I.Vinogradov

FUNDAMENTOS DE LA TEORIA DE LOS NUMEROS

EDITORIAL · MIR · MOSCU

EDITORIAL MIR

И. Виноградов

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

ИЗДАТЕЛЬСТВО · НАУКА ·

I.Vinográdov

FUNDAMENTOS DE LA TEORIA DE LOS NUMEROS

Traducido del ruso por
Candidato a doctor
en ciencias físico-matemáticas,
catedrático
de matemáticas superiores
E. Aparicio Bernardo

EDITORIAL · MIR · MOSCU

Impreso en la URSS

Segunda edición

PROLOGO

RESEÑA BIOGRAFICA dedicada al 80 aniversario del nacimiento del académico I. M. Vinográdov

El autor de este libro, Iván Matvéevich Vinográdov (nacido el 14 (2) de Septiembre de 1891), es uno de los más célebres matemáticos de la actualidad. Las investigaciones de I. M. Vinográdov están directamente ligadas a los estudios de la escuela de teoría de los números de Petersburgo, a la cual pertenecieron P. L. Chébishev (1821-1894), E. I. Zolotariov (1847-1878), C. F. Voronoy (1868-1908) y otros eminentes matemáticos.

El desarrollo de la teoría analítica de los números en la URSS durante los últimos 50 años está estrechamente relacionado con el nombre de Vinográdov y su escuela. Actualmente se han publicado más de 140 trabajos científicos de I. M. Vinográdov, entre los cuales merecen especial atención las monografías fundamentales: «Un método nuevo en la teoría analítica de los números» (año 1937) y «Método de las sumas trigonométricas en la teoría de los números» (año 1947). En estas dos monografías se condensan los resultados de todas las investigaciones anteriores del autor, que contribuyeron a la creación de un nuevo

método en la teoria de los números. En la actualidad, éste se conoce como el método de Vinográdov de las sumas trigonométricas. Los fundamentos de este método fueron creados ya por él mismo en el año 1934. Este es un método muy general, muy profundo y sumamente fecundo, mediante el cual I. M. Vinográdov consiguió resolver los problemas clásicos de Goldbach, Waring y otros más. En las monografías de I. M. Vinográdov desempeña un papel decisivo la acotación de las sumas trigonométricas múltiples, cuya introducción y estudio representaba de por sí un éxito de grandísima importancia en la teoria de los números. Una de estas acotaciones viene expuesta en el presente libro (véase la pregunta 14 del capítulo VI).

En esta reseña no tenemos posibilidad de hacer una exposición detallada de la obra científica de I. M. Vinográdov. Nos limitaremos solamente a enunciar algunos de sus resultados fundamentales.

En el año 1917, I. M. Vinográdov se dedica al problema del cálculo asintótico de los puntos enteros dentro de los circuitos (véanse en el cap. II, las preguntas 1 a, b, c, d, e, 22 a, b y en el cap. III, las preguntas 5, 6). En su tiempo se ocupó de estos problemas G. F. Voronoy. Los resultados que obtuvo Voronoy para un caso particular (la hipérbola), los consiguió también Vinográdov para una clase muy amplia de circuitos, basándose en unas ideas geométricas más claras y empleando unos métodos analíticos más sencillos. En el año 1926, el matemático checo V. Yarnik demostró que estos teoremas no podían mejorarse

considerablemente. En el año 1963, I. M. Vinográdov obtuvo también el resultado más exacto respecto del número F de puntos enteros en la esfera $x^2 + y^2 + z^2 \leqslant a^2$. *Este número se expresa por la fórmula asintótica*

$$F = \frac{4}{3}\pi a^3 + O\left(a^{4/3}(\ln a)^6\right).$$

Algunos de los resultados de I. M. Vinográdov ya son clásicos. Por ejemplo, ya en el año 1918 demostró que la raíz primitiva mínima de un número primo $p > 3$ *(sobre las raíces primitivas, véase el cap. VI, § § 1-5 y las preguntas del mismo capítulo, 5, 12 c, 14) no es superior a* $2^{2h}\sqrt{p}\ln p$, *donde h denota la cantidad de divisores primos distintos de* $p - 1$.

Es bien conocido también el siguiente teorema de I. M. Vinográdov (año 1926). Sea p un número primo y sea n un divisor de $p - 1$, *donde* $n \neq 1$. *Entonces, el no-resto mínimo de grado n respecto del módulo p (véanse los conceptos de resto y no-resto en el cap. V, § 1, preguntas 8 d, 12 b y en el cap. VI, § 5) no es superior a* $p^{\frac{1}{2k}}(\ln p)^2$, *donde* $k = e^{1-\frac{1}{n}}$. *En relación con esto, obsérvese que en el año 1796 Gauss demostró que el no-resto cuadrático mínimo (mód. p) no es superior a* $2\sqrt{p}$. *El resultado de Vinográdov fue el primer adelanto en esta cuestión desde los tiempos de Gauss.*

Mucha atención prestó I. M. Vinográdov al problema de la resolución de la ecuación $x_1^n + \ldots + x_r^n = N$ *en números enteros* $x_i \geqslant 0$ *(el llamado problema de Waring, planteado por éste en el año 1770). En el año 1909, D. Hilbert demuestra que esta*

ecuación es resoluble para valores acotados de r. En los años 1919-1920, Hardy y Littlewood estudiaron el comportamiento asintótico del número de soluciones de las ecuaciones de Waring para $r \geqslant n\,2^n$. *El valor mínimo de r, para el cual la ecuación de Waring admite solución para todos los números N suficientemente grandes, se denota mediante* $G(n)$. *Para esta magnitud, en el año 1934, I. M. Vinográdov obtuvo la cota* $G(n) < n(3 \ln n + 11)$ *y en el año 1959, la cota más exacta* $G(n) < n(2 \ln n + 4 \ln \ln n + 2 \ln \ln \ln n + 13)$. *Estas cotas no pueden mejorarse considerablemente, puesto que es sabido que* $G(n) > n$ $(n \geqslant 2)$.

I. M. Vinográdov demostró también que la fórmula asintótica, propuesta por Hardy y Littlewood,

$$I(N) = \frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu)} N^{r\nu-1}\sigma + O(N^{r\nu-1-\nu^2})$$

($\nu = \frac{1}{n}$, $\Gamma(s)$ *es la función Gamma de Euler;* σ *es «la serie especial», introducida por Hardy y Littlewood) para la cantidad de expresiones del número entero* $N > 0$ *en la forma* $N = x_1^n + \ldots + x_r^n$, *con enteros positivos* $x_1, \ldots, x_r$ *es válida para* $r \geqslant [10n^2 \ln n]$.

I. M. Vinográdov obtuvo una serie de cotas importantes: para las sumas de Weil, de la forma $S = \sum_{x=1}^{P} \exp 2\pi i m F(x)$, *donde* $m > 0$ *es un número entero y* $F(x)$ *es un polinomio de coeficientes reales; para las sumas extendidas a números primos,*

de la forma $\sum_{p<N} \exp(2\pi i \alpha p)$, *donde* α *es un número real; para las sumas de la forma* $\sum_{p \leq N} \chi(p+k)$, *donde* χ *denota un carácter no principal (véase la definición de carácter en el cap. VI, pregunta 9), y también en la teoria de la aproximación de polinomios mediante partes fraccionarias.*

En general, es difícil indicar problemas de la teoria analítica de los números, a los cuales I. M. Vinográdov no haya prestado atención alguna. Por otra parte, algunos de los problemas resueltos por I. M. Vinográdov habían sido ya planteados más de 150 años atrás, sin encontrar resolución alguna durante dichos años, a pesar de los esfuerzos realizados para resolverlos por los científicos más notables del mundo. Tales son, por ejemplo, los problemas de Waring y Goldbach mencionados anteriormente. Este último problema apareció en el año 1742 en la correspondencia entre Chr. Goldbach y L. Euler. Chr. Goldbach manifestó la hipótesis de que todo número entero, mayor que tres, podía expresarse en forma de una suma de no más de tres números primos. Todos los intentos de los grandes matemáticos de resolver este problema resultaban inútiles. En lo fundamental, este problema fue resuelto por primera vez por I. M. Vinográdov en el año 1937, demostrando que todo número impar, mayor que cierto número N_0 *(la constante de Vinográdov), se expresa en forma de una suma de no más de tres números primos. También demostró que el número de expresiones* $I(N)$ *de un número impar* $N > 0$ *en forma de una suma de tres números primos,*

$N = p_1 + p_2 + p_3$, *se expresa por la fórmula asintótica*

$$I(N) = \frac{N^2}{2r^3} S(N) + O\left(\frac{N^2}{r^{3,5-\varepsilon}}\right),$$

donde $S(N) > 0{,}6$, $r = \ln N$ *y* $\varepsilon > 0$ *es un número arbitrariamente pequeño. Para la constante de Vinográdov, los matemáticos soviéticos ya han demostrado que*

$$N_0 \leqslant \exp \exp (16{,}038).$$

Son importantes también los resultados obtenidos por I. M. Vinográdov respecto de la ζ*-función de Riemann (véase la definición en el cap. II, preguntas 12-14,20). I. M. Vinográdov demostró que*

$$\zeta(1 + it) = O((\ln t)^{2/3})$$

y que $\zeta(1 + it)$ *no tiene ceros en la región*

$$\sigma > 1 - \frac{A}{(\ln t)^{2/3}}.$$

Para la cantidad de números primos $\pi(x)$ *que no son superiores a* x *(véase el cap. II, preguntas 19c, 24), de aquí resulta la acotación*

$$\pi(x) = \int_2^x \frac{dx}{\ln x} + O(xe^{-\alpha(\ln x)^{0,6}}),$$

donde $\alpha > 0$ *es una constante.*

Los métodos de Vinográdov fueron desarrollados también, y siguen desarrollándose actualmente, por sus numerosos alumnos, de los cuales en esta breve reseña no tenemos posibilidad de relatar.

Para concluir, indiquemos que desde el año 1932 I. M. Vinográdov encabeza el centro matemático principal de la Unión

Soviética, el Instituto Matemático V. A. Steklov de la Academia de Ciencias de la URSS. I. M. Vinográdov es miembro numerario de la Academia de Ciencias de la URSS desde el año 1929.

Los méritos de I. M. Vinográdov en la teoría de los números también han sido reconocidos como corresponde fuera de la Unión Soviética. I. M. Vinográdov es miembro extranjero de la Sociedad Real de Londres, de la Academia de Ciencias de Dinamarca y de la Academia Nacional dei Lincei (Roma); es miembro honorífico de la Academia de Ciencias de Hungría; es miembro correspondiente de la Academia de Ciencias de Alemania en Berlín y de la Academia de Ciencias de París; es Doctor honorífico de filosofía de la Universidad de Oslo (Noruega); es miembro extranjero honorífico de las Sociedades Matemáticas de Amsterdam, Londres y de la India, así como de la Sociedad Filosófica americana en Filadelfia y de la Academia americana de Artes y Ciencias en Bostón.

El libro que proponemos, «Fundamentos de la teoría de los números», a distinción de otras obras de I. M. Vinográdov, es un manual de texto destinado a los estudiantes de las facultades de matemáticas de las universidades. Es difícil hallar otro libro tan conciso sobre teoría de los números, donde el material esté expuesto con tanta claridad y rigurosidad.

En lo fundamental, está dedicado al estudio de la teoría de las congruencias. No obstante, las preguntas expuestas al final de cada capítulo abarcan un material que está relacionado

ya con los problemas fundamentales de la teoría analítica de los números.

Durante la preparación de la traducción castellana, el autor expuso al traductor su opinión acerca de la utilización del libro por el lector. El autor considera que al preparar las respuestas a las preguntas, primero hay que hacer la prueba de resolver los problemas planteados individualmente. Solamente cuando se hayan agotado todos los medios para su resolución, el lector deberá examinar las respuestas e indicaciones que se dan al final del libro.

El presente libro «Fundamentos de la teoría de los números», fue escrito sobre la base de los cursos explicados por el autor en los años 1918-1920 en la Universidad de Perm y en los años 1920-1934 en la Universidad de Leningrado. La primera edición del libro salió en el año 1936. En adelante, el libro ha sido mejorado y completado. La presente traducción se ha hecho de la séptima edición rusa.

25. XII. 1970 E. APARICIO BERNARDO

CAPITULO PRIMERO

Teoría de la divisibilidad

§ 1. Conceptos y teoremas fundamentales a. La teoría de los números se dedica al estudio de las propiedades de los números enteros. Llamaremos enteros no sólo a los números de la serie natural 1, 2, 3, . . . (enteros positivos), sino también al cero y a los enteros negativos —1, —2, —3, . . .

Por regla general, al exponer la teoría designaremos con letras solamente los números enteros. Los casos en que las letras no designen números enteros los advertiremos especialmente, si es que ello mismo no está claro.

La suma, diferencia y producto de dos enteros a y b también serán enteros, pero el cociente de la división de a por b (si b es distinto de cero) puede ser tanto entero como no entero.

b. Si el cociente de la división de a por b es entero, designándole con la letra q, se tiene $a = bq$, es decir, *a es igual al producto de b por un entero*. Diremos entonces que a es divisible por b o que b divide a a. En este caso, a se llama *múltiplo* de b y b se llama *divisor* de a. El hecho de que b divide a a se escribe así: $b \setminus a$.

Subsisten los dos teoremas siguientes:

1. *Si a es múltiplo de m y m es múltiplo de b, a es múltiplo de b.*

En efecto, de $a = a_1 m$, $m = m_1 b$ se deduce que $a = a_1 m_1 b$, donde $a_1 m_1$ es entero. Esto demuestra el teorema.

2. *Si en una igualdad de la forma* $k + l + \ldots + n = p + q + \ldots + s$, *respecto de todos los términos, a excepción de uno cualquiera de ellos, se sabe que son múltiplos de b, entonces este término también es múltiplo de b.*

En efecto, sea k tal término. Se tiene

$$l = l_1 b, \ \ldots, \ n = n_1 b, \ p = p_1 b, \ q = q_1 b, \ \ldots, \ s = s_1 b,$$
$$k = p + q + \ldots + s - l - \ldots - n =$$
$$= (p_1 + q_1 + \ldots + s_1 - l_1 - \ldots - n_1) b.$$

Esto demuestra el teorema.

c. En el caso general, que incluye particularmente el caso en que a es divisible por b, se tiene el teorema:

Todo entero a se expresa de un módo único mediante un entero positivo b en la forma

$$a = bq + r; \ 0 \leqslant r < b.$$

En efecto, se obtiene una expresión de a en tal forma tomando bq igual al máximo múltiplo del número b que no es superior a a. Suponiendo que también $a = bq_1 + r_1$, $0 \leqslant r_1 < b$, resulta $0 = b(q - q_1) + r - r_2$, de donde se deduce **(2, b)** que $r - r_1$ es múltiplo de b. Pero en virtud de $|r - r_1| < b$, lo último es posible solamente si $r - r_1 = 0$, es decir, si $r = r_1$, de donde se deduce también que $q = q_1$.

El número q se llama *cociente incompleto* y el número r, *residuo* o *resto* de la división de a por b.

Ejemplo. Sea $b = 14$. Se tiene

$$177 = 14 \cdot 12 + 9; \qquad 0 < 9 < 14,$$
$$-64 = 14 \cdot (-5) + 6; \qquad 0 < 6 < 14,$$
$$154 = 14 \cdot 11 + 0; \qquad 0 = 0 < 14.$$

§ 2. Máximo común divisor

a. A continuación consideraremos sólo los divisores positivos de los números. Todo entero que divide simultáneamente a los enteros $a, b, \ldots, l$, se llama *divisor común* de los mismos. El mayor de los divisores comunes se llama *máximo común divisor* y se designa con la notación $(a, b, \ldots, l)$. Como la cantidad de divisores comunes es finita, la existencia del máximo común divisor es evidente. Si $(a, b, \ldots l) = 1$, $a, b, \ldots, l$ se llaman primos entre sí. Si cada uno de los números $a, b, \ldots, l$, es primo con cada uno de los demás, $a, b, \ldots, l$ se llaman *primos entre sí dos a dos*. Es obvio que los números primos entre sí dos a dos son también primos entre sí; en el caso de dos números los conceptos de «primos entre sí dos a dos» y «primos entre sí» coinciden.

Ejemplos. Como $(6, 10, 15) = 1$, los números 6, 10, 15 son primos entre sí. Como $(8, 13) = (8, 21) = (13, 21) = 1$, los números 8, 13, 21 son primos entre sí dos a dos.

b. Ocupémonos primero de los divisores comunes de dos números.

1. *Si a es múltiplo de b, el conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores del solo número b; en particular, $(a, b) = b$.*

En efecto, todo divisor común de los números a y b es un divisor de b. Recíprocamente, siendo a múltiplo de b, todo divisor del número b (**1, b, § 1**) es también un divisor del número a, es decir, es un divisor común de los números b y a. Por lo tanto, el conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores del solo número b. Y como el máximo divisor del número b es el mismo b, resulta $(a, b) = b$.

2. *Si*

$$a = bq + c,$$

entonces el conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores comunes de los números b y c; en particular, $(a, b) = (b, c)$.

En efecto, la igualdad escrita más arriba muestra que todo común divisor de los números a y b divide también a c (**2, b, § 1**) y, por consiguiente es un común divisor de los números b y c. Recíprocamente, la misma igualdad muestra que todo común divisor de los números b y c divide a a y, por consiguiente, es un común divisor de los números a y b. Por lo tanto, los divisores comunes de los números a y b son los mismos que los divisores comunes de los números b y c; en particular, tienen que coincidir también los mayores de estos divisores, es decir, $(a, b) = (b, c)$.

c. Para buscar el máximo común divisor, así como para deducir sus propiedades principales, se emplea el *algoritmo de Euclides*. Este último consiste en lo siguiente. Sean a y b enteros positivos. Según **c, § 1**, hallamos la serie de igualdades:

$$\left.\begin{aligned} a &= bq_1 + r_2, & 0 < r_2 < b, \\ b &= r_2q_2 + r_3, & 0 < r_3 < r_2, \\ r_2 &= r_3q_3 + r_4, & 0 < r_4 < r_3, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_n, \end{aligned}\right\} \qquad (1)$$

que termina cuando se obtiene cierto $r_{n+1} = 0$. Esto último es indispensable, puesto que la sucesión $b, r_2, r_3, \ldots$, como sucesión de enteros decrecientes, no puede contener más de b positivos.

d. *Examinando las igualdades (1) de arriba a abajo*, nos convencemos (**b**) de que los divisores comunes de los números a y b son iguales a los divisores comunes de los números b y r_2, luego son iguales a los divisores comunes de los números r_2 y r_3, de los números r_3 y $r_4, \ldots$, de los números r_{n-1} y r_n, finalmente, a los divisores del solo número r_n. A la vez, se tiene

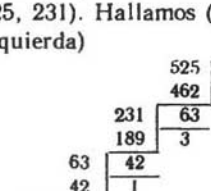
$$(a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n.$$

Obtenemos los siguientes resultados.

1. *El conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores de su máximo común divisor.*

2. *Este máximo común divisor es igual a* r_n es decir, *es igual al último resto del algoritmo de Euclides, distinto de cero.*

Ejemplo. Apliquemos el algoritmo de Euclides para averiguar (525, 231). Hallamos (los cálculos auxiliares se exponen a la izquierda)



$525 = 231 \cdot 2 + 63,$
$231 = 63 \cdot 3 + 42,$
$63 = 42 \cdot 1 + 21,$
$42 = 21 \cdot 2.$

Aquí el último resto positivo es $r_4 = 21$. Por lo tanto, $(525, 231) = 21$.

e. 1. *Designando con la letra m cualquier entero positivo, se tiene* $(am, bm) = (a, b)\, m$.

2. *Designando con la letra* δ *cualquier divisor común de los números a y b, se tiene* $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$; *en particular, se tiene* $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$, *es decir, los cocientes de la división de dos números por su máximo común divisor son números primos entre sí.*

En efecto, multipliquemos las relaciones (1) término a término por m. Obtendremos nuevas relaciones, donde en lugar de $a, b, r_2, \ldots, r_n$ figurarán $am, bm, r_2m, \ldots r_nm$. Por esto, $(am, bm) = r_nm$, y por lo tanto, el aserto **1** es cierto.

Aplicando el aserto **1**, hallamos

$$(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta,$$

de donde se deduce el aserto **2**.

f. 1. *Si* $(a, b) = 1$, *se tiene* $(ac, b) = (c, b)$.
En efecto, (ac, b) divide a ac y bc y, por consiguiente, (1, d), también divide a (ac, bc), igual a c, debido a 1, e; pero (ac, b) divide a b, por lo cual también divide a (c, b). Recíprocamente, (c, b) divide a ac y b, por lo cual también divide a (ac, b). Por lo tanto, (ac, b) y (c, b) se dividen mutuamente y, por consiguiente, son iguales entre sí.
2. *Si* $(a, b) = 1$ *y ac es divisible por b, entonces c es divisible por b.*
En efecto, de $(a, b) = 1$ y de 1 se deduce que $(ac, b) = (c, b)$, y de la divisibilidad de ac por b y de 1, b se deduce que $(ac, b) = b$. Por esto $(c, b) = b$ y, por consiguiente, c es divisible por b.
3. *Si cada uno de los números* $a_1, a_2, \ldots, a_m$ *es primo con cada uno de los números* $b_1, b_2, \ldots, b_n$, *el producto* $a_1 a_2 \ldots a_m$ *es primo con el producto* $b_1 b_2 \ldots b_n$.
En efecto, (teorema 1), se tiene

$$(a_1a_2a_3 \ldots a_m, b_k) = (a_2a_3 \ldots a_m, b_k) = \\ = (a_3 \ldots a_m, b_k) = \ldots = (a_m, b_k) = 1,$$

y haciendo luego para abreviar $a_1a_2 \ldots a_m = A$, hallamos del mismo modo

$$(b_1b_2b_3 \ldots b_n, A) = (b_2b_3 \ldots b_n, A) = \\ = (b_3 \ldots b_n, A) = \ldots = (b_n, A) = 1.$$

g. El problema de la averiguación del máximo común divisor de más de dos números se reduce al mismo para dos números. Precisando, para hallar el máximo común divisor de los números $a_1, a_2, \ldots, a_n$, formamos la sucesión de números:

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, (d_3, a_4) = d_4, \\ \ldots, (d_{n-1}, a_n) = d_n.$$

El número d_n será el máximo común divisor de todos los números dados.
En efecto, (1, d), los divisores comunes de los números a_1 y a_2

coinciden con los divisores de d_2; por esto, los divisores comunes de los números a_1, a_2 y a_3 coinciden con los divisores comunes de los números d_2 y a_3, es decir, coinciden con los divisores de d_3. Luego nos convencemos de que los divisores comunes de los números a_1, a_2, a_3, a_4 coinciden con los divisores de d_4, etc., y, finalmente que los divisores comunes de los números $a_1, a_2, \ldots, a_n$ coinciden con los divisores de d_n. Y como el mayor divisor de d_n es el mismo d_n, éste será el máximo común divisor de los números $a_1, a_2, \ldots, a_n$.

Examinando la demostración expuesta nos convencemos de que el teorema **1, d** subsiste también para más de dos números. Subsisten también los teoremas **1, e** y **2, e**, puesto que al multipilicar por m o al dividir por δ todos los números $a_1, a_2, \ldots, a_n$ también se multiplican por m o se dividen por δ todos los números $d_2, d_3, \ldots, d_n$.

§ 3. Mínimo común múltiplo

a. Todo entero que es un múltiplo de todos los números dados se llama *múltiplo común* de los mismos. El menor múltiplo común positivo se llama *mínimo común múltiplo*.

b. Ocupémonos primero del mínimo común múltiplo de dos números. Sea M algún múltiplo común de los enteros a y b. Como éste es múltiplo de a, se tiene $M = ak$, donde k es entero. Pero M también es múltiplo de b, por lo cual también tiene que ser entero

$$\frac{ak}{b},$$

el cual, haciendo $(a, b) = d$, $a = a_1 d$, $b = b_1 d$, se puede expresar en la forma $\frac{a_1 k}{b_1}$, donde $(a_1, b_1) = 1$ **(2, e, § 2)**. Por esto **(2, f, § 2)**, k tiene que ser divisible por b_1, $k = b_1 t = \frac{b}{d} t$, donde t es entero. De aquí que

$$M = \frac{ab}{d} t.$$

Recíprocamente, es evidente que cualquier M de esta forma es múltiplo tanto de a como de b, y, por consiguiente, esta forma proporciona todos los múltiplos comunes de los números a y b.

El menor positivo de estos múltiplos, es decir, el mínimo común múltiplo, se obtiene para $t = 1$. Este es

$$m = \frac{ab}{d}.$$

Introduciendo m, la fórmula obtenida para M se puede escribir así:

$$M = mt.$$

La última y penúltima igualdades dan lugar a los teoremas:

1. *El conjunto de los múltiplos comunes de dos números coincide con el conjunto de los múltiplos de su mínimo común múltiplo.*

2. *Este mínimo común múltiplo de dos números es igual a su producto, dividido por su máximo común divisor.*

c. Supongamos que se necesita hallar el mínimo común múltiplo de más de dos números $a_1, a_2, \ldots, a_n$. Designando en general con la notación $[a, b]$ el mínimo común múltiplo de los números a y b, formemos la sucesión de números:

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \ldots, [m_{n-1}, a_n] = m_n.$$

El número m_n obtenido de este modo será el mínimo común múltiplo de todos los números dados.

En efecto, (1, b), los múltiplos comunes de los números a_1 y a_2 coinciden con los múltiplos de m_2, por lo cual los múltiplos comunes de los números a_1, a_2, y a_3 coinciden con los múltiplos comunes de m_2 y a_3, es decir, coinciden con los múltiplos de m_3. Luego nos convencemos de que los múltiplos comunes de los números a_1, a_2, a_3, a_4 coinciden con los múltiplos de m_4, etc., y, finalmente, de que los múltiplos comunes de los números $a_1, a_2, \ldots, a_n$ coinciden con los múltiplos de m_n, y como el menor múltiplo positivo de m_n es el mismo m_n, éste

es el mínimo común múltiplo de dos números a_1, a_2, . . ., a_n.

Examinando la demostración expuesta, vemos que el teorema **1, b** subsiste también para más de dos números. Además, nos convencemos de que se verifica el siguiente teorema:

El mínimo común múltiplo de números que son primos dos a dos es igual al producto de los mismos.

§ 4. Relación del algoritmo de Euclides con las fracciones continuas

a. Sea α cualquier número real. Designemos con la letra q_1 el mayor entero que no supera a α. Si α no es entero, se tiene

$$\alpha = q_1 + \frac{1}{\alpha_2}\,;\ \alpha_2 > 1.$$

Exactamente igual, si α_2, . . ., α_{s-1} no son enteros, se tiene

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}\,;\ \alpha_3 > 1;$$

. . . . . .

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}\,;\ \alpha_s > 1,$$

en virtud de lo cual obtenemos el siguiente *desarrollo de* α *en fracción continua*:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdot\ \cdot\ \cdot + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}} \qquad (1)$$

b. Si α es irracional, todos los números α_s son irracionales (si α_s fuese racional, en virtud de (1), resultaría también α racional) y el proceso indicado puede prolongarse indefinidamente.

Si α es racional y, por consiguiente, puede expresarse por una fracción racional irreducible con denominador positivo: $\alpha = \frac{a}{b}$, el proceso indicado será finito y puede efectuarse me-

diante el algoritmo de Euclides. En efecto se tiene:

$$a = bq_1 + r_2; \qquad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$b = r_2q_2 + r_3; \qquad \frac{b}{r^2} = q_2 + \frac{1}{\frac{r_2}{r_3}},$$

. . . . . .

$$r_{n-2} = r_{n-1}q_{n-1} + r_n; \qquad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_nq_n; \qquad \frac{r_{n-1}}{r_n} = q_n,$$

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdot \cdot + \cfrac{1}{q_n}}}.$$

c. Los números $q_1, q_2, \ldots$, que figuran en el desarrollo del número α en fracción continua, se llaman *cocientes incompletos* (en caso de α racional, según **b**, éstos son los cocientes incompletos de las divisiones sucesivas del algoritmo de Euclides), las fracciones

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}, \ldots$$

se llaman *reducidas*.

d. Fácilmente se halla una ley muy simple de formación de las reducidas, observando que $\delta_s\,(s > 1)$ se obtiene de δ_{s-1} sustituyendo los números q_{s-1} por $q_{s-1} + \frac{1}{q_s}$ en la expresión literal δ_{s-1}. En efecto, haciendo para unificar $P_0 = 1$, $Q_0 = 0$, podemos representar sucesivamente las fracciones reducidas en la forma siguiente (aquí se escribe la igualdad $\frac{A}{B} = \frac{P_s}{Q_s}$

para designar A con la notación P_s y B con la notación Q_s) :

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}$$

etc, y, en general,

$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s}.$$

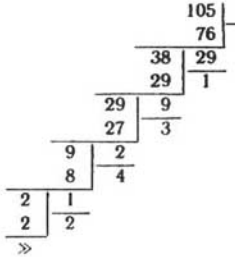
Por lo tanto, los numeradores y denominadores de las fracciones reducidas los podemos calcular sucesivamente por las fórmulas

$$\left.\begin{aligned} P_s &= q_s P_{s-1} + P_{s-2}, \\ Q_s &= q_s Q_{s-1} + Q_{s-2}. \end{aligned}\right\} \qquad (2)$$

Es útil realizar estos cálculos según el esquema siguiente (las últimas dos columnas se escriben solamente en el caso en que α es una fracción irreducible con el denominador positivo: $\alpha = \frac{a}{b}$):

q_s		q_1	q_2	...			q_s...		q_n
P_s	1	q_1	P_2	...	P_{s-2}	P_{s-1}	P_s...	P_{n-1}	a
Q_s	0	1	Q_2	...	Q_{s-2}	Q_{s-1}	Q_s...	Q_{n-1}	b

Ejemplo. Desarrollemos en fracción continua el número $\frac{105}{38}$. Aquí



$$\frac{105}{38} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \frac{1}{2}}}}.$$

Por esto, el esquema indicado anteriormente da:

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

e. Examinemos la diferencia $\delta_s - \delta_{s-1}$ de dos fracciones reducidas consecutivas. Para $s > 1$ hallamos

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}},$$

donde $h_s = P_s Q_{s-1} - Q_s P_{s-1}$; poniendo en lugar de P_s y Q_s sus expresiones (2) y haciendo las simplificaciones evidentes, obtenemos $h_s = -h_{s-1}$. Esto último, junto con $h_1 = q_1 \cdot 0 - -1 \cdot 1 = -1$ da $h_s = (-1)^s$. Así, pues,

$$P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s \qquad (s > 0), \tag{3}$$

$$\delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_s Q_{s-1}} \qquad (s > 1). \tag{4}$$

Ejemplo. En la tabla del ejemplo expuesto en **d**, se tiene

$$105 \cdot 17 - 38 \cdot 47 = (-1)^5 = -1.$$

f. De (3) se deduce que (P_s, Q_s) divide a $(-1)^s = \pm 1$ (2, b, § 1). Por esto $(P_s, Q_s) = 1$, es decir, las *fracciones reducidas* $\frac{P_s}{Q_s}$ *son irreducibles.*

g. Supongamos que $s \geqslant 2$ y que δ_s no es igual a α. Las expresiones para δ_{s-1} y para δ_s se obtienen fácilmente de la expresión (1) para α: la primera, sustituyendo $\frac{1}{\alpha_s}$ por cero, la segunda, sustituyendo $\frac{1}{\alpha_s}$ por el número $\frac{1}{q_s}$. Pero de las igualdades indicadas en **a** para $\alpha_{s-1}, \ldots, \alpha_2, \alpha$, fácilmente comprobamos que

al hacer la primera sustitución	al hacer la segunda sustitución
α_{s-1} disminuye,	α_{s-1} aumenta,
α_{s-2} aumenta,	α_{s-2} disminuye,
α_{s-3} disminuye,	α_{s-3} aumenta,
. . . . .	

y que, finalmente, al hacer una de dichas sustituciones α disminuye, y al hacer la otra α aumenta. Esto último muestra que uno de los números δ_{s-1} y δ_s es menor que α, y el otro es mayor que α, y que, por lo tanto, α *está comprendido entre* δ_{s-1} y δ_s.

h. Se tiene

$$|\alpha - \delta_{s-1}| \leqslant \frac{1}{Q_s Q_{s-1}}.$$

En efecto, si $\delta_s = \alpha$ este aserto se deduce (con el signo de igualdad) de (4). Si δ_s no es igual a α, se deduce (con el signo de desigualdad) de *g* y de (4).

§ 5. Números primos **a.** El número 1 sólo tiene un divisor positivo, precisamente 1. En este sentido el número 1 en la sucesión de números naturales, es particular.

Todo entero mayor que 1 tiene al menos dos divisores, precisamente 1 y él mismo; si con estos divisores se agotan todos

los divisores positivos del número entero, éste se llama *primo*. Un entero mayor que 1, que tenga además de 1 y de sí mismo otros divisores positivos, se llama *compuesto*.

b. *El divisor menor, distinto de la unidad, de un entero mayor que la unidad, es un número primo.*

En efecto, sea q el divisor menor, distinto de la unidad, de un entero $a > 1$. Si q fuese compuesto tendría un divisor q_1 con la condición $1 < q_1 < q$; pero el número a, siendo divisible por q, tendría que ser divisible también por q_1 (**1, b, § 1**), y esto contradice a la hipótesis respecto del número q.

c. *El divisor menor, distinto de la unidad, de un número compuesto a (según* **b**, *tiene que ser primo) no es superior a* $\sqrt{a}$.

En efecto, sea q este divisor, entonces $a = qa_1$, $a_1 \geqslant q$, de donde, multiplicando y simplificando por a_1, obtenemos $a \geqslant q^2$, $q \leqslant \sqrt{a}$.

d. *La cantidad de números primos es infinita.*

La validez de este teorema se deduce de que, cualesquiera que sean los números primos distintos $p_1, p_2, \ldots, p_k$, se puede obtener un número primo nuevo que no está comprendido entre ellos. Tal es el divisor primo de la suma $p_1 p_2 \ldots p_k + 1$, el cual, dividiendo a toda la suma, no puede coincidir con ninguno de los primos $p_1, p_2, \ldots, p_k$ (**2, b, § 1**).

e. Para formar la tabla de números primos que no superan a un número dado N, existe un método sencillo, denominado criba de Eratóstenes. Este consiste en lo siguiente.

Escribamos los números

$$1, 2, \ldots, N. \qquad (1)$$

El primer número de esta sucesión que es mayor que la unidad es el 2; éste sólo es divisible por 1 y por sí mismo y, por consiguiente, es primo.

Borremos de la sucesión (1) (como compuestos) todos los números que son múltiplos de 2, a excepción del mismo 2. El primer número no borrado que le sucede al 2 es el 3; éste no es divisible por 2 (pues en caso contrario estaría borrado), por lo cual 3 sólo es divisible por 1 y por sí mismo y, por consiguiente, es primo.

Borramos de la sucesión (1) todos los números que son múltiplos de 3, a excepción del mismo 3. El primer número no borrado que le sucede al 3 es el 5; éste no es divisible por 2 ni por 3 (pues en caso contrario estaría borrado). Por consiguiente, 5 sólo es divisible por 1 y por sí mismo, por lo cual, también es primo. Etc.

Cuando se hayan borrado del modo indicado todos los números que son múltiplos de los números primos menores que un número primo p, todos los números no borrados, menores que p^2, serán primos. En efecto, cualquier número compuesto a, menor que p^2, ya está borrado, por ser múltiplo de su divisor primo menor, el cual $\leqslant \sqrt{a} < p$. De aquí se deduce que:

1. *Al comenzar a borrar los múltiplos de un número primo p, hay que empezar a borrar desde p^2.*

2. *La formación de la tabla de números primos $\leqslant N$ se termina en cuanto se hayan borrado todos los números compuestos que son múltiplos de los números primos que no son superiores a $\sqrt{N}$.*

§ 6. Unicidad de la descomposición en factores primos

a. *Todo entero a, o es primo con un número primo dado p, o es divisible por p.*

En efecto, (a, p), siendo un divisor de p, puede ser igual a 1 o a p. En el primer caso a es primo con p, en el segundo a es divisible por p.

b. *Si el producto de varios factores es divisible por p, al menos uno de los factores es divisible por p.*

En efecto, (a), cada factor es primo con p o es divisible por p. Si todos los factores fuesen primos con p, su producto (3, f, § 2) sería primo con p; por esto, al menos uno de los factores es divisible por p.

c. *Todo entero, mayor que la unidad, se descompone en un producto de factores primos y, además, de modo único, si no se tiene en cuenta el orden de los factores.*

En efecto, sea a un entero, mayor que la unidad; designando con la letra p_1 su divisor primo menor, se tiene $a = p_1a_1$. Si $a_1 > 1$, designando con la letra p_2 su divisor primo menor, se tiene $a_1 = p_2a_2$. Si $a_2 > 1$, de un modo semejante se obtiene $a_2 = p_3a_3$, etc, y así hasta que se llegue a obtener un número a_n igual a la unidad. Entonces $a_{n-1} = p_n$. Multiplicando todas las igualdades obtenidas y efectuando la simplificación, resulta la siguiente descomposición del número a en factores primos:

$$a = p_1p_2 \cdot \cdot \cdot p_n.$$

Supongamos que para el mismo número a existe también una segunda descomposición en factores primos $a = q_1q_2 \cdot \cdot \cdot \cdot \cdot \cdot q_s$. Entonces

$$p_1p_2 \cdot \cdot \cdot p_n = q_1q_2 \cdot \cdot \cdot q_s.$$

El segundo miembro de esta igualdad es divisible por q_1. Por lo tanto (b), al menos uno de los factores del primer miembro tiene que ser divisible por q_1. Supongamos, por ejemplo, que p_1 es divisible por q_1 (el orden de numeración de los factores está a cargo nuestro); entonces $p_1 = q_1$ (p_1 además de 1 es divisible por p_1). Simplificando ambos miembros de la igualdad por $p_1 = q_1$, se tiene $p_2p_3 \cdot \cdot \cdot p_n = q_2q_3 \cdot \cdot \cdot q_s$. Repitiendo el razonamiento anterior para esta igualdad, obtenemos $p_3 \cdot \cdot \cdot p_n = q_3 \cdot \cdot \cdot q_s$, etc. Continuamos así hasta que al fin y al cabo en un miembro de la igualdad, por ejemplo, en el primero, se simplifiquen todos los factores. Pero simultáneamente tienen que simplificarse

también todos los factores del segundo miembro, puesto que la igualdad $1 = q_{n+1} \ldots q_s$ siendo $q_{n+1}, \ldots, q_s$ superiores a 1, es imposible.

Por lo tanto, la segunda descomposición en factores primos es idéntica a la primera.

d. En la descomposición del número a en factores primos algunos de ellos pueden repetirse. Designando con las letras $p_1, p_2, \ldots, p_k$ los primos distintos que figuran en dicha descomposición y con las letras $\alpha_1, \alpha_2, \ldots, \alpha_k$ sus órdenes de multiplicidad en a, obtenemos la llamada *descomposición canónica del número a en factores*:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

Ejemplo. La descomposición canónica del número 588 000 es: $588\,000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$.

e. *Sea* $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ *la descomposición canónica del número a. Entonces todos los divisores de a son todos los números de la forma*

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}; \qquad (1)$$

$$0 \leqslant \beta_1 \leqslant \alpha_1, \ 0 \leqslant \beta_2 \leqslant \alpha_2, \ \ldots, \ 0 \leqslant \beta_k \leqslant \alpha_k.$$

En efecto, supongamos que d divide a a. Entonces (**b, § 1**) $a = dq$ y, por consiguiente, todos los divisores primos de d figuran en la descomposición canónica de a con exponentes no menores que los exponentes con que ellos mismos figuran en la descomposición canónica de d. Por esto d tiene la forma (1).

Recíprocamente, todo número d de la forma (1) es, evidentemente, un divisor de a.

Ejemplo. Se obtienen todos los divisores del número $720 = 2^4 \cdot 3^2 \cdot 5$ haciendo recorrer en la expresión $2^{\beta_1} 3^{\beta_2} 5^{\beta_3}$ a β_1, β_2, β_3, independientemente unos de otros, los valores $\beta_1 = 0, 1, 2, 3, 4$; $\beta_2 = 0, 1, 2$; $\beta_3 = 0, 1$. Por esto, los

divisores indicados son: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720.

Preguntas referentes al capítulo I

1. Sean a y b enteros, no simultáneamente iguales a cero, y sea $d = ax_0 + by_0$ el número positivo menor de la forma $ax + by$ (x e y son enteros). Demostrar que $d = (a, b)$. Deducir de aquí el teorema **1, d, § 2** y los teoremas **e, § 2**. Generalizar estos resultados, considerando los números de la forma $ax + by + \ldots + fu$.

2. Demostrar que la fracción reducida δ_s representa al número α con más exactitud que cualquier fracción irreducible $\frac{k}{l}$ que cumpla la condición $0 < l < Q_s$.

3. Supongamos que el número real α se ha desarrollado en una fracción continua; sea N un entero positivo, k el número de sus cifras decimales y n el entero mayor que cumple la condición $Q_n \leqslant N$. Demostrar que $n \leqslant 5k + 1$. Para la demostración se deben comparar las expresiones para Q_2, Q_3, Q_4, $\ldots$, Q_n con las que éstos tendrían si todos los q_s fuesen iguales a 1, y comparar luego con los números 1, ξ, ξ^2, $\ldots$, ξ^{n-1}, donde ξ es la raíz positiva de la ecuación $\xi^2 = \xi + 1$.

4. Sea $\tau \geqslant 1$. Una sucesión de fracciones racionales irreducibles, dispuestas en orden de crecimiento, con denominadores positivos no superiores a τ, se llama *sucesión de Farey correspondiente a* τ.

a. Demostrar que la parte de la sucesión de Farey correspondiente a τ, que contiene fracciones α con la condición $0 \leqslant \alpha \leqslant 1$, puede obtenerse del modo siguiente: escribimos las fracciones $\frac{0}{1}$, $\frac{1}{1}$. Si $2 \leqslant \tau$, entonces entre estas fracciones introducimos también la fracción $\frac{0+1}{1+1} = \frac{1}{2}$,

después, en la sucesión obtenida $\frac{0}{1}$, $\frac{1}{2}$, $\frac{1}{1}$ entre cada dos fracciones consecutivas $\frac{a_1}{b_1}$ y $\frac{c_1}{d_1}$ con $b_1+d_1 \leqslant \tau$ introducimos la fracción $\frac{a_1+c_1}{b_1+d_1}$, etc, y así continuamos siempre que esto sea posible. Demostrar previamente que para cualquier par de fracciones consecutivas $\frac{a}{b}$ y $\frac{c}{d}$ de la sucesión obtenida de este modo, se tiene $ad-bc=-1$.

b. Considerando la sucesión de Farey, demostrar el teorema: sea $\tau \geqslant 1$, entonces cualquier número real α se puede expresar en la forma

$$\alpha = \frac{P}{Q} + \frac{\theta}{Q\tau}; \quad 0 < Q \leqslant \tau, \quad (P, Q) = 1, \quad |\theta| < 1.$$

c. Demostrar el teorema de la pregunta **b**, aplicando **g**, § 4.

5, a. Demostrar que hay una cantidad infinita de números primos de la forma $4m + 3$.

b. Demostrar que hay una cantidad infinita de números primos de la forma $6m + 5$.

6. Demostrar que la cantidad de números primos es infinita, calculando para ello la cantidad de números, no superiores a N, en cuyas descomposiciones canónicas no figuran números primos distintos de $p_1, p_2, \ldots, p_k$.

7. Sea K un número entero positivo. Demostrar que en la sucesión de números naturales hay un conjunto infinito de sucesiones $M, M+1, \ldots, M+K-1$, que no contienen números primos.

8. Demostrar que entre los números representados por el polinomio $a_0x^n + a_1x^{n-1} + \ldots + a_n$, donde $n > 0$, $a_0, a_1, \ldots, a_n$ son enteros y $a_0 > 0$, hay un conjunto infinito de números compuestos.

9, a. Demostrar que a la ecuación indeterminada

$$x^3 + y^3 = z^3, \; x > 0, \; y > 0, \; z > 0, \; (x, y, z) = 1 \quad (1)$$

satisfacen aquellos sistemas x, y, z, y sólo aquéllos, en los

que uno de los números x e y tiene la forma $2uv$, el otro tiene la forma $u^2 - v^2$ y, finalmente, z tiene la forma $u^2 + v^2$; en este caso $u > v > 0$, $(u, v) = 1$; uv es par.

b. Aplicando el teorema de la pregunta **a**, demostrar que la ecuación $x^4 + y^4 = z^2$ es irresoluble en enteros positivos x, y, z.

10. Demostrar el teorema: si la ecuación $x^n + a_1x^{n-1} + \ldots + a_n = 0$, donde $n > 0$ y $a_1, \ldots, a_n$ son enteros, tiene una raíz racional, esta raíz es un número entero.

11, a. Sea $S = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$; $n > 1$. Demostrar que S no es entero.

b. Sea $S = \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$; $n > 0$. Demostrar que S no es entero.

12. Sea n entero, $n > 0$. Demostrar que todos los coeficientes del desarrollo del binomio de Newton $(a + b)^n$ son impares cuando, y sólo cuando, n tiene la forma $2^h - 1$.

Ejercicios numéricos referentes al capítulo I

1, a. Aplicando el algoritmo de Euclides, hallar (6 188, 4 709).

b. Hallar (81 719, 52 003, 33 649, 30 107).

2, a. Desarrollando el número $\alpha = \frac{125}{92}$ en fracción continua y formando la tabla de fracciones reducidas (**d, § 4**), hallar: α) δ_4, β) la expresión de α en la forma indicada en la pregunta **4, b**, considerando $\tau = 20$.

b. Desarrollando $\alpha = \frac{5391}{3976}$ en fracción continua y formando la tabla de fracciones reducidas, hallar: α) δ_6, β) la expresión de α en la forma indicada en la pregunta **4, b**, considerando $\tau = 1\,000$.

3. Formar la sucesión de fracciones de Farey (pregunta **4**) desde 0 hasta 1, excluyendo 1, con los denominadores no superiores a 8.

4. Formar la tabla de números primos menores de 100.

5, a. Hallar la descomposición canónica del número 82 798 848.

b. Hallar la descomposición canónica del número 81 057 226 635 000.

CAPITULO SEGUNDO

Las funciones más importantes de la teoría de los números

§ 1. *Funciones* $[x]$, $\{x\}$ **a.** En la teoría de los números desempeña un papel importante la función $[x]$; ésta se define para todos los valores reales de x y representa el entero mayor, no superior a x. Esta función se llama *parte entera de x.*

Ejemplos.

$$[7] = 7; \quad [2{,}6] = 2; \quad [-4{,}75] = -5.$$

A veces se considera también la función $\{x\} = x - [x]$. Esta función se llama *parte fraccionaria de x.*

Ejemplos.

$$\{7\} = 0; \quad \{2{,}6\} = 0{,}6; \quad \{-4{,}75\} = 0{,}25.$$

b. Para mostrar la utilidad de las funciones introducidas, demostremos el teorema:

El exponente, con el que un número primo dado p figura en el producto n!, es igual a

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\dots$$

En efecto, el número de factores en el producto $n!$ que son múltiplos de p, es igual a $\left[\frac{n}{p}\right]$, entre ellos, múltiplos de p^2 hay $\left[\frac{n}{p^2}\right]$; entre estos últimos, múltiplos de p^3 hay

$\left[\frac{n}{p^3}\right]$, etc. La suma de los números indicados da precisamente el exponente buscado, puesto que cada factor en el producto $n!$ que sea múltiplo de p^m, pero no de p^{m+1}, se cuenta del modo indicado m veces, como múltiplo de p, p^2, p^3, ..., y, finalmente, de p^m.

Ejemplo. El exponente con el que el número 3 figura en el producto 40! es igual a

$$\left[\frac{40}{3}\right]+\left[\frac{40}{9}\right]+\left[\frac{40}{27}\right]=13+4+1=18.$$

§ 2. Sumas extendidas a los divisores de un número

a. En la teoría de los números desempeñan un papel particularmente importante las funciones multiplicativas. Una función $\theta(a)$ se llama *multiplicativa*, si se cumplen las condiciones siguientes:

1. *La función $\theta(a)$ está definida para todos los enteros positivos a y no se anula para ningún a de éstos.*

2. *Para cualesquiera positivos a_1 y a_2, primos entre sí, se tiene*

$$\theta(a_1a_2)=\theta(a_1)\,\theta(a_2).$$

Ejemplo. Fácilmente se observa que es multiplicativa la función $\theta(a)=a^s$, donde s es un número real o complejo arbitrario.

b. De las propiedades indicadas de la función $\theta(a)$ se deduce, en particular, que $\theta(1)=1$. En efecto, supongamos que $\theta(a_0)$ no es igual a cero, entonces $\theta(a_0)=\theta(1\cdot a_0)=\theta(1)\,\theta(a_0)$, es decir, $\theta(1)=1$. Además, resulta la siguiente propiedad importante: si $\theta_1(a)$ y $\theta_2(a)$ son funciones multiplicativas, entonces $\theta_0(a)=\theta_1(a)\,\theta_2(a)$ también es una función multiplicativa. En efecto, se tiene

$$\theta_0(1)=\theta_1(1)\,\theta_2(1)=1.$$

Además, para $(a_1, a_2) = 1$, obtenemos:

$$\begin{aligned}\theta_0(a_1a_2) &= \theta_1(a_1a_2)\,\theta_2(a_1a_2) = \\ &= \theta_1(a_1)\,\theta_1(a_2)\,\theta_2(a_1)\,\theta_2(a_2) = \\ &= \theta_1(a_1)\,\theta_2(a_1)\,\theta_1(a_2)\,\theta_2(a_2) = \\ &= \theta_0(a_1)\,\theta_0(a_2).\end{aligned}$$

c. *Sea* $\theta(\alpha)$ *una función multiplicativa y sea* $a = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ *la descomposición canónica del número* a. *Designando con la notación* $\sum_{d\backslash a}$ *la suma, extendida a todos los divisores* d *del número* a, *se tiene*

$$\sum_{d\backslash a}\theta(d) = (1+\theta(p_1)+\theta(p_1^2)+\ldots+\theta(p_1^{\alpha_1}))\ldots$$

$$\ldots(1+\theta(p_k)+\theta(p_k^2)+\ldots+\theta(p_k^{\alpha_k}))$$

(*en el caso* $a = 1$ *se supone que el segundo miembro es igual a* 1).

Para demostrar esta identidad, abramos los paréntesis en el segundo miembro. Se obtiene una suma de términos de la forma

$$\theta(p_1^{\beta_1})\,\theta(p_2^{\beta_2})\ldots\theta(p_k^{\beta_k}) = \theta(p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k});$$

$$0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \ldots,\ 0\leqslant\beta_k\leqslant\alpha_k,$$

donde ninguno de tales términos se omite y no se repite más de una vez; esto es (**e, § 6, cap. I**), precisamente, lo que figura en el primer miembro.

d. Para $\theta(a) = a^s$ la identidad **c** toma la forma

$$\sum_{d\backslash a}d^s = (1+p_1^s+p_1^{2s}+\ldots+p_1^{\alpha_1 s})\ldots$$

$$\ldots(1+p_k^s+p_k^{2s}+\ldots+p_k^{\alpha_k s}). \qquad (1)$$

En particular, para $s = 1$ el primer miembro de (1) representa la *suma de los divisores* $S(a)$ del número a. Simplificando el segundo miembro, obtenemos:

$$S(a) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

Ejemplo.

$$S(720) = S(2^4 \cdot 3^2 \cdot 5) = \frac{2^{4+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} \cdot \frac{5^{1+1}-1}{5-1} = 2\,418.$$

Para $s = 0$ el primer miembro de (1) representa el *número de divisores* $\tau(a)$ del número a, y se tiene:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1).$$

Ejemplo.

$$\tau(720) = (4 + 1)(2 + 1)(1 + 1) = 30.$$

§ 3. Función de Möbius a. *La función de Möbius* $\mu(a)$ se define para todos los enteros positivos a. Esta se determina por las igualdades: $\mu(a) = 0$ si a es divisible por un cuadrado distinto de la unidad; $\mu(a) = (-1)^k$, si a no es divisible por un cuadrado distinto de la unidad, donde k denota el número de divisores primos del número a; en particular, para $a = 1$ se considera $k = 0$, por lo cual admitimos que $\mu(1) = 1$.

Ejemplos.

$$\mu(1) = 1, \quad \mu(5) = -1, \quad \mu(9) = 0,$$
$$\mu(2) = -1, \quad \mu(6) = 1, \quad \mu(10) = 1,$$
$$\mu(3) = -1, \quad \mu(7) = -1, \quad \mu(11) = -1,$$
$$\mu(4) = 0, \quad \mu(8) = 0, \quad \mu(12) = 0.$$

b. Sea $\theta(a)$ una *función multiplicativa y sea*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

la descomposición canónica del número a. Entonces

$$\sum_{d \mid a} \mu(d)\,\theta(d) = (1 - \theta(p_1))(1 - \theta(p_2)) \ldots (1 - \theta(p_k)).$$

(En el caso $a = 1$ se supone que el segundo miembro es igual a 1).

En efecto, la función $\mu(a)$, evidentemente, es multiplicativa. Por esto, es multiplicativa también la función $\theta_1(a) = \mu(a)\,\theta(a)$. Aplicando a esta última la identidad c, § 2

y teniendo en cuenta que $\theta_1(p) = -\theta(p)$; $\theta_1(p^s) = 0$ para $s > 1$, nos convencemos de que el teorema es justo.

c. En particular, haciendo $\theta(a) = 1$, de b obtenemos

$$\sum_{d \setminus a} \mu(d) = \begin{cases} 0, & \text{si } a > 1, \\ 1, & \text{si } a = 1. \end{cases}$$

Haciendo $\theta(d) = \frac{i}{d}$, resulta

$$\sum_{d \setminus a} \frac{\mu(d)}{d} = \begin{cases} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_h}\right), & \text{si } a > 1, \\ 1, & \text{si } a = 1. \end{cases}$$

d. *Supongamos que a los enteros positivos*

$$\delta = \delta_1, \delta_2, \ldots, \delta_n$$

les corresponden cualesquiera valores reales o complejos $f = f_1, f_2, \ldots, f_n$. *Entonces, designando con la notación* S' *la suma de los valores* f *que corresponden a los valores iguales a 1, y con la notación* S_d *la suma de los valores* f *que corresponden a los valores* δ *que son múltiplos de* d, *se tiene*

$$S' = \sum \mu(d) S_d,$$

donde d *recorre todos los números enteros positivos que dividen al menos un valor* δ.

En efecto, en virtud de c, se tiene

$$S' = f_1 \sum_{d \setminus \delta_1} \mu(d) + f_2 \sum_{d \setminus \delta_2} \mu(d) + \ldots + f_n \sum_{d \setminus \delta_n} \mu(d).$$

Reuniendo todos los términos con un mismo valor de d y sacando fuera de paréntesis $\mu(d)$, obtendremos entre paréntesis la suma de aquellos números f, y sólo aquéllos, cuyos δ correspondientes son múltiplos de d, y esto es precisamente S_d.

§ 4. Función de Euler

a. *La función de Euler* $\varphi(a)$ se define para todos los enteros positivos a y representa la cantidad de números de la sucesión

$$0, 1, \ldots, a - 1 \qquad (1)$$

que son primos con a.

Ejemplos.

$$\varphi(1)=1, \quad \varphi(4)=2,$$
$$\varphi(2)=1, \quad \varphi(5)=4,$$
$$\varphi(3)=2, \quad \varphi(6)=2.$$

b. *Sea*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k} \tag{2}$$

la descomposición canónica del número a. Entonces

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right), \tag{3}$$

o también

$$\varphi(a)=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\dots(p_k^{\alpha_k}-p_k^{\alpha_k-1}); \tag{4}$$

en particular,

$$\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}, \quad \varphi(p)=p-1. \tag{5}$$

En efecto, apliquemos el teorema **d**, § 3. En este caso, los números δ_k y los números f_k los definimos así: Supongamos que k recorre los números de la sucesión (1). Hagamos $\delta_k = (k, a)$ y a cada valor δ_k le ponemos en correspondencia el número $f_k = 1$.

Entonces S' será igual al número de valores de $\delta_k = (k, a)$ que son iguales a 1, es decir, será igual a $\varphi(a)$, mientras que S_d será igual al número de valores de $\delta_k = (k, a)$ que son múltiplos de d. Pero (k, a) puede ser múltiplo de d solamente bajo la condición de que d sea un divisor de a. Cumpliéndose esta condición, S_d será igual al número de valores de k que son múltiplos de d, es decir, será igual a $\frac{a}{d}$. Así, pues, resulta

$$\varphi(a)=\sum_{d\mid a}\mu(d)\frac{a}{d},$$

de donde, en virtud de **c**, § 3, se deduce la fórmula (3), y de esta última, en virtud de (2), se deduce la fórmula (4).

Ejemplos.

$$\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16;$$

$$\varphi(81) = 81 - 27 = 54;$$

$$\varphi(5) = 5 - 1 = 4.$$

c. *La función* $\varphi(a)$ *es multiplicativa.*

En efecto, para $(a_1, a_2) = 1$ de **b**, evidentemente, se deduce que

$$\varphi(a_1 a_2) = \varphi(a_1)\,\varphi(a_2).$$

Ejemplo. $\varphi(405) = \varphi(81)\,\varphi(5) = 54 \cdot 4 = 216$

d. $\sum_{d \setminus a} \varphi(d) = a.$

Para verificar esta fórmula, aplicamos la identidad **c**, **§ 2**, la cual para $\theta(a) = \varphi(a)$ da

$$\sum_{d \setminus a} \varphi(d) = (1 + \varphi(p_1) + \varphi(p_1^2) + \ldots + \varphi(p_1^{\alpha_1})) \ldots$$

$$\ldots (1 + \varphi(p_k) + \varphi(p_k^2) + \ldots + \varphi(p_k^{\alpha_k})).$$

En virtud de (5) el segundo miembro se escribe así:

$$(1 + (p_1 - 1) + (p_1^2 - p_1) + \ldots + (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})) \ldots$$

$$\ldots (1 + (p_k - 1) + (p_k^2 - p_k) + \ldots + (p_k^{\alpha_k} - p_k^{\alpha_k - 1})),$$

lo cual, después de reducir los términos semejantes en cada paréntesis grande, resulta ser igual a $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = a$

Ejemplo. Haciendo $a = 12$, hallamos

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Preguntas referentes al capítulo II

1, a. Supongamos que en el intervalo $Q \leqslant x \leqslant R$ la función $f(x)$ es continua y no negativa. Demostrar que la suma

$$\sum_{Q < x \leq R} [f(x)]$$

expresa el número de puntos enteros (puntos de coordenadas enteras) de la región plana: $Q < x \leqslant R$, $0 < y \leqslant f(x)$.

b. Sean P y Q números positivos impares, primos entre sí. Demostrar que

$$\sum_{0<x<\frac{Q}{2}} \left[\frac{P}{Q}x\right] + \sum_{0<y<\frac{P}{2}} \left[\frac{Q}{P}y\right] = \frac{P-1}{2}\cdot\frac{Q-1}{2}.$$

c. Supongamos que $r>0$ y sea T el número de puntos enteros que hay en la región $x^2+y^2 \leqslant r^2$. Demostrar que

$$T = 1 + 4[r] + 8 \sum_{0<x\leq\frac{r}{\sqrt{2}}} [\sqrt{r^2-x^2}] - 4\left[\frac{r}{\sqrt{2}}\right]^2.$$

d. Supongamos que $n>0$ y sea T el número de puntos enteros que hay en la región $x>0$, $y>0$, $xy \leqslant n$. Demostrar que

$$T = 2 \sum_{0<x\leq\sqrt{n}} \left[\frac{n}{x}\right] - [\sqrt{n}]^2.$$

e. Consideremos un polígono, cuyos vértices son puntos enteros y cuyo contorno no se corta consigo mismo y no es tangente a sí mismo. Sea S el área del polígono y $T = \sum \delta - 1$, donde la sumación se extiende a todos los puntos enteros que están situados en el interior del polígono y en su contorno, siendo $\delta = 1$ para los puntos interiores y $\delta = 0{,}5$ para los puntos del contorno. Demostrar que $T = S$.

2. Supongamos que $n>0$, m es entero, $m>1$ y x recorre los números enteros positivos que no son divisibles por la m-ésima potencia de un entero superior a 1. Demostrar que

$$\sum_{x} \left[\sqrt[m]{\frac{n}{x}}\right] = [n].$$

3. Supongamos que los números positivos α y β son tales que

$$[\alpha x];\ x=1, 2, \ldots;\ [\beta y];\ y=1, 2, \ldots$$

forman conjuntamente todos los números de la sucesión natural sin repeticiones. Demostrar que esto se cumple cuando, y sólo cuando, α es irracional y

$$\frac{1}{\alpha}+\frac{1}{\beta}=1.$$

4, a. Sea $[\tau] \geqslant 1$, $t=[\tau]$ y sean $x_1, x_2, \ldots, x_t$ los números 1, 2, ..., t, dispuestos en tal orden que los números

$$0,\ \{\alpha x_1\},\ \{\alpha x_2\}, \ldots, \{\alpha x_t\},\ 1$$

no decrezcan. Demostrar el teorema de la pregunta **4, b,** cap. **I,** considerando las diferencias de los números consecutivos de la última sucesión.

b. Sean $\tau_1, \tau_2, \ldots, \tau_k$ números reales, cada uno de los cuales no es menor que 1; supongamos que $\alpha_1, \alpha_2, \ldots, \alpha_k$ son reales. Demostrar que existen unos números enteros $\xi_1, \xi_2, \ldots, \xi_k$, no simultáneamente iguales a cero, y un número entero η, que satisfacen a las condiciones:

$$|\xi_1| \leqslant \tau_1,\ |\xi_2| \leqslant \tau_2, \ldots, |\xi_k| \leqslant \tau_k, (\xi_1, \xi_2, \ldots, \xi_k, \eta)=1,$$

$$|\alpha_1\xi_1+\alpha_2\xi_2+\ldots+\alpha_k\xi_k-\eta| < \frac{1}{\tau_1\tau_2\ldots\tau_k}.$$

5. Sea α real y c entero, $c>0$. Demostrar que

$$\left[\frac{[\alpha]}{c}\right]=\left[\frac{\alpha}{c}\right].$$

6, a. Sean $\alpha, \beta, \ldots, \lambda$ números reales. Demostrar que

$$[\alpha+\beta+\ldots+\lambda] \geqslant [\alpha]+[\beta]+\ldots+[\lambda].$$

b. Supongamos que $a, b, \ldots, l$ son enteros positivos, $a+b+\ldots+l=n$. Aplicando **b, § 1,** demostrar que

$$\frac{n!}{a!\ b!\ \ldots\ l!}$$

es un número entero.

7. Supongamos que h es entero, $h > 0$, p es primo y

$$u_s = \frac{p^{s+1} - 1}{p - 1}.$$

Representando h en la forma $h = p_m u_m + p_{m-1} u_{m-1} + \ldots + p_1 u_1 + p_0$, donde u_m es el máximo u_s no superior a h, $p_m u_m$ es el máximo múltiplo de u_m no superior a h, $p_{m-1} u_{m-1}$ es el máximo múltiplo de u_{m-1} no superior a $h - p_m u_m$, $p_{m-2} u_{m-2}$ es el máximo múltiplo de u_{m-2} no superior a $h - p_m u_m - p_{m-1} u_{m-1}$, etc, demostrar que los números a que satisfacen a la condición de que en la descomposición canónica de $a!$ el número p figura con el exponente h, existen cuando, y sólo cuando, todos los números p_m, p_{m-1}, $\ldots$, p_1, p_0 son menores que p; además, en este caso los números a indicados son todos los de la forma

$$a = p_m p^{m+1} + p_{m-1} p^m + \ldots + p_1 p^2 + p_0 p + p',$$

donde p' toma los valores: $0, 1, \ldots, p - 1$.

8, a. Supongamos que en el intervalo $Q \leqslant x \leqslant R$ la función $f(x)$ admite derivada segunda continua. Haciendo

$$\rho(x) = \frac{1}{2} - \{x\}, \quad \sigma(x) = \int_0^x \rho(z)\, dz,$$

demostrar que (fórmula de Sonin)

$$\sum_{Q < x \leq R} f(x) = \int_Q^R f(x)\, dx + \rho(R) f(R) - \rho(Q) f(Q) -$$

$$- \sigma(R) f'(R) + \sigma(Q) f'(Q) + \int_Q^R \sigma(x) f''(x)\, dx.$$

b. Supongamos que se cumple la condición de la pregunta a para R arbitrariamente grandes, y que la integral

$\int_Q^\infty |f''(x)|\,dx$ es convergente. Demostrar que

$$\sum_{Q<x\leq R} f(x) =$$

$$= C + \int_Q^R f(x)\,dx + \rho(R) f(R) - \sigma(R) f'(R) - \int_R^\infty \sigma(x) f''(x)\,dx.$$

donde C no depende de R.

c. Si B toma solamente valores positivos y la razón $\frac{|A|}{B}$ permanece acotada superiormente, se escribe $A = O(B)$. Sea n entero, $n > 1$. Demostrar que

$$\ln(n!) = n \ln n - n + O(\ln n).$$

9, a. Sea $n \geqslant 2$, $\Theta(z, z_0) = \sum_{z_0 < p \leq z} \ln p$, donde p recorre los números primos. Sea también $\Theta(z) = \Theta(z, 0)$ y para $x > 0$

$$\psi(x) = \Theta(x) + \Theta(\sqrt{x}) + \Theta(\sqrt[3]{x}) + \ldots$$

Demostrar que

α) $\ln([n]!) = \psi(n) + \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) + \ldots$;

β) $\psi(n) < 2n$;

γ) $\Theta\left(n, \frac{n}{2}\right) + \Theta\left(\frac{n}{3}, \frac{n}{4}\right) + \Theta\left(\frac{n}{5}, \frac{n}{6}\right) + \ldots =$

$$= n \ln 2 + O(\sqrt{n}).$$

b. Para $n > 2$, demostrar que

$$\sum_{p \leq n} \frac{\ln p}{p} = \ln n + O(1),$$

donde p recorre números primos.

c. Sea ε una constante positiva arbitraria. Demostrar que en la sucesión de números naturales existe un conjunto infinito de pares de números primos p_n, p_{n+1} que satisfacen a la condición

$$p_{n+1} < p_n (1 + \varepsilon).$$

d. Sea $n > 2$. Demostrar que

$$\sum_{p \le n} \frac{1}{p} = C + \ln \ln n + O\left(\frac{1}{\ln n}\right),$$

donde p recorre números primos y C no depende de n.

e. Sea $n > 2$. Demostrar que

$$\prod_{p \le n} \left(1 - \frac{1}{p}\right) = \frac{C_0}{\ln n}\left(1 + O\left(\frac{1}{\ln n}\right)\right),$$

donde p recorre números primos y C_0 no depende de n.

f. Demostrar la existencia de una constante $s_0 > 2$ con la condición de que para cualquier entero $s > s_0$, para el s-ésimo número primo p_s de la sucesión 2, 3, 5, . . . se verifica la desigualdad

$$p_s < 1{,}5s \ln s.$$

g. Demostrar que

$$\frac{a}{\varphi(a)} = O(\ln \ln a).$$

10, a. Sea $\theta(a)$ una función multiplicativa. Demostrar que $\theta_1(a) = \sum_{d \setminus a} \theta(d)$ también es una función multiplicativa.

b. Supongamos que la función $\theta(a)$ está definida para todos los enteros positivos a y que la función $\psi(a) = \sum_{d \setminus a} \theta(a)$ es multiplicativa. Demostrar que la función $\theta(a)$ también es multiplicativa.

11. Supongamos que, para $m > 0$, $\tau_m(a)$ denota el número de soluciones de la ecuación indeterminada $x_1 x_2 \ldots x_m = a$ ($x_1, x_2, \ldots, x_m$ recorren los números enteros positivos

independientemente uno de otro); en particular, es evidente que $\tau_1(a) = 1$, $\tau_2(a) = \tau(a)$. Demostrar que

a. $\tau_m(a)$ es una función multiplicativa.

b. Sea p un número primo, $\alpha \geqslant 0$ y $m > 1$. Entonces

$$\tau_m(p^\alpha) = \frac{(\alpha+1)(\alpha+2)\ \ldots\ (\alpha+m-1)}{1\cdot 2\ \ldots\ (m-1)}.$$

c. Si ε es una constante positiva arbitraria, se tiene

$$\lim_{a\to\infty} \frac{\tau_m(a)}{a^\varepsilon} = 0.$$

d. $\sum_{0<a\leq n} \tau_m(a)$ expresa el número de soluciones de la desigualdad $x_1 x_2 \ldots x_m \leqslant n$ en números enteros positivos $x_1, x_2, \ldots, x_m$.

12. Supongamos que $R(s)$ representa la parte real del número s.

Si $R(s) > 1$, hacemos $\zeta(s) = \sum_{n=1} \frac{1}{n^s}$. Sea $m > 0$, m es entero. Demostrar que

$$(\zeta(s))^m = \sum_{n=1}^{\infty} \frac{\tau_m(n)}{n^s}.$$

13, a. Siendo $R(s) > 1$, demostrar que

$$\zeta(s) = \prod \frac{1}{1-\frac{1}{p^s}},$$

donde p recorre todos los números primos.

b. Demostrar que la cantidad de números primos es infinita, basándose en la divergencia de la serie armónica.

c. Demostrar que la cantidad de números primos es infinita, basándose en la irracionalidad del número $\zeta(2) = \frac{\pi^2}{6}$.

14. Sea $\Lambda(a) = \ln p$ para $a = p^l$, donde p es primo y l es un entero positivo; $\Lambda(a) = 0$ para los otros enteros posi-

tivos a. Siendo $R(s) > 1$, demostrar que

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

15. Sea $R(s) > 1$. Demostrar que

$$\prod_{p} \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

donde p recorre los números primos.

16, a. Sea $n \geqslant 1$. Aplicando **d, § 3**, demostrar que

$$1 = \sum_{0<d\leq n} \mu(d) \left[\frac{n}{d}\right].$$

b. Sea $M(z, z_0) = \sum_{z_0<a\leq z} \mu(a)$; $M(x) = M(x, 0)$. Demostrar que

$$\alpha) \quad M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + \ldots = 1, \quad n \geqslant 1,$$

$$\beta) \quad M\left(n, \frac{n}{2}\right) + M\left(\frac{n}{3}, \frac{n}{4}\right) + M\left(\frac{n}{5}, \frac{n}{6}\right) + \\ + \ldots = -1, \quad n \geqslant 2.$$

c. Supongamos que $n \geqslant 1$, l es entero, $l > 1$, $T_{l,n}$ es el número de enteros x con la condición $0 < x \leqslant n$, que no son divisibles por la l-ésima potencia de un entero superior a 1. Aplicando **d, § 3**, demostrar que

$$T_{l,n} = \sum_{d=1}^{\infty} \mu(d) \left[\frac{n}{d^l}\right].$$

17, a. Supongamos que a es entero, $a > 0$, y que para los enteros $x_1, x_2, \ldots, x_n$ se ha definido unívocamente una función $f(x)$. Demostrar que

$$S' = \sum_{d\backslash a} \mu(d) S_d,$$

donde S' denota la suma de los valores de $f(x)$, extendida a los valores de x que son primos con a, y S_d es la suma de

los valores de $f(x)$, extendida a los valores de x que son múltiplos de d.

b. Supongamos que $k > 1$ y que se han dado los sistemas

$$x_1', x_2', \ldots, x_k'; \quad x_1'', x_2'', \ldots, x_k''; \ldots; x_1^{(n)}, x_2^{(n)}, \ldots, x_k^{(n)},$$

donde cada uno de ellos consta de números enteros no simultáneamente iguales a cero. Supongamos también que para estos sistemas se ha definido unívocamente una función $f(x_1, x_2, \ldots, x_k)$. Demostrar que

$$S' = \sum \mu(d) S_d,$$

donde S' denota la suma de los valores de $f(x_1, x_2, \ldots, x_k)$, extendida a los sistemas de números primos entre sí, y S_d es la suma de los valores de $f(x_1, x_2, \ldots, x_k)$, extendida a los sistemas de números que son simultáneamente múltiplos de d. Aquí d recorre números enteros positivos.

c. Supongamos que a es entero, $a > 0$, y que para los divisores δ del número a se ha definido unívocamente una función $F(\delta)$. Haciendo

$$G(\delta) = \sum_{d \setminus \delta} F(d),$$

demostrar que (la ley de inversión para las funciones numéricas)

$$F(a) = \sum_{d \setminus a} \mu(d) G\left(\frac{a}{d}\right).$$

d. Supongamos que a los enteros positivos

$$\delta_1, \delta_2, \ldots, \delta_n$$

les corresponden cualesquiera números reales o complejos, no iguales a cero:

$$f_1, f_2, \ldots, f_n.$$

Demostrar que

$$P' = \prod P_d^{\mu(d)},$$

donde P' denota el producto de los valores f que corresponden a los valores δ que son iguales a 1, P_d denota el producto

de los valores f que corresponden a los valores δ que son múltiplos de d, y d recorre todos los números enteros positivos que dividen al menos a un δ.

18. Supongamos que a es entero, $a > 1$, $\sigma_m(n) = 1^m + 2^m + \ldots + n^m$, $\psi_m(a)$ es la suma de las m-ésimas potencias de los números de la sucesión $1, 2, \ldots, a$ que son primos con a; $p_1, p_2, \ldots, p_k$ son los divisores primos del número a.

a. Aplicando el teorema de la pregunta **17**, a, demostrar que

$$\psi_m(a) = \sum_{d \setminus a} \mu(d)\, d^m \sigma_m\left(\frac{a}{d}\right).$$

b. Demostrar que

$$\psi_1(a) = \frac{a}{2}\varphi(a).$$

c. Demostrar que

$$\psi_2(a) = \left(\frac{a^2}{3} + \frac{(-1)^k}{6} p_1 p_2 \ldots p_k\right)\varphi(a).$$

19. Supongamos que $z > 1$, a es entero, $a > 0$, T_z es la cantidad de números x con las condiciones $0 < x \leqslant z$, $(x, a) = 1$, ε es una constante positiva arbitraria.

a. Demostrar que

$$T_z = \sum_{d \setminus a} \mu(d)\left[\frac{z}{d}\right].$$

b. Demostrar que

$$T_z = \frac{z}{a}\varphi(a) + O(a^\varepsilon).$$

c. Supongamos que $z > 1$, $\pi(z)$ denota la cantidad de números primos no superiores a z, a es el producto de los números primos no superiores a $\sqrt{z}$. Demostrar que

$$\pi(z) = \pi(\sqrt{z}) - 1 + \sum_{d \setminus a} \mu(d)\left[\frac{z}{d}\right].$$

20. Supongamos $R(s) > 1$, a es entero, $a > 0$. Demostrar que

$$\sum{}' \frac{1}{n^s} = \zeta(s) \prod \left(1 - \frac{1}{p^s}\right),$$

donde n recorre en el primer miembro los números enteros positivos que son primos con a, y p recorre en el segundo miembro todos los divisores primos del número a.

21, a. La probabilidad P de que k números enteros positivos $x_1, x_2, \ldots, x_k$ sean primos entre sí, la definiremos como el límite para $N \to \infty$ de la probabilidad P_N de que sean primos entre sí k números $x_1, x_2, \ldots x_k$, a cada uno de los cuales, independientemente de los demás, se le ha asignado uno de los valores 1, 2, ..., N, los cuales se consideran como valores igualmente posibles. Aplicando el teorema de la pregunta **17, b**, demostrar que $P = (\zeta(k))^{-1}$.

b. Definiendo la probabilidad P de que la fracción $\frac{x}{y}$ sea irreducible del mismo modo que en la pregunta **a** para $k = 2$, demostrar que

$$P = \frac{6}{\pi^2}.$$

22, a. Supongamos que $r \geqslant 2$, y sea T el número de puntos enteros (x, y) situados en la región $x^2 + y^2 \leqslant r^2$, y cuyas coordenadas son números primos entre sí. Demostrar que

$$T = \frac{6}{\pi} r^2 + O(r \ln r).$$

b. Supongamos que $r \geqslant 2$, y sea T el número de puntos enteros (x, y, z) situados en la región $x^2 + y^2 + z^2 \leqslant r^2$, y cuyas coordenadas son números primos entre sí. Demostrar que

$$T = \frac{4\pi}{3\zeta(3)} r^3 + O(r^2).$$

23, a. Demostrar el teorema **c, § 3**, contando los divisores del número a que no son divisibles por el cuadrado de un entero superior a 1 y que tienen 1, 2, ... divisores primos.

b. Supongamos que a es entero, $a > 1$, d recorre los divisores del número a que tienen no más de m divisores primos. Demostrar que para m par, $\sum \mu(d) \geqslant 0$, y para m impar, $\sum \mu(d) \leqslant 0$.

c. En las condiciones del teorema **d**, § 3, considerando que todos los valores f son no negativos y haciendo recorrer a d solamente los números que tienen no más de m divisores primos, demostrar que

$$S' \leqslant \sum \mu(d) S_d, \quad S' \geqslant \sum \mu(d) S_d$$

según que m sea par o impar.

d. En las condiciones de la pregunta **17, a**, demostrar unas desigualdades iguales a las de la pregunta **c**, considerando que todos los valores de $f(x)$ son no negativos; hacer lo mismo también en las condiciones **17, b**, considerando que todos los valores $f(x_1, x_2, \ldots, x_k)$ son no negativos.

24. Supongamos que ε es cualquier constante con las condiciones $0 < \varepsilon < \frac{1}{6}$, $N \geqslant 8$, $r = \ln N$, $0 < q \leqslant N^{1-\varepsilon}$, $0 \leqslant l < q$, $(q, l) = 1$, $\pi(N, q, l)$ es la *cantidad de números primos* con las condiciones: $p \leqslant N$, $p = qt + l$, donde t es entero. Demostrar que

$$\pi(N, q, l) = O(\Delta); \quad \Delta = \frac{Nr^{\varepsilon}}{r\varphi(q)}.$$

Para la demostración, haciendo $h = r^{1-0,5\varepsilon}$, los números primos con las condiciones indicadas se deben considerar como un caso particular de todos los números con estas condiciones que son primos con a, donde a es el producto de todos los primos que no son superiores a e^h y que no dividen a q. Se debe aplicar el teorema de la pregunta **23, d** (condiciones de la pregunta **17, a**) con el a indicado y $m = 2[2 \ln r + 1]$.

25. Supongamos que k es par, $k > 0$, la descomposición canónica del número a tiene la forma $a = p_1 p_2 \ldots p_k$ y d recorre los divisores del número a con la condición

$0 < d < \sqrt{a}$. Demostrar que

$$\sum_d \mu(d) = 0.$$

26. Supongamos que k es entero, $k > 0$, d recorre los números con la condición $\varphi(d) = k$. Demostrar que

$$\sum_d \mu(d) = 0.$$

27. Utilizando la expresión de $\varphi(a)$, demostrar que la cantidad de números primos es infinita.

28, a. Demostrar el teorema **d, § 4**, estableciendo que la cantidad de números de la sucesión 1, 2, . . ., a que tienen con a un mismo máximo común divisor δ, es igual a $\varphi\left(\frac{a}{\delta}\right)$.

b. Deducir la expresión para $\varphi(a)$:

α) aplicando el teorema de la pregunta **10, b**;

β) aplicando el teorema de la pregunta **17, c**.

29. Sea $R(s) > 2$. Demostrar que

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

30. Sea n entero, $n \geqslant 2$. Demostrar que

$$\sum_{m=1}^{n} \varphi(m) = \frac{3}{\pi^2} n^2 + O(n \ln n).$$

Ejercicios numéricos referentes al capítulo II

1, a. Hallar el exponente con el que el número 5 figura en la descomposición canónica de 5 258! (véase la pregunta 5).

b. Hallar la descomposición canónica del número 125!

2, a. Hallar τ (5 600) y S (5 600).

b. Hallar τ (116 424) y S (116 424).

3. Formar la tabla de los valores de la función $\mu(a)$ para todos los $a = 1, 2, \ldots, 100$.

4. Hallar α) φ (5 040), β) φ (1 294 700).

5. Formar la tabla de los valores de la función $\varphi(a)$ para todos los $a = 1, 2, \ldots, 50$, aplicando solamente la fórmula (5), **§ 4** y el teorema **c, § 4**.

CAPITULO TERCERO

Congruencias

§ 1. Conceptos fundamentales **a.** Vamos a estudiar los números enteros en relación con los restos de la división de los mismos por un entero positivo m dado, al cual lo llamaremos *módulo*.

A cada número entero le corresponde el resto de su división por m (c, § 1, cap. I); si a dos enteros a y b les corresponde un mismo resto r, éstos se llaman *congruentes según el módulo m, o respecto del módulo m,* o simplemente, *congruentes módulo m.*

b. La congruencia de los números a y b respecto del módulo m se escribe así:

$$a \equiv b \text{ (mód. } m).$$

lo cual se lee: a es congruente con b respecto del módulo m.

c. *La congruencia de los números a y b respecto del módulo m es equivalente a:*

1. *La posibilidad de expresar a en la forma* $a = b + mt$, *donde t es entero.*
2. *La divisibilidad de* $a - b$ *por m.*

En efecto, de $a \equiv b$ (mód. m) se deduce que

$$a = mq + r, \quad b = mq_1 + r; \quad 0 \leqslant r < m,$$

de donde

$$a - b = m(q - q_1),\ a = b + mt,\quad t = q - q_1.$$

Recíprocamente, de $a = b + mt$, representando b en la forma

$$b = mq_1 + r,\quad 0 \leqslant r < m,$$

deducimos que

$$a = mq + r;\quad q = q_1 + t,$$

es decir,

$$a \equiv b \text{ (mód. } m).$$

Por esto, la afirmación **1** es justa.
De **1** se deduce inmediatamente la afirmación **2**.

§ 2. Propiedades de las congruencias, semejantes a las propiedades de las igualdades

a. *Dos números que son congruentes con un tercero, son congruentes entre sí.*
Se deduce de **a**, § 1.
b. *Las congruencias se pueden sumar término a término.*
En efecto, sea

$$a_1 \equiv b_1 \text{ (mód. } m),\quad a_2 \equiv b_2 \text{ (mód. } m),\ \ldots,\quad a_k \equiv b_k \text{ (mód. } m). \qquad (1)$$

Entonces, (**1**, **c**, § 1),

$$a_1 = b_1 + mt_1,\ a_2 = b_2 + mt_2,\ \ldots,\ a_k = b_k + mt_k, \qquad (2)$$

de donde

$$a_1 + a_2 + \ldots a_k = \\ = b_1 + b_2 + \ldots + b_k + m(t_1 + t_2 + \ldots + t_k),$$

o sea, (**1**, **c**, § 1),

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \text{ (mód. } m).$$

Un sumando que figure en un miembro cualquiera de la congruencia se puede pasar al otro miembro, cambiándole el signo.
En efecto, sumando la congruencia $a + b \equiv c$ (mód. m) con la congruencia evidente $-b \equiv -b$ (mód. m), resulta $a \equiv c - b$ (mód. m).

A cada miembro de una congruencia se le puede sumar (o *restar*) *cualquier número que sea múltiplo del módulo.*

En efecto, sumando la congruencia $a \equiv b$ (mód. m) con la congruencia evidente $mk \equiv 0$ (mód. m), resulta $a + mk \equiv b$ (mód. m).

c. *Las congruencias se pueden multiplicar término a término.*

En efecto, examinemos de nuevo las congruencias (1) y las igualdades (2) que se deducen de ellas. Multiplicando término a término las igualdades (2), obtenemos

$$a_1 a_2 \ldots a_k = b_1 b_2 \ldots b_k + mN,$$

donde N es entero. Por consiguiente, (1, c, § 1),

$$a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \text{ (mód. } m).$$

Ambos miembros de la congruencia se pueden elevar a una misma potencia.

Esto se deduce del aserto anterior.

Ambos miembros de la congruencia se pueden multiplicar por un mismo entero.

En efecto, multiplicando la congruencia $a \equiv b$ (mód. m) por la congruencia evidente $k \equiv k$ (mód. m), obtenemos $ak \equiv bk$ (mód. m).

d. Las propiedades b y c (la adición y multiplicación de congruencias) se generalizan mediante el siguiente teorema.

Si en la expresión de una función racional entera de coeficientes enteros

$$S = \sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$$

se sustituyen los números $A_{\alpha_1, \ldots, \alpha_k}$, $x_1, \ldots, x_k$ *por los números* $B_{\alpha_1, \ldots, \alpha_k}$, $y_1, \ldots, y_k$, *los cuales son congruentes con los anteriores respecto del módulo* m, *la expresión nueva de* S *será congruente con la precedente respecto del módulo* m.

En efecto, de

$$A_{\alpha_1, \ldots, \alpha_k} \equiv B_{\alpha_1, \ldots, \alpha_k} \text{ (mód. } m\text{)}.$$

$$x_1 \equiv y_1 \text{ (mod. } m\text{)}, \ \ldots, \ x_k \equiv y_k \text{ (mód. } m\text{)}$$

hallamos (c)

$$x_1^{\alpha_1} \equiv y_1^{\alpha_1} \text{ (mód. } m\text{)}, \ \ldots, \ x_k^{\alpha_k} \equiv y_k^{\alpha_k} \text{ (mód, } m\text{)},$$

$$A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv B_{\alpha_1, \ldots, \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k} \text{ (mód. } m\text{)}.$$

de donde, sumando, obtenemos

$$\sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv \sum B_{\alpha_1, \ldots, \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k} \text{ (mód. } m\text{)}.$$

Si

$$a \equiv b \text{ (mód. } m\text{)}, \quad a_1 \equiv b_1 \text{ (mód. } m\text{)}, \ \ldots \ a_n \equiv b_n \text{ (mód. } m\text{)},$$

$$x \equiv x_1 \text{ (mód. } m\text{)},$$

se tiene

$$ax^n + a_1 x^{n-1} + \ \ldots \ + a_n \equiv$$

$$\equiv bx_1^n + b_1 x_1^{n-1} + \ \ldots \ + b_n \text{ (mód. } m\text{)}.$$

Este aserto es un caso particular del anterior.

e. *Ambos miembros de la congruencia se pueden dividir por su común divisor, si este último es primo con el módulo.*

En efecto, si $a \equiv b$ (mód. m), $a = a_1 d$, $b = b_1 d$, $(d, m) = 1$ resulta que la diferencia $a - b$, igual a $(a_1 - b_1)\, d$, es divisible por m. Por esto (**2, f, § 2**, cap. **I**) $a_1 - b_1$ es divisible por m, es decir, $a_1 \equiv b_1$ (mód. m).

§ 3. Otras propiedades de las congruencias

a. *Ambos miembros de una congruencia y el módulo se pueden multiplicar por un mismo número entero.*

En efecto, de $a \equiv b$ (mód. m) se deduce que

$$a = b + mt, \quad ak = bk + mkt$$

y, por consiguiente, $ak \equiv bk$ (mód. mk).

b. *Ambos miembros de una congruencia y el módulo se pueden dividir por cualquier común divisor suyo.*

En efecto, sea

$$a \equiv b \text{ (mód. } m\text{)}, \ a = a_1 d, \quad b = b_1 d, \quad m \parallel m_1 d.$$

Se tiene

$$a = b + mt,\ a_1 d = b_1 d + m_1 dt,\ a_1 = b_1 + m_1 t$$

y, por lo tanto, $a_1 \equiv b_1$ (mód. m).

c. *Si se verifica la congruencia $a \equiv b$ respecto de varios módulos, entonces se verifica también respecto del módulo que es igual al mínimo común múltiplo de estos módulos.*

En efecto, de $a \equiv b$ (mód. m_1), $a \equiv b$ (mód. m_2), . . ., $a \equiv b$ (mód. m_k) se deduce que la diferencia $a - b$ es divisible por todos los módulos $m_1, m_2, \ldots, m_k$. Por esto, (**c, § 3**, cap. **I**), también es divisible esta diferencia por el mínimo común múltiplo m de estos módulos, es decir, $a \equiv b$ (mód. m).

d. *Si una congruencia se verifica respecto de un módulo m, también se verifica respecto de un módulo d que sea igual a cualquier divisor del número m.*

En efecto, de $a \equiv b$ (mód. m) se deduce que la diferencia $a - b$ tiene que ser divisible por m; por esto, (**1, b, § 1**, cap. **I**), esta diferencia tiene que ser divisible también por cualquier divisor d del número m, es decir, $a \equiv b$ (mód. d).

e. *Si un miembro de una congruencia y el módulo son divisibles por algún número, el otro miembro de la congruencia tiene que ser divisible por el mismo número.*

En efecto, de $a \equiv b$ (mód. m) se deduce que $a = b + mt$; si a y m son múltiplos de d, entonces (**2, b, § 1**, cap. **I**) también b tiene que ser múltiplo de d, como se afirmaba.

f. *Si $a \equiv b$ (mód. m), entonces $(a, m) = (b, m)$.*

En efecto, en virtud de **2, b, § 2**, cap. **I**, esta igualdad se deduce inmediatamente de $a = b + mt$.

§ 4. Sistema completo de restos

a. Los números que dan un mismo resto, o lo que es lo mismo, los que son congruentes respecto del módulo m, forman una *clase de números respecto del módulo m.*

De esta definición se deduce que a todos los números de una clase les corresponde un mismo resto r, por lo cual,

haciendo recorrer a q en la forma $mq + r$ todos los números enteros, se obtienen todos los números de la clase.
Correspondientemente a m valores distintos de r, se tienen m clases de números respecto del módulo m.

b. Cualquier número de la clase se llama *resto* o *residuo respecto del módulo m* con relación a todos los números de la misma clase. El resto que se obtiene para $q = 0$, igual al residuo mismo r, se llama *resto no negativo mínimo*.
El resto ρ que es el menor en valor absoluto, se llama *resto absoluto mínimo*.

Evidentemente, si $r < \frac{m}{2}$ se tiene $\rho = r$; si $r > \frac{m}{2}$ se tiene $\rho = r - m$; finalmente, si m es par y $r = \frac{m}{2}$, se puede tomar por ρ cualquiera de los dos números $\frac{m}{2}$ y $\frac{m}{2} - m = -\frac{m}{2}$.
Tomando un resto de cada clase se obtiene un *sistema completo de restos respecto del módulo m*. Por lo general, como sistema completo de restos se emplean los restos no negativos mínimos $0, 1, \ldots, m-1$ o también los restos absolutos mínimos; como se deduce de lo expuesto anteriormente, estos últimos, en caso de m impar, se representan por la sucesión

$$-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2},$$

y en el caso de m par, por una cualquiera de las dos sucesiones

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2},$$

$$-\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1.$$

c. *Cualesquiera m números que sean incongruentes dos a dos respecto del módulo m, forman un sistema completo de restos de este módulo.*
En efecto, estos números, siendo incongruentes, tienen que pertenecer a distintas clases, y como en total hay m números,

es decir, tantos cuantas clases hay, en cada una de las clases tiene que haber, indudablemente, un número único.

d. *Si* $(a, m) = 1$ *y* x *recorre el sistema completo de restos respecto del módulo* m, *entonces* $ax + b$, *donde* b *es un entero cualquiera, también recorre el sistema completo de restos respecto del módulo* m.

En efecto, hay tantos números de la forma $ax + b$ cuantos números x hay, es decir, m. Según **c**, no queda más que mostrar que dos números cualesquiera $ax_1 + b$ y $ax_2 b$, que corresponden a dos números incongruentes x_1 y x_2, son también incongruentes entre sí respecto del módulo m.

Pero suponiendo que $ax_1 + b \equiv ax_2 + b$ (mód. m), se obtiene la congruencia $ax_1 \equiv ax_2$ (mód. m), de donde, en virtud de que $(a, m) = 1$, resulta $x_1 \equiv x_2$ (mód. m), lo cual contradice a la incongruencia de los números x_1 y x_2.

§ 5. Sistema reducido de restos

a. En virtud de **f**, § 3, los números de una misma clase respecto del módulo m tienen con el módulo un mismo máximo común divisor. Son de suma importancia las clases para las cuales este divisor es igual a la unidad, es decir, las clases que contienen números que son primos con el módulo.

Tomando sendos restos en estas clases, se obtiene el *sistema reducido de restos respecto del módulo* m. Por consiguiente, el sistema reducido de restos se puede formar de los números del sistema completo que son primos con el módulo. Ordinariamente, el sistema reducido de restos se extrae del sistema de restos no negativos mínimos: $0, 1, \ldots, m - 1$. Como entre éstos hay $\varphi(m)$ números que son primos con m, la cantidad de números del sistema reducido, así como la cantidad de clases que contienen números primos con el módulo, es igual a $\varphi(m)$.

Ejemplo. El sistema reducido de restos según el módulo 42 es

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

b. *Cualesquiera* $\varphi(m)$ *números que sean incongruentes dos a dos respecto del módulo* m *y que sean primos con el módulo, forman un sistema reducido de restos según el módulo* m.

En efecto, estos números, siendo incongruentes dos a dos y primos con el módulo, tienen que pertenecer a distintas clases que contienen números que son primos con el módulo, y como en total hay $\varphi(m)$ de tales números, es decir, tantos cuantas clases hay del tipo indicado, en cada una de las clases habrá, indispensablemente, un número único.

c. *Si* $(a, m) = 1$ *y* x *recorre el sistema reducido de restos según el módulo* m, ax *también recorre el sistema reducido de restos según el módulo* m.

En efecto, hay tantos números ax cuantos números x hay, es decir, $\varphi(m)$. Por lo tanto, en virtud de **b**, no queda más que demostrar que los números ax son incongruentes dos a dos respecto del módulo m y son primos con el módulo. Pero lo primero se demostró en **d**, **§ 4** para los números de la forma más general $ax + b$; lo segundo se deduce de que $(a, m) = 1$, $(x, m) = 1$.

§ 6. Teoremas de Euler y Fermat

a. *Si* $m > 1$ *y* $(a, m) = 1$ *se tiene (teorema de Euler)*:

$$a^{\varphi(m)} \equiv 1 \text{ (mód. } m).$$

En efecto, si x recorre el sistema reducido de restos

$$x = r_1, r_2, \ldots, r_c; \quad c = \varphi(m),$$

formado por los restos no negativos mínimos, entonces los restos no negativos mínimos $\rho_1, \rho_2, \ldots, \rho_c$ de los números ax también recorren el mismo sistema, pero, generalmente, dispuestos en otro orden (**c**, **§ 5**).

Multiplicando término a término las congruencias

$$ar_1 \equiv \rho_1 \text{ (mód. } m), \; ar_2 \equiv \rho_2 \text{ (mód. } m), \ldots,$$
$$\ldots, \; ar_c \equiv \rho_c \text{ (mód. } m),$$

obtenemos

$$a^c r_1 r_2 \ldots r_c \equiv \rho_1 \rho_2 \ldots \rho_c \text{ (mód. } m).$$

de donde, dividiendo ambos miembros por el producto $r_1 r_2 \ldots r_c = \rho_1 \rho_2 \ldots \rho_c$, resulta

$$a^c \equiv 1 \text{ (mód. } m\text{)}.$$

b. *Si p es primo y a no es divisible por p, se tiene (teorema de Fermat):*

$$a^{p-1} \equiv 1 \text{ (mód. } p\text{)}. \qquad (1)$$

Este teorema es una consecuencia del teorema a para $m = p$. Al último teorema se le puede dar una forma más cómoda. Precisando, si se multiplican ambos miembros de la congruencia (1) por a, se obtiene la congruencia

$$a^p \equiv a \text{ (mód. } p\text{)}.$$

la cual es válida ya para todos los valores enteros de a, puesto que también es válida si a es múltiplo de p.

Preguntas referentes al capítulo III

1, a. Expresando los números enteros en el sistema decimal de numeración, deducir los criterios de divisibilidad por 3, 9, 11.

b. Expresando los números enteros en el sistema de numeración de base 100, deducir el criterio de divisibilidad por 101.

c. Expresando los números enteros en el sistema de numeración de base 1 000, deducir los criterios de divisibilidad por 37, 7, 11, 13.

2. Supongamos que $m > 0$, $(a, m) = 1$, b es entero, x recorre el sistema completo y ξ el sistema reducido de restos respecto del módulo m. Demostrar que

$$\alpha) \sum_x \left\{\frac{ax+b}{m}\right\} = \frac{1}{2}(m-1),$$

$$\beta) \sum_\xi \left\{\frac{a\xi}{m}\right\} = \frac{1}{2}\varphi(m).$$

3, **a.** Supongamos que $m>0\,(a, m)=1$, $h\geqslant 0$, c es real

$$S=\sum_{x=0}^{m-1}\left\{\frac{ax+\psi(x)}{m}\right\},$$

donde $\psi(x)$ para los valores considerados de x toma valores que cumplen la condición $c\leqslant\psi(x)\leqslant c+h$. Demostrar que

$$\left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

b. Supongamos que M es entero, $m>0$, $(a, m)=1$, A y B son reales,

$$A=\frac{a}{m}+\frac{\lambda}{m^2};\quad S=\sum_{x=M}^{M+m-1}\{Ax+B\}.$$

Demostrar que

$$\left|S-\frac{1}{2}m\right|\leqslant|\lambda|+\frac{1}{2}.$$

c. Sea M entero, $m>0$, $(a, m)=1$,

$$S=\sum_{x=M}^{M+m-1}\{f(x)\},$$

donde la función $f(x)$ admite derivadas continuas $f'(x)$ y $f''(x)$ en el intervalo $M\leqslant x\leqslant M+m-1$, y se cumplen las condiciones

$$f'(M)=\frac{a}{m}+\frac{\theta}{m^2};\quad (a, m)=1;\quad |\theta|<1,\quad \frac{1}{A}\leqslant|f''(x)|\leqslant\frac{k}{A},$$

siendo

$$1\leqslant m\leqslant\tau,\quad \tau=A^{\frac{1}{3}},\quad A\geqslant 2,\quad k\geqslant 1,$$

Demostrar que

$$\left|S-\frac{1}{2}m\right|<\frac{k+3}{2}.$$

4. Supongamos que en el desarrollo del número irracional A en fracción continua todos los cocientes incompletos están acotados, M es entero, m es entero, $m>0$, B es real.

Demostrar que

$$\sum_{x=M}^{M+m-1} \{Ax+B\} = \frac{1}{2}m + O(\ln m).$$

5, a. Supongamos que $A > 2$, $k \geqslant 1$ y que la función $f(x)$ admite derivada segunda continua en el intervalo $Q \leqslant x \leqslant R$, la cual satisface a las condiciones

$$\frac{1}{A} \leqslant |f''(x)| \leqslant \frac{k}{A}.$$

Demostrar que

$$\sum_{Q \leqslant x \leqslant R} \{f(x)\} = \frac{1}{2}(R-Q) + \theta\Delta; \quad |\theta| < 1,$$

$$\Delta = (2k^2(R-Q)\ln A + 8kA)\, A^{-\frac{1}{3}}.$$

b. Supongamos que $0 < \sigma \leqslant 1$, Q y R son enteros. En las condiciones de la pregunta **a**, demostrar que el número $\psi(\sigma)$ de fracciones $\{f(x)\}$; $x = Q+1, \ldots, R$ con la condición $0 \leqslant f(x) < \sigma$ se expresa por la fórmula

$$\psi(\sigma) = \sigma(R-Q) + \theta' \cdot 2\Delta; \ |\theta'| < 1.$$

6, a. Sea T la cantidad de puntos enteros (x, y) que hay en la región $x^2 + y^2 \leqslant r^2$ $(r \geqslant 2)$. Demostrar que

$$T = \pi r^2 + O(r^{\frac{2}{3}} \ln r).$$

b. Supongamos que n es entero, $n > 2$, E es la constante de Euler. Demostrar que

$$\tau(1) + \tau(2) + \ldots + \tau(n) = n(\ln n + 2E - 1) + O(n^{\frac{1}{3}}(\ln n)^2).$$

7. A un sistema de n números enteros positivos, en que cada número viene expresado en el sistema de numeración de base 2, lo llamaremos regular, si para cualquier entero no negativo s la cantidad de números, en cuya expresión figura 2^s, es par, e irregular, si al menos para un s este número es impar.

Demostrar que un sistema irregular se puede hacer regular disminuyendo o excluyendo completamente un solo término del mismo, y en sistema regular se hace irregular disminuyendo o excluyendo completamente cualquiera de sus términos.

8, a. Demostrar que la forma

$$3^n x_n + 3^{n-1} x_{n-1} + \ldots + 3x_1 + x_0,$$

donde x_n, x_{n-1}, ..., x_1, x_0 recorren independientemente uno de otro los valores —1, 0, 1, representa todos los números

$$-H, \ \ldots, \ -1, \ 0, \ 1, \ \ldots, \ H; \quad H = \frac{3^{n+1}-1}{3-1}.$$

y, además, cada número, de un modo único.

b. Sean m_1, m_2, ..., m_k positivos, primos dos a dos. Aplicando c, § 4, demostrar que se obtiene el sistema completo de restos respecto del módulo $m_1 m_2, \ \ldots, \ m_k$, haciendo recorrer a los números x_1, x_2, ..., x_k en la forma

$$x_1 + m_1 x_2 + m_1 m_2 x_3 + \ldots + m_1 m_2 \ldots m_{k-1} x_k$$

los sistemas completos de restos respecto de los módulos m_1, m_2, ..., m_k.

9. Sean m_1, m_2, ..., m_k primos dos a dos y sea

$$m_1 m_2 \ldots m_k = M_1 m_1 = M_2 m_2 = \ldots = M_k m_k.$$

a. Aplicando c, § 4, demostrar que se obtiene el sistema completo de restos respecto del módulo $m_1 m_2 \ldots m_k$, haciendo recorrer a los números x_1, x_2, ..., x_k en la forma

$$M_1 x_1 + M_2 x_2 + \ldots + M_k x_k$$

los sistemas completos de restos respecto de los módulos m_1, m_2, ..., m_k.

b. Aplicando c, § 4, cap. II y b, § 5, demostrar que se obtiene el sistema reducido de restos respecto del módulo $m_1 m_2 \ldots \ldots m_k$, haciendo recorrer a los números x_1, x_2, ..., x_k

en la forma

$$M_1x_1 + M_2x_2 + \ldots + M_kx_k$$

los sistemas reducidos de restos respecto de los módulos $m_1, m_2, \ldots, m_k$.

c. Demostrar el teorema de la pregunta **b** independientemente del teorema **c**, § **4**, cap. **II** y deducir entonces el último teorema como consecuencia del primero.

d. Hallar de un modo elemental la expresión para $\varphi(p^\alpha)$ y, aplicando la igualdad **c**, § **4**, cap. **II**, deducir la expresión conocida para $\varphi(a)$.

10. Sean $m_1, m_2, \ldots, m_k$ primos dos a dos, superiores a 1, $m = m_1m_2 \ldots m_k$; $m = M_sm_s$.

a. Supongamos que $x_1, x_2, \ldots, x_k$, x recorren los sistemas completos de restos, y $\xi_1, \xi_2, \ldots, \xi_k$, ξ los sistemas reducidos de restos respecto de los módulos $m_1, m_2, \ldots, m_k$, m. Demostrar que las fracciones

$$\left\{\frac{x_1}{m_1} + \frac{x_2}{m_2} + \ldots + \frac{x_k}{m_k}\right\}$$

coinciden con las fracciones $\left\{\frac{x}{m}\right\}$, y las fracciones

$$\left\{\frac{\xi_1}{m_1} + \frac{\xi_2}{m_2} + \ldots + \frac{\xi_k}{m_k}\right\} \text{ con las fracciones } \left\{\frac{\xi}{m}\right\}.$$

b. Sean dadas k funciones racionales enteras de coeficientes enteros de r variables $x, \ldots, w$ $(r \geqslant 1)$:

$$f_s(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c_{\alpha, \ldots, \delta}^{(s)} x^\alpha \ldots w^\delta; \quad s = 1, \ldots, k,$$

y sea

$$f(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c_{\alpha, \ldots, \delta} x^\alpha \ldots w^\delta;$$

$$c_{\alpha, \ldots, \delta} = \sum_{s=1}^{k} M_s c_{\alpha, \ldots, \delta}^{(s)};$$

$x_s, \ldots, w_s$ recorren los sistemas completos de restos y $\xi_s, \ldots, \omega_s$ los sistemas reducidos de restos respecto del

módulo m_s; $x, \ldots, w$ recorren los sistemas completos de restos y $\xi, \ldots, \omega$ los sistemas reducidos de restos respecto del módulo m. Demostrar que las fracciones

$$\left\{\frac{f_1(x_1, \ldots, w_1)}{m_1} + \ldots + \frac{f_k(x_k, \ldots, w_k)}{m_k}\right\}$$

coinciden con las fracciones $\left\{\frac{f(x, \ldots, w)}{m}\right\}$ y las fracciones

$$\left\{\frac{f_1(\xi_1, \ldots, \omega_1)}{m_1} + \ldots + \frac{f_k(\xi_k, \ldots, \omega_k)}{m_k}\right\}$$

con las fracciones $\left\{\frac{f(\xi, \ldots, \omega)}{m}\right\}$ (generalización de los teoremas de la pregunta **a**).

11, a. Supongamos que m es entero, $m > 0$, a es entero, x recorre el sistema completo de restos respecto del módulo m. Demostrar que

$$\sum e^{2\pi i \frac{ax}{m}} = \begin{cases} m, \text{ si } a \text{ es múltiplo de } m. \\ 0 \text{ en caso contrario.} \end{cases}$$

b. Supongamos que α es real, M es entero, P es entero, $P > 0$. Designando con la notación (α) el valor absoluto de la diferencia entre α y el número entero más próximo a α (distancia de α al entero más próximo) demostrar que

$$\left|\sum_{x=M}^{M+P-1} e^{2\pi i a x}\right| \leqslant \min\left(P, \frac{1}{h(\alpha)}\right); \quad h \geqslant \begin{cases} 2 \text{ siempre} \\ 3, \text{ si } (\alpha) \leqslant \frac{1}{6}. \end{cases}$$

c. Supongamos que m es entero, $m > 1$ y que las funciones $M(a)$ y $P(a)$ para los valores $a = 1, 2, \ldots, m-1$ toman valores enteros con la condición $P(a) > 0$. Demostrar que

$$\sum_{a=1}^{m-1} \left|\sum_{x=M(a)}^{M(a)+P(a)-1} e^{2\pi i \frac{a}{m} x}\right| < \begin{cases} m \ln m - \frac{m}{3} \ln\left(2\left[\frac{m}{6}\right]+1\right), \\ m \ln m - \frac{m}{2}, \text{ si } m \geqslant 12, \\ m \ln m - m, \quad \text{si } m \geqslant 60. \end{cases}$$

12, a. Supongamos que m es entero, $m > 0$, ξ recorre el sistema reducido de restos respecto del módulo m. Demostrar que

$$\mu(m) = \sum_{\xi} e^{2\pi i \frac{\xi}{m}}.$$

b. Aplicando el teorema de la pregunta a, demostrar el primero de los teoremas c, § 3, cap. II (véase la resolución de la pregunta 28, a, cap. II).

c. Deducir el teorema de la pregunta a, aplicando el teorema de la pregunta 17, a, cap. II.

d. Supongamos que

$$f(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c_{\alpha, \ldots, \delta}\, x^{\alpha} \ldots w^{\delta}$$

es una función racional entera de coeficientes enteros de r variables $x, \ldots, w$ $(r \geqslant 1)$, a es entero, m es entero, $m > 0$; $x, \ldots, w$ recorren el sistema completo de restos y $\xi, \ldots, \omega$ el sistema reducido de restos respecto del módulo m. Introducimos las notaciones

$$S_{a,m} = \sum_{x} \ldots \sum_{w} e^{2\pi i \frac{af(x, \ldots, w)}{m}},$$

$$S'_{a,m} = \sum_{\xi} \ldots \sum_{\omega} e^{2\pi i \frac{af(\xi, \ldots, \omega)}{m}}.$$

Supongamos también que $m = m_1 \ldots m_k$, donde $m_1, \ldots, m_k$ son primos dos a dos, superiores a 1, y sea $m = M_s m_s$. Demostrar que

$$S_{a_1, m_1} \ldots S_{a_k, m_k} = S_{M_1 a_1 + \ldots + M_k a_k, m},$$

$$S'_{a_1, m_1} \ldots S'_{a_k, m_k} = S'_{M_1 a_1 + \ldots + M_k a_k, m}.$$

e. Con las notaciones de la pregunta d, hacemos

$$A(m) = m^{-r} \sum_{a} S_{a,m}, \quad A'(m) = m^{-r} \sum_{a} S'_{a,m},$$

donde a recorre el sistema reducido de restos respecto del módulo m.

Demostrar que

$$A(m_1) \ldots A(m_k) = A(m),$$
$$A'(m_1) \ldots A'(m_k) = A'(m).$$

13, a. Demostrar que

$$\varphi(a) = \sum_{n=0}^{a-1} \prod_{p} \left(1 - \frac{1}{p} \sum_{x=0}^{p-1} e^{2\pi i \frac{nx}{p}}\right),$$

donde p recorre los divisores primos del número a.

b. Deducir la expresión conocida para $\varphi(a)$ de la identidad de la pregunta a.

14. Demostrar que

$$\tau(a) = 2 \sum_{0<x<\sqrt{a}} \frac{1}{x} \sum_{k=0}^{x-1} e^{2\pi i \frac{ak}{x}} + \delta,$$

donde $\delta = 1$ ó $\delta = 0$, según que a sea el cuadrado de un número entero o no lo sea.

15, a. Supongamos que p es primo y $h_1, h_2, \ldots, h_a$ son enteros. Demostrar que

$$(h_1 + h_2 + \ldots + h_a)^p \equiv$$
$$\equiv h_1^p + h_2^p + \ldots + h_a^p \text{ (mód. } p).$$

b. Deducir el teorema de Fermat del teorema de la pregunta a.

c. Deducir el teorema de Euler del teorema de Fermat.

Ejercicios numéricos referentes al capítulo III

1, a. Hallar el resto de la división de

$$(12\,371^{56} + 34)^{28} \text{ por } 111.$$

b. ¿Es divisible el número $2^{1\,093} - 2$ por $1\,093^2$?

2, a. Aplicando los criterios de divisibilidad de la pregunta 1, hallar el desarrollo canónico del número 244 943 325.

b. Hallar el desarrollo canónico del número 282 321 246 671 737.

CAPITULO CUARTO

Congruencias con una incógnita

§ 1. Conceptos fundamentales Nuestro objetivo próximo es el estudio de las congruencias de la siguiente forma general:

$$f(x) \equiv 0 \text{ (mód. } m); \quad f(x) = ax^n + a_1x^{n-1} + \ldots + a_n \quad (1)$$

Si a no es divisble por m, el número n se llama *grado de la congruencia.*

Resolver la congruencia, significa hallar todos los valores de x que la satisfacen. Dos congruencias, a las que satisfacen unos mismos valores de x, se llaman *equivalentes.*

Si a la congruencia (1) la satisface algún $x = x_1$, entonces (**d, § 2, cap. III**) a la misma congruencia la satisfacen también todos los números que son congruentes con x_1 respecto del módulo m: $x \equiv x_1$ (mód. m). Toda esta clase de números se considera como *una solución.* Por lo tanto, la *congruencia* (1) *tendrá tantas soluciones cuantos restos del sistema completo la satisfagan.*

Ejemplo. A la congruencia

$$x^5 + x + 1 \equiv 0 \text{ (mód. 7)},$$

entre los números 0, 1, 2, 3, 4, 5, 6 del sistema completo de restos respecto del módulo 7, la satisfacen dos números: $x = 2$ y $x = 4$. Por ello, la congruencia indicada tiene dos soluciones:

$$x \equiv 2 \text{ (mód. 7)}, \quad x \equiv 4 \text{ (mód. 7)}.$$

§ 2. Congruencias de primer grado

a. La congruencia de primer grado, después de trasladar el término independiente (con el signo contrario) al segundo miembro, se reduce a la forma

$$ax \equiv b \text{ (mód. } m\text{)}. \qquad (1)$$

b. Comenzando a estudiar el problema del número de soluciones de la congruencia (1), nos limitaremos primero al caso $(a, m) = 1$. En virtud del **§ 1**, la congruencia considerada admite tantas soluciones cuantos restos del sistema completo la satisfacen. Mas, cuando x recorre el sistema completo de restos respecto del módulo m, ax recorre el sistema completo de restos (**d**, **§ 4**, cap. **III**). Por consiguiente, para un valor de x tomado del sistema completo, y sólo para uno, ax será congruente con b. Así, pues, si $(a, m) = 1$ la congruencia (1) admite una sola solución.

c. Supongamos ahora que $(a, m) = d > 1$. Entonces, para que la congruencia (1) tenga solución es necesario (**e**, **§ 3**, cap. **III**) que b sea divisible por d, pues en caso contrario la congruencia (1) sería imposible para algún x entero. Por esta razón, suponiendo que b es un múltiplo de d, hacemos $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Entonces la congruencia (1) (después de haber simplificado por d) resulta equivalente a $a_1 x \equiv b_1$ (mód. m_1), en la cual $(a_1, m_1) = 1$ y, por lo tanto admite una solución respecto del módulo m_1. Sea x_1 el resto no negativo mínimo de esta solución respecto del módulo m_1, entonces todos los números x que forman esta solución serán de la forma

$$x \equiv x_1 \text{ (mód. } m_1\text{)}. \qquad (2)$$

Respecto del módulo m los números (2) forman más de una solución; forman precisamente tantas soluciones cuantos números (2) haya en la sucesión $0, 1, 2, \ldots, m - 1$ que sean restos no negativos mínimos respecto del módulo m. Tales números son:

$$x_1,\ x_1 + m_1,\ x_1 + 2m_1,\ \ldots,\ x_1 + (d - 1)\, m_1,$$

es decir, en total d numeros (2) y, por consiguiente, la congruencia (1) admite d soluciones.

d. Haciendo un resumen de todo lo demostrado, resulta el teorema siguiente:

Sea $(a, m) = d$. *La congruencia* $ax \equiv b$ (mód. m) *es imposible si* b *no es divisible por* d. *Si* b *es múltiplo de* d, *la congruencia admite* d *soluciones.*

e. Para averiguar las soluciones de la congruencia (1), indicaremos solamente un método, basado en la teoría de las fracciones continuas; además, es suficiente limitarse al caso $(a, m) = 1$.

Desarrollando en fracción continua la razón $m : a$,

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \quad \cdot \quad \cdot + \cfrac{1}{q_n}}}$$

y considerando las dos fracciones reducidas últimas:

$$\frac{P_{n-1}}{Q_{n-1}}, \quad \frac{P_n}{Q_n} = \frac{m}{a},$$

en virtud de las propiedades de las fracciones continuas (**e, § 4**, cap. **I**), se tiene:

$$mQ_{n-1} - aP_{n-1} = (-1)^n,$$

$$aP_{n-1} \equiv (-1)^{n-1} \text{ (mód. } m),$$

$$a \cdot (-1)^{n-1} P_{n-1} b \equiv b \text{ (mód. } m).$$

Así, pues, la congruencia en cuestión admite la solución

$$x \equiv (-1)^{n-1} P_{n-1} b \text{ (mód. } m),$$

para cuya averiguación es suficiente calcular P_{n-1} según el método señalado en **d, § 4**, cap. **I**.

Ejemplo. Resolvamos la congruencia

$$111x \equiv 75 \text{ (mód. } 321). \qquad (3)$$

Aquí $(111, 321) = 3$, siendo 75 múltiplo de 3. Por esta razón, la congruencia admite tres soluciones.

Dividiendo ambos miembros de la congruencia y el módulo por 3, obtenemos la congruencia

$$37x \equiv 25 \text{ (mód. } 107), \qquad (4)$$

la cual debe resolverse primeramente. Se tiene

$$\begin{array}{r|l} 107 & 37 \\ 74 & 2 \\ \hline 37 & 33 \\ 33 & 1 \\ \hline 33 & 4 \\ 32 & 8 \\ \hline 4 & 1 \\ 4 & 4 \\ \hline \gg & \end{array}$$

q		2	1	8	4
P_s	1	2	3	26	107

Por lo tanto, en el caso dado $n = 4$, $P_{n-1} = 26$, $b = 25$, y obtenemos la solución de la congruencia (4) en la forma

$$x \equiv -26 \cdot 25 \equiv 99 \text{ (mód. } 107).$$

De aquí, las soluciones de la congruencia (3) se expresan así:

$$x \equiv 99; \quad 99 + 107; \quad 99 + 2 \cdot 107 \text{ (mód. } 321),$$

es decir,

$$x \equiv 99; \quad 206; \quad 313 \text{ (mód. } 321).$$

§ 3. Sistema de congruencias de primer grado

a. Estudiaremos solamente el sistema más simple de congruencias

$$x \equiv b_1 \text{ (mód. } m_1),$$

$$x \equiv b_2 \text{ (mód. } m_2), \ \ldots, \ x \equiv b_k \text{ (mód. } m_k) \qquad (1)$$

con una incógnita, pero con distintos módulos que son primos dos a dos.

b. Se puede resolver el sistema (1), es decir, se pueden hallar *todos los valores de* x *que le satisfacen, aplicando el teorema* siguiente:

Supongamos que los números M_s y M'_s vienen definidos por las condiciones

$$m_1 m_2 \ldots m_k = M_s m_s, \quad M_s M'_s \equiv 1 \text{ (mód. } m_s)$$

y sea

$$x_0 = M_1 M'_1 b_1 + M_2 M'_2 b_2 + \ldots + M_k M'_k b_k.$$

Entonces el conjunto de valores de x que satisfacen al sistema (1) *se determina por la congruencia*

$$x \equiv x_0 \text{ (mód. } m_1 m_2 \ldots m_k). \qquad (2)$$

En efecto, como todos los números M_j, distintos de M_s, son divisibles por m_s, para cualquier $s = 1, 2, \ldots, k$ se tiene

$$x_0 \equiv M_s M'_s b_s \equiv b_s \text{ (mód. } m_s),$$

y, por consiguiente, el sistema (1) es equivalente al sistema

$$x \equiv x_0 \text{ (mód. } m_1), \quad x \equiv x_0 \text{ (mód. } m_2), \ldots$$
$$\ldots, \quad x \equiv x_0 \text{ (mód. } m_k) \qquad (3)$$

(es decir, a los sistemas (1) y (3) les satisfacen unos mismos valores de x). Pero, en virtud de los teoremas **c**, § **3**, cap. **III** y **d**, § **3**, cap. **III**, al sistema (3) le satisfacen aquellos valores de x, y sólo aquellos, que satisfacen a la congruencia (2).

c. *Si $b_1, b_2, \ldots, b_k$ recorren independientemente uno de otro los sistemas completos de restos respecto de los módulos $m_1, m_2, \ldots, \ldots, m_k$, entonces x_0 recorre el sistema completo de restos respecto del módulo $m_1 m_2 \ldots m_k$.*

En efecto, x_0 recorre $m_1 m_2 \ldots m_k$ valores, los cuales, en virtud de **d**, § **3**, cap. **III**, son incongruentes respecto del módulo $m_1 m_2 \ldots m_k$.

d. Ejemplo. Resolvamos el sistema

$$x \equiv b_1 \text{ (mód. 4)}, \quad x \equiv b_2 \text{ (mód. 5)}, \quad x \equiv b_3 \text{ (mód. 7)}.$$

Aquí $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$, y además,

$$35 \cdot 3 \equiv 1 \text{ (mód. 4)}, \quad 28 \cdot 2 \equiv 1 \text{ (mód. 5)},$$
$$20 \cdot 6 \equiv 1 \text{ (mód. 7)}.$$

Por lo tanto

$$x_0 = 35 \cdot 3b_1 + 28 \cdot 2b_2 + 20 \cdot 6b_3 = 105b_1 + 56b_2 + 120b_3$$

y, por consiguiente, el conjunto de valores de x que satisfacen al sistema puede expresarse en la forma

$$x \equiv 105b_1 + 56b_2 + 120b_3 \text{ (mód. 140)}.$$

Por ejemplo, el conjunto de valores de x que satisfacen al sistema

$$x \equiv 1 \text{ (mód. 4)}, \quad x \equiv 3 \text{ (mód. 5)}, \quad x \equiv 2 \text{ (mód. 7)},$$

es

$$x \equiv 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 \equiv 93 \text{ (mód. 140)},$$

y el conjunto de valores de x que satisfacen al sistema

$$x \equiv 3 \text{ (mód. 4)}, \quad x \equiv 2 \text{ (mód. 5)}, \quad x \equiv 6 \text{ (mód. 7)},$$

es

$$x = 105 \cdot 3 + 56 \cdot 2 + 120 \cdot 6 \equiv 27 \text{ (mód. 140)}.$$

§ 4. Congruencias de cualquier grado respecto de un módulo primo

a. Sea p un número primo. Demostremos unos teoremas generales relativos a una congruencia de la forma

$$f(x) \equiv 0 \text{ (mód. } p); \qquad f(x) = ax^n + a_1x^{n-1} + \ldots + a_n. \quad (1)$$

b. *Una congruencia de la forma* (1) *es equivalente a una congruencia de grado no superior a* $p - 1$.

En efecto, dividiendo $f(x)$ por $x^p - x$, se tiene

$$f(x) = (x^p - x)\,Q(x) + R(x),$$

donde el grado de $R(x)$ no es superior a $p - 1$. Como $x^p - x \equiv 0$ (mód. p), resulta $f(x) \equiv R(x)$ (mód. p), de donde se deduce el teorema indicado.

c. *Si la congruencia* (1) *admite más de n soluciones, todos los coeficientes de* $f(x)$ *son múltiplos de p.*

En efecto, supongamos, que la congruencia (1) admite al menos $n + 1$ soluciones. Designando los restos de estas

soluciones con las letras $x_1, x_2, \ldots, x_n, x_{n+1}$, podemos expresar $f(x)$ en la forma

$$\begin{aligned} f(x) = a(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\ + b(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) + \\ + c(x-x_1)(x-x_2)\ldots(x-x_{n-2}) + \\ + \ldots\ldots\ldots\ldots\ldots + \\ + k(x-x_1)(x-x_2) + \\ + l(x-x_1) + \\ + m. \end{aligned} \tag{2}$$

Con este fin, transformando (abriendo paréntesis) los sumandos del segundo miembro en polinomios, elegimos b de tal modo que la suma de los coeficientes de x^{n-1} en los dos primeros polinomios coincida con a_1; una vez hallado b, elegimos c de tal modo que la suma de los coeficientes de x^{n-2} en los primeros tres polinomios coincida con a_2, etc.

Haciendo en (2) $x = x_1, x_2, \ldots, x_n, x_{n+1}$, sucesivamente, comprobamos que todos los números $m, l, k, \ldots, c, b, a$ son múltiplos de p. Por lo tanto, también son múltiplos de p todos los números $a, a_1, \ldots, a_n$ (como sumas de números que son múltiplos de p).

d. *Si p es un número primo, se verifica la congruencia* (*teorema de Wilson*)

$$1 \cdot 2 \ldots (p-1) + 1 \equiv 0 \text{ (mód. } p). \tag{3}$$

En efecto, si $p = 2$ el teorema es evidente. Si $p > 2$ consideramos la congruencia

$$(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \text{ (mód. } p),$$

ésta es de grado no superior a $p-2$ y admite $p-1$ soluciones; precisamente las soluciones cuyos restos son $1, 2, \ldots, p-1$. Por consiguiente, según el teorema c todos sus coeficientes son múltiplos de p; en particular, también es

divisible por p el término independiente, el cual es precisamente igual al primer miembro de la congruencia (3).

Ejemplo. Se tiene $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 721 \equiv 0$ (mód. 7).

§ 5. Congruencias de cualquier grado respecto de un módulo compuesto

a. *Si $m_1, m_2, \ldots, m_k$ son primos dos a dos, la congruencia*

$$f(x) \equiv 0 \text{ (mód. } m_1 m_2 \ldots m_k) \qquad (1)$$

es equivalente al sistema

$$f(x) \equiv 0 \text{ (mód. } m_1),$$

$$f(x) \equiv 0 \text{ (mód. } m_2), \ \ldots, \ f(x) \equiv 0 \text{ (mód. } m_k).$$

Además, designando con $T_1, T_2, \ldots, T_k$ los números de soluciones de cada una de las congruencias de este sistema respecto de los módulos correspondientes y con T el número de soluciones de la congruencia (1), *se tiene*

$$T = T_1 T_2 \ldots T_k.$$

En efecto, la primera parte del teorema se deduce de **c** y **d**, § 3, cap. **III**. La segunda parte se deduce de que cada una de las congruencias

$$f(x) \equiv 0 \text{ (mód. } m_s) \qquad (2)$$

se cumple cuando, y sólo cuando, se cumple una de las T_s congruencias de la forma

$$x \equiv b_s \text{ (mód. } m_s)$$

donde b_s recorre los restos de las soluciones de la congruencia (2); además, son posibles en total $T_1 T_2 \ldots T_k$ combinaciones distintas de la forma

$x \equiv b_1$(mód. m_1), $x \equiv b_2$ (mód. m_2), $\ldots$ $x \equiv b_k$ (mód. m_k),

que dan lugar (**c**, § 3) a clases distintas respecto del módulo

$$m_1 m_2 \ldots m_k.$$

Ejemplo. La congruencia

$$f(x) \equiv 0 \text{ (mód. 35)}, \quad f(x) = x^4 + 2x^3 + 8x + 9 \qquad (3)$$

es equivalente al sistema

$$f(x) \equiv 0 \text{ (mód. 5)}, \quad f(x) \equiv 0 \text{ (mód. 7)}.$$

Fácilmente se comprueba (§ 1) que la primera congruencia de este sistema tiene 2 soluciones: $x \equiv 1;\ 4$ (mód. 5), la segunda congruencia tiene 3 soluciones: $x \equiv 3;\ 5;\ 6$ (mód. 7). Debido a esto, la congruencia (3) tiene $2 \cdot 3 = 6$ soluciones. Para hallar estas 6 soluciones, hay que resolver 6 sistemas de la forma

$$x \equiv b_1 \text{ (mód. 5)}, \quad x \equiv b_2 \text{ (mód. 7)}, \tag{4}$$

las cuales se obtienen haciendo recorrer a b_1 los valores $b_1 = 1;\ 4$, y a b_2 los valores $b_2 = 3;\ 5;\ 6$. Pero, como

$$35 = 7 \cdot 5 = 5 \cdot 7, \quad 7 \cdot 3 \equiv 1 \text{ (mód. 5)}, \quad 5 \cdot 3 \equiv 1 \text{ (mód. 7)},$$

el conjunto de valores de x que satisfacen al sistema (4) se expresa en la forma (b, § 3)

$$x \equiv 21b_1 + 15b_2 \text{ (mód. 35)}.$$

Por lo tanto, las soluciones de la congruencia (3) son

$$x \equiv 31;\ 26;\ 6;\ 24;\ 19;\ 34 \text{ (mód. 35)}.$$

b. En virtud del teorema a, la discusión y solución de la congruencia

$$f(x) \equiv 0 \text{ (mód. } p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k})$$

se reduce a la discusión y solución de las congruencias de la forma

$$f(x) \equiv 0 \text{ (mód. } p^{\alpha}); \tag{5}$$

como ahora aclararemos, esta última congruencia se reduce en general a la congruencia

$$f(x) \equiv 0 \text{ (mód. } p). \tag{6}$$

En efecto, todo x que satisface a la congruencia (5) necesariamente tiene que satisfacer también a la congruencia (6) Sea

$$x \equiv x_1 \text{ (mód. } p)$$

alguna solución de la congruencia (6). Entonces $x = x_1 + pt_1$, donde t_1 es entero. Poniendo este valor de x en la congruencia

$$f(x) \equiv 0 \text{ (mód. } p^2)$$

y desarrollando el primer miembro según la fórmula de Taylor, hallamos (teniendo en cuenta que $\frac{1}{k!} f^{(k)}(x_1)$ es entero y despreciando los términos que son múltiplos de p^2):

$$f(x_1) + pt_1 f'(x_1) \equiv 0 \text{ (mód. } p^2), \quad \frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0 \text{ (mód. } p).$$

Limitándonos aquí al caso en que $f'(x_1)$ no es divisible por p, resulta una solución:

$$t_1 \equiv t_1' \text{ (mód. } p); \quad t_1 = t_1' + pt_2.$$

La expresion de x toma la forma

$$x = x_1 + pt_1' + p^2 t_2 = x_2 + p^2 t_2;$$

poniéndola en la congruencia

$$f(x) \equiv 0 \pmod{p^2},$$

resulta

$$f(x_2) + p^2 t_2 f'(x_2) \equiv 0 \text{ (mód. } p^2),$$

$$\frac{f(x_2)}{p^2} + t_2 f'(x_2) \equiv 0 \text{ (mód. } p).$$

Aquí $f'(x_2)$ no es divisible por p, puesto que

$$x_2 \equiv x_1 \text{ (mód. } p),$$

$$f'(x_2) \equiv f'(x_1) \text{ (mód. } p),$$

y, por lo tanto, la última congruencia tiene una sola solución:

$$t_2 \equiv t_2' \text{ (mód. } p);$$

$$t_2 \equiv t_2' + pt_3.$$

La expresión de x toma la forma

$$x = x_2 + p^2 t_2' + p^3 t_3 = x_3 + p^3 t_3;$$

etc. De este modo, partiendo de la solución dada de la congruencia (6) hallamos la solución congruente con ella de la

congruencia (5). En resumen, *toda solución* $x \equiv x_1 \pmod{p}$ *de la congruencia* (6), *con la condición de que* $f'(x_1)$ *no sea divisible por* p, *proporciona una solución de la congruencia* (5):

$$x = x_\alpha + p^\alpha t_\alpha;$$
$$x \equiv x_\alpha \pmod{p^\alpha}.$$

Ejemplo. Resolvamos la congruencia

$$\left.\begin{aligned} f(x) &\equiv 0 \pmod{27}; \\ f(x) &= x^4 + 7x + 4. \end{aligned}\right\} \tag{7}$$

La congruencia $f(x) \equiv 0 \pmod{3}$ tiene una solución $x \equiv 1 \pmod{3}$; en este caso $f'(1) \equiv 2 \pmod{3}$ y, por consiguiente, no es divisible por 3. Hallamos:

$$x = 1 + 3t_1,$$
$$f(1) + 3t_1 f'(1) \equiv 0 \pmod{9},\quad 3 + 3t_1 \cdot 2 \equiv 0 \pmod{9},$$
$$2t_1 + 1 \equiv 0 \pmod{3},\quad t_1 \equiv 1 \pmod{3},\quad t_1 = 1 + 3t_2,$$
$$x = 4 + 9t_2,$$
$$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27},\quad 18 + 9t_2 \cdot 2 \equiv 0 \pmod{27},$$
$$2t_2 + 2 \equiv 0 \pmod{3},\quad t_2 \equiv 2 \pmod{3},\quad t_2 = 2 + 3t_3,$$
$$x = 22 + 27t_3.$$

Por lo tanto, la congruencia (7) tiene una solución

$$x \equiv 22 \pmod{27}.$$

Preguntas referentes al capítulo IV

1, a. Supongamos que m es entero, $m > 0$, $f(x, \ldots, w)$ es una función racional entera de r variables $x, \ldots, w$ $(r \geqslant 1)$ con coeficientes enteros. Si el sistema $x = x_0, \ldots, w = w_0$ satisface a la congruencia

$$f(x, \ldots, w) \equiv 0 \pmod{m} \tag{1}$$

entonces (generalización de la definición del § 1), el sistema de clase de números respecto del módulo m:

$$x \equiv x_0 \pmod{m}, \ldots, w \equiv w_0 \pmod{m}$$

lo consideramos como una solución de la congruencia (1).
Sea T el número de soluciones de la congruencia (1). Demostrar que

$$Tm = \sum_{a=0}^{m-1} \sum_{x=0}^{m-1} \cdots \sum_{w=0}^{m-1} e^{2\pi i \frac{af(x, \ldots, w)}{m}},$$

b. Con las notaciones de la pregunta **a** y de la pregunta **12, e**, cap. **III**, demostrar que

$$Tm = m^r \sum_{m_0 \setminus m} A(m_0).$$

c. Aplicar la igualdad de la pregunta **a** para demostrar el teorema del número de soluciones de una congruencia de primer grado.
d. Supongamos que m es entero, $m > 0$; $a, \ldots, f, g$ son enteros, en total $r + 1$ números ($r > 0$); $d = (a, \ldots, f, m)$; T es el número de soluciones de la congruencia

$$ax + \ldots + fw + g \equiv 0 \text{ (mód. } m).$$

Aplicando la igualdad de la pregunta, **a**, demostrar que

$$T = \begin{cases} m^{r-1}d, & \text{si } g \text{ es múltiplo de } d, \\ 0 & \text{en caso contrario.} \end{cases}$$

e. Demostrar el teorema de la pregunta **d** partiendo del teorema del número de soluciones de la congruencia $ax \equiv b$ (mód. m).
2, a. Sea $m > 1$, $(a, m) = 1$. Demostrar que la congruencia $ax \equiv b$ (mód. m) admite la solución $x \equiv ba^{\varphi(m)-1}$ (mód. m).
b. Sea p un número primo, $0 < a < p$. Demostrar que la congruencia $ax \equiv b$ (mód. p) admite la solución

$$x \equiv b(-1)^{a-1} \frac{(p-1)(p-2)\ldots(p-a+1)}{1 \cdot 2 \ldots a} \text{ (mód. } p).$$

c. α) Indicar el método más simple posible de resolución de una congruencia de la forma

$$2^k x \equiv b \text{ (mód. } m); \quad (2, m) = 1.$$

β) Indicar el método más simple posible de resolución de la congruencia

$$3^k x \equiv b \text{ (mód. } m); \ (3, m) = 1.$$

γ) Sea $(a, m) = 1$, $1 < a < m$. Desarrollando los métodos indicados en las preguntas α) y β), demostrar que la búsqueda de la solución de la congruencia $ax \equiv b$ (mód. m) puede reducirse a la búsqueda de las soluciones de congruencias de la forma $b + mt \equiv 0$ (mód. p), donde p es un divisor primo del número a.

3. Sea m entero, $m > 1$, $1 \leqslant \tau < m$, $(a, m) = 1$. Empleando la teoría de congruencias, demostrar la existencia de enteros x e y con las condiciones

$$ax \equiv y \text{ (mód. } m), \quad 0 < x \leqslant \tau, \quad 0 < |y| < \frac{m}{\tau}.$$

4, a. Siendo $(a, m) = 1$, consideramos la fracción simbólica $\frac{b}{a}$ respecto del módulo m, la cual denota cualquier resto de la solución de la congruencia $ax \equiv b$ (mód. m). Demostrar (las congruencias se toman respecto del módulo m) que:

α) Si $a \equiv a_1$, $b \equiv b_1$, se tiene $\frac{b}{a} \equiv \frac{b_1}{a_1}$.

β) El numerador b de la fracción simbólica $\frac{b}{a}$ se puede sustituir por un número congruente b_0, múltiplo de a. Entonces, la fracción simbólica $\frac{b}{a}$ es congruente con el número entero que se expresa por la fracción ordinaria $\frac{b_0}{a}$.

γ) $\frac{b}{a} + \frac{d}{c} \equiv \frac{bc + ad}{ac}$.

δ) $\frac{b}{a} \cdot \frac{d}{c} \equiv \frac{bd}{ac}$.

b, α) Supongamos que p es primo, $p > 2$, a es entero, $0 < a < p - 1$. Demostrar que

$$\binom{p-1}{a} \equiv (-1)^a \text{ (mód. } p).$$

β) Sea p un número primo, $p>2$. Demostrar que

$$\frac{2^p-2}{p} \equiv 1-\frac{1}{2}+\frac{1}{3}-\ldots-\frac{1}{p-1} \text{ (mód. } p).$$

5, a. Sea d un divisor del número a, que no sea divisible por el cuadrado de un número entero superior a 1 y tampoco por los números primos menores que n, y sea $\varkappa$ el número de divisores primos distintos del número d. Demostrar que en la sucesión

$$1\cdot 2 \ldots n,\ 2\cdot 3 \ldots (n+1),\ \ldots,\ a(a+1)\ldots(a+n-1) \quad (1)$$

hay $\frac{n^{\varkappa}a}{d}$ números que son múltiplos de d.

b. Sean $p_1, p_2, \ldots, p_k$ los divisores primos distintos del número a, donde ninguno de ellos es inferior a n. Demostrar que la cantidad de números de la sucesión (1) que son primos con a, es igual a

$$a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\ldots\left(1-\frac{n}{p_k}\right).$$

6. Sea $m_{1,2,\ldots,k}$ el mínimo común múltiplo de los números $m_1, m_2, \ldots, m_k$.

a. Supongamos que $d=(m_1, m_2)$. Demostrar que el sistema

$$x \equiv b_1 \text{ (mód. } m_1), \quad x \equiv b_2 \text{ (mód. } m_2)$$

admite solución, y sólo cuando, b_2-b_1 es múltiplo de d. Además, cuando admite solución, el conjunto de valores de x que satisfacen a este sistema se determina por una congruencia de la forma

$$x \equiv x_{1,2} \text{ (mód. } m_{1,2}).$$

b. Demostrar que en caso de que el sistema $x \equiv b_1$ (mód. m_1), $x \equiv b_2$ (mód. m_2), $\ldots$, $x \equiv b_k$ (mód. m_k) admita solución, el conjunto de valores x que le satisfacen se determina por una congruencia de la forma

$$x \equiv x_{1,2,\ldots,k} \text{ (mód. } m_{1,2,\ldots,k}).$$

7. Supongamos que m es entero, $m > 1$, a y b son enteros,

$$\left(\frac{a, b}{m}\right) = \sum_{x} e^{2\pi i \frac{ax+bx'}{m}},$$

donde x recorre el sistema reducido de restos respecto del módulo m, y $x' \equiv \frac{1}{x} \pmod{m}$ (en el sentido de la pregunta 4, a). Demostrar las siguientes propiedades del símbolo $\left(\frac{a, b}{m}\right)$:

α) $\left(\frac{a, b}{m}\right)$ es real.

β) $\left(\frac{a, b}{m}\right) = \left(\frac{b, a}{m}\right)$.

γ) Si $(h, m) = 1$ se tiene $\left(\frac{a, bh}{m}\right) = \left(\frac{ah, b}{m}\right)$.

δ) Si $m_1, m_2, \ldots, m_k$ son primos dos a dos, haciendo $m_1, m_2 \ldots m_k = m$, $M = M_s m_s$, se tiene

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right) \ldots \left(\frac{a_k, 1}{m_k}\right) = \left(\frac{M_1^2 a_1 + M_2^2 a_2 + \ldots + m_k^2 a_k, 1}{m}\right).$$

8. Supongamos que la congruencia

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$$

admite n soluciones

$$x \equiv x_1, x_2, \ldots, x_n \pmod{p}.$$

Demostrar que

$$a_1 \equiv -a_0 S_1 \pmod{p},$$
$$a_2 \equiv a_0 S_2 \pmod{p},$$
$$a_3 \equiv -a_0 S_3 \pmod{p},$$
$$\ldots\ldots\ldots\ldots$$
$$a_n \equiv (-1)^n a_0 S_n \pmod{p},$$

donde S_1 es la suma de todas las x_s, S_2 es la suma de sus productos dos a dos, S_3 es la suma de sus productos tres a tres, etc.

9, a. Demostrar el teorema de Wilson, considerando los pares de números x, x' de la sucesión $2, 3, \ldots, p-2$, que satisfacen a la condición $xx' \equiv 1$ (mód. p).

b. Sea P entero, $P > 1$, $1, 2 \ldots (P-1) + 1 \equiv 0$ (mód. P). Demostrar que P es primo.

10, a. Sea $(a_0, m) = 1$. Indicar una congruencia de n-ésimo grado con el coeficiente superior igual a 1, que sea equivalente a la congruencia

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \text{ (mód. } m).$$

b. Demostrar que la condición necesaria y suficiente para que la congruencia $f(x) \equiv 0$ (mód. p); $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$; $n \leqslant p$, admita n soluciones, es que sean divisibles por p todos los coeficientes del resto de la división de $x^p - x$ por $f(x)$.

c. Sea n un divisor de $p-1$, $n > 1$, $(A, p) = 1$. Demostrar que la condición necesaria y suficiente para que sea resoluble la congruencia $x^n \equiv A$ (mód. p) es que se cumpla la congruencia $A^{\frac{p-1}{n}} \equiv 1$ (mód. p); además, en caso de resolubilidad, la congruencia indicada admite n soluciones.

11. Supongamos que n es entero, $n > 0$, $(A, m) = 1$, y que se conoce una solución $x \equiv x_0$ (mód. m) de la congruencia $x^n \equiv A$ (mód. m). Demostrar que todas las soluciones de esta congruencia se expresan por el producto de x_0 por los restos de las soluciones de la congruencia $y^n \equiv 1$ (mód. m).

Ejercicios numéricos referentes al capítulo IV

1, a. Resolver la congruencia $256x \equiv 179$ (mód. 337).

b. Resolver la congruencia $1\,215x \equiv 560$ (mód. 2 755).

2, a. Resolver las congruencias de los ejercicios **1, a** y **1, b** por el método de la pregunta **2, c.**

b. Resolver la congruencia $1\,296x \equiv 1\,105$ (mód. 2 413) por el método de la pregunta **2, c.**

3. Hallar todos los pares de números enteros x, y que satisfacen a la ecuación indeterminada $47x - 111y = 89$.

4, a. Indicar la solución general para el sistema

$$x \equiv b_1 \text{ (mód. 13)}, \quad x \equiv b_2 \text{ (mód. 17)}.$$

Sirviéndose de esta solución general, hallar luego tres números que *al dividirlos por 13 y 17 den los restos 1 y 12, 6 y 8, 11 y 4, respectivamente.*

b. Indicar la solución general para el sistema

$$x \equiv b_1 \text{ (mód. 25)}, \quad x \equiv b_2 \text{ (mód. 27)}, \quad x \equiv b_3 \text{ (mód. 59)}.$$

5, a. Resolver el sistema de congruencias (pregunta 6, a)

$$x \equiv 3 \text{ (mod. 8)}, \quad x \equiv 11 \text{ (mód 20)}, \quad x \equiv 1 \text{ (mód. 15)}.$$

b. Resolver el sistema de congruencias

$$x \equiv 1 \text{ (mód. 3)}, \quad x \equiv 4 \text{ (mód. 5)}, \quad x \equiv 2 \text{ (mód. 7)},$$
$$x \equiv 9 \text{ (mód. 11)}, \quad x \equiv 3 \text{ (mód. 13)}.$$

6. Resolver el sistema de congruencias

$$3x + 4y - 29 \equiv 0 \text{ (mód. 143)}, \quad 2x - 9y + 84 \equiv 0 \text{ (mód. 143)}.$$

7, a. ¿A qué congruencia de grado inferior a 5 es equivalente la congruencia

$$3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^6 + 4x^7 + x^5 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \text{ (mód. 5)}?$$

b. ¿A qué congruencia de grado inferior a 7 es equivalente la congruencia

$$2x^{17} + 6x^{16} + x^{14} + 5x^{13} + 3x^{11} + 2x^{10} + x^9 + 5x^8 + 2x^7 + 3x^5 + 4x^4 + 6x^3 + 4x^2 + x + 4 \equiv 0 \text{ (mód. 7)}?$$

8. ¿A qué congruencia, con el coeficiente superior igual a 1, es equivalente la congruencia (pregunta 10, a)

$$70x^5 + 78x^5 + 25x^4 + 68x^3 + 52x^2 + 4x + 3 \equiv 0 \text{ (mód. 101)}?$$

9, a. Resolver la congruencia

$$f(x) \equiv 0 \text{ (mód. 27)}, \quad f(x) = 7x^4 + 19x + 25,$$

hallando primero mediante un tanteo todas las soluciones de la congruencia

$$f(x) \equiv 0 \text{ (mód. 3)}.$$

b. Resolver la congruencia $9x^2 + 29x + 62 \equiv 0$ (mód. 64).

10, a. Resolver la congruencia $x^2 + 2x + 2 \equiv 0$ (mód. 125).

b. Resolver la congruencia $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0$ (mód. 625).

11, a. Resolver la congruencia $6x^2 + 27x^2 + 17x + 20 \equiv 0$ (mód. 30).

b. Resolver la congruencia $31x^4 + 57x^3 + 96x + 191 \equiv 0$ (mód. 225).

CAPITULO QUINTO

Congruencias de segundo grado

§ 1. Teoremas generales a. Entre las congruencias de grado $n > 1$, a continuación se estudiarán solamente las más simples, precisamente, las *congruencias binómicas*:

$$x^n \equiv a \text{ (mód. } m); \quad (a, m) = 1. \tag{1}$$

Si la congruencia (1) admite solución, el número a se llama *resto de grado n*, en caso contrario, a se llama *no-resto de grado n*. En particular, si $n = 2$, los restos y los no-restos se llaman *cuadráticos*; si $n = 3$, *cúbicos*; si $n = 4$, *bicuadráticos*.

b. En el presente capítulo se estudiará detalladamente el caso $n = 2$ y, en primer lugar, las congruencias binómicas de segundo grado respecto de un módulo impar p:

$$x^2 \equiv a \text{ (mód. } p); \quad (a, p) = 1. \tag{2}$$

c. *Si a es un resto cuadrático respecto del módulo p, la congruencia* (2) *tiene dos soluciones.*

En efecto, si a es un resto cuadrático, la congruencia (2) admite al menos una solución $x \equiv x_1$ (mód. p). Pero entonces, *como* $(-x_1)^2 = x_1^2$, *la misma congruencia admite también una* segunda solución $x \equiv -x_1$ (mód. p). Esta segunda solución es distinta de la primera, puesto que de $x_1 \equiv -x_1$ (mód. p)

tendríamos que $2x_1 \equiv 0$ (mód. p), lo cual es imposible, ya que $(2, p) = (x_1, p) = 1$.

Estas dos soluciones indicadas agotan todas las soluciones de la congruencia (2), puesto que esta última, siendo una congruencia de segundo grado, no puede admitir más de dos soluciones (c, § 4, cap IV).

d. *El sistema reducido de restos respecto del módulo p consta de* $\frac{p-1}{2}$ *restos cuadráticos, los cuales son congruentes con los números*

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2, \tag{3}$$

y de $\frac{p-1}{2}$ *no-restos cuadráticos.*

En efecto, entre los restos del sistema reducido respecto del módulo p, son restos cuadráticos aquéllos, y sólo aquellos, que son congruentes con los cuadrados de los números (sistema reducido de restos)

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}, \tag{4}$$

es decir, con los números (3). Por otra parte, los números (3) no son congruentes entre sí respecto del módulo p, puesto que de $k^2 \equiv l^2$ (mód. p), $0 < k < l \leqslant \frac{p-1}{2}$, se deduciría, en contra de c, que a la congruencia $x^2 \equiv l^2$ (mód. p) la satisfacen cuatro de los números (4): $x = -l, -k, k, l$.

e. *Si a es un resto cuadrático respecto del módulo p, se tiene:*

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (mód. } p); \tag{5}$$

si a es un no-resto cuadrático respecto del módulo p, se tiene

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (mód. } p). \tag{6}$$

En efecto, según el teorema de Fermat,

$$a^{p-1} \equiv 1 \text{ (mód. } p); \quad \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \text{ (mód. } p).$$

Uno de los factores del primer miembro de la última congruencia, y sólo uno, es divisible por p (ambos factores no pueden simultáneamente ser divisibles por p, pues, en caso contrario, su diferencia 2 sería divisible por p). Por lo tanto, se verifica una de las congruencias (5) y (6), y sólo una.

Pero todo resto cuadrático a satisface para cierto x a la congruencia

$$a \equiv x^2 \text{ (mód. } p) \qquad (7)$$

y, por consiguiente, satisface también a la congruencia (5), la cual puede obtenerse elevando (7), término a término a la potencia $\frac{p-1}{2}$. Además, los restos cuadráticos agotan todas las soluciones de la congruencia (5), puesto que, siendo ésta de grado $\frac{p-1}{2}$, no puede tener más de $\frac{p-1}{2}$ soluciones. Por esto, los no-restos cuadráticos satisfacen a la ecuación (6).

§ 2. *Símbolo de Legendre* a. Introduzcamos el *símbolo de Legendre* $\left(\frac{a}{p}\right)$ (se lee así: símbolo de a con respecto a p). Este símbolo se define para todos los números a que no son divisibles por p, y es igual a 1, si a es un resto cuadrático, e igual a -1, si a es un no-resto cuadráitco. El número a se llama numerador del símbolo y el número p, denominador del mismo.

b. En virtud de e, § 1, evidentemente, se tiene:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \text{ (mód. } p).$$

c. Aquí deduciremos las propiedades principales del símbolo de Legendre y en el párrafo siguiente, las del símbolo de Jacobi (éste es una generalización del símbolo anterior), las cuales facilitarán el cálculo rápido de dicho símbolo, y, por consiguiente, permitirán resolver el problema de la resolubilidad de la congruencia

$$x^2 \equiv a \text{ (mód. } p).$$

d. *Si* $a \equiv a_1 \pmod{p}$, *se tiene,* $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$. Esta propiedad se debe a que los números de una misma clase son simultáneamente restos o no-restos cuadráticos.

e. $\left(\frac{1}{p}\right) = 1$.

En efecto, $1 = 1^2$ y, por lo tanto, 1 es un resto cuadrático.

f. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Esta propiedad se deduce de **b** para $a = -1$.

Como $\frac{p-1}{2}$ es par si p es de la forma $4m+1$ y es impar si p es de la forma $4m+3$, de aquí se deduce que -1 es un resto cuadrático respecto del módulo p, si p es de la forma $4m+1$, y es un no-resto cuadrático respecto del módulo p, si p es de la forma $4m+3$.

g. $\left(\frac{ab\ldots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right)$.

En efecto, se tiene:

$$\left(\frac{ab\ldots l}{p}\right) \equiv (ab\ldots l)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \cdots l^{\frac{p-1}{2}} \equiv$$

$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right) \pmod{p},$$

de donde se deduce lo que se afirmaba. De aquí, como consecuencia, resulta que

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right),$$

o sea, en el numerador del símbolo de Legendre se puede despreciar cualquier factor cuadrado.

h. Para deducir las propiedades ulteriores del símbolo de Legendre daremos primero otra interpretación del mismo.

Haciendo $p_1 = \frac{p-1}{2}$, consideremos las congruencias

$$\left.\begin{aligned} a\cdot 1 &\equiv \varepsilon_1 r_1 \text{ (mód. } p), \\ a\cdot 2 &\equiv \varepsilon_2 r_2 \text{ (mód. } p), \\ &\cdots\cdots\cdots \\ a\cdot p_1 &\equiv \varepsilon_{p_1} r_{p_1} \text{ (mód. } p), \end{aligned}\right\} \qquad (1)$$

donde $\varepsilon_x r_x$ es el resto absoluto mínimo de ax, r_x es su módulo, de modo que $\varepsilon_x = \pm 1$.

Los números $a\cdot 1$, $-a\cdot 1$, $a\cdot 2$, $-a\cdot 2$, ..., $a\cdot p_1$, $-a\cdot p_1$ forman el sistema reducido de restos respecto del módulo p (**c**, § 5, cap. **III**); sus restos mínimos absolutos son $\varepsilon_1 r_1$, $-\varepsilon_1 r_1$, $\varepsilon_2 r_2$, $-\varepsilon_2 r_2$, ..., $\varepsilon_{p_1} r_{p_1}$, $-\varepsilon_{p_1} r_{p_1}$. Los positivos entre estos últimos, es decir, r_1, r_2, ..., r_{p_1}, tienen que coincidir con los números 1, 2, ..., p_1 (**b**, § 4, cap. **III**).

Multiplicando ahora las congruencias (1) y simplificando por

$$1\cdot 2 \ldots p_1 = r_1 r_2 \ldots r_{p_1},$$

obtenemos $a^{\frac{p-1}{2}} \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p_1} \text{ (mód. } p)$, de donde, (**b**), se tiene

$$\left(\frac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p_1}. \qquad (2)$$

i. Demos una forma más terminada a la expresión hallada del símbolo de Legendre. Se tiene

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right],$$

lo cual es par o impar según que el resto mínimo no negativo del número ax sea menor o mayor que $\frac{1}{2}p$, es decir, según que sea $\varepsilon_x = 1$ o $\varepsilon_x = -1$. De aquí, evidentemente, se tiene

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]},$$

por lo cual, de (2), hallamos:

$$\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}.$$

j. Suponiendo a impar, transformemos la última igualdad. Se tiene ($a+p$ es par)

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\frac{a+p}{2}}{p}\right)=\left(\frac{\frac{a+p}{2}}{p}\right)=$$

$$=(-1)^{\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]}=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum_{x=1}^{p_1}x},$$

de donde

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}. \qquad (3)$$

La fórmula (3) nos permitirá deducir dos propiedades muy importantes del símbolo de Legendre.

k.

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Es consecuencia de la fórmula (3) para $a=1$.

Pero p puede expresarse en la forma $p=8m+s$, donde s es uno de los números 1, 3, 5, 7. Además $\frac{p^2-1}{8}=8m^2+$ $+2ms+\frac{s^2-1}{8}$, siendo este número par si $s=1$ ó $s=7$ e impar si $s=3$ ó $s=5$. Por lo tanto, el número 2 es un resto cuadrático respecto del módulo p si p es de la forma $8m+1$ o de la forma $8m+7$ y es un no-resto cuadrático respecto del módulo p si p es de la forma $8m+3$ o de la forma $8m+5$.

1. *Si p y q son primos impares, se tiene (ley recíproca de los restos cuadráticos).*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Como $\frac{p-1}{2}\cdot\frac{q-1}{1}$ es impar solamente cuando ambos números p y q son de la forma $4m+3$, y es par si al menos uno de estos números es de la forma $4m+1$, la propiedad señalada se puede formular así:
Si ambos números p y q son de la forma $4m+3$, se tiene:

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right);$$

si al menos uno de ellos es de la forma $4m+1$, se tiene:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Para llevar a cabo la demostración, obsérvese que, en virtud de κ, la fórmula (3) toma la forma

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]}. \qquad (4)$$

Haciendo ahora $\frac{q-1}{2} = q_1$, consideremos los p_1q_1 pares de números que se obtienen cuando en las expresiones qx, py los números x e y recorren, independientemente uno del otro, los sistemas de valores

$$x = 1, 2, \ldots, p_1,\ y = 1, 2, \ldots, q_1.$$

Nunca puede ocurrir que sea $qx = py$, puesto que de esta igualdad se deduciría que py es múltiplo de q, lo cual es imposible, puesto que $(p, q) = (y, q) = 1$ (ya que $0 < y < q$). Por lo tanto, se puede hacer $p_1q_1 = S_1 + S_2$, donde S_1 es el número de pares con $qx < py$ y S_2 es el número de pares con $py < qx$.

Evidentemente, S_1 es también el número de pares con $x < \frac{p}{q} y$. Aquí, para cada y dado se puede tomar $x = 1, 2, \ldots, \left[\frac{p}{q} y\right]$. $\left(\text{Como } \frac{p}{q} y \leqslant \frac{p}{q} q_1 < \frac{p}{2}, \text{ se tiene } \left[\frac{p}{q} y\right] \leqslant \leqslant p_1\right)$. Por consiguiente,

$$S_1 = \sum_{y=1}^{q_1} \left[\frac{p}{q} y\right].$$

De un modo análogo, nos convencemos de que

$$S_2 = \sum_{x=1}^{p_1} \left[\frac{q}{p} x\right].$$

Pero entonces, según la igualdad (4), se tiene

$$\left(\frac{p}{q}\right) = (-1)^{S_1}, \quad \left(\frac{q}{p}\right) = (-1)^{S_2},$$

por lo cual,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1+S_2} = (-1)^{p_1 q_1},$$

de donde se deduce la propiedad indicada.

§ 3. Símbolo de Jacobi a. Para conseguir mayor rapidez en el cálculo del símbolo de Legendre, se considera el *símbolo más general de Jacobi*. Sea P impar, mayor que la unidad, y sea $P = p_1 p_2 \ldots p_r$ su descomposición en factores primos (entre ellos también puede haber iguales). Supongamos también que $(a, P) = 1$. Entonces el símbolo de Jacobi $\left(\frac{a}{P}\right)$ se define por la igualdad [1])

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_r}\right).$$

---

[1]) En el segundo miembro, $\left(\frac{a}{p_s}\right)$ denota el símbolo de Legendre. Por lo tanto, para P primo, los símbolos de Jacobi y de Legendre coinciden (*N. del T.*).

Las propiedades conocidas del símbolo de Legendre permiten establecer las propiedades análogas para el símbolo de Jacobi.

b. *Si* $a \equiv a_1 \pmod{P}$, *se tiene* $\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right)$.

En efecto,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\cdots$$
$$\cdots\left(\frac{a_1}{p_r}\right) = \left(\frac{a_1}{P}\right),$$

puesto que a, siendo congruente con a_1 respecto del módulo P, es también congruente con a_1 respecto de los módulos p_1, $p_2, \ldots, p_r$, ya que éstos son divisores de P.

c. $\left(\frac{1}{P}\right) = 1$.

En efecto,

$$\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_r}\right) = 1.$$

d. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

Para demostrar esto, obsérvese que

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_r}\right) =$$
$$= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\ldots+\frac{p_r-1}{2}}; \qquad (1)$$

pero

$$\frac{P-1}{2} = \frac{p_1 p_2 \ldots p_r - 1}{2} =$$
$$= \frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\cdots\left(1+2\frac{p_r-1}{2}\right) - 1}{2} =$$
$$= \frac{p_1-1}{2} + \frac{p_2-1}{2} + \ldots + \frac{p_r-1}{2} + 2N,$$

en virtud de lo cual, de la fórmula (1) deducimos que

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

e. $\left(\frac{ab\ldots l}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\cdots\left(\frac{l}{P}\right)$.

En efecto,

$$\left(\frac{ab\ldots l}{P}\right)=\left(\frac{ab\ldots l}{p_1}\right)\cdots\left(\frac{ab\ldots l}{p_r}\right)=$$

$$=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{l}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\cdots\left(\frac{l}{p_r}\right);$$

reuniendo los símbolos que tienen iguales numeradores, se obtiene la propiedad en cuestión. De aquí resulta la consecuencia

$$\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right).$$

f. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$.

En efecto,

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right)=$$

$$=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_r^2-1}{8}}. \qquad (2)$$

Pero

$$\frac{P^2-1}{8}=\frac{p_1^2p_2^2\ldots p_r^2-1}{8}=$$

$$=\frac{\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right)\ldots\left(1+8\frac{p_r^2-1}{8}\right)-1}{8}=$$

$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_r^2-1}{8}+2N,$$

en virtud de lo cual, de la fórmula (2) deducimos que

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

g. *Si P y Q son números impares positivos, primos entre sí, se tiene*

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

En efecto, supongamos que $Q = q_1 q_2 \dots q_s$ es la descomposición de Q en factores primos (entre éstos, de nuevo puede haber iguales). Se tiene

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\dots\left(\frac{Q}{p_r}\right) = \prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right) =$$

$$= (-1)^{\sum_{\alpha=1}^{r}\sum_{\beta=1}^{s}\frac{p_\alpha-1}{2}\frac{q_\beta-1}{2}} \prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right) =$$

$$= (-1)^{\left(\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)} \left(\frac{P}{Q}\right).$$

Pero, de un modo semejante a lo que se hizo en **d**, hallamos

$$\frac{P-1}{2} = \sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2} + 2N, \quad \frac{Q-1}{2} = \sum_{\beta=1}^{s}\frac{q_\beta-1}{2} + 2N_1,$$

en virtud de lo cual, la última fórmula implica que

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Ejemplo. Como un ejemplo de cálculo del símbolo de Legendre (además, a éste lo vamos a considerar como un caso particular del símbolo de Jacobi) averiguemos si admite solución la congruencia

$$x^2 \equiv 219 \pmod{383}.$$

Se tiene (aplicando sucesivamente las propiedades **g**, **b**, la consecuencia **e**, **g**, **b**, **e**, **f**, **g**, **b**, **d**):

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) =$$

$$= -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) =$$

$$= -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = 1;$$

por lo tanto, la congruencia considerada tiene dos soluciones.

§ 4. Caso de un módulo compuesto

a. Las congruencias de segundo grado respecto de un módulo compuesto se estudian y resuelven de acuerdo a las indicaciones del **§ 5**, cap. **IV**.

b. Comencemos con las congruencias de la forma

$$x^2 \equiv a \text{ (mód. } p^\alpha\text{)}; \quad \alpha > 0, \quad (a, p) = 1, \tag{1}$$

donde p es un número primo impar.

Haciendo $f(x) = x^2 - a$, se tiene $f'(x) = 2x$, y si $x \equiv x_1$ (mód. p) es una solución de la congruencia

$$x^2 \equiv a \text{ (mód. } p\text{)}, \tag{2}$$

entonces, en virtud de que $(a, p) = 1$ también $(x_1, p) = 1$, y como p es impar, resulta $(2x_1, p) = 1$, es decir, $f'(x_1)$ no es divisible por p. Por lo tanto, para la búsqueda de las soluciones de la congruencia (1) se pueden aplicar los razonamientos **b**, **§ 5**, cap **IV**, *proporcionando cada solución de la congruencia* (2) una solución de la congruencia (1). De lo expuesto deducimos que:

La congruencia (1) *tiene dos soluciones o ninguna, según que el número a sea un resto cuadrático o un no-resto cuadrático respecto del módulo p.*

c. Consideremos ahora la congruencia

$$x^2 \equiv a \text{ (mód. } 2^\alpha\text{)}; \quad \alpha > 0, \quad (a, 2) = 1. \tag{3}$$

En este caso $f'(x_1) = 2x_1$ es divisible por 2, por lo cual no pueden aplicarse los razonamientos expuestos en **b**, **§ 5**, cap **IV**; éstos deben modificarse del modo siguiente:

d. Si la congruencia (3) admite solución, entonces, como $(a, 2) = 1$, se tiene $(x, 2) = 1$; por consiguiente **(k, § 2)**, $x^2 - 1$ es divisible por 8. Por esta razón, reduciendo la congruencia (3) a la forma

$$(x^2 - 1) + 1 \equiv a \text{ (mód. } 2^\alpha\text{)}.$$

nos convencemos de que para que esta congruencia admita solución es necesario que sea

$$a \equiv 1 \text{ (mód. 4) si } \alpha = 2; \quad a \equiv 1 \text{ (mód. 8) si } \alpha \geqslant 3. \quad (4)$$

e. Supongamos cumplidas las condiciones (4), examinemos el problema de la búsqueda de las soluciones y de la cantidad de ellas.

En virtud de d, en los casos en que $\alpha \leqslant 3$, a la congruencia satisfacen todos los números impares. Por lo tanto, la congruencia $x^2 \equiv a$ (mód. 2) tiene una solución: $x \equiv 1$ (mod. 2) la congruencia $x^2 \equiv a$ (mód. 4) tiene dos soluciones: $x \equiv 1$; 3 (mód. 4), la congruencia $x^2 \equiv a$ (mód. 8) tiene cuatro soluciones: $x \equiv 1;, 3; 5; 7$ (mód. 8).

Para examinar los casos $\alpha = 4, 5, \ldots$ es conveniente reunir todos los números impares en dos progresiones aritméticas:

$$x = \pm (1 + 4t_3) \quad (5)$$

($1 + 4t_3 \equiv 1$ (mód. 4); $-1 - 4t_3 \equiv -1 \equiv 3$ (mód. 4)).

Veamos cuáles de los números (5) satisfacen a la congruencia $x^2 \equiv a$ (mód. 16). Obtenemos

$$(1 + 4t_3)^2 \equiv a \text{ (mód. 16)}, \quad t_3 \equiv \frac{a-1}{8} \text{ (mód. 2)},$$

$$t_3 = t_3' + 2t_4, \quad x = \pm (1 + 4t_3' + 8t_4) = \pm (x_4 + 8t_4).$$

Veamos cuáles de los últimos números satisfacen a la congruencia $x^2 \equiv a$ (mod. 32). Obtenemos

$$(x_4 + 8t_4)^2 \equiv a \text{ (mód. 32)}, \quad t_4 = t_4' + 2t_5,$$
$$x = \pm (x_5 + 16t_5),$$

etc. De este modo, demostramos que para cualquier $\alpha > 3$ los valores x que satisfacen a la congruencia (3) se expresan en la forma

$$x = \pm (x_\alpha + 2^{\alpha-1} t_\alpha).$$

Estos valores x forman cuatro soluciones distintas de la congruencia (3)

$$x \equiv x_\alpha; \quad x_\alpha + 2^{\alpha-1}; \quad -x_\alpha; \quad -x_\alpha - 2^{\alpha-1} \text{ (mód. } 2^\alpha)$$

(respecto del módulo 4, las dos primeras son congruentes con 1 y las dos últimas con -1).

Ejemplo. La congruencia

$$x^2 \equiv 57 \text{ (mód. 64)} \qquad (6)$$

admite cuatro soluciones, puesto que $57 \equiv 1$ (mód. 8). Expresando x en la forma $x = \pm (1 + 4t_3)$, obtenemos

$$(1 + 4t_3)^2 \equiv 57 \text{ (mód. 16)}, \quad 8t_3 \equiv 56 \text{ (mód. 16)},$$
$$t_3 \equiv 1 \text{ (mód. 2)}, \quad t_3 = 1 + 2t_4, \quad x = \pm (5 + 8t_4),$$
$$(5 + 8t_4)^2 \equiv 57 \text{ (mód. 32)}, \quad 5 \cdot 16t_4 \equiv 32 \text{ (mód. 32)},$$
$$t_4 \equiv 0 \text{ (mód. 2)}, \quad t_4 = 2t_5, \quad x = \pm (5 + 16t_5),$$
$$(5 + 16t_5)^2 \equiv 57 \text{ (mód. 64)}, \quad 5 \cdot 32t_5 \equiv 32 \text{ (mód. 64)}.$$
$$t_5 \equiv 1 \text{ (mód. 2)}, \quad t_5 = 1 + 2t_6, \quad x = \pm (21 + 32t_6).$$

Por lo tanto, las soluciones de la congruencia (6) son:

$$x \equiv \pm 21; \quad \pm 53 \text{ (mód. 64)}.$$

f. De **c**, **d** y **e** se deduce que:
Para la congruencia

$$x^2 \equiv a \text{ (mód. } 2^\alpha); \quad (a, 2) = 1$$

las condiciones necesarias de resolubilidad son: $a \equiv 1$ (mód. 4) *si* $\alpha = 2$, $a \equiv 1$ (mód. 8) *si* $\alpha \geqslant 3$. *Si se cumplen estas condiciones, el número de soluciones es igual a*: 1 *si* $\alpha = 1$; 2 *si* $\alpha = 2$; 4 *si* $\alpha \geqslant 3$.

g. De **b**, **f** y **a**, **§ 5.** cap **IV** se deduce que:
Para la congruencia de la forma general

$$x^2 \equiv a \text{ (mód. } m); \quad m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}; \quad (a, m) = 1$$

las condiciones necesarias de resolubilidad son:

$$a \equiv 1 \text{ (mód. 4) } si \ \alpha = 2, \quad a \equiv 1 \text{ (mód. 8) } si \ \alpha \geqslant 3,$$
$$\left(\frac{a}{p_1}\right) = 1, \quad \left(\frac{a}{p_2}\right) = 1, \ \ldots, \ \left(\frac{a}{p_k}\right) = 1.$$

Si se cumplen todas estas condiciones, el número de soluciones es igual a: 2^h *si* $\alpha = 0$ y *si* $\alpha = 1$; 2^{h+1} *si* $\alpha = 2$; 2^{h+2} *si* $\alpha \geqslant 3$.

Preguntas referentes al capítulo V

A continuación, la letra p denotará siempre un número primo impar.

1. Demostrar que la búsqueda de las soluciones de una congruencia de la forma

$$ax^2 + bx + c \equiv 0 \text{ (mód. } m), \quad (2a, m) = 1,$$

se reduce a la búsqueda de las soluciones de una congruencia de la forma $x^2 \equiv q$ (mód. m).

2. a. Aplicando **e**, **§ 1**, hallar las soluciones de la congruencia (en caso de que ello sea posible)

$$x^2 \equiv a \text{ (mód. } p); \quad p = 4m + 3.$$

b. Aplicando **b** y **k**, **§ 2**, indicar un método para buscar las soluciones de las congruencias de la forma

$$x^2 \equiv a \text{ (mód. } p); \quad p = 8m + 5.$$

c. Indicar el método más sencillo posible para buscar las soluciones de las congruencias de la forma

$$x^2 \equiv a \text{ (mód. } p); \quad p = 8m + 1,$$

si se conoce un número N que es un no-resto cuadrático respecto del módulo p.

d. Aplicando el teorema de Wilson, demostrar que las soluciones de la congruencia

$$x^2 + 1 \equiv 0 \text{ (mód. } p); \quad p = 4m + 1$$

son

$$x \equiv \pm 1 \cdot 2 \ldots 2m \text{ (mód. } p).$$

3. a. Demostrar que la congruencia

$$x^2 + 1 \equiv 0 \text{ (mód. } p) \tag{1}$$

admite solución cuando, y sólo cuando, p es de la forma $4m + 1$; la congruencia

$$x^2 + 2 \equiv 0 \text{ (mód. } p) \tag{2}$$

admite solución cuando, y sólo cuando, p, es de la forma $8m + 1$ ó $8m + 3$; la congruencia

$$x^3 + 3 \equiv 0 \text{ (mód. } p) \qquad (3)$$

admite solución cuando, y sólo cuando, p es de la forma $6m + 1$.

b. Demostrar que la cantidad de números primos de la forma $4m + 1$ es infinita.

c. Demostrar que la cantidad de números primos de la forma $6m + 1$ es infinita.

4. Supongamos que, dividiendo a los números $1, 2, \ldots, p-1$ en dos conjuntos, de modo que el segundo contenga al menos un número, se tiene:
el producto de dos números de un conjunto es congruente respecto del módulo p con un número del primer conjunto, mientras que el producto de dos números de distintos conjuntos es congruente respecto del módulo p con un número del segundo conjunto. Demostrar que esto ocurre cuando, y sólo cuando, el primer conjunto consta de los restos cuadráticos y el segundo, de los no-restos cuadráticos respecto del módulo p.

5, a. Deducir la teoría de las congruencias de la forma

$$x^2 \equiv a \text{ (mód. } p^\alpha); \quad (a, p) = 1,$$

expresando a y x en el sistema de numeración de base p.

b. Deducir la teoría de las congruencias de la forma

$$x^2 \equiv a \text{ (mód. } 2^\alpha); \quad (a, 2) = 1,$$

expresando a y x en el sistema de numeración de base 2.

6. Demostrar que las soluciones de la congruencia

$$x^2 \equiv a \text{ (mód. } p^\alpha); \quad (a, p) = 1,$$

son $x \equiv \pm PQ'$ (mód. p^α), donde

$$P = \frac{(z+\sqrt{a})^\alpha + (z-\sqrt{a})^\alpha}{2}, \quad Q = \frac{(z+\sqrt{a})^\alpha - (z-\sqrt{a})^\alpha}{2\sqrt{a}},$$

$$z^2 \equiv a \text{ (mód. } p), \; QQ' \equiv 1 \text{ (mód. } p^\alpha).$$

7. Indicar un método de resolución de la congruencia $x^2 \equiv \equiv 1$ (mód. m), que se base en la circunstancia de que la congruencia expuesta es equivalente a la siguiente: $(x-1)(x+1) \equiv 0$ (mód. m).

8. Sea $\left(\frac{a}{p}\right) = 0$ si $(a, p) = p$.

a. Siendo $(k, p) = 1$, demostrar que

$$\sum_{x=0}^{p-1} \left(\frac{x(x+k)}{p}\right) = -1.$$

b. Supongamos que cada uno de los números ε y η tiene uno de los valores ± 1, T es la cantidad de pares x, $x+1$, con la condición $\left(\frac{x}{p}\right) = \varepsilon$, $\left(\frac{x+1}{p}\right) = \eta$, donde $x = 1, 2, \ldots$ $\ldots, p-2$. Demostrar que

$$T = \frac{1}{4}\left(p - 2 - \varepsilon\left(\frac{-1}{p}\right) - \eta - \varepsilon\eta\right).$$

c. Supongamos que $(k, p) = 1$,

$$S = \sum_x \sum_y \left(\frac{xy+k}{p}\right),$$

donde x e y recorren las sucesiones crecientes, formadas por X e Y restos, respectivamente, del sistema completo respecto del módulo p. Demostrar que

$$|S| < \sqrt{XYp}.$$

Para la demostración se debe aplicar la desigualdad [1])

$$S^2 \leqslant X \sum_x \left| \sum_y \left(\frac{xy+k}{p}\right)\right|^2.$$

---

[1]) Esta desigualdad se obtiene aplicando la desigualdad bien conocida:

$$\left(\sum_{k=1}^{n} x_k\right)^2 < n \sum_{k=1}^{n} x_k^2.$$

(*N. del T.*).

d. Sea Q entero, $1 < Q < p$,

$$S = \sum_{x=0}^{p-1} S_x^2; \quad S_x = \sum_{z=0}^{Q-1} \left(\frac{x+z}{p}\right).$$

α) Demostrar que $S = (p - Q)\, Q$.

β) *Sea λ constante;* $0 < \lambda < 1$. *Demostrar que la cantidad* T de números de la sucesión $x = 0, 1, \ldots, p - 1$, para los cuales no se cumple la condición $S_x \leqslant Q^{0,5+0,5\lambda}$, satisface a la condición $T \leqslant pQ^{-\lambda}$.

γ) Sea M entero, $Q = [\sqrt{p}]$, $0 < M$, $M + 2Q \leqslant p$. Demostrar que en la sucesión

$$M, M + 1, \ldots, M + 2Q - 1$$

hay un no-resto cuadrático respecto del módulo p.

9, a. Demostrar que el número de expresiones de un entero $m > 1$ en la forma

$$m = x^2 + y^2, \quad (x, y) = 1, \; x > 0, \; y > 0 \qquad (1)$$

es igual al número de soluciones de la congruencia

$$z^2 + 1 \equiv 0 \text{ (mód. } m). \qquad (2)$$

Para la demostración, hacer $\tau = \sqrt{m}$, utilizar la expresión de $\alpha = \frac{z}{m}$ según el teorema de la pregunta **4, b**, cap. **I**, y considerar la congruencia que se obtiene al multiplicar término a término (2) por Q^2.

b. Sea a uno de los números 2 y 3. Demostrar que el número de expresiones de un número primo p, con la condición $p > a$, en la forma

$$p = x^2 + ay^2, \quad x > 0, \; y > 0, \qquad (3)$$

es igual a la mitad del número de soluciones de la congruencia

$$z^2 + a \equiv 0 \text{ (mód. } p). \qquad (4)$$

c. Sea p de la forma $4m + 1$, $(k, p) = 1$,

$$S(k) = \sum_{x=0}^{p-1} \left(\frac{x(x^2+k)}{p}\right).$$

Demostrar que

α) $S(k)$ es un número par.

β) $S(kt^2) = \left(\frac{t}{p}\right) S(k)$.

γ) Si $\left(\frac{r}{p}\right) = 1$, $\left(\frac{n}{p}\right) = -1$, se tiene (compárese con la pregunta **a**)

$$p = \left(\tfrac{1}{2} S(r)\right)^2 + \left(\tfrac{1}{2} S(n)\right)^2.$$

10. Sea D un entero positivo que no sea el cuadrado de un número entero. Demostrar que:

a. Si para un entero dado k, satisfacen a la ecuación

$$x^2 - Dy^2 = k$$

dos pares de números enteros $x = x_1$, $y = y_1$ y $x = x_2$, $y = y_2$, entonces a la ecuación

$$X^2 - DY^2 = k^2$$

satisfacen los números enteros X, Y que se determinan por la igualdad (el signo $\pm$ se elige arbitrariamente)

$$X + Y\sqrt{D} = (x_1 + y_1\sqrt{D})\,(x_2 \pm y_2\sqrt{D}).$$

b. La ecuación (ecuación de Pell)

$$x^2 - Dy^2 = 1 \qquad (1)$$

es resoluble en números enteros positivos x, y.

c. Si x_0, y_0 es el par de números positivos x, y con el valor menor de x (o, lo que es equivalente, con el valor menor de $x + y\sqrt{D}$), que satisface a la ecuación (1), entonces todos los pares de números positivos x, y que satisfacen a esta ecuación, se determinan por la igualdad

$$x + y\sqrt{D} = (x_0 + y_0\sqrt{D})^r; \quad r = 1, 2, \ldots \qquad (2)$$

11, a. Sea a un número entero.

$$U_{a,\,p} = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}}.$$

α) Siendo $(a, p) = 1$, demostrar que $|U_{a,p}| = \sqrt{p}$.
Para la demostración, se debe multiplicar la suma $U_{a,p}$ por la conjugada que se obtiene al sustituir i por $-i$. Designando con las letras x_1 y x las variables de sumación de la suma fundamental y de la conjugada, respectivamente, se deben reunir aquellos términos del producto en los que para un t dado

$$x_1 \equiv xt \text{ (mód. } p),$$

o bien

$$x_1 \equiv x + t \text{ (mód. } p).$$

β) Demostrar que

$$\left(\frac{a}{p}\right) = \frac{U_{a,p}}{U_{1,p}}.$$

b. Sea $m > 2$, $(a, m) = 1$,

$$S_{a,m} = \sum_{x=0}^{m-1} e^{2\pi i \frac{ax^2}{m}},$$

α) Demostrar que $S_{a,p} = U_{a,p}$ (pregunta a).
β) De los teoremas de las preguntas α) y a, α) se deduce que $|S_{a,p}| = \sqrt{p}$. Demostrar el siguiente aserto más general:

$$|S_{a,m}| = \sqrt{m}, \quad \text{si } m \equiv 1 \text{ (mód. 2)},$$
$$|S_{a,m}| = 0, \quad \text{si } m \equiv 2 \text{ (mód. 4)},$$
$$|S_{a,m}| = \sqrt{2m}, \quad \text{si } m \equiv 0 \text{ (mód. 4)}.$$

γ) Sea $m > 1$, $(2A, m) = 1$, $a =$ cualquier número entero. Demostrar que

$$\left| \sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2+ax}{m}} \right| = \sqrt{m}.$$

12, a. Supongamos que m es un número entero, superior a 1, z recorre Z números enteros dados, $\sum_z$ denota una suma extendida a todos estos números.

α) Sea la función $\Phi(x)$ tal, que para cualquier $a = 1, 2, \ldots$ $\ldots, m-1$ se tiene

$$\left|\sum_z \Phi(z)\, e^{2\pi i \frac{az}{m}}\right| \leqslant \Delta.$$

Supongamos también que M y Q son enteros, $0 \leqslant M < M + Q \leqslant m$, y que $\sum_z'$ denota una suma extendida solamente a aquellos valores de z que son congruentes con los números de la sucesión $M, M+1, \ldots, M+Q-1$ respecto del módulo m. Demostrar que

$$\sum_z{}' \Phi(z) = \frac{Q}{m} \sum_z \Phi(z) + \theta\Delta(\ln m - \delta),$$

donde $|\theta| < 1$, $\delta > 0$ siempre, $\delta > 0{,}5$ si $m \geqslant 12$. $\delta > 1$ si $m \geqslant 60$.

β) Supongamos que para cualquier $a = 1, 2, \ldots, m-1$ se tiene

$$\left|\sum_z e^{2\pi i \frac{az}{m}}\right| \leqslant \Delta_0$$

y sea N un número entero arbitrario. Entonces, para

$$l = \left[\frac{2\Delta_0 m}{Z}\right]$$

existe al menos un valor z que es congruente con uno de los números de la sucesión

$$N-l, \ldots, N-1, N, N+1, \ldots, N+l$$

respecto del módulo m.

b. Sean M y Q enteros, $0 < M < M + Q \leqslant p$.

α). Demostrar que

$$\left|\sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right)\right| < \sqrt{p}\ln p.$$

β) Sea R el número de restos cuadráticos y N el número de no-restos cuadráticos en la sucesión M. $M+1, \ldots$

$\ldots, M+Q-1$. Demostrar que

$$R=\frac{1}{2}Q+\frac{\theta}{2}\sqrt{p}\ln p,\quad N=\frac{1}{2}Q-\frac{\theta}{2}\sqrt{p}\ln p;\ |\theta|<1.$$

γ) Deducir la fórmula de la pregunta β) aplicando el teorema de la pregunta **11, b, β)** y el teorema de la pregunta **a.**

δ) Sea $(2A, m)=1$, M_0 y Q_0 son enteros, $0<M_0<M_0+Q_0\leqslant m$. Demostrar que para $m\geqslant 60$

$$\left|\sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i\frac{Ax^2}{m}}\right|<\sqrt{m}\ln m.$$

ε) Supongamos que $(A, p)=1$, M_0 y Q_0 son enteros, $0<M_0<M_0+Q_0\leqslant p$ y T denota la cantidad de números de la sucesión Ax^2, $x=M_0, M_0+1, \ldots, M_0+Q_0-1$, que son congruentes con los números de la sucesión $M, M+1, \ldots, M+Q-1$ respecto del módulo p. Demostrar que para $m\geqslant 60$

$$T=\frac{Q_0Q}{p}+\theta\sqrt{p}\,(\ln p)^2.$$

c. Deducir las fórmulas de la pregunta b, β) examinando la suma

$$\sum_{a=1}^{p-1}\sum_{\alpha=1}^{p-1}\sum_{x=M}^{M+Q-1}\sum_{y=M}^{M+Q-1}\left(\frac{\alpha}{p}\right)e^{2\pi i\frac{a(x-\alpha y)}{p}}.$$

Ejercicios numéricos referentes al capítulo V

1, a. Señálense los restos cuadráticos entre los restos del sistema reducido respecto del módulo 23.

b. Señálense los no-restos cuadráticos entre los restos del sistema reducido respecto del módulo 37.

2, a. Aplicando **e, § 1,** indicar el número de soluciones de las congruencias

α) $x^2\equiv 3$ (mód. 31); β) $x^2\equiv 2$ (mód. 31)

b. Indicar el número de soluciones de las congruencias

α) $x^2\equiv 5$ (mód. 73); β) $x^2\equiv 3$ (mód. 73)

3, a. Calculando el símbolo de Jacobi, indicar el número de soluciones de las congruencias

α) $x^2 \equiv 226$ (mód. 563); β) $x^2 \equiv 429$ (mód. 563).

b. Indicar el número de soluciones de las congruencias

α) $x^2 \equiv 3\,766$ (mód. 5 987); β) $x^2 \equiv 3\,149$ (mód. 5 987).

4, a. Aplicando los métodos de las preguntas **2, a; 2, b; 2, c** resolver las congruencias

α) $x^2 \equiv 5$ (mód. 19); β) $x^2 \equiv 5$ (mód. 29); γ) $x^2 \equiv 2$ (mód. 97).

b. Resolver las congruencias

α) $x^2 \equiv 2$ (mód. 311); β) $x^2 \equiv 3$ (mód. 277); γ) $x^2 \equiv 11$ (mód. 353).

5, a. Resolver la congruencia $x^2 \equiv 59$ (mód. 125) aplicando los métodos:

α) **b, § 4;** β) de la pregunta **5, a;** γ) de la pregunta **6.**

b. Resolver la congruencia $x^2 \equiv 91$ (mód. 243).

6, a. Resolver la congruencia $x^2 \equiv 41$ (mód. 64) aplicando los métodos:

α) **c, § 4;** β) de la pregunta **5, b.**

b. Resolver la congruencia $x^2 \equiv 145$ (mód. 256).