Sección Segunda

SOBRE

LAS CONGRUENCIAS DEL PRIMER GRADO

Teoremas preparatorios sobre los números primos, factores, etc.

13.

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

Sea p primo, y a positivo $< p$: entonces no puede encontrarse ningún número positivo b menor que p tal que $ab \equiv 0 \pmod{p}$.

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

14.

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

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

Euclides ya había demostrado este teorema en sus *Elementos* (libro VII, No. 32). No obstante deseábamos no omitirlo puesto que muchos autores modernos han usado razonamientos inciertos en vez de demostraciones, o bien han despreciado el teorema completamente. Además, mediante este uso muy sencillo, podemos con más facilidad comprender la naturaleza del método que se usará más adelante para resolver problemas mucho más difíciles.

15.

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

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

16.

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

Demostración. Que cualquier número compuesto pueda resolverse en factores primos, resulta de consideraciones elementales, pero está supuesto tácitamente, y en general sin demostración, que no puede hacerse de muchas maneras diferentes. Supongamos que algún número compuesto A, que es $= a^\alpha b^\beta c^\gamma$ etc., donde a, b, c, etc. denotan números primos diferentes, es resoluble en factores primos de otra manera.

Primero, es claro que no puede aparecer en este segundo sistema de factores ningún otro primo mas que a, b, c, etc. puesto que ningún otro primo puede dividir a A, el cual está compuesto de estos primos. De forma semejante, ninguno de los primos a, b, c, etc. puede estar ausente del segundo sistema de primos, puesto que si no, no podría dividir a A (artículo anterior). Así, estas dos resoluciones en factores pueden ser diferentes solamente si un primo aparece más veces en una resolución que en la otra. Sea p un tal primo que aparece m veces en una resolución, y n veces en la otra, y tal que $m > n$. Al disminuir en n el número de factores p en cada sistema,

quedarán $m-n$ factores p en un sistema mientras que no quedará ninguno en el otro. Esto es, tenemos dos resoluciones en factores del número $\frac{A}{p^n}$. El que una de ellas no contenga al factor p mientras que la otra lo contenga $m-n$ veces contradice lo que acabamos de demostrar.

17.

Si un número compuesto A es el producto de B, C, D, etc., entonces entre los factores primos de B, C, D, etc., no puede aparecer ninguno que no sea factor de A. Además cada uno de estos factores debe aparecer en la resolución de A tantas veces como aparece en B, C, D, etc., en total. Por lo tanto tenemos un criterio para determinar si un número B divide a un número A o no. B dividirá a A siempre que contenga sólo factores primos de A mismo, y siempre que no los contenga más veces que A. Si alguna condición no se cumple, B no divide a A.

Es fácil ver por el cálculo de las combinaciones que si, como arriba, a, b, c, etc., son números primos diferentes y si $A = a^\alpha b^\beta c^\gamma$ etc., entonces A tendrá

$$(\alpha+1)(\beta+1)(\gamma+1) \quad \text{etc.}$$

divisores diferentes, incluyendo a 1 y a A mismo.

18.

Por lo tanto si $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\kappa l^\lambda m^\mu$ etc., y si los primos a, b, c, etc., k, l, m, etc., son todos diferentes, entonces es claro que A y K no tienen un factor común aparte de 1, o sea: son primos relativos.

Dados varios números A, B, C, etc., el *máximo común divisor* se determina de la manera siguiente. Supóngase que todos los números están resueltos en sus factores primos, y de estos últimos se extraen aquéllos que sean comunes a A, B, C, etc., (si no hay ninguno, no habrá un divisor común de todos ellos). Luego, se nota el número de veces que aparece cada factor primo en A, en B, en C, etc., o sea se nota cuál exponente tiene cada uno de ellos en A, en B, en C, etc. Finalmente asignamos a cada factor el más pequeño de los exponentes que tenga en A, en B, en C, etc. Al formar el producto de estos obtendremos el común divisor buscado.

Cuando deseamos el *mínimo común múltiplo*, seguimos el siguiente procedimiento: se reunen todos los números primos que dividen a alguno de los números A,

B, C, etc., y se asigna a cada uno el mayor exponente que tiene en A, B, C, etc. Al formar el producto de éstos, tendremos el múltiplo que buscamos.

Ejemplo. Sea $A = 504 = 2^3 3^2 7$, $B = 2880 = 2^6 3^2 5$, $C = 864 = 2^5 3^3$. Para el máximo común divisor tenemos los factores primos 2 y 3 con los exponentes 3 y 2 respectivamente; esto será $2^3 3^2 = 72$, y el menor número divisible por ellos en común será $2^6 3^5 5 \cdot 7 = 60480$.

Omitimos las demostraciones debido a su facilidad. Además, sabemos por consideraciones elementales cómo resolver estos problemas cuando la resolución de los números A, B, C, etc., no viene dada.

19.

Si los números a, b, c, etc., son todos primos relativos a k, también su producto será primo relativo a k.

Como ninguno de los números a, b, c, etc., tiene un factor primo común con k, y como el producto abc etc., no tiene factores primos diferentes de los factores primos de uno de los números a, b, c, etc., el producto abc etc., tampoco tendrá ningún factor primo común con k. Por lo tanto se sigue del artículo anterior que k y abc etc. son primos relativos.

Si los números a, b, c, etc., son primos entre sí, y si cada uno de ellos divide a algún k, entonces su producto divide a k.

Esto se sigue fácilmente de los artículos 17 y 18. Sea p un divisor primo del producto abc etc. que lo contiene π veces. Es claro que alguno de los números a, b, c, etc., tiene que contener este mismo divisor π veces. Luego también k, al cual este número divide, contiene π veces a p. De manera semejante sucede con los restantes divisores del producto abc etc.

Así, *si dos números m y n son congruentes según varios módulos a, b, c, etc., que son primos entre sí, entonces serán congruentes según el producto de ellos.*

Como $m-n$ es divisible por cada uno de los números a, b, c, etc., será divisible por su producto también.

Finalmente, *si a es primo a b y ak es divisible por b, entonces k también es divisible por b. Porque ak es divisible por ambos a y b, es divisible por ab también; es decir* $\frac{ak}{ab} = \frac{k}{b}$ *es un entero.*

20.

Cuando $A = a^\alpha b^\beta c^\gamma$ *etc., donde* a, b, c, *etc., son números primos distintos, es alguna potencia, digamos* k^n, *todos los exponentes* α, β, γ, *etc., serán divisibles por* n.

Puesto que el número k no involucra factores primos diferentes de a, b, c, etc., supóngase que k contiene el factor a, α' veces. k^n, o A, contendrá este factor $n\alpha'$ veces. Por lo tanto $n\alpha' = \alpha$ y $\frac{\alpha}{n}$ es un número entero. De igual manera se demuestra que $\frac{\beta}{n}$, etc., son números enteros.

21.

Cuando a, b, c, *etc., son primos entre sí y el producto abc etc. es alguna potencia, por ejemplo* k^n, *entonces cada uno de los números* a, b, c, *etc., será una potencia semejante.*

Sea $a = l^\lambda m^\mu p^\pi$ etc. con l, m, p, etc., números primos diferentes. Por hipótesis, ninguno de ellos es factor de los números b, c, etc. Así, el producto abc etc. contendrá λ veces el factor l, μ veces el factor m, etc. Así que (por el artículo anterior) λ, μ, π, etc., son divisibles por n y resulta que

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}} \quad \text{etc.}$$

es un entero. De manera semejante para los restantes b, c, etc.

Estos teoremas sobre los números primos tenían que presentarse primero; ahora nos dedicaremos a las proposiciones propias de nuestros fines.

22.

Si los números a *y* b *son divisibles por otro número* k, *y si son congruentes según un módulo* m *que es primo a* k, *entonces* $\frac{a}{k}$ *y* $\frac{b}{k}$ *serán congruentes según el mismo módulo.*

Es claro que $a - b$ es divisible por k y además por m (por hipótesis); así que (art. 19) $\frac{a-b}{k}$ es divisible por m, o sea, $\frac{a}{k} \equiv \frac{b}{k} \pmod{m}$.

Manteniendo iguales las otras cosas, si m y k tienen un máximo común divisor e, entonces $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$, puesto que $\frac{k}{e}$ y $\frac{m}{e}$ son primos entre sí. Pero $a - b$ es divisible por k y por m, así que $\frac{a-b}{e}$ es divisible por $\frac{k}{e}$ y por $\frac{m}{e}$, entonces es divisible por $\frac{km}{e^2}$; esto es $\frac{a-b}{k}$ es divisible por $\frac{m}{e}$, lo cual implica que $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$.

23.

Si a es primo a m, y e y f, no son congruentes según el módulo m, entonces ae y af, tampoco serán congruentes según el módulo m.

Esto es simplemente el recíproco del teorema anterior.

Después de esto, es evidente que si se multiplica a por todos los números enteros de 0 hasta $m-1$, y se reduce cada producto a su menor resto según el módulo m, entonces todos serán diferentes. Como hay m de estos restos, ninguno de los cuales es $> m$, se encuentran entre ellos todos los números de 0 hasta $m-1$.

24.

La expresión $ax+b$, donde a y b son números dados y x denota un número indeterminado o variable, *puede hacerse congruente según el módulo m a cualquier número, siempre que m sea primo a a.*

Sea c el número al cual se hará congruente, y sea e el menor resto positivo de $c-b$ según el módulo m. Por el artículo anterior necesariamente se da un valor de x $< m$ tal que el menor resto del producto ax según el módulo m será e. Si este valor es v, $av \equiv e \equiv c-b$; por lo tanto $av+b \equiv c \pmod{m}$. *Q. E. F.*

25.

Llamamos *congruencia* a cualquier expresión que contiene dos cantidades congruentes como en una ecuación. Si involucra una incógnita, se dice que se *resuelve* cuando se encuentra un valor (*raíz*) que satisface la congruencia. Así es claro lo que significan una *congruencia resoluble y congruencia no resoluble.* Obviamente se pueden usar aquí las distinciones parecidas a las usadas al hablar de las ecuaciones. Ejemplos de congruencias *trascendentales* se darán más adelante. Las congruencias *algebraicas* se distribuyen según la mayor potencia de la incógnita en congruencias de primero, de segundo, y de más altos *grados.* De manera semejante se pueden proponer varias congruencias involucrando varias incógnitas, y podemos hablar de su *eliminación.*

La resolución de las congruencias del primer grado.

26.

La congruencia del primer grado $ax+b \equiv c$, según el artículo 24, siempre es

resoluble cuando el módulo es primo relativo a a. Ahora, si v es un valor conveniente de x, o sea, es una raíz de la congruencia, resulta claro que todo número congruente a v según el módulo involucrado también es raíz (art. 9). Con igual facilidad se ve que todas las raíces tienen que ser congruentes a v. De hecho si t es otra raíz, entonces $av + b \equiv at + b$, entonces $av \equiv at$, $v \equiv t$ (art. 22). Se concluye que la congruencia $x \equiv v \pmod{m}$ representa la solución completa de la congruencia.

Como todos los valores de x que son valores de la congruencia son congruentes entre sí, y como así los números congruentes pueden considerarse equivalentes, se puede considerar tales soluciones como una sola. Por lo cual, como nuestra congruencia $ax + b \equiv c$ no admite otras soluciones, diremos que tiene una, y únicamente una solución, o bien que tiene una, y únicamente una raíz. Así, por ejemplo, la congruencia $6x + 5 \equiv 13 \pmod{11}$ no admite más raíces que las que son $\equiv 5 \pmod{11}$. Esto no es cierto en las congruencias de otros grados ni en las congruencias del primer grado en las cuales se multiplica la incógnita por un número que no es primo relativo al módulo.

27.

Quedan por añadir algunos detalles sobre el cálculo de la solución de alguna congruencia. Primero notamos que una congruencia de la forma $ax + t \equiv u$, donde suponemos que el módulo es primo a a, depende de $ax \equiv \pm 1$. Porque si $x \equiv r$ satisface esta última, $x \equiv \pm(u - t)r$ satisfará la penúltima. Pero la congruencia $ax \equiv \pm 1$, cuyo módulo se denota por b, es equivalente a la ecuación indeterminada $ax = by \pm 1$. Como hoy en día es conocida la resolución de ella, basta presentar el algoritmo para su cálculo.

Si las cantidades A, B, C, D, E, etc., dependen de α, β, γ, δ, etc., de tal manera que

$$A = \alpha, \quad B = \beta A + 1, \quad C = \gamma B + A, \quad D = \delta C + B, \quad E = \epsilon D + C, \text{ etc.}$$

por brevedad las escribimos así:

$$A = [\alpha], \quad B = [\alpha, \beta], \quad C = [\alpha, \beta, \gamma], \quad D = [\alpha, \beta, \gamma, \delta], \quad \text{etc.*)}$$

*) Esta relación puede considerarse con más generalidad, como lo haremos en otra ocasión. Aquí solamente añadiremos dos proposiciones que serán útiles para nuestras investigaciones, a saber: 1º. $[\alpha, \beta, \gamma, \ldots, \lambda, \mu] \cdot [\beta, \gamma, \ldots, \lambda] - [\alpha, \beta, \gamma, \ldots, \lambda] \cdot [\beta, \gamma, \ldots, \lambda, \mu] = \pm 1$

Ahora consideramos la ecuación indeterminada $ax = by+1$, donde a y b, son positivos. Podemos suponer sin pérdida de generalidad que a no es $< b$. Ahora, mediante el algoritmo conocido para calcular el máximo común divisor de dos números, formamos a través de la división ordinaria las ecuaciones

$$a = \alpha b + c, \quad b = \beta c + d, \quad c = \gamma d + e, \quad \text{etc.},$$

así que α, β, γ, etc., c, d, e, etc., son enteros siempre positivos, y b, c, d, e, decrecen hasta que encontramos $m = \mu n + 1$, algo que eventualmente debe ocurrir. Así resulta

$$a = [n, \mu, \ldots, \gamma, \beta, \alpha], \qquad b = [n, \mu, \ldots, \gamma, \beta].$$

Si tomamos $\qquad x = [\mu, \ldots, \gamma, \beta], \qquad y = [\mu, \ldots, \gamma, \beta, \alpha]$

tendremos $ax = by + 1$ cuando el número de términos α, β, γ, $\ldots \mu$, es par, o bien $ax = by - 1$ cuando es impar.

28.

El ilustre Euler fue el primero en dar la resolución general para las ecuaciones indeterminadas de este tipo (*Comment. Petrop. T.* VII. *p.* 46). El método que él usó consistía en sustituir x e y por otras incógnitas, y hoy es bien conocido. El ilustre Lagrange trató el problema de una manera un tanto diferente. Como él mismo observó, es claro a partir de la teoría de las fracciones continuas que si la fracción $\frac{a}{b}$ se convierte en la fracción continua

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \text{ etc.}}}}$$

$$+\cfrac{1}{\mu + \cfrac{1}{n}}$$

donde se toma el signo superior cuando el número de términos α, β, γ, $\ldots \lambda$, μ es par, y el inferior cuando es impar.

2º. El orden de los números α, β, γ, etc. puede invertirse: $[\alpha, \beta, \gamma, \ldots, \lambda, \mu] = [\mu, \lambda, \ldots, \gamma, \beta, \alpha]$. Omitimos las demostraciones sencillas.

y si de la última parte se borra $\frac{1}{n}$ y se reconvierte en una fracción $\frac{x}{y}$, entonces $ax = by \pm 1$, siempre que a sea primo a b. Además, se obtiene el mismo algoritmo de los dos métodos. Las investigaciones del ilustre Lagrange aparecen en *Hist. de l'Ac. de Berlin*, 1767, *p.* 173, y con otros en los apéndices de la versión francesa del *Algebra* de Euler.

29.

La congruencia $ax + t \equiv u$, cuyo módulo no es primo a a, se reduce fácilmente al caso anterior. Sea m el módulo y sea δ el máximo común divisor de a y m. Es claro que cualquier valor de x que satisface la congruencia según el módulo m también la satisface según el módulo δ (art. 5). Pero $ax \equiv 0 \pmod{\delta}$ puesto que δ divide a a. Por tanto la congruencia no tiene solución a menos que $t \equiv u \pmod{\delta}$, esto es $t - u$ es divisible por δ.

Ahora, sean $a = \delta e$, $m = \delta f$, $t - u = \delta k$; e será primo a f. Entonces $ex + k \equiv 0 \pmod{f}$ será equivalente a la congruencia propuesta $ax + t \equiv u$; esto es, cualquier valor de x que cumple la una también satisfará la otra y viceversa. Porque claramente $ex + k$ es divisible por f cuando $\delta ex + \delta k$ es divisible por δf, y viceversa. Pero vimos antes cómo resolver la congruencia $ex + k \equiv 0 \pmod{f}$; así es claro que si v es uno de los valores de x, $x \equiv v \pmod{f}$ nos da la solución completa de la congruencia propuesta.

30.

Cuando el módulo es compuesto, a veces es ventajoso usar el siguiente método.

Sea el módulo $= mn$, y la congruencia propuesta $ax \equiv b$. Primero, se resuelve la congruencia según el módulo m, y se supone que resulta $x \equiv v \pmod{\frac{m}{\delta}}$ donde δ es el máximo común divisor de los números m y a. Es claro que cualquier valor de x que satisface la congruencia $ax \equiv b$ según el módulo mn también la satisface según el módulo m, y será expresable en la forma $v + \frac{m}{\delta}x'$ donde x' es algún número indeterminado. El recíproco, sin embargo, no es cierto puesto que no todos los números de la forma $v + \frac{m}{\delta}x'$ satisfacen la congruencia según el módulo mn. La manera de determinar x' tal que $v + \frac{m}{\delta}x'$ es una raíz de la congruencia $ax \equiv b \pmod{mn}$ puede deducirse de la solución de la congruencia $\frac{am}{\delta}x' + av \equiv b \pmod{mn}$ o de la congruencia equivalente $\frac{a}{\delta}x' \equiv \frac{b-av}{m} \pmod{n}$. Por tanto la resolución de cualquier congruencia según el módulo mn puede reducirse a la resolución de dos

congruencias según los módulos m y n. Y es evidente que si n es otra vez el producto de dos factores, la resolución de la congruencia, relativa al módulo n depende de la resolución de las congruencias cuyos módulos son estos factores. En general la resolución de una congruencia según el módulo compuesto depende de la resolución de otras congruencias cuyos módulos son factores del módulo compuesto. Estos factores pueden tomarse como números primos si esto es conveniente.

Ejemplo. Si se propone la congruencia $19x \equiv 1 \pmod{140}$, se resuelve primero según el módulo 2, y resulta $x \equiv 1 \pmod{2}$. Sea $x = 1+2x'$; se convierte en $38x' \equiv -18 \pmod{140}$, o lo que es equivalente, $19x' \equiv -9 \pmod{70}$. Si se resuelve esta otra vez según el módulo 2, resulta $x' \equiv 1 \pmod{2}$, y al colocar $x' = 1 + 2x''$ se convierte en $38x'' \equiv -28 \pmod{70}$ o $19x'' \equiv -14 \pmod{35}$. Según el módulo 5 nos da la solución $x'' \equiv 4 \pmod{5}$, y sustituyendo $x'' = 4 + 5x'''$ se convierte en $95x''' \equiv -90 \pmod{35}$ o $19x''' \equiv -18 \pmod{7}$. De esto resulta $x''' \equiv 2 \pmod{7}$, y al colocar $x''' = 2 + 7x''''$ resulta $x = 59 + 140x''''$; por lo tanto $x \equiv 59 \pmod{140}$ es la solución completa de la congruencia propuesta.

31.

De la misma manera que se expresa la raíz de la ecuación $ax = b$ por $\frac{b}{a}$, designamos por $\frac{b}{a}$ la raíz de la congruencia $ax \equiv b$, y adjuntamos el módulo de la congruencia para distinguirla. Así por ejemplo, $\frac{19}{17} \pmod{12}$ significa cualquier número que es $\equiv 11 \pmod{12}$*). Es claro de esto en general que $\frac{b}{a} \pmod{c}$ no significa nada real (o si se quiere, es imaginario) cuando a y c tienen un común divisor que no divide a b. Aparte de este caso excepcional, la expresión $\frac{b}{a} \pmod{c}$ siempre tendrá valores reales, de hecho, un número infinito de ellos. Todos ellos serán congruentes según c cuando a es primo a c, o primo a $\frac{c}{\delta}$ cuando δ es el máximo común divisor de c y a.

Estas expresiones tienen un algoritmo muy parecido al empleado para las fracciones ordinarias. Indicamos unas propiedades que pueden deducirse fácilmente de la discusión anterior.

1. Si según el módulo c, $a \equiv \alpha$, $b \equiv \beta$, entonces las expresiones $\frac{a}{b} \pmod{c}$ y $\frac{\alpha}{\beta} \pmod{c}$ son equivalentes.
2. $\frac{a\delta}{b\delta} \pmod{c\delta}$ y $\frac{a}{b} \pmod{c}$ son equivalentes.
3. $\frac{ak}{bk} \pmod{c}$ y $\frac{a}{b} \pmod{c}$ son equivalentes cuando k es primo a c.

*) Por analogía esto puede expresarse como $\frac{11}{1} \pmod{12}$.

Podríamos citar muchas otras proposiciones parecidas, pero, como no presentan ninguna dificultad ni son necesarias para lo siguiente, procedemos a otros temas.

La búsqueda de un número congruente a un número dado según un módulo dado.

32.

Se puede fácilmente, por medio de lo que precede, *hallar todos los números que tienen residuos dados, según cualquier módulo,* esto nos servirá mucho en lo que sigue.

Sean, en primer lugar, A y B, dos módulos según los cuales el número buscado z tiene que ser congruente a los números a y b. Todos los valores de z están necesariamente contenidos en la fórmula $Ax + a$, donde x es indeterminado, pero tal que $Ax + a \equiv b \pmod{B}$. De manera que si δ es el máximo común divisor de A y de B, la resolución completa de esta congruencia tomará la forma $x \equiv v \pmod{\frac{B}{\delta}}$, o sea, lo que es igual, $x = v + \frac{kB}{\delta}$, siendo k un número entero indeterminado. Por lo tanto, la fórmula $Av + a + \frac{kAB}{\delta}$ contiene todos los valores de z, lo que se reduce a $z \equiv Av + a \pmod{\frac{AB}{\delta}}$. Si hay un tercer módulo C según el cual el número buscado tiene que ser congruente a c, se sigue el mismo procedimiento, según el cual se debe reunir las dos primeras condiciones en una sola. Así, sea ϵ el máximo común divisor de los números $\frac{AB}{\delta}$ y C, entonces se obtendrá la congruencia $\frac{AB}{\delta}x + Av + a \equiv c \pmod{C}$, que será resuelta por una congruencia de la forma $x \equiv w \pmod{\frac{C}{\epsilon}}$ y la propuesta será resuelta completamente por la congruencia $z \equiv \frac{ABw}{\delta} + Av + a \pmod{\frac{ABC}{\delta\epsilon}}$. Se procede de la misma manera sea cual sea el número de módulos. Es conveniente observar que $\frac{AB}{\delta}$ y $\frac{ABC}{\delta\epsilon}$ son los menores números divisibles a la vez por A y B, o por A, B y C y se puede concluir fácilmente que sea cual sea la cantidad de módulos A, B, C, etc., si se representa por M el menor número divisible por cada uno de ellos, se tendrá la resolución completa al tomar $z \equiv r \pmod{M}$. Pero cuando alguna de las congruencias auxiliares es irresoluble, concluimos que el problema involucra una imposibilidad. Pero obviamente esto no puede ocurrir cuando todos los números A, B, C, etc., son primos entre sí.

Ejemplo. Sean los números A, B, C, a, b, c, iguales a 504, 35, 16, 17, -4, 33. Aquí las dos condiciones $z \equiv 17 \pmod{504}$ y $z \equiv -4 \pmod{35}$ son equivalentes a la única condición $z \equiv 521 \pmod{2520}$. Al adjuntar la condición $z \equiv 33 \pmod{16}$, nos dará finalmente $z \equiv 3041 \pmod{5040}$.

33.

Si todos los números A, B, C, etc., son primos entre sí, es claro que el producto de ellos es igual a su mínimo común múltiplo. En tal caso, todas las congruencias $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, etc., son equivalentes a la única congruencia $z \equiv r \pmod{R}$, donde R denota el producto de los números A, B, C, etc. Resulta en seguida que la sola condición $z \equiv r \pmod{R}$, puede descomponerse en varias; de hecho, si R se resuelve en factores A, B, C, etc., que son primos entre sí, entonces las condiciones $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$, $z \equiv r \pmod{C}$ etc., agotan la condición original. Esta observación nos abre no solamente un método de descubrimiento de la imposibilidad cuando existe, sino también un método más cómodo y más elegante para calcular las raíces.

34.

Sean, como arriba, $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$. Se resuelven todos los módulos en factores que son primos entre sí: A en A', A'', A''', etc., B en B', B'', B''', etc., y de tal manera que los números A', A'', etc., B', B'', etc., etc., o bien son primos o bien son potencias de primos. Si cualquiera de los números A, B, C, etc., ya es primo o la potencia de un primo, no hay que resolverlo en factores. Entonces, de lo anterior es claro que en vez de las condiciones propuestas podemos poner las siguientes: $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$, etc., $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$, etc., etc. Ahora, si no todos los números A, B, C, son primos entre sí (por ejemplo si A no es primo a B), es obvio que no pueden ser diferentes todos los factores primos de A y B. Tiene que ser uno u otro de ellos entre los factores A', A'', A''', etc., que tiene entre los factores B', B'', B''', etc., uno que es igual, o bien un múltiplo, o bien un divisor propio. Primero, supóngase que $A' = B'$. Entonces las condiciones $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$, tienen que ser idénticas; $a \equiv b \pmod{A' \text{ o } B'}$, y así se puede ignorar una. Sin embargo, si no se da que $a \equiv b \pmod{A}$, el problema es imposible de resolver. Si, en segundo lugar, B' es múltiplo de A', la condición $z \equiv a \pmod{A'}$ tiene que ser incluída en la condición $z \equiv b \pmod{B'}$; o sea la congruencia $z \equiv b \pmod{A'}$ que se deduce de la posterior tiene que ser idéntica a la primera. De esto se sigue que la condición $z \equiv a \pmod{A}$ puede rechazarse a menos que sea inconsistente con alguna otra condición (en cuyo caso el problema es imposible). Cuando todas las condiciones superfluas han sido rechazadas, todos los módulos que queden de los factores A', A'', A''', etc., B', B'', B''', etc., etc. serán primos entre sí. Entonces podemos estar seguros de la

posibilidad del problema y proceder como antes.

35.

Ejemplo. Si, como arriba (art. 32), $z \equiv 17 \pmod{504}$, $z \equiv -4 \pmod{35}$ y $z \equiv 33 \pmod{16}$, entonces estas condiciones pueden reducirse a las siguientes: $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$, $\equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$, $\equiv 33 \pmod{16}$. De estas condiciones $z \equiv 17 \pmod{8}$, $z \equiv 17 \pmod{7}$, pueden omitirse puesto que la primera está contenida en la condición $z \equiv 33 \pmod{16}$ y la segunda es idéntica a $z \equiv -4 \pmod{7}$. Permanecen:

$$z \equiv \left| \begin{array}{l} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{array} \right. \qquad \text{y así:} \quad z \equiv 3041 \pmod{5040}$$

Es cierto que a veces es más conveniente reunir las congruencias que se derivan de una misma condición separadamente de las condiciones restantes, puesto que es fácil hacerlo; e.g., cuando se eliminan unas de las condiciones $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, etc., se reemplazan las restantes por $z \equiv a$ según el módulo que es el producto de todos los módulos que se quedan del conjunto A', A'', A''', etc. Así que, en nuestro ejemplo, las condiciones $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$ se reemplazan por $z \equiv -4 \pmod{35}$. Además resulta que no es indiferente para abreviar los cálculos cuáles condiciones superfluas se rechazan. Pero no es nuestro propósito tratar estos detalles ni otros artificios prácticos que pueden aprenderse más fácilmente por práctica que por preceptos.

36.

Cuando todos los módulos A, B, C, D, etc., son primos entre sí, muchas veces es mejor usar el siguiente método.

Se determina un número congruente a la unidad según el módulo A, y congruente a 0 según el producto de los módulos restantes; o sea, será un valor (preferiblemente el menor) de la expresión $\frac{1}{BCD\,\text{etc.}} \pmod{A}$ multiplicado por BCD etc. (véase art. 32). De manera semejante, sea $\beta \equiv 1 \pmod{B}$ y $\equiv 0 \pmod{ACD\,\text{etc.}}$, $\gamma \equiv 1 \pmod{C}$ y $\equiv 0 \pmod{ABD\,\text{etc.}}$, etc. Entonces si se

desea un número z que según los módulos A, B, C, D, etc., sea congruente a a, b, c, d, etc., respectivamente, podemos colocar:

$$z \equiv \alpha a + \beta b + \gamma c + \delta d \text{ etc. } (\text{mod. } ABCD \text{ etc.})$$

Es obvio que $\alpha a \equiv a \pmod{A}$ y que todos los restantes números βb, γc, etc. son todos $\equiv 0 \pmod{A}$, así que $z \equiv a \pmod{A}$. Una demostración semejante vale para los otros módulos. Esta solución es preferible a la primera cuando tenemos que resolver más problemas del mismo tipo para los cuales los módulos A, B, C, etc., mantienen sus valores, puesto que así α, β, γ, etc., tienen valores constantes. Esto ocurre en el problema de la cronología donde se intenta determinar el año juliano dados su número dorado y su ciclo solar. Aquí $A = 15$, $B = 19$, $C = 28$, así que el valor de la expresión $\frac{1}{19 \cdot 28} \pmod{15}$, o $\frac{1}{532} \pmod{15}$ es 13, luego $\alpha = 6916$. De manera que β es 4200 y γ es 4845, así que el número que deseamos es el menor residuo del número $6916a + 4200b + 4845c$, donde a es la indicción, b el número dorado, c el ciclo solar.

Congruencias lineales con varias incógnitas.

37.

Esto basta para las congruencias del primer grado con una incógnita. Se procede a las congruencias que contienen varias incógnitas. Si expusiéramos el asunto con todo rigor, esta sección nunca terminaría. Por tanto, se propone tratar solamente lo que parezca merecer atención, restringir nuestra investigación a unas observaciones, y dejar una exposición completa para otra ocasión.

1) Al igual que en las ecuaciones, vemos que se debe tener tantas congruencias como incógnitas por determinar.

2) Se proponen, entonces, las congruencias

$$ax + by + cz + \cdots \equiv f \pmod{m} \qquad (A)$$
$$a'x + b'y + c'z + \cdots \equiv f' \qquad (A')$$
$$a''x + b''y + c''z + \cdots \equiv f'' \qquad (A'')$$
$$\text{etc.}$$

de las cuales hay tantas como incógnitas x, y, z, etc.

Ahora, se determinan los números ξ, ξ', ξ'', etc., tales que

$$\begin{gathered} b\xi + b'\xi' + b''\xi'' + \text{ etc.} = 0 \\ c\xi + c'\xi' + c''\xi'' + \text{ etc.} = 0 \\ \text{etc.} \end{gathered}$$

y tales que todos los números sean enteros sin común divisor, lo cual es siempre posible por la teoría de las ecuaciones lineales. De modo semejante ν, ν', ν'', etc., ζ, ζ', ζ'', etc., etc., tales que

$$\begin{gathered} a\nu + a'\nu' + a''\nu'' + \text{ etc.} = 0 \\ c\nu + c'\nu' + c''\nu'' + \text{ etc.} = 0 \\ \text{etc.} \\ a\zeta + a'\zeta' + a''\zeta'' + \text{ etc.} = 0 \\ b\zeta + b'\zeta' + b''\zeta'' + \text{ etc.} = 0 \\ \text{etc.} \quad \text{etc.} \end{gathered}$$

3) Es claro que si se multiplican las congruencias A, A', A'', etc., por ξ, ξ', ξ'', etc., luego por ν, ν', ν'', etc., etc., y luego se suman, resultarán las siguientes congruencias:

$$\begin{gathered} (a\xi + a'\xi' + a''\xi'' + \text{ etc.})x \equiv f\xi + f'\xi' + f''\xi'' + \text{ etc.} \\ (b\nu + b'\nu' + b''\nu'' + \text{ etc.})y \equiv f\nu + f'\nu' + f''\nu'' + \text{ etc.} \\ (c\zeta + c'\zeta' + c''\zeta'' + \text{ etc.})z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{ etc.} \\ \text{etc.} \end{gathered}$$

las cuales escribimos por brevedad de la manera siguiente:

$$\sum(a\xi)x \equiv \sum(f\xi), \quad \sum(b\nu)y \equiv \sum(f\nu), \quad \sum(c\zeta)z \equiv \sum(f\zeta), \quad \text{etc.}$$

4) Ahora se distinguen varios casos.

Primero, cuando todos los coeficientes $\sum(a\xi)$, $\sum(b\nu)$, etc. son primos a m, el módulo de las congruencias, ellas se resuelven según los preceptos ya tratados, y se

encuentra la solución completa por congruencias de la forma $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}$, etc.*) E.g., si se proponen las congruencias

$$x + 3y + z \equiv 1, \quad 4x + y + 5z \equiv 7, \quad 2x + 2y + z \equiv 3 \pmod{8}$$

se encuentra que $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, luego $-15x \equiv -26$ luego $x \equiv 6 \pmod{8}$. De igual manera se encuentra que $15y \equiv -4$, $15z \equiv 1$, y así que $y \equiv 4$, $z \equiv 7 \pmod{8}$.

5) *Segundo,* cuando no todos los coeficientes $\sum(a\xi)$, $\sum(b\nu)$, etc., son primos al módulo, sean α, β, γ, etc., los máximos comunes divisores del módulo m con $\sum(a\xi)$, $\sum(b\nu)$, $\sum(c\zeta)$, etc. respectivamente. Es claro que el problema es imposible a menos que ellos dividan los números $\sum(f\xi)$, $\sum(f\nu)$, $\sum(f\zeta)$, etc., respectivamente. Sin embargo, cuando se cumplan estas condiciones, es claro que las congruencias en (3) se resolverán completamente por congruencias de la forma $x \equiv p \pmod{\frac{m}{\alpha}}$, $y \equiv q \pmod{\frac{m}{\delta}}$, $z \equiv r \pmod{\frac{m}{\gamma}}$, etc., o si se quiere hay α valores diferentes de x (o sea, no congruentes según m), digamos p, $p + \frac{m}{\alpha}, \ldots p + \frac{(\alpha-1)m}{\alpha}$, β valores diferentes de y, etc., que satisfacen las congruencias. Es evidente que todas las soluciones de las congruencias propuestas (si hay) se encuentran entre éstas. Pero esta solución no puede invertirse puesto que en general no todas las combinaciones de todos los valores de x, al combinarlos con todos los de y y z etc., satisfacen el problema, sino únicamente aquéllas cuya interrelación puede mostrarse por una o varias de las congruencias condicionales. Sin embargo, como la solución completa de este problema no es necesaria para lo que sigue, no desarrollaremos el argumento más sino que ilustraremos la idea por medio de un ejemplo.

Sean las congruencias propuestas:

$$3x + 5y + z \equiv 4, \quad 2x + 3y + 2z \equiv 7, \quad 5x + y + 3z \equiv 6 \pmod{12}$$

Entonces, ξ, ξ', ξ''; ν, ν', ν''; ζ, ζ', ζ'' serán respectivamente iguales a 1, -2, 1; 1, 1, -1; -13, 22, -1, y de esto $4x \equiv -4$, $7y \equiv 5$, $28z \equiv 96$. A partir de esto se crean cuatro valores de x, digamos $\equiv 2, 5, 8, 11$; un valor de y, digamos $\equiv 11$, y cuatro valores de z, digamos $\equiv 0, 3, 6, 9 \pmod{12}$. Ahora, para saber cuáles

*) Esta conclusión requiere demostración, pero la hemos suprimido aquí. Nada más resulta de nuestro análisis que las congruencias propuestas no pueden resolverse por otros valores de las incógnitas x, y, etc. No hemos mostrado que estos valores de hecho la satisfacen. Aún es posible que no haya ninguna solución. Un paralelismo ocurre en el tratamiento de las ecuaciones lineales.

combinaciones de los valores de x pueden usarse con los valores de z, se sustituyen en las congruencias propuestas para x, y, z, respectivamente, $2 + 3t$, 11, $3u$. Esto convierte las congruencias en

$$57 + 9t + 3u \equiv 0, \quad 30 + 6t + 6u \equiv 0, \quad 15 + 15t + 9u \equiv 0 \pmod{12},$$

y fácilmente se ven equivalentes a

$$19 + 3t + u \equiv 0, \quad 10 + 2t + 2u \equiv 0, \quad 5 + 5t + 3u \equiv 0 \pmod{4}.$$

La primera claramente requiere que $u \equiv t + 1 \pmod{4}$; al sustituir este valor en las restantes congruencias, también las satisface. Se concluye que los valores 2, 5, 8, 11 de x, que resultan al poner $t \equiv 0, 1, 2, 3$, están necesariamente combinados con los valores de $z \equiv 3, 6, 9, 0$, respectivamente. En total tenemos cuatro soluciones:

$$\begin{aligned} x &\equiv \quad 2, \quad 5, \quad 8, 11 \pmod{12} \\ y &\equiv 11, 11, 11, 11 \\ z &\equiv \quad 3, \quad 6, \quad 9, \quad 0 \end{aligned}$$

A estas investigaciones, las cuales completan la finalidad que habíamos propuesto para esta sección, adjuntamos unas cuantas proposiciones que dependen de los mismos principios y que serán útiles frecuentemente en lo que sigue.

Varios Teoremas.

38.

PROBLEMA. *Hallar cuántos números positivos hay menores que un número positivo dado A, y a la vez primos a él.*

Por brevedad simbolizamos el número de enteros positivos que son primos a A y menores que él por el prefijo φ. Por lo tanto se busca a φA.

I. Cuando A *es primo,* es claro que todos los números desde 1 hasta $A - 1$ son primos a A; y así en este caso resultará

$$\varphi A = A - 1$$

II. Cuando A *es la potencia de un primo,* digamos $= p^m$, ninguno de los números divisibles por p será primo a A, pero los demás sí. Entonces, de los $p^m - 1$

números, tienen que rechazarse: p, $2p$, $3p$, $\ldots$, $(p^{m-1}-1)p$. Por lo tanto sobran $p^m - 1 - (p^{m-1}-1)$ o sea $p^{m-1}(p-1)$ de ellos. Así

$$\varphi p^m = p^{m-1}(p-1)$$

III. Los casos restantes se reducen fácilmente a estos mediante la siguiente proposición: *Si A se resuelve en factores M, N, P, etc., que son primos entre sí, será*

$$\varphi A = \varphi M \cdot \varphi N \cdot \varphi P \text{ etc.}$$

Esto se demuestra como sigue. Sean m, m', m'', etc., los números primos a M y menores que M, y sea el número de ellos $= \varphi M$. De manera semejante, sean n, n', n'', etc., p, p', p'', etc., los números primos a N y a P, respectivamente y menores que ellos, y sean φN, φP, etc., los números de ellos. Es evidente que todos los números que son primos al producto A, también serán primos a los factores individuales M, N, P, etc., y viceversa (art. 19); y además que todos los números congruentes a cualquiera de m, m', m'', etc., serán primos a M y viceversa. De modo semejante para N, P, etc. Así el problema se reduce a éste: determinar cuántos números hay menores que A y también congruentes según el módulo M a los números m, m', m'', etc., y que son congruentes según el módulo N a los números n, n', n'', etc. Pero del artículo 32 se sigue que todos los números que tienen residuos dados según cada uno de los módulos M, N, P, etc., serán congruentes según su producto A. Así habrá únicamente uno que es menor que A y congruente a los residuos dados según M, N, P, etc. Por lo tanto, el número que buscamos es igual al número de combinaciones de cada uno de los números m, m', m'', etc., con cada uno de los n, n', n'', etc., y p, p', p'', etc., etc. Es evidente que por la teoría de las combinaciones esto será $= \varphi M \cdot \varphi N \cdot \varphi P$ etc. *Q. E. D.*

IV. Ahora es fácil ver cómo aplicar esto al caso considerado. Sea A resuelto en sus factores primos; esto es, reducido a la forma $a^\alpha b^\beta c^\gamma$ etc., donde a, b, c, etc., son números primos diferentes. Entonces se tendrá

$$\varphi A = \varphi a^\alpha \cdot \varphi b^\beta \cdot \varphi c^\gamma \text{ etc.} = a^{\alpha-1}(a-1)b^{\beta-1}(b-1)c^{\gamma-1}(c-1) \text{ etc.}$$

o, con más elegancia,

$$\varphi A = A \cdot \frac{a-1}{a} \cdot \frac{b-1}{b} \cdot \frac{c-1}{c} \text{ etc.}$$

Ejemplo. Sea $A = 60 = 2^2 \cdot 3 \cdot 5$; entonces $\varphi A = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 60 = 16$. Los números que son primos a 60 son 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

La primera resolución de este problema aparece en la memoria del ilustre Euler titulada *Theoremata arithmetica nova methodo demostrata* (Comm. nov. Ac. Petrop. VIII p. 74). La demostración se repitió en otra disertación titulada *Speculationes circa quasdam insignes propietates numerorum* (Acta Petrop. VIII, p. 17).

39.

Si determinamos el significado del símbolo φ de tal manera que φA exprese el número de enteros que son primos a A y *no mayores* que A, es evidente que ya no vale $\varphi 1 = 0$ sino $= 1$. No se cambia nada en ningún otro caso. Tomando esta definición, tendremos el teorema siguiente:

Si a, a', a'', etc. son todos los divisores de A (incluyendo a 1 y a A mismo), se tendrá

$$\varphi a + \varphi a' + \varphi a'' + \text{ etc.} = A$$

Ejemplo. Si $A = 30$, entonces $\varphi 1 + \varphi 2 + \varphi 3 + \varphi 5 + \varphi 6 + \varphi 10 + \varphi 15 + \varphi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$

Demostración. Se multiplican por $\frac{A}{a}$ todos los números que sean primos a a y no mayores que a, por $\frac{A}{a'}$ todos los números primos a a' y no mayores que a', etc., y se tendrán $\varphi a + \varphi a' + \varphi a'' +$ etc. números, ninguno mayor que A mismo. Pero:

1) Todos estos números serán diferentes. De hecho, es evidente que todos aquéllos engendrados por un mismo divisor de A serán diferentes. Ahora, si dos números diferentes fueran engendrados por dos divisores diferentes M y N, y por dos números μ y ν que fueran primos respectivamente a M y N, esto es, si $(\frac{A}{M})\mu = (\frac{A}{N})\nu$, resultaría que $\mu N = \nu M$. Supóngase que $M > N$ (lo cual se puede). Como M es primo a μ , y como divide al número μN, tiene que dividir a N. Por lo tanto, un número mayor divide a un número menor. *Q. E. A.*

2) Se incluyen todos los números 1, 2, 3, $\ldots A$, entre estos números. Sea t un número cualquiera no mayor que A, y sea δ el máximo común divisor de A y t. $\frac{A}{\delta}$ será el divisor de A que es primo a $\frac{t}{\delta}$. Es evidente que este número se encuentra entre los engendrados por el divisor $\frac{A}{\delta}$.

3) Resulta de esto que el número de estos enteros será A y por lo tanto

$$\varphi a + \varphi a' + \varphi a'' + \text{ etc.} = A. \quad Q.\ E.\ D.$$

40.

Si el máximo común divisor de los números A, B, C, D, etc. $= \mu$, siempre pueden determinarse números a, b, c, d, etc., tal que

$$aA + bB + cC + \text{ etc.} = \mu.$$

Demostración. Consideramos primero dos de tales números A y B, y sea su máximo común divisor $= \lambda$. Entonces, la congruencia $Ax \equiv \lambda \pmod{B}$ será resoluble (art. 30). Sea la raíz $= \alpha$, y se pone $\frac{\lambda - A\alpha}{B} = \beta$. Entonces se obtendrá $\alpha A + \beta B = \lambda$ como deseamos.

Si hay un tercer número C, sea λ' el máximo común divisor de los números λ y C, el cual será también el máximo común divisor de los números A, B y C*). Determínense números k y γ tales que $k\lambda + \gamma C = \lambda'$, entonces $k\alpha A + k\beta B + \gamma C = \lambda'$.

Si hay un cuarto número D, sea λ'' el máximo común divisor de los números λ' y D (es fácil ver que será también el máximo común divisor de A, B, C y D), y sea $k'\lambda' + \delta D = \lambda''$. Entonces tenemos $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

De manera semejante se procede si todavía hay más números.

Y si los números A, B, C, D, etc., no tienen divisor común, claramente se tiene

$$aA + bB + cC + \text{ etc.} = 1$$

41.

Si p es número primo y se tienen p objetos, entre los que cualquier número de ellos pueden ser iguales, pero no todos, el número de permutaciones de estos objetos será divisible por p.

---

*) Obviamente λ' divide a todos los números A, B y C. Si no fuera el *máximo* común divisor, el máximo sería mayor que λ'. Ahora, puesto que este máximo divisor divide a A, B y C, también divide a $k\alpha A + k\beta B + \gamma C$, es decir, a λ' mismo. Así un número grande divide a uno pequeño Q. E. A. Este resultado puede ser aún más fácilmente establecido del art. 18.

Ejemplo. Cinco objetos A, A, A, B, B pueden disponerse de diez maneras diferentes.

La demostración de este teorema puede derivarse fácilmente de la conocida teoría de permutaciones. Supóngase que entre estos objetos hay a iguales a A, B iguales a B, c iguales a C, etc. (cualesquiera de a, b, c, etc. pueden ser iguales a la unidad), entonces se tiene

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

y el número de permutaciones será

$$\frac{1 \cdot 2 \cdot 3 \cdots p}{1 \cdot 2 \cdot 3 \cdots a \cdot 1 \cdot 2 \cdots b \cdot 1 \cdot 2 \cdots c \text{ etc.}}$$

Ahora, es claro que el numerador tiene que ser divisible por el denominador, puesto que el número de permutaciones debe ser un entero. Pero el numerador es divisible por p, mientras que el denominador, el cual está compuesto de factores menores que p, no es divisible por p (art. 15). Así el número de permutaciones será divisible por p (art. 19).

Esperamos que la siguiente demostración complacerá al lector.

Cuando en dos permutaciones de los mismos objetos el orden de ellas no difiere salvo que el primero en una ocupa una posición diferente en la otra mientras que los restantes siguen el mismo orden, de manera que, en el segundo orden, el primer objeto del primer orden sigue al último de él, las llamamos: *permutaciones semejantes**). Así, en nuestro ejemplo, las permutaciones $ABAAB$ y $ABABA$ serán semejante puesto que los objetos que ocupan los lugares primero, segundo, etc., según la primera, ocuparán los lugares tercero, cuarto, etc., en la última, siguiendo la misma sucesión.

Ahora, como cualquier permutación está compuesta de p objetos, es evidente que se pueden encontrar $p - 1$ permutaciones que sean semejantes a ella avanzando el objeto del primer lugar al segundo, al tercero, etc. Es evidente que el número de todas las permutaciones no idénticas es divisible por p puesto que este número es p veces mayor que el número de todas las permutaciones no semejantes.

Supongamos, pues, que dos permutaciones

$$PQ \ldots TV \ldots YZ; \quad V \ldots YZPQ \ldots T,$$

*) Si se conciben las permutaciones semejantes como escritas sobre una circunferencia, de modo que la última sea contigua a la primera, no habrá ninguna discrepancia puesto que ningún lugar puede llamarse primero o último.

donde se engendra una a partir de la otra avanzando sus términos, sean idénticas, o sea $P = V$, etc. Sea el término P, que es el primero en la primera, el $(n+1)$-ésimo en la siguiente. Entonces, en la sucesión siguiente el $(n+1)$-ésimo término será igual al primero, el $(n+2)$-ésimo al segundo, etc., y el $(2n+1)$-ésimo vuelve a ser igual al primero, como el $(3n+1)$-ésimo, etc.; y , en general, el $(kn+m)$-ésimo término igual al m-ésimo (donde, cuando $kn+m$ supera a p mismo, es necesario concebir la sucesión $V \ldots YZPQ \ldots T$ como repetida contínuamente desde el comienzo, o se resta de $kn+m$ el múltiplo de p menor que $kn+m$ y más próximo en magnitud). Así pues, si se determina k tal que $kn \equiv 1 \pmod{p}$, lo cual siempre puede hacerse, pues p es primo, resulta en general que el m-ésimo término es igual al $(m+1)$-ésimo, o que cada término es igual a su sucesor, i.e., todos los términos son iguales, contrariamente a la hipótesis.

42.

Si los coeficientes A, B, C, ..., N; a, b, c, ..., n de dos funciones de la forma

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots + N \qquad (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \cdots + n \qquad (Q)$$

son todos racionales, y no todos enteros, y si el producto de (P) *y* (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{ etc. } + \mathfrak{Z}$$

entonces no todos los coeficientes $\mathfrak{A}$, $\mathfrak{B}$, $\ldots \mathfrak{Z}$ *pueden ser enteros.*

Demostración. Se expresan todos las fracciones entre los coeficientes A, B, etc., a, b, etc., en su forma reducida, y se elige libremente un primo p que divida uno o varios de los denominadores de estas fracciones. Supongamos que p divide al denominador de uno de los coeficientes en (P). Es claro que si se divide (Q) por p, por lo menos uno de los coeficientes fraccionales en $\frac{(Q)}{p}$ tendrá a p como factor de su denominador (por ejemplo, el primer coeficiente, $\frac{1}{p}$). Ahora, es fácil ver en (P) que siempre habrá un término, una fracción, cuyo denominador involucra potencias *más altas* de p que los denominadores de todos los coeficientes fraccionales que lo preceden y *ninguna* potencia *menor* que los denominadores de todos los coeficientes fraccionales subsiguientes. Sea este término $= Gx^g$, y sea la potencia de p en el denominador

de G, $= t$. Un término semejante puede encontrarse en $\frac{(Q)}{p}$. Sea $= \Gamma x^\gamma$, y sea la potencia de p en el denominador de Γ, $= \tau$. Es evidente que $t + \tau$ será $= 2$ por lo menos. Ahora se demostrará que el término $x^{g+\gamma}$ en el producto de (P) y (Q) tendrá un coeficiente fraccional cuyo denominador involucrará $t + \tau - 1$ potencias de p.

Sean $'Gx^{g+1}$, $''Gx^{g+2}$, etc., los términos en (P) que preceden a Gx^g, y $G'x^{g-1}$, $G''x^{g-2}$, los que le siguen; de manera semejante sean $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$, etc., los términos que preceden a Γx^γ, y los términos que lo siguen serán $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$, etc. Es claro que en el producto de (P) y $\frac{(Q)}{p}$ el coeficiente del término $x^{g+\gamma}$ será

$$\begin{aligned} &= G\Gamma + {}'G\Gamma' + {}''G\Gamma'' + \text{ etc.} \\ &\quad + {}'\Gamma G' + {}''\Gamma G'' + \text{ etc.} \end{aligned}$$

La parte $G\Gamma$ será una fracción, y si se expresa en forma reducida, se involucrarán $t+\tau$ potencias de p en el denominador; las partes restantes, si son fracciones, contendrán en sus denominadores menos potencias de p puesto que todos son productos de dos factores de los cuales uno no contiene más que t potencias de p, el otro menos que τ potencias de p; o el otro no tiene más que τ, y el primero menos que t. Así $G\Gamma$ será de la forma $\frac{e}{fp^{t+\tau}}$, mientras que la suma de las restantes de la forma $\frac{e'}{f'p^{t+\tau-\delta}}$, donde δ es positivo y e, f, f' están libres del factor p: por lo cual la suma de todos será

$$= \frac{ef' + e'fp^\delta}{ff'p^{t+\tau}}$$

cuyo numerador no es divisible por p. De tal manera el denominador no puede obtener potencias menores que $t + \tau$ por ninguna reducción. Por lo tanto, el coeficiente del término $x^{g+\gamma}$ en el producto de (P) y (Q) será

$$= \frac{ef' + e'fp^\delta}{ff'p^{t+\tau-1}},$$

i.e., una fracción cuyo denominador contiene $t + \tau - 1$ potencias de p. *Q. E. D.*

43.

Las congruencias del m-ésimo grado

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \text{ etc.} + Mx + N \equiv 0$$

cuyo módulo es el número primo p que no divide a A, no pueden resolverse más que de m maneras diferentes, o sea, no pueden tener más que m raíces no congruentes según p. (Vea artículos 25 y 26).

Si se asume falso, tendremos congruencias de grados diferentes m, n, etc., con más de m, n, etc. raíces, y si el menor grado es m, todas las congruencias semejantes de menor grado se encuentran en concordancia con nuestro teorema. Como ya hemos demostrado esto para el primer grado (art. 26), es claro que m es $= 2$ o mayor. Por eso la congruencia

$$Ax^m + Bx^{m-1} + \text{ etc.} + Mx + N \equiv 0$$

admite por lo menos $m + 1$ raíces, $x \equiv \alpha$, $x \equiv \beta$, $x \equiv \gamma$, etc., y suponemos (lo que es válido) que α, β, γ, etc., son positivos y menores que p, y que α es el menor de todos. Ahora, en la congruencia propuesta se sustituye x por $y + \alpha$. La congruencia se transforma en

$$A'y^m + B'y^{m-1} + C'y^{m-2} + \cdots + M'y + N' \equiv 0$$

Entonces es evidente que se satisface esta congruencia si se pone $y \equiv 0$, o $\equiv \beta - \alpha$, o $\equiv \gamma - \alpha$, etc. Todas estas raíces serán diferentes, y el número de ellas $= m + 1$. Pero como $y \equiv 0$ es raíz, N' es divisible por p. Así que también la expresión

$$y(A'y^{m-1} + B'y^{m-2} + \text{ etc.} + M') \quad \text{será} \quad \equiv 0 \pmod{p}$$

si se reemplaza y por uno de los m valores $\beta - \alpha$, $\gamma - \alpha$, etc., todos los cuales son > 0 y $< p$. Así, en todos estos casos, también

$$A'y^{m-1} + B'y^{m-2} + \text{ etc.} + M' \quad \text{será} \quad \equiv 0 \pmod{p}$$

i.e., la congruencia

$$A'y^{m-1} + B'y^{m-2} + \text{ etc.} + M' \equiv 0 \qquad \text{(art. 22)}$$

que es de grado $m - 1$, tiene m raíces, contrariamente a nuestro teorema (es evidente que A' será $= A$ y así no divisible por p, como se requiere), pero hemos supuesto que nuestro teorema vale para toda congruencia de grado inferior a m. *Q. E. A.*

44.

Aunque hemos supuesto que el módulo p no divide al coeficiente del término más alto, el teorema no se restringe sólo a este caso. Porque, si el primer coeficiente o cualquiera de los otros, es divisible por p, puede rechazarse sin riesgo, por eso se reduce la congruencia a un grado inferior, para el cual el primer coeficiente ya no sería divisible por p, a menos que todos los coeficientes sean divisibles por p, en cuyo caso la congruencia sería una identidad y la incógnita completamente indeterminada.

Este teorema primero fue propuesto y demostrado por Lagrange (*Mem. de l'Ac. de Berlin*, 1768 *p.* 192). También se encuentra en la memoria de Legendre, *Recherches d'Analyse indéterminée, Hist. de l'Acad. de Paris* 1785 *p.* 466. El gran Euler en *Nov. Comm. Ac. Petr.* XVIII, *p.* 93 demostró que la congruencia $x^n - 1 \equiv 0$ no puede tener más que n raíces diferentes. A pesar de que era un caso particular, el método que usó este gran señor puede adaptarse fácilmente a todas las congruencias. Anteriormente él había resuelto un caso aún más limitado, *Comm. nov. Ac. Petr.* V *p.* 6 , pero este método no puede generalizarse. En la sección VIII demostraremos este teorema por un método todavía diferente; aunque a primera vista parecen diferentes estos métodos, los expertos que quieran compararlos llegarán fácilmente a ver que todos están construidos sobre el mismo principio. Sin embargo, como el teorema considerado aquí no es más que un lema, y como la exposición completa no pertenece a este lugar, no pararemos aquí para tratar los módulos compuestos por separado.