60 de cualquier número primo a m es congruente a la unidad, pues 60 es el mínimo común múltiplo de 6, 10 y 12. El caso donde el módulo es el doble de un número primo, o el doble de una potencia de un primo es totalmente

análogo al caso donde es primo o una potencia de un primo.

93.

Ya se ha hecho mención de los escritos donde otros geómetras han hablado del argumento tratado en esta sección. Para los que desean otros detalles más amplios, mencionamos en particular los siguientes comentarios del ilustre Euler que, por su perspicacia distinguen a este hombre de los demás.

Theoremata circa residua ex divisione potestatum relicta, Comm. nov. Petr., VII p. 49 y siguientes.

Demostrationes circa residua ex divisione potestatum per numeros primos resultantia, ibid., XVIII p. 85 y siguientes.

También puede agregarse *Opusculorum analyt.* 1, disertaciones 5 y 8.