CAPITULO SEXTO

Raíces primitivas e índices

§ 1. Teoremas generales a. Si $(a, m) = 1$, existen enteros positivos γ con la condición $a^\gamma \equiv 1$ (mód. m), por ejemplo (según el teorema de Euler), $\gamma = \varphi(m)$. El menor de ellos se llama *exponente, al cual pertenece el número a respecto del módulo m.*

b. *Si a pertenece al exponente δ respecto del módulo m, los números* $1 = a^0, a^1, \ldots, a^{\delta-1}$ *no son congruentes entre sí respecto del módulo m.*

En efecto, si fuese $a^l \equiv a^k$ (mód. m), $0 \leqslant k < l < \delta$ resultaría que $a^{l-k} \equiv 1$ (mód. m), siendo $0 < l - k < \delta$, lo cual contradice a la definición de δ.

c. *Si a pertenece al exponente δ respecto del módulo m, entonces* $a^\gamma \equiv a^{\gamma'}$ (mód. m) *cuando, y sólo cuando,* $\gamma \equiv \gamma'$ (mód. δ); *en particular (si* $\gamma' = 0$), $a^\gamma \equiv 1$ (mód. m) *cuando, y sólo cuando,* γ *es divisible por* δ.

En efecto, sean r y r_1 los restos no negativos mínimos de los números γ y γ' respecto del módulo δ; entonces, para ciertos enteros q y q_1, se tiene $\gamma = \delta q + r$, $\gamma' = \delta q_1 + r_1$. De aquí, en virtud de que $a^\delta \equiv 1$ (mód. m), resulta que

$$a^\gamma = (a^\delta)^q a^r \equiv a^r \text{ (mód. } m),$$

$$a^{\gamma'} = (a^\delta)^{q_1} a^{r_1} \equiv a^{r_1} \text{ (mód. } m).$$

Por lo tanto, $a^\gamma \equiv a^{\gamma_1}$ (mód. m) cuando, y sólo cuando, $a^r \equiv a^{r_1}$ (mód. m), es decir, (b), cuando $r = r_1$.

d. Como $a^{\varphi(m)} \equiv 1$ (mód. m), de **c** ($\gamma' = 0$) se deduce que $\varphi(m)$ es divisible por δ. Por consiguiente, *los exponentes a los cuales pertenecen los números respecto del módulo m, son divisores de* $\varphi(m)$. El mayor entre estos divisores es el mismo número $\varphi(m)$. Los números que pertenecen al exponente $\varphi(m)$ (si tales existen) se llaman *raíces primitivas respecto del módulo m,*

§ 2. Raíces primitivas respecto de los módulos p^α y $2p^\alpha$

a. Sea p un número primo impar y $\alpha \geqslant 1$. Demostremos la existencia de raíces primitivas respecto de los módulos p^α y $2p^\alpha$.

b. *Si x pertenece al exponente ab respecto del módulo m, entonces x^a pertenece al exponente b.*

En efecto, supongamos que x^a pertenece al exponente δ. Entonces $(x^a)^\delta \equiv 1$ (mód. m), de donde $x^{a\delta} \equiv 1$ (mód. m); por lo tanto (**c**, § **1**), $a\delta$ es divisible por ab, es decir, δ es divisible por b. Por otra parte, $x^{ab} \equiv 1$ (mód. m), de donde $(x^a)^b \equiv 1$ (mód. m); por consiguiente (**c**, § **1**), b es divisible por δ. Por lo tanto, $\delta = b$.

c. *Si x pertenece al exponente a e y pertenece al exponente b respecto del módulo m, y $(a, b) = 1$, entonces xy pertenece al exponente ab.*

En efecto, supongamos que xy pertenece al exponente δ. Entonces $(xy)^\delta \equiv 1$ (mód. m). De aquí resulta que $x^{b\delta}\, y^{b\delta} \equiv 1$ (mód. m) y (**c**, § **1**) $x^{b\delta} \equiv 1$ (mód. m). Por lo tanto (**c**, § **1**), $b\delta$ es divisible por a, y como $(b, a) = 1$, δ es divisible por a. Del mismo modo hallamos que δ es divisible por b. El número δ, siendo divisible por a y por b, y teniendo en cuenta que $(a, b) = 1$, es también divisible por ab. Por otra parte, de $(xy)^{a\delta} \equiv 1$ (mód. m) se deduce (**c**, § **1**) que ab es divisible por δ. Por lo tanto, $\delta = ab$.

d. *Existen raíces primitivas respecto del módulo p.*

En efecto, sean

$$\delta_1, \delta_2, \ldots, \delta_r \qquad (1)$$

todos los exponentes distintos a que pertenecen los números 1, 2, . . ., $(p-1)$ respecto del módulo p. Supongamos que τ es el mínimo común múltiplo de estos exponentes y que $\tau = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ es su descomposición canónica. Cada factor $q_s^{\alpha_s}$ de esta descomposición divide al menos a uno de los números δ_j de la sucesión (1), el cual, por consiguiente, puede expresarse en la forma; $\delta_j = a q_s^{\alpha_s}$. Sea ξ_j uno de los números de la sucesión 1, 2, . . ., $p-1$, pertenecientes al exponente δ_j. Según b, el número $\eta_j = \xi_j^a$ pertenece al exponente $q_s^{\alpha_s}$, y según c, el producto $g = \eta_1 \eta_2 \ldots \eta_k$ pertenece al exponente $q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k} = \tau$.

Pero, como todos los números (1) dividen a τ, todos los números 1, 2, . . ., $p-1$ son soluciones (c, § 1) de la congruencia $x^\tau \equiv 1$ (mód. p); por esta razón, en virtud de **c, § 4**, cap. **IV**, se tiene, $p-1 \leqslant \tau$. Pero (**d**, § 1) τ es un divisor del número $p-1$. Por lo tanto, $\tau = p-1$ y g es una raíz primitiva.

e. *Sea g una raiz primitiva respecto del módulo p. Se puede señalar un número t de modo que el número u que se determina por la igualdad* $(g + pt)^{p-1} = 1 + pu$ *no sea divisible por p. El número correspondiente* $g + pt$ *es una raiz primitiva respecto del módulo* p^α *para cualquier* $\alpha > 1$.

En efecto, se tiene

$$g^{p-1} = 1 + pT_0,$$
$$(g + pt)^{p-1} = 1 + p(T_0 - g^{p-2}t + pT) = 1 + pu, \qquad (2)$$

donde u, simultáneamente con t, recorre el sistema completo de restos respecto del módulo p. Por lo tanto, se puede indicar un número t de modo que u no sea divisible por p. Para tal valor t, de (2) se deduce también que

$$\left.\begin{aligned} (g + pt)^{p(p-1)} &= (1 + pu)^p = 1 + p^2 u_2, \\ (g + pt)^{p^2(p-1)} &= (1 + p^2 u_2)^p = 1 + p^3 u_3, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \qquad (3)$$

donde u_2, u_3, . . . no son divisibles por p.

Supongamos que $g + pt$ pertenece al exponente δ respecto del módulo p^α Entonces

$$(g + pt)^\delta \equiv 1 \text{ (mód. } p^\alpha). \qquad (4)$$

De aquí que $(g + pt)^\delta \equiv 1$ (mód. p); por consiguiente, δ es un múltiplo de $p - 1$, y como δ divide a $\varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ se tiene que $\delta = p^{r-1}(p - 1)$, donde r es uno de los números $1, 2, \ldots, \alpha$. Sustituyendo el primer miembro de la congruencia (4) por su expresión de la igualdad correspondiente de (2) y (3), resulta ($u = u_1$):

$1 + p^r u_r \equiv 1$ (mód. p^α), $p^r \equiv 0$ (mód. p^α), $r = \alpha$, $\delta = \varphi(p^\alpha)$,

es decir, $g + pt$ es una raíz primitiva respecto del módulo p^α.

f. *Sea g_1 una raíz primitiva respecto del módulo p^α, donde $\alpha \geqslant 1$. Entonces, el impar entre los números g_1 y $g_1 + p^\alpha$, es una raíz primitiva respecto del módulo $2p^\alpha$.*

En efecto, es obvio que cualquier número impar x que satisfaga a una de las congruencias $x^\nu \equiv 1$ (mód. p^α) y $x^\nu \equiv -1$ (mód. $2p^\alpha$) satisface también a la otra. Por lo tanto, como $\varphi(p^\alpha) = \varphi(2p^\alpha)$, cualquier impar x que sea una raíz primitiva respecto de uno de los módulos p^α y $2p^\alpha$ es también una raíz primitiva respecto del otro. Pero, entre las dos raíces primitivas g_1 y $g_1 + p^\alpha$ respecto del módulo p^α, una de ellas es, inevitablemente, impar, por consiguiente, ésta será también una raíz primitiva respecto del módulo $2p^\alpha$.

§ 3. Búsqueda de las raíces primitivas respecto de los módulos p^α y $2p^\alpha$

Las raíces primitivas respecto de los módulos p^α y $2p^\alpha$, donde p es un número primo impar y $\alpha \geqslant 1$, pueden buscarse aplicando el siguiente teorema general:

Sea $c = \varphi(m)$ y sean $q_1, q_2, \ldots, q_k$ los divisores primos distintos del número c. Para que un número g, que es primo con m, sea una raíz primitiva respecto del módulo m, es necesario y suficiente que este número g no satisfaga a nin-

guna de las congruencias.

$$g^{\frac{c}{q_1}} \equiv 1 \text{ (mód. } m\text{)}, \; g^{\frac{c}{q_2}} \equiv 1 \text{ (mód. } m\text{)}, \; \ldots,$$
$$\ldots, \; g^{\frac{c}{q_k}} \equiv 1 \text{ (mód. } m\text{)}. \qquad (1)$$

En efecto, si g es una raíz primitiva, éste pertenece al exponente c y, por consiguiente, no puede satisfacer a ninguna de las congruencias (1).

Recíprocamente, supongamos que g no satisface a ninguna de las congruencias (1). Si el exponente δ, al cual pertenece g, fuese menor que c, entonces, designando con la letra q alguno de los divisores primos de $\frac{c}{\delta}$, tendríamos que $\frac{c}{\delta} = qu$, $\frac{c}{q} = \delta u$, $g^{\frac{c}{q}} \equiv 1$ (mód. p), lo cual contradice a la hipótesis hecha. Por lo tanto, $\delta = c$ y g es una raíz primitiva.

Ejemplo 1. Sea $m = 41$. Se tiene $\varphi(41) = 40 = 2^3 \cdot 5$, $\frac{40}{5} = 8$, $\frac{40}{2} = 20$. Por consiguiente, para que un número g, no divisible por 41, sea una raíz primitiva respecto del módulo 41, es necesario y suficiente que este número g no satisfaga a ninguna de las congruencias

$$g^8 \equiv 1 \text{ (mód. } 41\text{)}, \; g^{20} \equiv 1 \text{ (mód. } 41\text{)}. \qquad (2)$$

Ensayando los números 2, 3, 4, . . ., hallamos (respecto del módulo 41):

$$2^8 \equiv 10, \quad 3^8 \equiv 1, \quad 4^8 \equiv 18, \quad 5^8 \equiv 18, \quad 6^8 \equiv 10,$$
$$2^{20} \equiv 1, \qquad 4^{20} \equiv 1, \quad 5^{20} \equiv 1, \quad 6^{20} \equiv 40.$$

Vemos, pues, que los números 2, 3, 4, 5 no son raíces primitivas, puesto que cada uno de ellos satisface al menos a una de las congruencias (2). El número 6 es una raíz primitiva, pues no satisface a ninguna de las congruencias (2).

Ejemplo 2. Sea $m = 1\,681 = 41^2$. En este caso también se podría buscar una raíz primitiva aplicando el teorema general. Sin embargo, la hallaremos más fácilmente aplicando el

teorema e, § 2. Teniendo en cuenta (ejemplo 1) que el número 6 es una raíz primitiva respecto del módulo 41, hallamos:

$$6^{40} = 1 + 41\,(3 + 41l),$$

$$(6 + 41t)^{40} = 1 + 41\,(3 + 41l - 6^{39}t + 41T) = 1 + 41u.$$

Para que u no sea divisible por 41, es suficiente tomar $t = 0$. Por ello, se puede tomar por raíz primitiva respecto del módulo 1 681 el número $6 + 41 \cdot 0 = 6$.

Ejemplo 3. Sea $m = 3\,362 = 2 \cdot 1\,681$. En este caso también se podría buscar una raíz primitiva aplicando el teorema general. Sin embargo, la hallaremos más fácilmente aplicando el teorema f, § 2. Teniendo en cuenta (ejemplo 2) que el número 6 es una raiz primitiva respecto del módulo 1 681, se puede tomar por raíz primitiva respecto del módulo 3 362 el número impar entre los números 6, 6 + 1 681, o sea, el número 1 687.

§ 4. Indices respecto de los módulos p^α y $2p^\alpha$

a. Supongamos que p es un número primo impar, $\alpha \geqslant 1$; m es uno de los números p^α y $2p^\alpha$; $c = \varphi(m)$, g es una raíz primitiva respecto del módulo m.

b. *Si γ recorre los restos no negativos mínimos $\gamma = 0, 1, \ldots, c - 1$ respecto del módulo c, entonces g^γ recorre el sistema reducido de restos respecto del módulo m.*

En efecto, g^γ recorre c números que son primos con m y que, en virtud de b, § 1, no son congruentes entre sí respecto del módulo m.

c. Para los números a que son primos con m introduciremos el concepto de índice, el cual representa una analogía del concepto de logaritmo; en este caso, la raíz primitiva desempeña un papel similar al de la base de los logaritmos.

Si

$$a \equiv g^\gamma \pmod{m}$$

(se supone que $\gamma \geqslant 0$), el número γ se llama *índice del número a, respecto del módulo m, de base g* y se designa con la notación $\gamma = \text{ind } a$ (más exactamente $\gamma = \text{ing}_g a$).
En virtud de **b**, todo a que sea primo con m admite un índice único γ' entre los números de la sucesión

$$\gamma = 0, 1, \ldots, c - 1.$$

Una vez conocido γ', se pueden señalar también todos los índices del número a; según **c**, **§ 1**, éstos serán todos los números no negativos de la clase

$$\gamma \equiv \gamma' \text{ (mód. } c).$$

De la definición de índice dada se deduce inmediatamente que los números que poseen un índice dado γ forman una clase de números respecto del módulo m.
d. *Se tiene*

$$\text{ind } ab \ldots l \equiv \text{ind } a + \text{ind } b + \ldots + \text{ind } l \text{ (mód. } c)$$

y, en particular,

$$\text{ind } a^n \equiv n \text{ ind } a \text{ (mód. } c).$$

En efecto,

$$a \equiv g^{\text{ind } a} \text{ (mód. } m), \quad b \equiv g^{\text{ind } b} \text{ (mód. } m), \ldots$$
$$\ldots, l \equiv g^{\text{ind } l} \text{ (mód. } m),$$

de donde, multiplicando, hallamos

$$ab \ldots l \equiv g^{\text{ind } a + \text{ind } b + \ldots + \text{ind } l} \text{ (mód. } m).$$

Por consiguiente, ind a + ind b + ... + ind l es uno de los índices del producto $ab \ldots l$.
e. Debido a las aplicaciones prácticas de los índices, para cada módulo p (claro, no muy grande) se han compuesto *tablas de índices*. Estas son dos: una para hallar el índice de un número dado, otra para hallar los números por el índice. Las tablas contienen los restos no negativos mínimos de los números (el sistema reducido) y sus índices mínimos (el sistema completo) respecto de los módulos p y $c = \varphi(p) = p - 1$, respectivamente.

Ejemplo. Formemos las tablas indicadas para el módulo $p = 41$. Anteriormente se demostró (ejemplo 1, § 3) que el número $g = 6$ es una raíz primitiva respecto del módulo 41; tomémoslo por base de los índices. Hallamos (las congruencias se toman respecto del módulo 41):

$$\begin{array}{lllll} 6^0 \equiv 1 & 6^8 \equiv 10 & 6^{16} \equiv 18 & 6^{24} \equiv 16 & 6^{32} \equiv 37 \\ 6^1 \equiv 6 & 6^9 \equiv 19 & 6^{17} \equiv 26 & 6^{25} \equiv 14 & 6^{33} \equiv 17 \\ 6^2 \equiv 36 & 6^{10} \equiv 32 & 6^{18} \equiv 33 & 6^{26} \equiv 2 & 6^{34} \equiv 20 \\ 6^3 \equiv 11 & 6^{11} \equiv 28 & 6^{19} \equiv 34 & 6^{27} \equiv 12 & 6^{35} \equiv 38 \\ 6^4 \equiv 25 & 6^{12} \equiv 4 & 6^{20} \equiv 40 & 6^{28} \equiv 31 & 6^{36} \equiv 23 \\ 6^5 \equiv 27 & 6^{13} \equiv 24 & 6^{21} \equiv 35 & 6^{29} \equiv 22 & 6^{37} \equiv 15 \\ 6^6 \equiv 39 & 6^{14} \equiv 21 & 6^{22} \equiv 5 & 6^{30} \equiv 9 & 6^{38} \equiv 8 \\ 6^7 \equiv 29 & 6^{15} \equiv 3 & 6^{23} \equiv 30 & 6^{31} \equiv 13 & 6^{39} \equiv 7, \end{array}$$

por lo tanto, las tablas indicadas son:

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Aquí el número de la fila denota las decenas y el número de la columna denota las unidades del número (del índice). En la casilla que es común para la fila y columna indicadas viene colocado el índice (el número) correspondiente.

Por ejemplo, el ind 25 se halla en la casilla de la primera tabla que es común a la fila que posee el número 2 y a la columna que posee el número 5, es decir, ind 25 = 4. El número cuyo índice es 33 se halla en la casilla de la segunda tabla que es común a la fila que posee el número 3 y a la columna que posee el número 3, es decir, 33 = ind 17.

§ 5. Consecuencias de la teoría antecedente

a. Supongamos que p es un número primo impar; $\alpha \geqslant 1$, m es uno de los números p^α, $2p^\alpha$, y, finalmente, $c = \varphi(m)$.

b. *Sea* $(n, c) = d$; *entonces*:

1. *La congruencia*

$$x^n \equiv a \text{ (mód. } m) \qquad (1)$$

admite solución (*y, por consiguiente, a es un resto de grado n respecto del módulo m*) *cuando, y sólo cuando,* ind *a es un múltiplo de d.*

Si la congruencia (1) *es resoluble, ésta admite d soluciones.*

2. *En el sistema reducido de restos respecto del módulo m, el número de restos de grado n es igual a* $\frac{c}{d}$.

En efecto, la congruencia (1) es equivalente a la siguiente:

$$n \text{ ind } x \equiv \text{ind } a \text{ (mód. } c), \qquad (2)$$

la cual admite solución cuando, y sólo cuando, ind a es un múltiplo de d (**d**, § 2, cap **IV**).

Si la congruencia (2) admite solución, para el ind x se obtienen d valores incongruentes respecto del módulo c; a éstos les corresponden d valores de x que son incongruentes respecto del módulo m.

Por lo tanto, la afirmación **1** es cierta.

Entre los números $0, 1, \ldots, c-1$, los cuales son los índices mínimos de los restos del sistema reducido respecto del módulo m, hay $\frac{c}{d}$ números que son múltiplos de d. Por lo tanto, la afirmación **2** es cierta.

Ejemplo 1. Para la congruencia

$$x^8 \equiv 23 \text{ (mód. } 41) \qquad (3)$$

se tiene $(8, 40) = 8$, y como ind $23 = 36$ no es divisible por 8, la congruencia (3) es irresoluble.

Ejemplo 2. Para la congruencia

$$x^{12} \equiv 37 \text{ (mód. } 41) \qquad (4)$$

se tiene $(12, 40) = 4$, y ind $37 = 32$ es divisible por 4. Por lo tanto, la congruencia (4) es resoluble y admite 4 soluciones. Las soluciones indicadas se hallan del modo siguiente.

La congruencia (4) es equivalente a las siguientes:

$$12 \text{ ind } x \equiv 32 \text{ (mód. 40)}, \quad \text{ind } x \equiv 6 \text{ (mód. 10)}.$$

De aquí, para el ind x se hallan 4 valores incongruentes respecto del módulo 40:

$$\text{ind } x = 6,\ 16,\ 26,\ 36,$$

correspondientemente a lo cual se hallan 4 soluciones de la congruencia (4):

$$x \equiv 39;\ 18;\ 2;\ 23 \text{ (mód. 41)}.$$

Ejemplo 3. Los *números*

$$1,\ 4,\ 10,\ 16,\ 18,\ 23,\ 25,\ 31,\ 37,\ 40, \tag{5}$$

cuyos índices son múltiplos de 4, son todos los restos bicuadráticos (o también todos los restos de cualquier grado $n = 12$, 28, 36, . . ., donde $(n, 40) = 4$), que hay entre los restos positivos mínimos respecto del módulo 41. La cantidad de números *en la sucesión* (5) *es igual a* $10 = \frac{40}{4}$.

c. Junto con el aserto **b, 1** es útil el siguiente:

El número a es un resto de grado n respecto del módulo m cuando, y sólo cuando,

$$a^{\frac{c}{d}} \equiv 1 \text{ (mód. } m). \tag{6}$$

En efecto, la condición ind $a \equiv 0$ (mód. d) es equivalente a la siguiente: $\frac{c}{d}$ ind $a \equiv 0$ (mód. c). Por su parte, esta última es equivalente a la condición (6).

Ejemplo. En el teorema del **§ 3**, la imposibilidad de la congruencia $g^{\frac{c}{q}} \equiv 1$ (mód. m) es equivalente a la condición de que g sea un no-resto de grado q respecto del módulo m.

En particular, la imposibilidad de la congruencia $g^{\frac{c}{2}} \equiv 1$ (mód. m) es equivalente a la condición de que g sea un no-resto cuadrático respecto del módulo m (compárese con **e**, § 1, cap. V).

d. 1. *El exponente* δ, *al cual pertenece a respecto del módulo* m, *se determina por la igualdad* (ind. a, c) $= \frac{c}{\delta}$; *en particular, la pertenencia de* a *al conjunto de raíces primitivas respecto del módulo* m *se determina por la igualdad* (ind a, c) $= 1$.

2. *En el sistema reducido de restos respecto del módulo* m, *la cantidad de números que pertenecen al exponente* δ *es igual a* $\varphi(\delta)$; *en particular, la cantidad de raíces primitivas es igual a* $\varphi(c)$.

En efecto, δ es el divisor mínimo de c que satisface a la condición $a^{\delta} \equiv 1$ (mód. m). Esta condición es equivalente a

$$\delta \operatorname{ind} a \equiv 0 \text{ (mód. } c),$$

o sea,

$$\operatorname{ind} a \equiv 0 \left(\text{mód. } \frac{c}{\delta}\right).$$

Por lo tanto, δ es el divisor menor de c para el cual $\frac{c}{\delta}$ divide a ind a, de donde $\frac{c}{\delta}$ es el divisor mayor de c que divide a ind a, es decir, $\frac{c}{\delta} = (\text{ind } a, c)$. Por lo tanto, la afirmación 1 es cierta.

Entre los números $0, 1, \ldots, c-1$, los cuales son los índices mínimos de los restos del sistema reducido respecto del módulo m, son múltiplos de $\frac{c}{\delta}$ los números de la forma $\frac{c}{\delta} y$, donde $y = 0, 1, \ldots, \delta - 1$. La condición $\left(\frac{c}{\delta} y, c\right) = \frac{c}{\delta}$ equivale a que sea $(y, \delta) = 1$; a esta última condición satisfacen $\varphi(\delta)$ valores de y. Por lo tanto, la afirmación 2 es cierta.

Ejemplo 1. En el sistema reducido de restos respecto del módulo 41, los números que pertenecen al exponente 10 son aquellos números a que satisfacen a la condición $(\text{ind } a, 40) = \frac{40}{10} = 4$, es decir, son los números

$$4,\ 23,\ 25,\ 31.$$

En total se tienen $4 = \varphi(10)$ números.

Ejemplo 2. En el sistema reducido de restos respecto del módulo 41 son raíces primitivas los números a que satisfacen a la condición $(\text{ind } a, 40) = 1$, es decir, los números

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

En total se tienen $16 = \varphi(40)$ raíces primitivas.

§ 6. Indices respecto del módulo 2^α

a. Para el módulo 2^α la teoría precedente se sustituye por otra un poco más complicada.

b. Sea $\alpha = 1$. Entonces $2^\alpha = 2$. Se tiene $\varphi(2) = 1$. Es una raíz primitiva respecto del módulo 2, por ejemplo, $1 \equiv -1 \pmod 2$. El número $1^0 = (-1)^0 = 1$ forma el sistema reducido de restos respecto del módulo 2.

c. Sea $\alpha = 2$. Entonces $2^\alpha = 4$. Se tiene $\varphi(4) = 2$. Es una raíz primitiva respecto del módulo 4, por ejemplo, $3 \equiv -1 \pmod 4$. Los números $(-1)^0 = 1$, $(-1)^1 \equiv 3 \pmod 4$ forman el sistema reducido de restos respecto del módulo 4.

d. Sea $\alpha \geqslant 3$. Entonces $2^\alpha \geqslant 8$. Se tiene $\varphi(2^\alpha) = 2^{\alpha-1}$ Fácilmente se observa que en este caso no hay raíces primitivas; más exactamente: el exponente al que pertenece un número impar x respecto del módulo 2^α no es superior a $2^{\alpha-2} = \frac{1}{2}\varphi(2^\alpha)$. En efecto, se tiene

$$x^2 = 1 + 8t_1,$$
$$x^4 = 1 + 16t_2,$$
$$\cdots\cdots\cdots$$
$$x^{2\alpha-2} = 1 + 2^\alpha t_{\alpha-2} \equiv 1 \pmod{2^\alpha}.$$

Ahora bien, existen números que pertenecen al exponente $2^{\alpha-2}$. Tal es, por ejemplo, el número 5. En efecto,

$$5 = 1 + 4,$$
$$5^2 = 1 + 8 + 16,$$
$$5^4 = 1 + 16 + 32u_2,$$
$$\cdots\cdots\cdots$$
$$5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + 2^{\alpha}u_{\alpha-3},$$

de donde se ve que ninguna de las potencias 5^1, 5^2, 5^4, ..., $5^{2^{\alpha-3}}$ es congruente con 1 respecto del módulo 2^{α}. Fácilmente se observa que los números de las dos filas siguientes:

$$5^0, \quad 5^1, \ldots, \quad 5^{2^{\alpha-2}-1},$$
$$-5^0, \quad -5^1, \ldots, \quad -5^{2^{\alpha-2}-1}$$

forman el sistema reducido de restos respecto del módulo 2^{α}. En efecto, en total se tienen $2 \cdot 2^{\alpha-2} = \varphi(2^{\alpha})$ números; los números de cada fila por separado son incongruentes entre sí respecto del módulo 2^{α} (**b**, § **1**); finalmente, los números de la fila superior son incongruentes con los de la inferior, puesto que, respecto del módulo 4, los primeros son congruentes con 1 mientras que los segundos son congruentes con -1.

e. Para mayor comodidad en las investigaciones posteriores expresaremos los resultados **b**, **c**, **d** en una forma más uniforme, la cual valdrá también para el caso $\alpha = 0$.

Sea

$$c = 1, \ c_0 = 1, \qquad si \ \alpha = 0, \quad o \ si \ \alpha = 1;$$
$$c = 2, \ c_0 = 2^{\alpha-2}, \quad si \ \alpha \geqslant 2,$$

(por lo tanto, siempre $cc_0 = \varphi(2^{\alpha})$*) y supongamos que* γ *y* γ_0 *recorren, independientemente uno del otro, los restos mínimos no negativos*

$$\gamma = 0, \ \ldots, \ c-1; \quad \gamma_0 = 0, \ \ldots, \ c_0 - 1$$

respecto de los módulos c *y* c_0. *Entonces* $(-1)^{\gamma} 5^{\gamma_0}$ *recorre el sistema reducido de restos respecto del módulo* 2^{α}.

f. *La congruencia*

$$(-1)^{\gamma} 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma'_0} \text{ (mód. } 2^\alpha) \qquad (1)$$

se verifica cuando, y sólo cuando

$$\gamma \equiv \gamma' \text{ (mód. } c) \quad \gamma_0 \equiv \gamma'_0 \text{ (mód. } c_0).$$

En efecto, para $\alpha = 0$ el teorema es obvio. Por lo tanto, supongamos que $\alpha > 0$. Sean r y r_0 los restos mínimos no negativos respecto de los módulos c y c_0 para los números γ y γ_0, y sean r' y r'_0 los restos correspondientes para los números γ' y γ'_0. En virtud de **c**, § 1 (-1 pertenece al exponente c mientras que 5 pertenece al exponente c_0), se verifica la congruencia (1) cuando, y sólo cuando, $(-1)^r 5^{r_0} \equiv (-1)^{r'} 5^{r'_0}$ (mód. 2^α), es decir, (en virtud de **e**) cuando $r = r'$, $r_0 = r'_0$.

g. Si

$$a \equiv (-1)^{\gamma} 5^{\gamma_0} \text{ (mód. } 2^\alpha),$$

el sistema γ, γ_0 se llama *sistema de índices del número a respecto del módulo* 2^α.

En virtud de **e**, todo a que sea primo con 2^α (o sea, impar) admite un sistema único de índices γ', γ'_0 entre los $cc_0 = \varphi(2^\alpha)$ pares de valores γ, γ_0 indicados en **e**.

Conociendo el sistema γ', γ'_0 se pueden indicar también todos los sistemas de índices del número a; según **f**, éstos serán todos los pares γ, γ_0 formados por las clases de números no negativos

$$\gamma \equiv \gamma' \text{ (mód. } c), \ \gamma_0 \equiv \gamma'_0 \text{ (mód. } c_0).$$

De la definición dada de sistema de índices se deduce inmediatamente que los números que poseen un sistema de índices dado γ, γ_0 forman una clase de números respecto del módulo 2^α.

h. *Los índices del producto son congruentes con las sumas de los índices de los factores respecto de los módulos c y* c_0.

En efecto, sean $\gamma(a)$, $\gamma_0(a)$; . . .; $\gamma(l)$, $\gamma_0(l)$ los sistemas de

índices de los números $a, \ldots, l$. Se tiene

$$a \ldots l \equiv (-1)^{\gamma(a)+\ldots+\gamma(l)} 5^{\gamma_0(a)+\ldots+\gamma_0(l)}.$$

Por consiguiente, $\gamma(a) + \ldots + \gamma(l)$, $\gamma_0(a) + \ldots + \gamma_0(l)$ son los índices del producto $a \ldots l$.

§ 7. Índices respecto de cualquier módulo compuesto

a. Sea $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ la descomposición canónica del número m. Supongamos que c y c_0 denotan los valores indicados en **e**, § 6; $c_s = \varphi(p_s^{\alpha_s})$; g_s es la raíz primitiva mínima respecto del módulo p^{α_s}.

b. Si

$$\left.\begin{aligned} a &\equiv (-1)^\gamma 5^{\gamma_0} \pmod{2^\alpha}, \\ a &\equiv g_1^{\gamma_1} \pmod{p_1^{\alpha_1}}, \ \ldots, \ a \equiv g_k^{\gamma_k} \pmod{p_k^{\alpha_k}}. \end{aligned}\right\} \quad (1)$$

el sistema $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ se llama *sistema de índices del número a respecto del módulo m*.

De esta definición se deduce que γ, γ_0 es el sistema de índices del número a respecto del módulo 2^α y $\gamma_1, \ldots, \gamma_k$ son los índices del número a respecto de los módulos $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$. Por ello (**g**, § 6; **c**, § 4), todo a que es primo con m (y que, por consiguiente, es primo con todos los números $2^\alpha, p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$) admite un sistema único de índices $\gamma', \gamma_0', \gamma_1', \ldots, \gamma_k'$ *entre los* $cc_0c_1 \ldots c_k = \varphi(m)$ sistemas $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ que se obtienen cuando $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ recorren, independientemente uno de otro, los restos mínimos no negativos respecto de los módulos $c, c_0, c_1, \ldots, c_k$. Formando todos los sistemas $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$, compuestos por los números no negativos de las clases

$$\gamma \equiv \gamma_1' \pmod{c}, \quad \gamma_0 \equiv \gamma_0' \pmod{c_0},$$
$$\gamma_1 \equiv \gamma_1' \pmod{c_1}, \ \ldots, \ \gamma_k \equiv \gamma_k' \pmod{c_k}.$$

se obtienen todos los sistemas de índices del número a.

Los números a que poseen un sistema dado de índices $\gamma, \gamma_0,$

$\gamma_1, \ldots, \gamma_k$ pueden hallarse resolviendo el sistema (1) y, por consiguiente (b, § 3, cap. **IV**), forman una clase de números respecto del módulo m.

c. Como los índices γ, γ_0, γ_1, $\ldots$, γ_k del número a respecto del módulo m son los índices del mismo respecto de los módulos 2^α, $p_1^{\alpha_1}$, $\ldots$, $p_k^{\alpha_k}$, respectivamente, subsiste el teorema:

Los índices del producto son congruentes respecto de los módulos c, c_0, c_1, $\ldots$, c_k *con las sumas de los índices de los factores.*

d. Sea $\tau = \varphi(2^\alpha)$ si $\alpha \leqslant 2$ y $\tau = \frac{1}{2}\varphi(2^\alpha)$ si $\alpha > 2$ y designemos con h el mínimo común múltiplo de los números τ, c_1, $\ldots$, c_k. Para cualquier a que sea primo con m, se cumple la congruencia $a^h \equiv 1$ respecto de todos los módulos 2^α, $p_1^{\alpha_1}$, $\ldots$, $p_k^{\alpha_k}$, por lo cual, también se cumple esta congruencia respecto del módulo m. Por lo tanto, a no puede ser una raíz primitiva respecto del módulo m si $h < \varphi(m)$. Pero esto último ocurre cuando $\alpha > 2$ siendo $k > 1$, y también cuando $\alpha = 2$, $k = 1$. Por consiguiente, para $m > 1$ pueden existir raíces primitivas solamente en los casos $m = 2$, 4, $p_1^{\alpha_1}$, $2p_1^{\alpha_1}$. Pero precisamente en estos casos fue demostrada anteriormente (**§ 6**, **§ 2**) la existencia de raíces primitivas. En resumen, *todos los casos en que existen raíces primitivas respecto de un módulo* m, *superior a 1, son*

$$m = 2,\ 4,\ p^\alpha,\ 2p^\alpha.$$

Preguntas referentes al capítulo VI

A continuación, la letra p siempre denota un número primo impar, y en la pregunta **11**, **b**, también el número 2.

1, a. Sea a un número entero, $a > 1$. Demostrar que los divisores primos impares del número $a^p - 1$ dividen a $a - 1$ o son de la forma $2px + 1$.

b. Sea a un número entero, $a > 1$. Demostrar que los divisores primos impares del número $a^p + 1$ dividen a $a + 1$ o son de la forma $2px + 1$.

c. Demostrar que hay una cantidad infinita de números primos de la forma $2px + 1$.

d. Sea n un número entero, $n > 0$. Demostrar que los divisores primos del número $2^{2^n} + 1$ son de la forma $2^{n+1}x + 1$.

2. Sea a un número entero, $a > 1$, y sea n un número entero, $n > 0$. Demostrar que $\varphi(a^n - 1)$ es un múltiplo de n.

3, a. Sea n un número entero, $n > 1$. Con los números 1, 2, . . ., n, siendo n impar, formemos las permutaciones

$$1, 3, 5, \ldots, n-2, n, n-1, n-3, \ldots, 4, 2;$$
$$1, 5, 9, \ldots, 7, 3,$$

etc. y siendo n par, formemos las permutaciones

$$1, 3, 5, \ldots, n-1, n, n-2, \ldots, 4, 2;$$
$$1, 5, 9, \ldots, 7, 3,$$

etc. Demostrar que la k-ésima operación da la sucesión inicial cuando, y sólo cuando, $2^k \equiv \pm 1$ (mód. $2n-1$).

b. Sean n y m dos números enteros, $n > 1$, $m > 1$. Contemos los números 1, 2, . . ., n en orden directo desde 1 hasta n, después en orden inverso desde n hasta 2, luego de nuevo en orden directo desde 1 hasta n, después otra vez en orden inverso desde n hasta 2, etc. En este cálculo, escribamos los números: el 1°, el $(m+1)$-ésimo, el $(2m+1)$-ésimo, etc., hasta que se obtengan n números. Repitamos la misma operación con la nueva sucesión de n números, etc. Demostrar que la k-ésima operación de la sucesión inicial cuando, y sólo cuando,

$$m^k \equiv \pm 1 \text{ (mód. } 2n - 1).$$

4. Demostrar la existencia de $\varphi(\delta)$ números pertenecientes al exponente δ, considerando para ello la congruencia $x^\delta \equiv 1$ (mód. p) (pregunta **10, c**, cap. **IV**) y aplicando **d, § 3**, cap. **II**.

5, a. Demostrar que el número 3 es una raíz primitiva de los números primos de la forma $2^n + 1$, $n > 1$.

b. Demostrar que el número 2 ó -2 es una raíz primitiva de los números primos de la forma $2p + 1$, según que el número p sea de la forma $4n + 1$ o de la forma $4n + 3$.

c. Demostrar que el número 2 es una raíz primitiva de los números primos de la forma $4p + 1$.

d. Demostrar que el número 3 es una raíz primitiva de los números primos de la forma

$$2^n p + 1, \quad \text{si} \quad n > 1 \quad \text{y} \quad p > \frac{3^{2^n - 1}}{2^n}.$$

6, a. α) Sea n entero, $n \geqslant 0$, $S_n = 1^n + 2^n + \ldots + (p-1)^n$. Demostrar que

$S_n \equiv -1$ (mód. p), si n es un múltiplo de $p-1$,

$S_n \equiv 0$ (mód. p) en caso contrario.

β) Conservando las notaciones de la pregunta **9, c**, cap. **V**, demostrar que

$$S(1) \equiv -\left(\frac{\frac{p-1}{2}}{\frac{p-1}{4}}\right) \text{(mód. } p\text{)}.$$

b. Demostrar el teorema de Wilson aplicando **b, § 4.**

7. Supongamos que g y g_1 son raíces primitivas respecto del módulo p, y que $\alpha \operatorname{ind}_g g_1 \equiv 1$ (mód. $p-1$).

a. Sea $(a, p) = 1$. Demostrar que

$$\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a \text{ (mód. } p-1\text{)}.$$

b. Sea n un divisor de $p-1$, $1 < n < p-1$. Los números que son primos con p pueden dividirse en n clases, refiriendo a la s-ésima clase ($s = 0, 1, \ldots, n-1$) los números que satisfacen a la condición $\operatorname{ind} a \equiv s$ (mód. n). Demostrar que la clase de orden s según la base g es equivalente a la clase de orden s_1 según la base g_1, donde $s_1 \equiv \alpha s$ (mód. n).

8. Señalar el método más simple posible de resolución de la congruencia $x^n \equiv a$ (mód. p) (que sea cómodo si $(n, p-1)$ no

es muy grande) en el caso en que se conoce una raíz primitiva g respecto del módulo p.

9. Supongamos que $m, a, c, c_0, c_1, \ldots, c_k, \gamma, \gamma_0, \gamma_1, \ldots, \gamma_k$ denotan los valores indicados en el § 7. Tomando cualesquiera raíces $R, R_0, R_1, \ldots, R_k$ de las ecuaciones

$$R^c = 1, \quad R_0^{c_0} = 1, \quad R_1^{c_1} = 1, \quad \ldots, \quad R_k^{c_k} = 1.$$

hacemos

$$\chi(a) = R^{\gamma} R_0^{\gamma_0} R_1^{\gamma_1}, \quad \ldots, \quad R_k^{\gamma_k}.$$

Si $(a, m) > 1$, hacemos $\chi(a) = 0$.

La función definida de este modo para todos los valores enteros de a, la llamaremos *carácter* respecto del módulo m. Si $R = R_0 = R_1 = \ldots, = R_k = 1$, al carácter lo llamaremos *principal*; éste admite el valor 1 si $(a, m) = 1$ y el valor 0 si $(a, m) > 1$.

a. Demostrar que del modo indicado se obtienen $\varphi(m)$ caracteres distintos (dos caracteres se llaman distintos, si al menos para un valor de a éstos no son iguales entre sí).

b. Deducir las propiedades siguientes de los caracteres:

α) $\chi(1) = 1$,

β) $\chi(a_1 a_2) = \chi(a_1)\chi(a_2)$,

γ) $\chi(a_1) = \chi(a_2)$, si $a_1 = a_2$ (mód. m).

c. Demostrar que

$$\sum_{a=0}^{m-1} \chi(a) = \begin{cases} \varphi(m) & \text{para el carácter principal,} \\ 0 & \text{para los demás caracteres.} \end{cases}$$

d. Demostrar que, sumando para un valor de a dado respecto de todos los $\varphi(m)$ caracteres, se tiene

$$\sum_{\chi} \chi(a) = \begin{cases} \varphi(m), & \text{si } a \equiv 1 \text{ (mód. } m), \\ 0 & \text{en caso contrario.} \end{cases}$$

e. Considerando la suma

$$H = \sum_{\chi} \sum_{a} \frac{\chi(a)}{\psi(a)}$$

donde a recorre el sistema reducido de restos respecto del módulo m, demostrar que la función $\psi(a)$, definida para todos los valores enteros de a y que satisface a las condiciones:

$$\psi(a) = 0, \text{ si } (a, m) > 1,$$
$$\psi(a) \text{ no es idénticamente igual a } 0,$$
$$\psi(a_1 a_2) = \psi(a_1)\psi(a_2),$$
$$\varphi(a_1) = \psi(a_2), \text{ si } a_1 \equiv a_2 \text{ (mód. } m),$$

es un carácter.

f. Demostrar los teoremas siguientes:

α) Si $\chi_1(a)$ y $\chi_2(a)$ son dos caracteres, entonces $\chi_1(a)\chi_2(a)$ también es un carácter.

β) Si $\chi_1(a)$ es un carácter y $\chi(a)$ recorre todos los caracteres, entonces $\chi_1(a)\chi(a)$ también recorre todos los caracteres.

γ) Si $(l, m) = 1$, se tiene

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \begin{cases} \varphi(m), & \text{si } a \equiv 1 \text{ (mód. } m) \\ 0 & \text{en caso contrario.} \end{cases}$$

10, a. Sea n divisor de $p-1$, $1 < n \leqslant p-1$, y l un entero que no sea divisible por n. El número $R_1 = e^{2\pi i \frac{l}{n}}$ es una raíz de la ecuación $R_1^n = 1$ y, por consiguiente, la potencia $e^{2\pi i \frac{l \operatorname{ind} x}{n}}$, a la cual hay que asignarle el valor 0 cuando x es un múltiplo de p, es un carácter respecto del módulo p.

α) Demostrar que si $(k, p) = 1$, se tiene

$$\sum_{x=1}^{p-1} e^{2\pi i \frac{l \operatorname{ind}(x+k) - l \operatorname{ind} x}{n}} = -1.$$

β) Sea Q entero. $1 < Q < p$,

$$S = \sum_{x=0}^{p-1} |S_{l,n,x}|^2; \quad S_{l,n,x} = \sum_{z=0}^{Q-1} e^{2\pi i \frac{l \operatorname{ind}(x+z)}{n}}$$

Demostrar que $S=(p-Q)Q$.

11, a. Supongamos que a es un entero, n es divisor de $p-1$, $1<n\leqslant p-1$, k es un entero que no es divisible por n,

$$U_{a,p}=\sum_{x=1}^{p-1} e^{2\pi i \frac{k\,\mathrm{ind}\,x}{n}} e^{2\pi i \frac{ax}{p}}.$$

α) Siendo $(a,\ p)=1$, demostrar que $|U_{a,p}|=\sqrt{p}$.

β) Demostrar que

$$e^{2\pi i \frac{-k\,\mathrm{ind}\,a}{n}}=\frac{U_{a,p}}{U_{1,p}}.$$

γ) Supongamos que p es de la forma $4m+1$,

$$S=\sum_{x=1}^{p-2} e^{2\pi i \frac{\mathrm{ind}\,(x^2+x)}{4}}.$$

Demostrar que $p=A^2+B^2$ (compárese con las preguntas **9, a** y **9, c,** cap. **V**), donde A y B son enteros, definidos por la igualdad $S=A+Bi$.

δ) Supongamos que x_s recorre los números del sistema reducido de restos respecto del módulo p que satisfacen a la condición $\mathrm{ind}\ x_s\equiv s\ (\mathrm{mód.}\ n)$. Haciendo

$$S=\sum_{x_s} e^{2\pi i \frac{ax_s}{p}},$$

demostrar que

$$\left|S+\frac{1}{n}\right|<\left(1-\frac{1}{n}\right)\sqrt{p}.$$

b. Sea n entero, $n>2$, $m>1$, $(a,\ m)=1$,

$$S_{a,m}=\sum_{x} e^{2\pi i \frac{ax^n}{m}},\quad S'_{a,m}=\sum_{\xi}{}' e^{2\pi i \frac{a\xi^n}{m}},$$

donde x recorre el sistema completo y ξ el sistema reducido de restos respecto del módulo m (compárese con la pregunta **12, d,** cap. **III** y con la pregunta **11, b,** cap. **V**).

α) Sea $\delta=(n,\ p-1)$. Demostrar que

$$|S_{a,\,p}|\leqslant(\delta-1)\sqrt{p}.$$

β) Sea $(n,\ p)=1$ y sea s un entero, $1<s\leqslant n$. Demostrar que

$$S_{a,\,p^s}=p^{s-1},\quad S'_{a,\,p^s}=0.$$

γ) Sea s un entero, $s>n$. Demostrar que

$$S_{a,\,p^s}=p^{n-1}S_{a,\,p^{s-n}},\quad S'_{a,\,p^s}=0.$$

δ) Demostrar que

$$|S_{a,\,m}|<Cm^{1-\frac{1}{n}},$$

donde C depende solamente de n.

12. Sean M y Q enteros, $0\leqslant M<M+Q\leqslant p$.

a. Supongamos que n es un divisor de $p-1$, $1<n<$ $<p-1$, k es un entero, no divisible por n. Demostrar que

$$\Big|\sum_{x=M}^{M+Q-1}e^{2\pi i\frac{k\operatorname{ind}x}{n}}\Big|<\sqrt{p}\ln p.$$

b, α) Sea T la cantidad de números de la s-ésima clase de la pregunta **7**, **b**, comprendidos entre los números M, $M+$ $+1$, ..., $M+Q-1$. Demostrar que

$$T=\frac{Q}{n}+\theta\sqrt{p}\ln p;\quad|\theta|<1.$$

β) Sea N un entero arbitrario y $l_0=[2n\sqrt{p}-1]$. Demostrar que entre los números de la s-ésima clase de la pregunta **7**, **b** existe al menos uno que es congruente respecto del módulo p con alguno de los números de la sucesión

$$N-l_0,\ \ldots,\ N-1,\ N,\ N+1,\ \ldots,\ N+l_0.$$

c. Supongamos que k denota el número de divisores primos de $p-1$ y que H es el número de raíces primitivas respecto del módulo p, comprendidas entre los números M, $M+1$, ..., $M+Q-1$. Demostrar que

$$H=\frac{\varphi(p-1)}{p-1}Q+\theta 2^k\sqrt{p}\ln p;\quad|\theta|<1.$$

d. Supongamos que M_1 y Q_1 son enteros, $0 \leqslant M_1 < M_1 + Q_1 \leqslant p-1$, y que J denota la cantidad de números de la sucesión ind M, ind $(M+1)$, ..., ind $(M+Q-1)$, comprendidos entre los números de la sucesión M_1, M_1+1, ..., M_1+Q_1-1. Demostrar que

$$J = \frac{QQ_1}{p-1} + \theta\sqrt{p}(\ln p)^2; \quad |\theta| < 1.$$

13. Demostrar la existencia de una constante p_0 que satisface a la condición: si $p > p_0$, n es un divisor de $p-1$, $1 < n < p-1$, entonces, el menor entre los no-restos positivos de grado n respecto del módulo p, es $< h$;

$$h = p^{\frac{1}{c}}(\ln p)^2; \quad c = 2e^{1-\frac{1}{n}}.$$

14, a. Sea $m > 1$, $(a, m) = 1$,

$$S = \sum_{x=0}^{m-1}\sum_{y=0}^{m-1} \nu(x)\rho(y)e^{2\pi i\frac{axy}{m}};$$

$$\sum_{x=0}^{m-1}|\nu(x)|^2 + X, \quad \sum_{y=0}^{m-1}|\rho(y)|^2 = Y.$$

Demostrar que $|S| \leqslant \sqrt{XYm}$.

b, α) Supongamos que $m > 1$, $(a, m) = 1$, n es un entero, $n > 0$, K es el número de soluciones de la congruencia $x^n \equiv 1$ (mód. m),

$$S = \sum_{x=1}^{m-1}\chi(x)e^{2\pi i\frac{ax^n}{m}}.$$

Demostrar que $|S| \leqslant K\sqrt{m}$.

β) Sea ε una constante positiva arbitraria. Siendo n constante, demostrar para el número K de la pregunta α) que $K = O(m^\varepsilon)$.

c. Sean $2, q_2, \ldots, q_h$ los divisores primos distintos del número $p-1$.

α) Supongamos que g recorre las raíces primitivas respecto del módulo p, comprendidas en el sistema reducido de

restos, $(a,\ p)=1$,

$$S=\sum_{g} e^{2\pi i \frac{ag}{p}}.$$

Demostrar que

$$|S|<\frac{9}{8}\frac{\varphi(p-1)}{p-1}2^k\sqrt{p}.$$

Para la demostración se debe hacer recorrer a s y s' los números que satisfacen a las condiciones respectivas:

$$0\leqslant s<p-1;\ \ s\equiv 0 \text{ (mód. 2)};$$

$$s\equiv s_r \text{ (mód. } q_r),\ \ 0\leqslant s_r\leqslant\frac{q_r-1}{2}\quad (r=2,\ \ldots,\ k),$$

$$0\leqslant s'<p-1;\ \ s'\equiv 1 \text{ (mód. 2)};$$

$$s'\equiv s'_r \text{ (mód. } q_r),\ \ 0\leqslant s'_r\leqslant\frac{q_r-1}{2}\quad (r=2,\ \ldots,\ k),$$

y se debe considerar la suma

$$W=\sum_{t} S_t;\ \ S_t=\sum_{s}\sum_{s'} e^{2\pi i \frac{au_t v_t}{p}},\quad u_t=g_0^{ts},\ \ v_t=g_0^{ts'},$$

donde t recorre el sistema reducido de restos respecto del módulo p y g_0 es una de las raíces primitivas.

β) Sean M y Q enteros, $0\leqslant M<M+Q\leqslant p$. Demostrar que la cantidad T de raíces primitivas respecto del módulo p, contenidas en la serie $M,\ M+1,\ \ldots,\ M+Q-1$, se expresa por la fórmula

$$T=\frac{\varphi(p-1)}{p-1}\left(Q+\theta\frac{9}{8}2^k\sqrt{p}\ln p\right);\quad |\theta|<1.$$

γ) Sea N un número entero y $l_0=\left[\frac{12}{5}2^k\sqrt{p}\right]$. Demostrar que existe una raíz primitiva respecto del módulo p que es congruente con alguno de los números

$$N-l_0,\ \ldots,\ N-1,\ N,\ N+1,\ \ldots,\ N+l_0.$$

15, a. Supongamos que $(a,\ p)=(b,\ p)=1$, y sea n un número entero distinto de 1, $|n|=n_1$, $0<n_1<p$,

$$S=\sum_{x=1}^{p-1} e^{2\pi i\frac{ax^n+bx}{p}}.$$

Demostrar que

$$|S|<\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}.$$

b. Sea $(A,\ p)=1$ y supongamos que n es un entero, distinto de 1, $|n|=n_1$, $0<n_1<p$, M_0 y Q_0 son enteros, $0\leqslant M_0<M_0+Q_0\leqslant p$.

α) Sea

$$S=\sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i\frac{Ax^n}{p}}.$$

Demostrar que

$$|S|<\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}\ln p.$$

β) Supongamos que M y Q son enteros, $0\leqslant M<M+Q\leqslant p$, T es la cantidad de números de la sucesión Ax^n, $x=M_0$, $M_0+1,\ \ldots,\ M_0+Q_0-1$, que son congruentes respecto del módulo p con los números de la sucesión $M,\ M+1,\ \ldots$ $\ldots,\ M+Q-1$.

Demostrar que

$$T=\frac{Q_0Q}{p}+\theta\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}(\ln p)^2;\quad |\theta|<1.$$

c. Supongamos que $(a,\ p)=1$ y sean b y c enteros, $(b^2-4ac,\ p)=1$.

α) Sea γ un entero,

$$S=\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)e^{2\pi i\frac{\gamma x}{p}}.$$

Demostrar que $|S|<\frac{3}{2}p^{\frac{3}{4}}$.

β) Sean M y Q enteros, $0 \leqslant M < M+Q \leqslant p$,

$$S = \sum_{x=M}^{M+Q-1} \left(\frac{ax^2+bx+c}{p}\right).$$

Demostrar que $|S| < \frac{3}{2} p^{\frac{3}{4}} \ln p$.

Ejercicios numéricos referentes al capítulo VI

1, a. Hallar (mediante los cálculos más simples posible) el exponente al cual pertenece el número 7 respecto del módulo 43.

b. Hallar el exponente al cual pertenece el número 5 respecto del módulo 108.

2, a. Hallar las raíces primitivas respecto de los módulos 17, 289, 578.

b. Hallar las raíces primitivas respecto de los módulos 23, 529, 1 058.

c. Hallar la raíz primitiva mínima respecto del módulo 242.

3, a. Formar la tabla de índices respecto del módulo 17.

b. Formar la tabla de índices respecto del módulo 23.

4, a. Hallar una raíz primitiva respecto del módulo 71, empleando la nota del ejemplo c, § 5.

b. Hallar una raíz primitiva respecto del módulo 191.

5, a. Sirviéndose de la tabla de índices, indicar la cantidad de soluciones de las congruencias:

α). $x^{60} \equiv 79$ (mód. 97), β) $x^{35} \equiv 17$ (mód. 97), γ) $x^{15} \equiv 46$ (mód. 97).

b. Indicar la cantidad de soluciones de las congruencias:

α) $3x^{13} \equiv 31$ (mód. 41), β) $7x^7 \equiv 11$ (mód. 41), γ) $5x^{20} \equiv 37$ (mód. 41).

6, a. Sirviéndose de la tabla de índices, resolver las congruencias:

α) $x^3 \equiv 59$ (mód. 67), β) $x^{25} \equiv 17$ (mód. 67),

γ) $x^{30} \equiv 14$ (mód. 67).

b. Resolver las congruencias:

α) $23x^5 \equiv 15$ (mód. 73), β) $37x^6 \equiv 69$ (mód. 73),

γ) $44x^{31} \equiv 53$ (mód. 73).

7, a. Aplicando el teorema c, § 5, determinar la cantidad de soluciones de las congruencias:

α) $x^3 \equiv 2$ (mód. 37), β) $x^{16} \equiv 10$ (mód. 37).

b. Determinar la cantidad de soluciones de las congruencias:

α) $x^5 \equiv 3$ (mód. 71), β) $x^{21} \equiv 5$ (mód. 71).

8, a. Empleando el método de la pregunta 8, resolver las congruencias (al resolver la segunda congruencia se debe utilizar la tabla de raíces primitivas que viene insertada al final del libro):

$$\alpha)\ x^7 \equiv 37 \pmod{101}, \quad \beta)\ x^5 \equiv 44 \pmod{101}.$$

b. Resolver la congruencia

$$x^3 \equiv 23 \pmod{109}.$$

9, a. Empleando la tabla de índices, indicar, entre los restos del sistema reducido de restos respecto del módulo 19: α) los restos cuadráticos, β) los restos cúbicos.

b. Indicar, entre los restos del sistema reducido de restos respecto del módulo 37: α) los restos de grado 15, β) los restos de grado 8.

10, a. Indicar, entre los restos del sistema reducido de restos respecto del módulo 43: α) los números que pertenecen al exponente 6, β) las raíces primitivas.

b. Indicar entre los restos del sistema reducido de restos respecto del módulo 61: α) los números que pertenecen al exponente 10, β) las raíces primitivas.

Respuestas a las preguntas

Respuestas a las preguntas del capítulo I

1. El resto de la división de $ax + by$ por d, teniendo la forma $ax' + by'$ y siendo menor que d, es necesariamente igual a cero. Por ello, d es un divisor de todos los números de la forma $ax + by$ y, en particular, es un divisor común de los números $a \cdot 1 + b \cdot 0 = a$ y $a \cdot 0 + b \cdot 1 = b$. Por otra parte, la expresión de d muestra que todo divisor común de los números a y b divide a d. Por lo tanto, $d = (a, b)$ y el teorema **1, d, § 2** es justo. Los teoremas **e, § 2** se demuestran así: el menor número positivo de la forma $amx + bmy$ es $amx_0 + bmy_0$; el menor número positivo de la forma $\frac{a}{\delta}x + \frac{b}{\delta}y$ es $\frac{a}{\delta}x_0 + \frac{b}{\delta}y_0$.

La generalización de estos resultados es trivial.

2. Sea $\delta' = \frac{k}{l}$ una fracción irreducible con la condición $0 < l < Q_s$. Para $\delta_s = \alpha$ el teorema es evidente. Por ello, suponemos que δ_s no es igual a α y que, por consiguiente, existe δ_{s+1}. Limitémonos al caso $\delta_s < \delta_{s+1}$. Está claro que

$$|\delta' - \delta_s| \leqslant \frac{1}{lQ_s} > \frac{1}{Q_{s+1}Q_s}, \quad |\delta' - \delta_{s+1}| \geqslant \frac{1}{lQ_{s+1}} > \frac{1}{Q_{s+1}Q_s}.$$

Por esto, no puede ser $\delta_s \leqslant \delta' \leqslant \delta_{s+1}$ y, por lo tanto, o $\delta' < \delta_s$, o bien $\delta_{s+1} < \delta'$. En ambos casos δ_s está más próximo a α que δ'.

3. Si $n \leqslant 6$ el teorema es evidente; por lo tanto, suponemos que $n > 6$. Se tiene

$$\xi = \frac{1+\sqrt{5}}{2} = 1{,}618\ldots; \quad \log_{10}\xi = 0,\ 2\ldots;$$

$$\begin{aligned} Q_2 &\geqslant 1 && = g_1 = 1, \\ Q_3 &\geqslant Q_2 + 1 && \geqslant g_2 = 2 > \xi, \\ Q_4 &\geqslant Q_3 + Q_2 && \geqslant g_3 = g_2 + g_1 > \xi + 1 = \xi^2, \end{aligned}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Q_n \geqslant Q_{n-1} + Q_{n-2} \geqslant g_{n-1} = g_{n-2} + g_{n-3} > \xi^{n-3} + \xi^{n-4} = \xi^{n-2}.$$

De aquí que

$$N > \xi^{n-2}; \quad n < \frac{\log_{10} N}{\log_{10} \xi} + 2 < 5k + 2; \quad n \leqslant 5k + 1.$$

4, a. Para las fracciones $\frac{0}{1}$ y $\frac{1}{1}$ se tiene $0 \cdot 1 - 1 \cdot 1 = -1$. Intercalando la fracción $\frac{A+C}{B+D}$ entre las fracciones $\frac{A}{B}$ y $\frac{C}{D}$ que satisfacen a la condición $AD - BC = -1$, se tiene $A(B+D) - B(A+C) = (A+C)D - (B+D)C = -1$. Por lo tanto, es cierta la afirmación señalada al final de la pregunta. La existencia de una fracción $\frac{k}{l}$ con las condiciones $\frac{a}{b} < \frac{k}{l} < \frac{c}{d}$, $l \leqslant \tau$, es imposible. En caso contrario se tendría que

$$\frac{k}{l} - \frac{a}{b} \geqslant \frac{1}{lb}; \quad \frac{c}{d} - \frac{k}{l} \geqslant \frac{1}{ld}; \quad \frac{c}{d} - \frac{a}{b} \geqslant \frac{b+d}{lbd} > \frac{1}{bd}.$$

b. Está claro que es suficiente considerar el caso $0 \leqslant \alpha < 1$. Supongamos que $\frac{a}{b} \leqslant \alpha < \frac{c}{d}$, donde $\frac{a}{b}$ y $\frac{c}{d}$ son fracciones consecutivas de la sucesión de Farey, correspondientes a τ. Son posibles dos casos:

$$\frac{a}{b} \leqslant \alpha < \frac{a+c}{b+d}; \quad \frac{a+c}{b+d} \leqslant \alpha < \frac{c}{d}.$$

Por lo tanto, se verifica una de las dos desigualdades

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b(b+d)}; \quad \left|\alpha - \frac{c}{d}\right| \leqslant \frac{1}{d(b+d)},$$

de donde, en virtud de que $b + d > \tau$, se deduce inmediatamente el teorema indicado.

c. Si α es una fracción irreducible $\alpha = \frac{a}{b}$ con la condición $b \leqslant \tau$, por $\frac{P}{Q}$ se puede tomar la fracción misma $\frac{a}{b}$. En caso contrario, por $\frac{P}{Q}$ *se puede tomar la fracción reducida* $\frac{P_s}{Q_s}$ *que cumple la condición* $Q_s \leqslant \tau < Q_{s+1}$.

5, a. Los residuos que resultan al dividir los números primos impares por 4 son iguales a 1 ó a 3. El producto de números de la forma $4m + 1$ es de la forma $4m + 1$. Por lo tanto, el número $4p_1 \ldots p_k - 1$, donde $p_1, \ldots, p_k$ son primos de la forma $4m + 3$, tiene que tener un divisor primo q de la forma $4m + 3$. El número q no coincide con ninguno de los números $p_1, \ldots, p_k$.

b. Los números primos superiores a 3 son de la forma $6m + 1$ o de la forma $6m + 5$. El número $6p_1 \ldots p_k - 1$, donde $p_1, \ldots, p_k$ son primos de la forma $6m + 5$, tiene que tener un divisor primo q de la forma $6m + 5$. El número q no coincide con ninguno de los números $p_1, \ldots, p_k$.

6. Supongamos que $p_1, \ldots, p_k$ son k números primos cualesquiera y sea N un entero que cumpla las condiciones $2 < N$, $(3 \ln N)^k < N$. La cantidad de números a de la sucesión $1, 2, \ldots, N$, cuyas descomposiciones canónicas tienen la forma $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ no es superior a

$$\left(\frac{\ln N}{\ln 2} + 1\right)^k < (3 \ln N)^k < N,$$

puesto que $\alpha_s \leqslant \frac{\ln N}{\ln 2}$.

Por lo tanto, en la sucesión $1, 2, \ldots, N$ hay números en cuyas descomposiciones canónicas figuran primos distintos de $p_1, \ldots, p_k$.

7. Se obtienen tales sucesiones, por ejemlpo, para

$$M = 2 \cdot 3 \ldots (K + 1)\, t + 2; \quad t = 1, 2, \ldots .$$

8. Tomando un entero x_0 con la condición de que para $x \geqslant x_0$ sea $f(x) > 1$ y $f'(x) > 0$, hagamos $f(x_0) = X$. Todos los números $f(x_0 + Xt)$, $t = 1, 2, \ldots$, son compuestos (múltiplos de X).

9, a. Si se cumple (1), entonces uno de los números x, y es par; sea x par. De la igualdad

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2},$$

donde, evidentemente, $\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$, nos convencemos de la existencia de números enteros positivos u y v que cumplen las condiciones

$$\frac{x}{2} = uv, \quad \frac{z+y}{2} = u^2, \quad \frac{z-y}{2} = v^2.$$

De aquí se deduce que las condiciones indicadas en la pregunta son necesarias.

Es obvio que dichas condiciones son suficientes.

b. Convengamos en designar aquí con letras solamente los números enteros positivos. Supongamos que existen sistemas x, y, z, que cumplen las condiciones $x^4 + y^4 = z^2$, $x > 0$, $y > 0$, $z > 0$, $(x, y, z) = 1$; elijamos entre ellos el sistema con el valor menor de z. Suponiendo que x es par, obtenemos $x^2 = 2uv$, $y^2 = u^2 - v^2$, $u > v \geqslant 1$, $(u, v) = 1$, donde v es par (si u fuese par, tendríamos $y^2 = 4N + 1$, $u^2 = 4N_1$, $v^2 = 4N_2 + 1$, $4N + 1 = 4N_1 - 4N_2 - 1$, lo cual es

imposible). De aquí que

$$u=z_1^2,\quad v=2w^2,\quad y^2+4w^4=z_1^2,\quad 2w^2=2u_1v_1,$$

$u_1=x_1^2$, $v_1=y_1^2$, $x_1^2+y_1^2=z_1^2$, lo cual es imposible, puesto que $z_1<z$. De la irresolubilidad de la ecuación $x^4+y^4=z^2$, como un caso particular se deduce también, evidentemente, la irresolubilidad de la ecuación $x^4+y^4=t^4$ en enteros positivos x, y, t.

10. Haciendo $x=\frac{k}{l}$; $(k, l)=1$, obtenemos

$$k^n+a_1k^{n-1}l+\ldots+a_nl^n=0.$$

Por lo tanto, k^n es un múltiplo de l y, por consiguiente, $l=1$.

11, a. Supongamos que k es el mayor número entero que cumple la condición $2^k\leqslant n$ y sea P el producto de todos los números impares que no son superiores a n. El número $2^{k-1}PS$ se expresa en forma de una suma cuyos términos, a excepción de $2^{k-1}P\frac{1}{2^k}$, son números enteros.

b. Supongamos que k es el mayor número entero que cumple la condición $3^k\leqslant 2n+1$ y sea P el producto de todos los números que son primos con el número 6 y que no son superiores a $2n+1$. El número $3^{k-1}PS$ se expresa en forma de una suma cuyos términos, a excepción de $3^{k-1}P\frac{1}{3^k}$ son números enteros.

12. Para $n\leqslant 8$ el teorema se comprueba inmediatamente. Por lo tanto, suponiendo que $n>8$ y que el teorema es válido para los binomios $a+b$, $(a+b)^2$, ..., $(a+b)^{n-1}$, hay que demostrar el teorema para $(a+b)^n$. Pero los coeficientes del desarrollo de este binomio, a excepción de los extremos que son iguales a 1, son los números

$$\frac{n}{1},\quad \frac{n(n-1)}{1\cdot 2},\quad \ldots,\quad \frac{n(n-1)\ldots 2}{1\cdot 2\ldots(n-1)}.$$

Para que todos estos números sean impares es necesario y suficiente que sean impares los números de los extremos, los cuales son precisamente iguales a n, y también que sean impares todos los números que se obtienen al borrar los factores impares de los numeradores y denominadores de los números restantes. Pero, haciendo $n=2n_1+1$, estos números se pueden expresar como los términos de la sucesión

$$\frac{n_1}{1},\quad \frac{n_1(n_1-1)}{1\cdot 2},\quad \ldots,\quad \frac{n_1(n_1-1)\ldots 2}{1\cdot 2\ldots(n_1-1)}.$$

Mas éstos, como $n_1 < n$, son impares cuando, y sólo cuando, n_1 es de la forma $2^k - 1$, es decir, cuando n es de la forma $2(2^k - 1) + 1 = 2^{k+1} - 1$.

Respuestas a las preguntas del capítulo II

1, a. En la ordenada del punto de la curva $y = f(x)$ cuya abscisa es x, hay $[f(x)]$ puntos enteros de la región indicada.

b. La igualdad indicada se deduce de la igualdad $T_1 + T_2 = T$, donde T_1, T_2, T denotan la cantidad de puntos enteros en las regiones

$$0 < x < \frac{Q}{2}, \quad 0 < y < \frac{P}{Q}x.$$

$$0 < y < \frac{P}{2}, \quad 0 < x < \frac{Q}{P}y,$$

$$0 < x < \frac{Q}{2}, \quad 0 < y < \frac{P}{2}.$$

c. La igualdad indicada se deduce de la igualdad

$$T = 1 + 4(T_1 + T_2 + T_3 - T_4),$$

donde T_1, T_2, T_3, T_4 denotan la cantidad de puntos enteros en las regiones

$$x = 0, \qquad 0 < y < r;$$

$$0 < x \leqslant \frac{r}{\sqrt{2}}, \qquad 0 < y \leqslant \sqrt{r^2 - x^2};$$

$$0 < y \leqslant \frac{r}{\sqrt{2}}, \qquad 0 < x \leqslant \sqrt{r^2 - y^2};$$

$$0 < x \leqslant \frac{r}{\sqrt{2}}, \qquad 0 < y \leqslant \frac{r}{\sqrt{2}}.$$

d. La igualdad indicada se deduce de la igualdad $T = T_1 + T_2 - T_3$, donde T_1, T_2, T_3 denotan la cantidad de puntos enteros en las regiones

$$0 < x \leqslant \sqrt{n}, \qquad 0 < y \leqslant \frac{n}{x};$$

$$0 < y \leqslant \sqrt{n}, \qquad 0 < x \leqslant \frac{n}{y};$$

$$0 < x \leqslant \sqrt{n}, \qquad 0 < y \leqslant \sqrt{n}.$$

e. En el caso de un rectángulo con los lados paralelos a los ejes coordenados, el teorema es evidente. En el caso de un trapecio con las bases paralelas a uno de los ejes coordenados y con un lado perpendi-

cular a las bases, el teorema se demuestra fácilmente considerando el rectángulo que se forma al unir dos trapecios de éstos. El caso de un triángulo se reduce fácilmente al caso del trapecio indicado. Del caso del triángulo no es difícil pasar también al caso general, observando que un polígono con una cantidad de vértices mayor que 3 se puede dividir en dos polígonos que tenga cada uno de ellos menor cantidad de vértices. Esto se puede hacer mediante un segmento rectilíneo que tenga los extremos en los vértices del polígono y que cada punto del mismo, a excepción de los extremos, sea un punto interior del polígono.

2. La cantidad de números enteros positivos, no superiores a n, es igual a $[n]$. Cada uno de ellos se expresa de un modo único en la forma xk^m, donde k es un entero positivo; a cada x dado corresponden $\left[\sqrt[m]{\frac{n}{x}}\right]$ números de tal forma.

3. Demostremos que las condiciones indicadas son necesarias. El número de valores x que cumplen la condición $[\alpha x] \leqslant N$ se puede expresar en la forma $\frac{N}{\alpha}+\lambda$; $0 \leqslant \lambda < \frac{1}{\alpha}$, y el número de valores y que cumplen la condición $[\beta y] \leqslant N$ se puede expresar en la forma $\frac{N}{\beta}+\lambda_1$; $0 \leqslant \lambda_1 < \frac{1}{\beta}$. De la igualdad $\frac{N}{\alpha}+\lambda+\frac{N}{\beta}+\lambda_1=N$, dividiendo por N y pasando al límite para $N \to \infty$, obtenemos $\frac{1}{\alpha}+\frac{1}{\beta}=1$. Si α fuese racional, $\alpha=\frac{a}{b}$ $(a>b>0)$, de la última igualdad obtendríamos que $[\alpha b]=[\beta(a-b)]$. Por lo tanto, α y β no pueden ser racionales.

Supongamos que se cumplen las condiciones indicadas. Sea c un número natural. Sean $x_0=\frac{c}{\alpha}+\xi$ e $y_0=\frac{c}{\beta}+\eta$ los menores números enteros que cumplen las condiciones $x_0>\frac{c}{\alpha}$, $y_0>\frac{c}{\beta}$. Es obvio que $[\alpha x]$ no es igual a c si x no es igual a x_0, y $[\beta y]$ no es igual a c si y no es igual a y_0; además, $0<\xi<1$, $0<\eta<1$, $\alpha\xi$ y $\beta\eta$ son irracionales. Como $x_0+y_0=c+\xi+\eta$, se tiene $\xi+\eta=1$, $\frac{\alpha\xi}{\alpha}+\frac{\beta\eta}{\beta}=1$. Por lo tanto, uno y sólo uno de los números $[\alpha x_0]$ y $[\beta y_0]$ es igual a c.

4,a. Las diferencias mencionadas, para $\{\alpha x_t\}>0$ son iguales a

$$\{\alpha x_1\},\ \{\alpha(x_2-x_1)\},\ \ldots,\ \{\alpha(x_t-x_{t-1})\},\ \{-\alpha x_t\}.$$

Estas no son negativas, su suma es igual a 1, la cantidad de ellas es igual a $t+1$. Por lo tanto, al menos una de estas diferencias no es superior a $\frac{1}{t+1} < \frac{1}{\tau}$. Pero ésta tiene la forma $\{\alpha x'\} = \alpha x' - y'$, donde x' es un número entero que cumple la condición $0 < |x'| \leqslant \tau$ y $y' = \{\alpha x'\}$. Por consiguiente, designando con la letra h el número 1 ó -1, de modo que sea $hx' > 0$, se tiene $|\alpha hx' - hy'| < \frac{1}{\tau}$. De aquí, designando con las letras Q y P los cocientes que se obtienen al dividir hx' y hy' por (hx', hy'), resulta

$$|\alpha Q - P| < \frac{1}{\tau}; \quad 0 < Q \leqslant \tau,$$

de donde se deduce el teorema mencionado en la pregunta.

b. Haciendo $t_1 = [\tau_1]$, $t_2 = [\tau_2]$, ..., $t_k = [\tau_k]$ y suponiendo que x_1, x_2, ..., x_k recorren los valores

$$x_1 = 0, 1, \ldots, t_1; \quad x_2 = 0, 1, \ldots, t_2; \quad \ldots; \quad x_k = 0, 1, \ldots, t_k,$$

consideramos la sucesión formada por los números $\{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_k x_k\}$ y el número 1, dispuestos en orden no decreciente. Formando las diferencias de los números consecutivos de esta sucesión, se obtienen $(t_1+1)(t_2+1)\ldots(t_k+1)$ diferencias. Al menos una de éstas no es superior a

$$\frac{1}{(t_1+1)(t_2+1)\ldots(t_k+1)} < \frac{1}{\tau_1 \tau_2 \ldots \tau_k}.$$

Pero dicha diferencia tiene la forma $\{\alpha_1 x_1' + \alpha_2 x_2' + \ldots + \alpha_k x_k'\}$, donde $x_1', x_2', \ldots, x_k'$ son números enteros que cumplen las condiciones $|x_1'| \leqslant \tau_1$, $|x_2'| \leqslant \tau_2$, ..., $|x_k'| \leqslant \tau_k$, y no son simultáneamente iguales a cero. Haciendo $[\alpha_1 x_1' + \alpha_2 x_2' + \ldots + \alpha_k x_k'] = y'$ y designando con los símbolos $\xi_1, \xi_2, \ldots, \xi_k, \eta$ los cocientes que se obtienen al dividir $x_1', x_2', \ldots, x_k'$ y por $(x_1' x_2', \ldots, x_k', y')$, resulta

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

lo cual demuestra el teorema indicado en la pregunta.

5. Se tiene $\alpha = cq + r + \{\alpha\}$; $0 \leqslant r < c$,

$$\left[\frac{[\alpha]}{c}\right] = \left[q + \frac{r}{c}\right] = q, \quad \left[\frac{\alpha}{c}\right] = \left[q + \frac{r+\{a\}}{a}\right] = q.$$

6, a. Se tiene $[\alpha+\beta+\ldots+\lambda] = [\alpha]+[\beta]+\ldots+[\lambda]+[\{\alpha\}+\{\beta\}+\ldots+\{\lambda\}]$.

b. El número primo p figura en $n!$, $a!$, ..., $l!$ con los exponentes

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots,\ \left[\frac{a}{p}\right]+\left[\frac{a}{p^2}\right]+\ldots,\ \ldots,\ \left[\frac{l}{p}\right]+\left[\frac{l}{p^2}\right]+\ldots$$

Además

$$\left[\frac{n}{p^s}\right]\geqslant\left[\frac{a}{p^s}\right]+\ldots+\left[\frac{l}{p^s}\right].$$

7. Suponiendo que existe un número a con las propiedades indicadas, representémoslo en la forma

$$a=q_kp^{k+1}+q_{k-1}p^k+\ldots+q_1p^2+q_0p+q';$$
$$0<q_k<p,\ 0\leqslant q_{k-1}<p,\ \ldots,\ 0\leqslant q_1<p,\ 0\leqslant q_0<p,\ 0\leqslant q'<p.$$

Según **b**, § 1, tiene que ser

$$h=q_ku_k+q_{k-1}u_{k-1}+\ldots+q_1u_1+q_0u_0.$$

Por otra parte, para cualquier $s=1, 2, \ldots, m$, se tiene

$$q_{s-1}u_{s-1}+q_{s-2}u_{s-2}+\ldots+q_1u_1+q_0u_0<u_s.$$

Por lo tanto, la última expresión de h tiene que coincidir por completo con la señalada en la pregunta.

8, a. Sea x_1 un entero, $Q\leqslant\alpha<\beta\leqslant R$, $x_1<\alpha<\beta<x_1+1$. Integrando por partes, se obtiene

$$-\int_\alpha^\beta f(x)\,dx=\int_\alpha^\beta\rho'(x)f(x)\,dx=$$

$$=\rho(\beta)f(\beta)-\rho(\alpha)f(\alpha)-\sigma(\beta)f'(\beta)+\sigma(\alpha)f'(\alpha)+\int_\alpha^\beta\sigma(x)f''(x)\,dx.$$

En particular, para $Q\leqslant x_1$, $x_1+1\leqslant R$, pasando al límite se tiene

$$-\int_{x_1}^{x_1+1}f(x)\,dx=-\frac{1}{2}f(x_1+1)-\frac{1}{2}f(x_1)+\int_{x_1}^{x_1+1}\sigma(x)f''(x)\,dx.$$

La fórmula indicada se obtiene ahora sin dificultad.

b. Escribiendo la fórmula de la pregunta **a** en la forma

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

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

nos convencemos de que la fórmula indicada es justa.

c. Aplicando el resultado de la pregunta b, hallamos

$$\ln 1+\ln 2+\ldots+\ln n=$$

$$=C+n\ln n-n+\frac{1}{2}\ln n+\int_n^\infty \frac{\sigma(x)}{x^2}dx=n\ln n-n+O(\ln n).$$

9, a. α) Se tiene (b, § 1)

$$\ln([n]!)=\sum_{p\leqslant n}\left(\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots\right)\ln p. \qquad (1)$$

Aquí el segundo miembro representa la suma de los valores de la función $\ln p$, extendida a los puntos enteros (p, s, u) con valores primos p de la región $p>0$, $s>0$, $0<u\leqslant\frac{n}{p^s}$. La parte de la suma que corresponde a unos valores s y u dados, es igual a $\theta\left(\sqrt[s]{\frac{n}{u}}\right)$; la parte que corresponde a un valor dado u, es igual a $\psi\left(\frac{n}{u}\right)$.

β) Aplicando para $n\geqslant 2$ el resultado de la pregunta α), se tiene

$$\ln([n]!)-2\ln\left(\left[\frac{n}{2}\right]!\right)=$$

$$=\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\ldots\geqslant\psi(n)-\psi\left(\frac{n}{2}\right).$$

Haciendo $\left[\frac{n}{2}\right]=m$, de aquí hallamos que ($[n]=2m$, o $[n]=2m+1$)

$$\psi(n)-\psi\left(\frac{n}{2}\right)\leqslant\ln\frac{(2m+1)!}{(m!)^2}\leqslant$$

$$\leqslant\ln\left(2^m\frac{3\cdot 5\ldots,(2m+1)}{1\cdot 2\ldots m}\right)\leqslant\ln(2^m3^m)<n.$$

$$\psi(n)=\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{2}\right)-\psi\left(\frac{n}{4}\right)+$$

$$+\psi\left(\frac{n}{4}\right)-\psi\left(\frac{n}{8}\right)+\ldots<n+\frac{n}{2}+\frac{n}{4}+\ldots=2n.$$

γ) Se tiene (la solución de la pregunta β) y el resultado de la pregunta 8, c)

$$\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\ldots=\ln\frac{[n]!}{\left(\left[\frac{n}{2}\right]!\right)^2}=$$

$$=[n]\ln[n]-[n]-2\left[\frac{n}{2}\right]\ln\left[\frac{n}{2}\right]+2\left[\frac{n}{2}\right]+O(\ln n)=$$

$$=n\ln 2+O(\ln n).$$

Por otra parte, para $s \geqslant 2$ obtenemos (pregunta β))

$$\theta(\sqrt[s]{n}) - \theta\left(\sqrt[s]{\frac{n}{2}}\right) + \theta\left(\sqrt[s]{\frac{n}{3}}\right) - \ldots \begin{cases} < 2\sqrt[s]{n} \text{ siempre} \\ = 0 \text{ si } s > \tau;\ \tau = \left[\dfrac{\ln n}{\ln 2}\right]. \end{cases}$$

Por lo tanto

$$0 \leqslant \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + \ldots - \left(\theta(n) - \theta\left(\frac{n}{2}\right) + \theta\left(\frac{n}{3}\right) - \theta\left(\frac{n}{4}\right) + \ldots\right) <$$

$$< 2\sqrt{n} + 2\sqrt[3]{n} + 2\sqrt[4]{n} + \ldots + 2\sqrt[\tau]{n} < 2(\sqrt{n} + \tau\sqrt[3]{n}) = O(\sqrt{n}).$$

b. Se deduce de la igualdad (1), de la desigualdad de la pregunta a, β) y de la igualdad de la pregunta 8, c.

c. Para m suficientemente grande, de la igualdad de la pregunta b, se tiene

$$\sum_{m<p\leq m^2} \frac{\ln p}{p} = \ln m + O(1) \geqslant \frac{\ln m}{2}, \qquad \sum_{m<p\leq m^2} \frac{4}{p} > 1.$$

Si para todos los pares p_n, p_{n+1} que cumplen la condición $m < p_n < p_{n+1} \leqslant m^2$ se verificase la desigualdad $p_{n+1} > p_n(1+\varepsilon)$, resultaría

$$\sum_{r=0}^{\infty} \frac{4}{m(1+\varepsilon)^r} > 1.$$

lo cual es imposible para valores suficientemente grandes de m.

d. Evidentemente, es suficiente considerar solamente el caso en que n es entero.

Haciendo $\gamma(r) = \dfrac{\ln r}{r}$ si r es primo y $\gamma(r) = 0$ si $r = 1$ o si r es compuesto, se tiene (pregunta b)

$$\gamma(1) + \gamma(2) + \ldots + \gamma(r) = \ln r + \alpha(r); \quad |\alpha(r)| < C_1,$$

donde C_1 es una constante. De aquí, para $r > 1$

$$\gamma(r) = \ln r - \ln(r-1) + \alpha(r) - \alpha(r-1),$$

$$\sum_{0<p\leq n} \frac{1}{p} = T_1 + T_2; \quad T_1 = \sum_{1<r\leq n} \frac{\ln r - \ln(r-1)}{\ln r}$$

$$T_2 = \sum_{1<r\leq n} \frac{\alpha(r) - \alpha(r-1)}{\ln r}.$$

Se tiene (8, b)

$$T_1 = \sum_{1<r\leq n} \frac{1}{r \ln r} + \sum_{1<r\leq n} \left(\frac{1}{2r^2 \ln r} + \frac{1}{3r^3 \ln r} + \dots \right) =$$

$$= C_2 + \ln \ln n + O\left(\frac{1}{\ln n}\right),$$

donde C_2 es una constante. Luego hallamos

$$T_2 = \alpha(2)\left(\frac{1}{\ln 2} - \frac{1}{\ln 3}\right) + \dots$$

$$\dots + \alpha(n-1)\left(\frac{1}{\ln(n-1)} - \frac{1}{\ln n}\right) + \frac{\alpha(n)}{\ln n},$$

de donde se deduce que

$$T_2 = C_3 + O\left(\frac{1}{\ln n}\right),$$

donde C_3 es la suma de la serie absolutamente convergente

$$\alpha(2)\left(\frac{1}{\ln 2} - \frac{1}{\ln 3}\right) + \alpha(3)\left(\frac{1}{\ln 3} - \frac{1}{\ln 4}\right) + \dots$$

e. Se tiene

$$\ln \prod_{p\leq n} \left(1 - \frac{1}{p}\right) = -\sum_{p\leq n} \frac{1}{p} - \sum_{p\leq n} \left(\frac{1}{2p^2} + \frac{1}{3p^3} + \dots\right) =$$

$$= C' - \ln \ln n + O\left(\frac{1}{\ln n}\right),$$

donde C' es una constante. De aquí, haciendo $C' = \ln C_0$, obtenemos la igualdad indicada.

f. Haciendo $n = [1{,}5\, s \ln s]$ y representando con la notación $\pi(n)$ la cantidad de números primos que no son superiores a n, de la igualdad de la pregunta 9, a, γ) deducimos (C es una constante positiva)

$$\pi(n) > \frac{n \ln 2 - C\sqrt{n}}{\ln n},$$

lo cual es mayor que s, si s_0 se ha elegido suficientemente grande. De aquí se deduce que, si $s \geqslant s_0$, el número p_s está comprendido entre los números primos que no son superiores a n.

g. Sean $q_1, q_2, \dots, q_s$ los divisores primos distintos del número a. Hallamos: $2, 3, 4, \dots, (s+1) \leqslant a$, de donde (pregunta 8, c)

$$(s+1)\ln(s+1) + O(s+1) \leqslant a,\ s = 0(\ln a).$$

Por lo tanto (preguntas e y f)

$$\frac{a}{\varphi(a)} = \frac{1}{\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\ldots\left(1-\frac{1}{q_s}\right)} \leqslant$$

$$\leqslant \frac{1}{\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\ldots\left(1-\frac{1}{p_s}\right)} = O(\ln p_s) = O(\ln \ln a).$$

10, a. Se deduce de **c, § 2.**

b. Como $\theta(1) = \psi(1) = 1$, se cumple la condición **1, a, § 2** para la función $\theta(a)$. Sea $a = a_1 a_2$ una de las descomposiciones de a en dos factores, primos entre sí. Se tiene

$$\sum_{d_1 \setminus a_1} \sum_{d_2 \setminus a_2} \theta(d_1 d_2) = \psi(a) = \psi(a_1)\,\psi(a_2) = \sum_{d_1 \setminus a_1} \sum_{d_2 \setminus a_2} \theta(d_1)\,\theta(d_2). \quad (1)$$

Si se cumple la condición **2, a, § 2** para todos los productos menores que a, entonces, para $d_1 d_2 < a$ se tiene $\theta(d_1 d_2) = \theta(d_1)\,\theta(d_2)$, y según la igualdad (1) resulta $\theta(a_1 a_2) = \theta(a_1)\,\theta(a_2)$, es decir, también se cumple la condición **2, a, § 2** para todos los productos $a_1 a_2$ que son iguales a a. Mas la condición **2, a, § 2** se cumple para el único producto $1 \cdot 1$, igual a 1. Por consiguiente, ésta se cumple también para todos los productos.

11, a. Sea $m > 1$; para cada x_m dado que sea divisor de a, la ecuación indeterminada $x_1 \ldots x_{m-1} x_m = a$ admite $\tau_{m-1}\left(\frac{a}{x_m}\right)$ soluciones. Por esto,

$$\tau_m(a) = \sum_{x_m \setminus a} \tau_{m-1}\left(\frac{a}{x_m}\right),$$

pero cuando x_m recorre todos los divisores del número a, el número $d = \frac{a}{x_m}$ recorre en orden inverso los mismos divisores. Por consiguiente,

$$\tau_m(a) = \sum_{d \setminus a} \tau_{m-1}(a).$$

Por lo tanto (pregunta **10, a**), si el teorema subsiste para la función $\tau_{m-1}(a)$, entonces también subsiste para la función $\tau_m(a)$. Pero el teorema es válido para la función $\tau_1(a) = 1$. Esto significa que el teorema siempre es válido.

b. Si el teorema subsiste para la función $\tau_m(p^\alpha)$, se tiene

$$\tau_{m+1}(p^\alpha) = \sum_{s=0}^{\alpha} \tau_m(p^s) = \sum_{s=0}^{\alpha} \frac{(s+1)(s+2)\ldots(s+m-1)}{1 \cdot 2 \ldots (m-1)} =$$

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

Por consiguiente, el teorema subsiste también para la función $\tau_{m+1}(p^{\alpha})$. Pero el teorema es válido para la función $\tau_2(p^{\alpha})$ $\left(\text{evidentemente, igual a } \frac{\alpha+1}{1}\right)$. Por lo tanto, siempre es válido.

c. Supongamos que $\varepsilon = m\varepsilon_2$, $\varepsilon_2 = 2\eta$, y que $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ es la descomposición canónica del número a, donde $p_1, \dots, p_k$ están dispuestos en orden creciente. Para la función $\tau_2(a) = \tau(a)$ se tiene

$$\frac{\tau(a)}{a^{\eta}} \leqslant \frac{\alpha_1+1}{2^{\alpha_1\eta}} \frac{\alpha_2+1}{3^{\alpha_2\eta}} \dots \frac{\alpha_k+1}{(k+1)^{\alpha_k\eta}}.$$

Suponiendo, para simplificar los razonamientos, que $\varepsilon < 1$, nos convencemos de que cada uno de los factores que figuran en el segundo miembro es menor que $\frac{1}{\eta}$; los factores $\frac{\alpha_{r-1}+1}{r^{\alpha_{r-1}\eta}}$ que cumplen la condición $r > 2^{\frac{1}{\eta}}$ son menores que 1. Por lo tanto, haciendo $C = \left(\frac{1}{\eta}\right)^{2^{\frac{1}{\eta}}}$, hallamos

$$\frac{\tau(a)}{a^{\eta}} < C, \quad \lim_{a\to\infty} \frac{\tau(a)}{a^{\varepsilon_2}} \leqslant \lim_{a\to\infty} \frac{C}{a^{\eta}} = 0.$$

Si $m > 2$, evidentemente, se tiene $\tau_m(a) \leqslant (\tau(a))^m$. Por ello

$$\lim_{a\to\infty} \frac{\tau_m(a)}{a^{\varepsilon}} \leqslant \lim \left(\frac{\tau(a)}{a^{\varepsilon_2}}\right)^m = 0.$$

d. Los sistemas de valores $x_1, \dots, x_m$ que satisfacen a la desigualdad indicada los dividimos en $[n]$ clases con los números de orden 1, 2, ..., $[n]$. A la clase del número de orden a referimos los sistemas que cumplen la condición $x_1 \dots x_m = a$; la cantidad de sistema de éstos es igual a $\tau_m(a)$.

12. Si $R(s) > 1$, la serie que expresa $\zeta(s)$ es absolutamente convergente. Por lo tanto

$$(\zeta(s))^m = \sum_{n_1=1}^{\infty} \dots \sum_{n_m=1}^{\infty} \frac{1}{(n_1 \dots n_m)^s}.$$

Además, para un n positivo dado, la cantidad de sistemas $n_1, \dots, n_m$ que cumplen la condición $n_1 \dots n_m = n$, es igual a $\tau_m(n)$.

13, a. Si $R(s)>1$, el producto $P=\prod_p \frac{1}{1-\frac{1}{p^s}}$ es absolutamente convergente. Como $\frac{1}{1-\frac{1}{p^s}}=1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\ldots$, para $N>2$ se tiene

$$\prod_{p\leq N}\frac{1}{1-\frac{1}{p^s}}=\sum_{0<n\leq N}\frac{1}{n^s}+\sum{}'\frac{1}{n^s},$$

donde en la segunda suma del segundo miembro n recorre solamente los números que son superiores a N. Pasando al límite para $N\to\infty$, en el primer miembro resulta P, en la primera suma del segundo miembro resulta $\zeta(s)$, y en la segunda cero.

b. Sea $N>2$. Suponiendo que no hay números primos distintos de $p_1, \ldots, p_k$, obtenemos (compárese con la solución de la pregunta **a**)

$$\prod_{j=1}^{k}\frac{1}{1-\frac{1}{p_j}}\geqslant\sum_{0<n\leq N}\frac{1}{n}.$$

Como la serie armónica $1+\frac{1}{2}+\frac{1}{3}+\ldots$ es divergente, para N suficientemente grande, esta desigualdad es imposible.

c. Suponiendo que no hay números primos distintos de $p_1, \ldots, p_k$, obtenemos (pregunta **a**)

$$\prod_{j=1}^{k}\frac{1}{1-\frac{1}{p_j^2}}=\zeta(2).$$

Como el número $\zeta(2)=\frac{\pi^2}{6}$ es irracional, esta igualdad es imposible.

14. Si $R(s)>1$, el producto infinito para $\zeta(s)$ de la pregunta **13, a** es absolutamente convergente. Por lo tanto

$$\ln\zeta(s)=\sum_p\left(\frac{1}{p^s}+\frac{1}{2p^{2s}}+\frac{1}{3p^{3s}}+\ldots\right),$$

donde p recorre todos los números primos. Derivando, hallamos

$$\frac{\zeta'(s)}{\zeta(s)}=\sum_p\left(-\frac{\ln p}{p^s}-\frac{\ln p}{p^{2s}}-\frac{\ln p}{p^{3s}}-\ldots\right)=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

15. Sea $N > 2$. Aplicando el teorema **c**, § 3, se tiene

$$\prod_{p \leq N} \left(1 - \frac{1}{p^s}\right) = \sum_{0<n\leq N} \frac{\mu(n)}{n^s} + \sum{}' \frac{\mu(n)}{n^s},$$

donde en la segunda suma del segundo miembro n recorre solamente los números que son mayores que N. Pasando al límite para $N \to \infty$ se obtiene la identidad indicada.

16, a. Apliquemos **d**, § 3 al caso

$$\delta = 1, 2, \ldots, [n], \quad f = 1, 1, \ldots, 1.$$

Entonces, evidentemente, $S' = 1$. Por otra parte, S_d representa el número de valores δ que son múltiplos de d, es decir, es igual a $\left[\frac{n}{d}\right]$.

b. α) El segundo miembro de la igualdad de la pregunta **a** expresa la suma de los valores de la función $\mu(d)$, extentida a los puntos enteros (d, u) de la región $d > 0$, $0 < u \leqslant \frac{n}{d}$. La parte de esta suma que corresponde a un u dado, es igual a $M\left(\frac{n}{u}\right)$.

β) La igualdad indicada se obtiene restando término a término las igualdades

$$M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + M\left(\frac{n}{4}\right) + \ldots = 1,$$

$$2M\left(\frac{n}{2}\right) + \qquad 2M\left(\frac{n}{4}\right) + \ldots = 2.$$

c. Supongamos que $n_1 = [n]$; $\delta_1, \delta_2, \ldots, \delta_n$ se definen por la condición: δ_s es el mayor entero cuya t-ésima potencia es un divisor de s, $f_s = 1$. Entonces $S' = T_{t,n}$. S_d es igual a la cantidad de números, no superiores a n, que son múltiplos de d^t, o sea, $S_d = \left[\frac{n}{d^t}\right]$. De aquí resulta la expresión indicada para $T_{t,n}$.

En particular, como $\zeta(2) = \frac{\pi^2}{6}$, para la cantidad $T_{2,n}$ de números que no son superiores a n y que no son divisibles por el cuadrado de un entero, superior a 1, se tiene

$$T_{2,n} = \frac{6}{\pi^2} n + O(\sqrt{n}).$$

17, a. La igualdad indicada se obtiene de **d**, § 3, haciendo

$$\delta_s = (x_s, a), \quad f_s = f(x_s).$$

b. La igualdad indicada se obtiene de d, § 3, haciendo

$$\delta_s=(x_1^{(s)},\ \ldots,\ x_k^{(s)}),\quad f_s=f(x_1^{(s)},\ \ldots,\ x_k^{(s)}).$$

c. Aplicando d, § 3 al caso

$$\delta=\delta_1,\ \delta_2,\ \ldots,\ \delta_\tau,$$

$$f=F\left(\frac{a}{\delta_1}\right),\quad F\left(\frac{a}{\delta_2}\right),\ \ldots,\ F\left(\frac{a}{\delta_\tau}\right),$$

donde en la primera fila vienen escritos todos los divisores del número a, se tiene

$$S'=F(a),\quad S_d=\sum_{D\setminus\frac{a}{d}}F\left(\frac{a}{dD}\right)=G\left(\frac{a}{d}\right).$$

d. La igualdad indicada se deduce de

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

18, a. Apliquemos el teorema de la pregunta 17, a, suponiendo que x recorre los números 1, 2, ..., a y tomando $f(x)=x^m$. Entonces

$$S'=\psi_m(a),\quad S_d=d^m+2^m d^m+\ldots+\left(\frac{a}{d}\right)^m d^m=d^m\sigma_m\left(\frac{a}{d}\right).$$

b. Se tiene

$$\psi_1(a)=\sum_{d\setminus a}\mu(d)\left(\frac{a^2}{2d}+\frac{a}{2}\right)=\frac{a}{2}\varphi(a).$$

El mismo resultado se puede obtener más fácilmente. Escribamos los números de la sucesión 1, ..., a que son primos con a, primero en orden creciente y luego en orden decreciente. La suma de los términos de ambas sucesiones que equidistan del origen, es igual a a; la cantidad de términos de cada sucesión es igual a $\varphi(a)$.

c. Se tiene

$$\psi_2(a)=\sum_{d\setminus a}\mu(d)\left(\frac{a^3}{3d}+\frac{a^2}{2}+\frac{a}{6}d\right)=$$

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

19, a. Apliquemos el teorema de la pregunta 17, a, suponiendo que x recorre los números 1, 2, ..., $[z]$ y tomando $f(x)=1$. Entonces $S'=T_z$. S_d es igual a la cantidad de números, no superiores a z, que son múltiplos de d, o sea, $S_d=\left[\frac{z}{d}\right]$.

b. Se tiene

$$T_z = \sum_{d \setminus a} \mu(d) \frac{z}{d} + O(\tau(a)) = \frac{z}{a} \varphi(a) + O(a^\varepsilon).$$

c. Se deduce de la igualdad de la pregunta **a.**

20. Apliquemos el teorema de la pregunta **17, a,** suponiendo que x recorre los números $1, 2, \ldots, N$, donde $N > a$, y tomando $f(x) = \frac{1}{x^s}$. Entonces se obtiene

$$\sum_{x \leq N}{}' \frac{1}{x^s} = \sum_{d \setminus a} \mu(d) \sum_{0 < x \leq \frac{N}{d}} \frac{1}{d^s x^s} = \sum_{d \setminus a} \frac{\mu(d)}{d^s} \sum_{0 < x \leq \frac{N}{d}} \frac{1}{x^s}.$$

Pasando al límite para $N \to \infty$ se obtiene la identidad indicada.

21, a. Apliquemos el teorema de la pregunta **17, b,** considerando los sistemas de valores $x_1, x_2, \ldots, x_k$ indicados en la definición de probabilidad P_N y tomando $f(x_1, x_2, \ldots, x_k) = 1$. Entonces $P_N = \frac{S'}{N^k}$, $S_d = \left[\frac{N}{d}\right]^k$, y se tiene

$$P_N = \frac{\sum_{d=1}^{N} \mu(d) \left[\frac{N}{d}\right]^k}{N^k} = \sum_{d=1}^{N} \frac{\mu(d)}{d^k} + O\left(\sum_{d=1}^{N} \frac{1}{N d^{k-1}}\right).$$

Por lo tanto

$$P_N = (\zeta(k))^{-1} + O(\Delta); \quad \Delta = \frac{1}{N} \text{ si } k > 2,$$

$$\Delta = \frac{\ln N}{N} \text{ si } k = 2.$$

b. Se tiene $\zeta(2) = \frac{\pi^2}{6}$.

22, a. Razonamientos elementales muestran que la cantidad de puntos enteros (u, v) que hay en la región $u^2 + v^2 \leq \rho^2$; $\rho < 0$, es igual a $\pi\rho^2 + O(\rho)$. Apliquemos el teorema **17, b,** considerando las coordenadas x, y de los puntos enteros de la región $x^2 + y^2 \leq r^2$, distintos del punto $(0, 0)$, y haciendo $f(x, y) = 1$. Entonces $T = S' + 1$, S_d es igual a la cantidad de puntos enteros que hay en la región $u^2 + v^2 \leq$

$\leqslant \left(\frac{r}{d}\right)^2$, sin contar el punto (0, 0). Por lo tanto

$$S_d = \pi \frac{r^2}{d^2} + O\left(\frac{r}{d}\right),$$

$$T = \sum_{d=1}^{[r]} \mu(d)\, \pi \frac{r^2}{d^2} + O\left(\sum_{d=1}^{[r]} \frac{r}{d}\right) = \frac{6}{\pi} r^2 + O(r \ln r)$$

b. Razonando igual que anteriormente, se obtiene

$$T = \sum_{d=1}^{[r]} \mu(d)\, \frac{4}{3}\, \pi \frac{r^3}{d^3} + O\left(\sum_{d=1}^{[r]} \frac{r^2}{d^2}\right) = \frac{4\pi r^3}{3\zeta(3)} + O(r^2).$$

23, a. La cantidad de divisores d de un número $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, que no son divisibles por el cuadrado de un entero, superior a 1, y que tienen $\varkappa$ divisores primos, es igual a $\binom{k}{\varkappa}$; en este caso $\mu(d) = (-1)^{\varkappa}$. Por lo tanto

$$\sum_{d \setminus a} \mu(d) = \sum_{\varkappa=0}^{k} \binom{k}{\varkappa} (-1)^{\varkappa} = (1-1)^k = 0.$$

b. *Supongamos que a tiene la misma forma que en la pregunta a.* Es suficiente considerar el caso $m < k$. Para la suma indicada se tienen dos expresiones

$$\sum \mu(d) = \binom{k}{0} - \binom{k}{1} + \ldots + (-1)^m \binom{k}{m} =$$

$$= (-1)^m \left(\binom{k}{m+1} - \binom{k}{m+2} + \ldots \right).$$

Si m es par, entonces, para $m \leqslant \frac{k}{2}$ la primera expresión es >0, y para $m > \frac{k}{2}$ la segunda expresión es $\geqslant 0$. Si m es impar, entonces, para $m \leqslant \frac{k}{2}$ la primera expresión es <0, y para $m > \frac{k}{2}$ la segunda expresión es $\leqslant 0$.

c. La demostración es casi igual que en **d, §, 3**, pero teniendo en cuenta el resultado de la pregunta **b**.

d. La demostración es casi igual que en las preguntas **17, a** y **17, b**.

24. Supongamos que d recorre los divisores del número a. $\Omega(d)$ denota la cantidad de divisores primos del número d, $\Omega(a) = s$. De acuerdo

a la indicación hecha en la pregunta, se tiene (suponemos que N es suficientemente grande)

$$\pi(N, q, l) \leqslant \sum_{\Omega(d)\leqslant m} \mu(d)\left(\frac{N}{qd}+\theta_d\right) = T + T_0 - T_1; \quad |\theta_d| \leqslant 1.$$

$$|T| \leqslant \sum_{\Omega(d)\leqslant m} 1, \quad T_0 = \frac{N}{q}\sum_{d}\frac{\mu(d)}{d}, \quad |T_1| = \sum_{\Omega(d)>m}\frac{N}{qd}.$$

Luego hallamos

$$|T| \leqslant \sum_{n=0}^{m}\binom{s}{n} \leqslant s^m \leqslant e^{hm} < e^{5r^{1-\sigma}} \ln r \frac{qr}{N}\frac{N}{qr} = O(\Delta),$$

$$T_0 = \frac{N}{q}\frac{\prod_{p\leqslant e^h}\left(1-\frac{1}{p}\right)}{\prod_{p\mid q}\left(1-\frac{1}{p}\right)} = O(\Delta).$$

Finalmente, designando con las letras C_1 y C_2 unas constantes, se tiene

$$T_1 \leqslant \frac{N}{q}\sum_{n=m+1}^{s}\sum_{\Omega(d)=n}\frac{1}{d} \leqslant \frac{N}{q}\sum_{n=m+1}^{s}\frac{\left(\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p_s}\right)^n}{n!} \leqslant$$

$$\leqslant \frac{N}{q}\sum_{n=m+1}^{s}\left(\frac{C_1+\ln r}{4\ln r}e\right)^n \leqslant$$

$$\leqslant \frac{N}{q}\sum_{n=m+1}^{s}\left(\frac{3}{4}\right)^n < C_2\frac{N}{q}r^{-4\ln\frac{4}{3}} = O(\Delta).$$

25. A todo divisor d_1 del número a, que cumple la condición $d_1 < \sqrt{a}$, le corresponde un divisor d_2 que cumple las condiciones $d_2 > \sqrt{a}$, $d_1 d_2 = a$. Ahora bien, $\mu(d_1) = \mu(d_2)$. Por lo tanto,

$$2\sum_{d_1}\mu(d_1) = \sum_{d_1}\mu(d_1) + \sum_{d_2}\mu(d_2) = \sum_{d\mid a}\mu(d) = 0$$

26. Los números d que no son divisibles por el cuadrado de un entero, superior a 1, y que satisfacen a la condición $\varphi(d) = k$, los consideramos

a pares, de modo que en cada par figure un impar d_1 y un par $2d_1$. Se tiene $\mu(d_1)+\mu(2d_1)=0$.

27. Sean $p_1, \ldots, p_k$ distintos números primos. Haciendo $a=p_1 \ldots p_k$, se tiene

$$\varphi(a)=(p_1-1)\ldots(p_k-1).$$

Sin embargo, si no hubiese números primos, distintos de $p_1, \ldots, p_k$, se tendría $\varphi(a)=1$.

28, a. Los números indicados se hallan entre los números $s\delta$; $s=1, 2, \ldots, \frac{a}{\delta}$. Pero $(s\delta, a)=\delta$ cuando, y sólo cuando, $\left(s, \frac{a}{\delta}\right)=1$ (c, § 2, cap. I). Por lo tanto, es justa la afirmación señalada en la pregunta, y se tiene

$$a=\sum_{\delta \backslash a} \varphi\left(\frac{a}{\delta}\right)=\sum_{d \backslash a} \varphi(d).$$

b, α) Sea $a=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ la descomposición canónica del número a. En virtud de **a**, la función $\varphi(a)$ es multiplicativa, y se tiene

$$p_s^{\alpha_s}=\sum_{d \backslash p_s^{\alpha_s}} \varphi(d), \quad p_s^{\alpha_s-1}=\sum_{d \backslash p_s^{\alpha_s-1}} \varphi(d), \quad p_s^{\alpha_s}-p_s^{\alpha_s-1}=\varphi(p_s^{\alpha_s}).$$

β) Para un entero $m>0$ se tiene

$$m=\sum_{d \backslash m} \varphi(d).$$

Por lo tanto

$$\varphi(a)=\sum_{d \backslash a} \mu(d)\frac{a}{d}.$$

29. Se tiene (p recorre todos los números primos)

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}=\prod_p\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\ldots\right)=$$

$$=\prod_p \frac{1-\frac{1}{p^s}}{1-\frac{1}{p^{s-1}}}=\frac{\zeta(s-1)}{\zeta(s)}.$$

30. Se tiene

$$\varphi(1)+\varphi(2)+\ldots+\varphi(n)=$$

$$=\sum_{d\backslash 1}\frac{\mu(d)}{d}+2\sum_{d\backslash 2}\frac{\mu(d)}{d}+\ldots+n\sum_{d\backslash n}\frac{\mu(d)}{d}=$$

$$=\sum_{d=1}^{n}\mu(d)\left(1+2+\ldots+\left[\frac{n}{d}\right]\right)=\sum_{d=1}^{n}\mu(d)\frac{n^2}{2d^2}+O(n\ln n)=$$

$$=\frac{n^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(n\ln n)=\frac{3}{\pi^2}n^2+O(n\ln n).$$

Respuestas a las preguntas del capítulo III

1, a. De

$$P=a_n10^{n-1}+a_{n-1}10^{n-2}+\ldots+a_1,$$

observando que $10\equiv 1$ (mód. 9), se tiene

$$P\equiv a_n+a_{n-1}+\ldots+a_1 \text{ (mód. 9)}.$$

Por consiguiente, P es un múltiplo de 3 cuando, y sólo cuando, la suma de las cifras que le representan es un múltiplo de 3; P es un múltiplo de 9 cuando, y sólo cuando, la suma indicada es un múltiplo de 9. Observando que $10\equiv -1$ (mód. 11), se tiene

$$P\equiv (a_1+a_3+\ldots)-(a_2+a_4+\ldots) \text{ (mód. 11)}.$$

Por lo tanto, P es un múltiplo de 11 cuando, y sólo cuando, la diferencia entre la suma de las cifras que ocupan lugares impares (contando desde la derecha) y la suma de las cifras que ocupan lugares pares, es un múltiplo de 11.

b. De

$$P=b_n100^{n-1}+b_{n-1}100^{n-2}+\ldots+b_1$$

debido a que $100\equiv -1$ (mód. 101), se tiene

$$P\equiv (b_1+b_3+\ldots)-(b_2+b_4+\ldots) \text{ (mód. 101)}.$$

Por consiguiente, P es un múltiplo de 101 cuando, y sólo cuando, $(b_1+b_3+\ldots)-(b_2+b_4+\ldots)$ es un múltiplo de 101.

c. De

$$P=c_n1\,000^{n-1}+c_{n-1}1\,000^{n-2}+\ldots+c_1$$

debido a que $1\,000\equiv 1$ (mód. 37), se tiene

$$P\equiv c_n+c_{n-1}+\ldots+c_1 \text{ (mód. 37)}.$$

Por lo tanto, P es un múltiplo de 37 cuando, y sólo cuando, $c_n+c_{n-1}+\ldots+c_1$ es un múltiplo de 37.

Como $1\,000 \equiv -1 \pmod{7 \cdot 11 \cdot 13}$, se tiene

$$P \equiv (c_1 + c_3 + \ldots) - (c_2 + c_4 + \ldots) \pmod{7 \cdot 11 \cdot 13}.$$

Por ello, P es un múltiplo de uno de los números 7, 11, 13 cuando, y sólo cuando, $(c_1 + c_3 + \ldots) - (c_2 + c_4 + \ldots)$ es un múltiplo *de este mismo número.*

2, α) Cuando x recorre el sistema completo de restos respecto del módulo m, $ax + b$ también recorre el sistema completo; el resto mínimo no negativo r del número $ax + b$ recorre los valores $0, 1, \ldots, m-1$ *De aquí que*

$$\sum_{x} \left\{ \frac{ax+b}{m} \right\} = \sum_{r=0}^{m-1} \frac{r}{m} = \frac{1}{2}(m-1).$$

β) Aplicando el resultado de la pregunta 18, b, cap. II, se obtiene

$$\sum_{\xi} \left\{ \frac{a\xi}{m} \right\} = \frac{\psi_1(m)}{m} = \frac{1}{2}\varphi(m).$$

3, a. Sea r el resto mínimo no negativo del número $ax + [c]$ respecto del módulo m. Se tiene

$$S = \sum_{r=0}^{m-1} \left\{ \frac{r+\Phi(r)}{m} \right\},$$

donde $\varepsilon \leqslant \Phi(r) \leqslant \varepsilon + h$; $\varepsilon = \{c\}$. Si $m \leqslant 2h+1$ el teorema es evidente. Por lo tanto, consideraremos sólo el caso en que $m > 2h+1$. Haciendo

$$\left\{ \frac{r+\Phi(r)}{m} \right\} - \frac{r}{m} = \delta(r),$$

se tiene $-1 + \frac{\varepsilon}{m} \leqslant \delta(r) \leqslant \frac{h+\varepsilon}{m}$ si $r = m - [h+\varepsilon], \ldots, m-1$; $\frac{\varepsilon}{m} \leqslant \delta(r) \leqslant \frac{h+\varepsilon}{m}$ en todos los demás casos. De aquí resulta que

$$-[h+\varepsilon] + \varepsilon \leqslant S - \frac{m-1}{2} \leqslant h + \varepsilon, \quad \left| S - \frac{1}{2}m \right| \leqslant h + \frac{1}{2}.$$

b. Se tiene

$$S = \sum_{z=0}^{m-1} \left\{ \frac{az + \psi(z)}{m} \right\};$$

$$\psi(z) = m(AM + B) + \frac{\lambda}{m} z.$$

Apliquemos el teorema de la pregunta **a**, haciendo $h=|\lambda|$. Entonces se obtiene el resultado señalado.

c. Se halla

$$\sum_{z=0}^{m-1}\left\{f(M)+\frac{az}{m}+\frac{\theta z}{m^2}+\frac{f''(M+z_0)}{2}z^2\right\};$$

$$0<z_0<m-1.$$

Aplicamos el teorema de la pregunta **a**, haciendo $h=1+\frac{k}{2}$. Entonces se obtiene el resultado indicado.

4. Desarrollemos A en fracción continua. Sea $Q_n = Q'$ el mayor de los denominadores de las fracciones reducidas, que no es superior a m. Se tiene (pregunta **4**, **b**, cap. **I**)

$$A=\frac{P'}{Q'}+\frac{\theta'}{Q'm}, \quad (P', Q')=1, \quad |\theta'|<1.$$

De las desigualdades $m < Q_{n+1} \leqslant (q_{n+1}+1)\,Q_n \leqslant CQ_n$, donde C es una constante, a la cual no superan todos los números q_s+1, para el mayor entero H' que cumple la condición $H'Q' \leqslant m$ se deduce que $H' < C$. Aplicando el teorema de la pregunta **3**, **b**, se obtiene

$$\left|\sum_{x=M}^{M+H'Q'-1}\{Ax+B\}-\frac{1}{2}H'Q'\right|\leqslant\frac{3}{2}C.$$

Sea $m_1 = m - H'Q'$. Si $m_1 > 0$, entonces, eligiendo los números Q'' y H'' en dependencia de m_1, del mismo modo que se eligieron antes los números Q' y H' en dependencia de m, se obtiene

$$\left|\sum_{x=M_1}^{M_1+H''Q''-1}\{Ax+B\}-\frac{1}{2}H''Q''\right|\leqslant\frac{3}{2}C,$$

donde aplicamos la notación $M_s = M_{s-1}+H^{(s)}Q^{(s)}$. Sea $m_2 = m_1 - H''Q''$. Si $m_2 > 0$, entonces, de un modo semejante a lo anterior, se halla

$$\left|\sum_{x=M_2}^{M_2+H''Q''-1}\{Ax+B\}-\frac{1}{2}H''Q''\right|<\frac{3}{2}C$$

etc., hasta que se llegue a un $m_k = 0$. Entonces se obtiene ($H'Q'+H''Q''+\ldots+H^{(k)}Q^{(k)}=m$)

$$\left|\sum_{x=M}^{M+m-1}\{Ax+B\}-\frac{1}{2}m\right|<\frac{3}{2}Ck.$$

Los números Q', Q'', . . ., $Q^{(k)}$ satisfacen a las condiciones

$$m \geqslant Q' > m_1 \geqslant Q'' > m_2 \geqslant \ldots > m_{k-1} \geqslant Q^{(k)} \geqslant 1.$$

De aquí que (pregunta 3, cap. I) $k = O(\ln m)$ y, por consiguiente, la fórmula indicada en la pregunta es cierta.

5, a. Designemos con S la suma que figura en el primer miembro. Sea $\tau = A^{\frac{1}{3}}$. Para $\tau \leqslant 40$ el teorema es evidente. Por lo tanto, suponemos que $\tau > 40$. Tomando $M_1 = [Q + 1]$, hallamos unos números a_1, m_1, θ_1 que cumplan las condiciones

$$f'(M_1) = \frac{a_1}{m_1} + \frac{\theta_1}{m_1\tau}; \quad 0 < m_1 \leqslant \tau, \quad (a_1, m_1) = 1, \quad |\theta_1| < 1.$$

Tomando $M_2 = M_1 + m_1$, del mismo modo hallamos los números a_2, m_2, θ_2; tomando $M_3 = M_2 + m_2$, hallamos los números a_3, m_3, θ_3; continuamos así hasta que se llegue a $M_{s+1} = M_s + m_s$ con la condición $0 \leqslant [R] - M_{s+1} < [\tau]$. Aplicando el teorema de la pregunta 3, c, se obtiene

$$\left|S - \frac{1}{2}(m_1 + m_2 + \ldots + m_s + [R] + 1 - M_{s+1})\right| <$$

$$< s\frac{k+3}{2} + \frac{1}{2}([R] + 1 - M_{s+1}),$$

$$\left|S - \frac{1}{2}(R - Q)\right| < s\frac{k+3}{2} + \frac{\tau+1}{2}.$$

La longitud del intervalo, para el cual

$$\frac{a}{m} - \frac{1}{m\tau} \leqslant f'(x) \geqslant \frac{a}{m} + \frac{1}{m\tau},$$

no es superior a $\frac{2A}{m\tau}$. Por consiguiente, con una misma fracción $\frac{a}{m}$ están ligados $\leqslant \frac{2A}{m^2\tau} + 1$ números $m_1, m_2, \ldots, m_s$. Sean a_1 y a_2 el valor mínimo y máximo de a que corresponden a un m dado.

Se tiene

$$\frac{a_2 - a_1}{m} - \frac{2}{m\tau} \leqslant \frac{k(R-Q)}{A}; \quad a_2 - a_1 + 1 \leqslant \frac{k(R-Q)m}{A} + 1{,}05.$$

Por consiguiente, con el m dado están ligados

$$< \left(\frac{2A}{m^2\tau} + 1\right)\left(\frac{k(R-Q)m}{A} + 1{,}05\right) =$$

$$= \frac{k(R-Q)}{\tau}\left(\frac{2}{m} + \frac{m}{\tau^2}\right)\left(\frac{2A}{m^2\tau} + 1\right) 1{,}05$$

números $m_1, m_2, \ldots, m_s$. Sumando la última expresión respecto de todos los $m=1, 2, \ldots, [\tau]$, se obtiene

$$s<\frac{k(R-Q)}{\tau}\left(2\ln\tau+2+\frac{\tau^2+\tau}{2\tau^2}+\frac{10A}{3\tau}\right)1{,}05<$$

$$<\frac{k(R-Q)}{\tau}\ln A+\frac{7}{2}\frac{A}{\tau},$$

$$\left|S-\frac{1}{2}(R-Q)\right|<2\frac{k^2(R-Q)}{\tau}\ln A+8k\frac{A}{\tau}.$$

b. Se tiene

$$\left|\sum_{Q<x\leq R}\{f(x)+1-\sigma\}-\frac{1}{2}(R-Q)\right|<\Delta,$$

$$\left|\sum_{Q<x\leq R}\{f(x)\}-\frac{1}{2}(R-Q)\right|<\Delta,$$

de donde, haciendo $\delta(x)=\{f(x)+1-\sigma\}-\{f(x)\}$, hallamos

$$\left|\sum_{Q<x\leq R}\delta(x)\right|<2\Delta.$$

Mas, si $\{f(x)\}<\sigma$ se tiene $\delta(x)=1-\sigma$, y si $\{f(x)\}\geqslant\sigma$ se tiene $\delta(x)=-\sigma$. Por lo tanto, $|(1-\sigma)\psi(\sigma)-\sigma(R-Q-\psi(\sigma))|<2\Delta$, de donde se obtiene la fórmula indicada.

6, a. Apliquemos la fórmula de la pregunta **1, c**, cap. **II**. Haciendo $f(x)=\sqrt{r^2-x^2}$, en el intervalo $0\leqslant x\leqslant\frac{r}{\sqrt{2}}$ se tiene

$$f'(x)=-\frac{x}{\sqrt{r^2-x^2}},\quad f''(x)=\frac{-r^2}{(r^2-x^2)^{\frac{3}{2}}},\quad \frac{1}{r}\leqslant|f''(x)|\leqslant\frac{\sqrt{8}}{r},$$

Por lo tanto (pregunta **8, a**, cap. **II**, pregunta **5, a**)

$$T=4r+8\int_0^{\frac{r}{\sqrt{2}}}\sqrt{r^2-x^2}\,dx+8\rho\left(\frac{r}{\sqrt{2}}\right)\frac{r}{\sqrt{2}}-8\rho(0)\cdot r-4\frac{r}{\sqrt{2}}-$$

$$-4\frac{r^2}{2}+8\frac{r}{\sqrt{2}}\left\{\frac{r}{2}\right\}+O(r^{\frac{2}{3}}\ln r)=\pi r^2+O(r^{\frac{2}{3}}\ln r).$$

b. Se tiene (preguntas **11, d** y **1, d**, cap. **II**)

$$\tau(1)+\tau(2)+\ldots+\tau(n)=2\sum_{0<x\leq\sqrt{n}}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

Es suficiente considerar solamente el caso $n > 64$. Dividamos el intervalo $X < x \leqslant \sqrt{n}$, donde $X = 2n^{\frac{1}{3}}$, en $O(\ln n)$ intervalos de la forma $M < x \leqslant M'$, donde $M' \leqslant 2M$. Haciendo $f(x) = \frac{n}{x}$, en el intervalo $M < x \leqslant M'$ se tiene

$$f'(x) = -\frac{n}{x^2}, \quad f''(x) = \frac{2n}{x^3};$$

$$\frac{n}{4M^3} \leqslant f''(x) \leqslant \frac{8n}{4M^3}.$$

De aquí que (pregunta 5, a)

$$\sum_{M<x\leqslant M'} \left\{\frac{n}{x}\right\} = \frac{1}{2}(M'-M) + O\left(n^{\frac{1}{3}} \ln n\right),$$

$$\sum_{0<x\leqslant \sqrt{n}} \left\{\frac{n}{x}\right\} = \frac{1}{2}\sqrt{n} + O\left(n^{\frac{1}{3}} (\ln n)^2\right).$$

Por otra parte (pregunta 8, b, cap. II)

$$\sum_{0<x\leqslant \sqrt{n}} \frac{n}{x} = En + \frac{1}{2} n \ln n + \rho(\sqrt{n})\sqrt{n} + O(1).$$

Por lo tanto

$$\tau(1) + \tau(2) + \ldots + \tau(n) = 2En + n \ln n + 2\rho(\sqrt{n})\sqrt{n} -$$

$$-\sqrt{n} - n + 2\sqrt{n}\{\sqrt{n}\} + O\left(n^{\frac{1}{3}} (\ln n)^2\right) = n(\ln n + 2E - 1) +$$

$$+ O\left(n^{\frac{1}{3}} (\ln n)^2\right).$$

7. Supongamos que el sistema es irregular y sea s el mayor número entero que cumple la condición de que 2^s figura en una cantidad impar de números del sistema. Uno de estos últimos números lo sustituimos por otro menor, que contenga solamente aquellas potencias 2^s que figuran en una cantidad impar de números del sistema restante. Supongamos que el sistema es regular. Un número, que sea menor que alguno de los números T de este sistema, se diferencia de T al menos en una cifra en el sistema de numeración de base 2.

8, a. Agregando el número $H = 3^n + 3^{n-1} + \ldots + 3 + 1$ a cada uno de los números, representados del modo indicado, se obtienen

los números que se pueden obtener si en la misma forma x_n, x_{n-1} . . . . . , x_1, x_0 recorren los valores 0, 1, 2, o sea, se obtienen todos los números 0, 1, . . . , $2H$.

b. Del modo indicado se obtienen $m_1 m_2 \ldots m_k$ números que no son congruentes entre sí respecto del módulo $m_1 m_2 \ldots m_k$, puesto que de

$$x_1 + m_1 x_2 + m_1 m_2 x_3 + \ldots + m_1 m_2 \ldots m_{k-1} x_k \equiv$$
$$\equiv x_1' + m_1 x_2' + m_1 m_2 x_3' + \ldots + m_1 m_2 \ldots m_{k-1} x_k' \text{ (mód. } m_1 m_2 \ldots m_k)$$

se halla sucesivamente

$$x_1 \equiv x_1' \text{ (mód. } m_1), \quad x_1 = x_1'; \quad m_1 x_2 \equiv m_1 x_2' \text{ (mód. } m_1 m_2), \quad x_2 = x_2';$$
$$m_1 m_2 x_3 \equiv m_1 m_2 x_3' \text{ (mód. } m_1 m_2 m_3), \quad x_3 = x_3',$$

etc.

9, a. Del modo indicado se obtienen $m_1 m_2 \ldots m_k$ números que no son congruentes respecto del módulo $m_1 m_2 \ldots m_k$, puesto que de

$$M_1 x_1 + M_2 x_2 + \ldots + M_k x_k \equiv$$
$$\equiv M_1 x_1' + M_2 x_2' + \ldots + M_k x_k' \text{ (mód. } m_1 m_2 \ldots m_k)$$

resultaría que (todo M_j, distinto de M_s, es un múltiplo de m_s)

$$M_s x_s \equiv M_s x_s' \text{ (mód. } m_s), \quad x_s \equiv x_s' \text{ (mód. } m_s), \quad x_s = x_s'.$$

b. Del modo indicado se obtienen $\varphi(m_1)\,\varphi(m_2) \ldots \varphi(m_k) = \varphi(m_1 m_2 \ldots m_k)$ números, los cuales, en virtud del teorema de la pregunta **a**, no son congruentes respecto del módulo $m_1 m_2 \ldots m_k$, y como $(M_1 x_1 + M_2 x_2 + \ldots + M_k x_k, \ m_s) = (M_s x_s, \ m_s) = 1$, son primos con $m_1 m_2 \ldots m_k$.

c. Según el teorema de la pregunta **a**, el número $M_1 x_1 + M_2 x_2 + \ldots + M_k x_k$, donde $x_1, x_2, \ldots, x_k$ reccorren los sistemas completos de restos respecto de los módulos $m_1, m_2, \ldots, m_k$, recorre el sistema completo de restos respecto del módulo $m_1 m_2 \ldots m_k$. Este número es primo con $m_1 m_2 \ldots m_k$ cuando, y sólo cuando, $(x_1, m_1) = (x_2, m_2) = \ldots = (x_k, m_k) = 1$. De aquí que $\varphi(m_1 m_2 \ldots m_k) = \varphi(m_1)\,\varphi(m_2) \ldots \varphi(m_k)$.

d. Para obtener todos los números de la sucesión 1, 2, . . . p^α que son primos con p^α, se deben borrar los números de esta sucesión que son múltiplos de p, es decir, los números p, $2p$, . . . , $p^{\alpha-1}p$. Por lo tanto, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. De aquí y del teorema **c**, § 4, cap. II se deduce inmediatamente la expresión para $\varphi(\alpha)$.

10, a. La primera afirmación se deduce de

$$\left\{\frac{x_1}{m_1} + \ldots + \frac{x_k}{m_k}\right\} = \left\{\frac{M_1 x_1 + \ldots + M_k x_k}{m}\right\};$$

la segunda se deduce de

$$\left\{\frac{\xi_1}{m_1}+\ldots+\frac{\xi_k}{m_k}\right\}=\left\{\frac{M_1\xi_1+\ldots+M_k\xi_k}{m}\right\}.$$

b. 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

$$\left\{\frac{f_1(M_1x_1+\ldots+M_kx_k,\ \ldots,\ M_1w_1+\ldots+M_kw_k}{m_1}+\ldots\right.$$
$$\left.\ldots+\frac{f_k(M_1x_1+\ldots+M_kx_k,\ \ldots,\ M_1w_1+\ldots+M_kw_k)}{m_k}\right\},$$

o sea, con las fracciones $\left\{\frac{f_1(x,\ \ldots,\ w)}{m_1}+\ldots+\frac{f_k(x,\ \ldots,\ w)}{m_k}\right\}$. De aquí se obtiene fácilmente la primera afirmación. La segunda se demuestra de un modo análogo.

11, a. Si a es un múltiplo de m, se tiene

$$\sum e^{2\pi i\frac{ax}{m}}=\sum_x 1=m.$$

Si a no es divisible por m, se tiene

$$\sum_x e^{2\pi i\frac{ax}{m}}=\frac{e^{2\pi i\frac{am}{m}}-1}{e^{2\pi i\frac{a}{m}}-1}=0.$$

b. Para α no entero, el primer miembro es igual a

$$\left|\frac{e^{2\pi i\alpha(M+P)}-e^{2\pi i\alpha M}}{e^{2\pi i\alpha}-1}\right|\leqslant\frac{1}{\operatorname{sen}\pi(\alpha)}\leqslant\frac{1}{h(\alpha)}$$

c. Según el teorema de la pregunta b, el primer miembro no es superior a T_m, donde

$$T_m=\sum_{a=1}^{m-1}\frac{1}{h\left(\frac{a}{m}\right)}.$$

Pero si m es impar

$$T_m<m\sum_{0<a<\frac{m}{2}}\ln\frac{2a+1}{2a-1}=m\ln m.$$

y si m es par

$$T_m < \frac{m}{2} \sum_{0<a\leq \frac{m}{2}} \ln \frac{2a+1}{2a-1} + \frac{m}{2} \sum_{0<a<\frac{m}{2}} \ln \frac{2a+1}{2a-1} < m \ln m.$$

Como $\frac{1}{2}-\frac{1}{3}=\frac{1}{6}$, para $m \geqslant 6$ la cota $m \ln m$ se puede disminuir en

$$2\frac{m}{6} \sum_{0<a\leq \frac{m}{6}} \ln \frac{2a+1}{2a-1} = \frac{m}{3} \ln \left(2\left[\frac{m}{6}\right]+1\right).$$

La última expresión es $> \frac{m}{2}$ si $m \geqslant 12$ y es $> m$ si $m \geqslant 60$.

12, a. Supongamos que $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ es la descomposición canónica del número m. Haciendo $p_1^{\alpha_1} = m_1, \ldots, p_k^{\alpha_k} = m_k$, y conservando las notaciones de la pregunta 10, a, se tiene

$$\sum_{\xi_1} e^{2\pi i \frac{\xi_1}{m_1}} \ldots \sum_{\xi_k} e^{2\pi i \frac{\xi_k}{m_k}} = \sum_{\xi} e^{2\pi i \frac{\xi}{m}}.$$

Pero, si $\alpha_s = 1$, se obtiene

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - 1 = -1.$$

Si $\alpha_s > 1$, haciendo $m_s = p_s m'_s$, se obtiene

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - \sum_{u=0}^{m'_s-1} e^{2\pi i \frac{u}{m'_s}} = 0.$$

b. Sea m entero, $m > 1$. Se tiene $\sum_{x=0}^{m-1} e^{2\pi i \frac{x}{m}} = 0$. La suma de los términos del primer miembro de esta igualdad que cumplen la condición $(x, m) = d$, es igual a $\mu\left(\frac{m}{d}\right)$, en virtud del teorema de la pregunta **a.**

c. Obtenemos

$$\sum_{\xi} e^{2\pi i \frac{\xi}{m}} = \sum_{d \mid m} \mu(d) S_d,$$

donde, haciendo $m = m_0 d$, se tiene

$$S_d = \sum_{u=0}^{m_0-1} e^{2\pi i \frac{u}{m_0}}.$$

Esta suma es igual a 0 si $d < m$ e igual a 1 si $d = m$. De aquí resulta el teorema de la pregunta **a**.

d. Las igualdades se deducen de la pregunta 10, b.

e. Se tiene

$$A(m_1)\dots A(m_k) = m^{-r} \sum_{a_1} \dots \sum_{a_k} S_{a_1, m_1} \cdots S_{a_k, m_k},$$

donde $a_1, \dots, a_k$ recorren los sistemas reducidos de restos respecto de los módulos $m_1, \dots, m_k$. De aquí (pregunta d) se deduce inmediatamente la primera igualdad de la pregunta. La segunda igualdad se demuestra de un modo análogo.

13, a. Se tiene

$$\sum_{x=0}^{p-1} e^{2\pi i \frac{nx}{p}} = \begin{cases} p, \text{ si } n \text{ es múltiplo de } p, \\ 0 \text{ en caso contrario.} \end{cases}$$

b. Desarrollando el producto que corresponde a un n dado resulta

$$\sum_{d \setminus a} \frac{\mu(d)}{d} \sum_{x=0}^{d-1} e^{2\pi i \frac{nx}{d}}.$$

De aquí, sumando respecto de todos los $n = 0, 1, \dots, a-1$, se obtiene la expresión conocida para $\varphi(a)$.

14. La parte de la expresión del segundo miembro que corresponde a un valor de x que es divisor de a, es igual a 1; la parte que corresponde a un valor de x que no es divisor de a, es igual a 0. De aquí que la expresión en cuestión es igual al doble del número de divisores de a, menores que $\sqrt{a}$, más 0, es decir, es igual a $\tau(a)$.

15, a. Se tiene

$$(h_1 + h_2)^p =$$

$$= h_1^p + \binom{p}{1} h_1^{p-1} h_2 + \dots + \binom{p}{p-1} h_1 h_2^{p-1} + h_2^p \equiv h_1^p + h_2^p \text{ (mód. } p);$$

$$(h_1 + h_2 + h_3)^p \equiv (h_1 + h_2)^p + h_3^p \equiv h_1^p + h_2^p + h_3^p \text{ (mód. } p), \text{ etc.}$$

b. Haciendo $h_1 = h_2 = \dots = h_a = 1$, del teorema de la pregunta **a** se obtiene el teorema de Fermat.

c. Sea $(a, p) = 1$. Para ciertos enteros $N_1, N_2, \dots, N\alpha$, se tiene

$$a^{(p-1)} = 1 + N_1 p, \quad a^{p(p-1)} = (1 + N_1 p)^p = 1 + N_2 p^2,$$

$$a^{p^2(p-1)} = 1 + N_3 p^3, \dots, a^{p^{\alpha-1}(p-1)} = 1 + N_\alpha p^\alpha,$$

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

Sea $m=p_{p_1}^{\alpha_1}\dots p_k^{\alpha_k}$ la descomposición canónica del número m. Se tiene

$$a^{\varphi(p_1^{\alpha_1})}\equiv 1\ (\text{mód. } p_1^{\alpha_1}),\ \dots,\ a^{\varphi(p_k^{\alpha_k})}\equiv 1(\text{mód. } p_k^{\alpha_k})$$
$$a^{\varphi(m)}\equiv 1\ (\text{mód. } p_1^{\alpha_1}),\ \dots,\ a^{\varphi(m)}\equiv 1\ (\text{mód. } p_k^{\alpha_k}),$$
$$a^{\varphi(m)}\equiv 1\ (\text{mód. } m).$$

Respuestas a las preguntas del capítulo IV

1, a. El teorema se deduce inmediatamente del teorema de la pregunta 11, a, cap. III.

b. Sea d un divisor del número m, $m=m_0d$, H_d denota la suma de los términos que cumplen la condición $(a, m)=d$ en la expresión para Tm de la pregunta a. Se obtiene

$$H_d=\sum_{a_0}\sum_{x=0}^{m-1}\dots\sum_{w=0}^{m-1}e^{2\pi i\frac{a_0f(x,\dots,w)}{m_0}},$$

donde a_0 recorre el sistema reducido de restos respecto del módulo m_0. De aquí se deduce que

$$H_d=d^r\sum_{a_0}\sum_{x_0=0}^{m_0-1}\dots\sum_{w_0=0}^{m_0-1}e^{2\pi i\frac{a_0f(x_0\dots w_0)}{m_0}}=m^rA(m_0).$$

c. Supongamos que $m>0$, $(a, m)=d$, $a=a_0d$, $m=m_0d$, T es la cantidad de soluciones de la congruencia $ax\equiv b$ (mód. m). Se tiene

$$T_m=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi i\frac{\alpha(ax-b)}{m}}=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi i\frac{\alpha a_0}{m_0}x-2\pi i\frac{b\alpha}{m}}=$$
$$=m\sum_{\alpha_1=0}^{d-1}e^{-2\pi i\frac{b\alpha_1}{d}}=\begin{cases}md, \text{ si } b \text{ es múltiplo de } d,\\ 0 \text{ en caso contrario.}\end{cases}$$

d. Haciendo $(a, m)=d_1$, $(b, d_1)=d_2$, $\dots$, $(f, d_{r-1})=d_r$, $m=d_1m_1$, $d_1=d_2m_2$, $\dots$, $d_{r-1}=d_rm_r$, hallamos $d=d_r$,

$$T_m=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\dots\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha(ax+by+\dots+fw+g)}{m}}=$$
$$=m\sum_{\alpha_1=0}^{d_1-1}\sum_{y=0}^{m-1}\dots\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_1(by+\dots+fw+g)}{d_1}}=$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$=m^{r-1}\sum_{\alpha_{r-1}=0}^{d_{r-1}-1}\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_{r-1}(fw+g)}{d_{r-1}}}=m^r\sum_{\alpha_r=0}^{d_r-1}e^{2\pi i\frac{\alpha_rg}{d_r}}.$$

e. Apliquemos el método de inducción. Conservando las notaciones de la pregunta **d**, supongamos que el teorema es válido para r variables. Consideremos la congruencia

$$lv + ax + \ldots + fw + g \equiv 0 \text{ (mód. } m). \qquad (2)$$

Sea $(l, m) = d_0$. La condición para que sea posible la congruencia (2), es $ax + \ldots + fw + g \equiv 0$ (mód. d_0). La última congruencia es posible solamente si g es múltiplo de d', donde $d' = (a, \ldots, f, d_0) = (l, a, \ldots, f, m)$; en este caso, ésta admite $d_0^{r-1}d'$ soluciones. Por consiguiente, la congruencia (2) es posible solamente en el caso en que g es múltiplo de d'; entonces, ésta admite $d_0^{r-1}d'\left(\frac{m}{d_0}\right)^r d_0 = m^r d'$ soluciones. Por lo tanto, el teorema también es válido para $r+1$ variables. Pero el teorema subsiste para una variable. Esto significa que éste siempre es válido.

2, a. Se tiene $a^{\varphi(m)} \equiv 1$ (mód. m), $a \cdot ba^{\varphi(m)-1} \equiv b$ (mód. m).

b. Se tiene

$$1 \cdot 2 \ldots (a-1)\, ab\, (-1)^{a-1} \frac{(p-1)\ldots(p-a+1)}{1 \cdot 2 \ldots a} \equiv$$

$$\equiv b \cdot 1 \cdot 2 \ldots (1-a) \text{ (mód. } p),$$

de donde, dividiendo término a término por $1 \cdot 2 \ldots (a-1)$, se obtiene el teorema indicado.

c. α) Evidentemente, es suficiente limitarnos al caso $(2, b) = 1$. Eligiendo el signo de un modo adecuado, se tiene $b \pm m \equiv 0$ (mód. 4). Sea 2^δ la máxima potencia de 2 que divide a $b \pm m$. Si $\delta \geqslant k$, se tiene

$$x \equiv \frac{b \pm m}{2^k} \text{ (mód. } m).$$

Si $\delta < k$, se tiene

$$2^{k-\delta}x \equiv \frac{b \pm m}{2^\delta} \text{ (mód. } m).$$

Con esta congruencia repetimos una operación análoga, etc.

β) Suponemos que $(3, b) = 1$. Eligiendo el signo de un modo adecuado, se tiene $b \pm m \equiv 0$ (mód. 3). Sea 3^δ la máxima potencia de 3 que divide a $b \pm m$. Si $\delta \geqslant k$, se tiene

$$x \equiv \frac{b \pm m}{3^k} \text{ (mód. } m).$$

Si $\delta < k$, se tiene

$$3^{k-\delta}x \equiv \frac{b \pm m}{2^\delta} \text{ (mód. } m).$$

Con esta congruencia repetimos una operación análoga, etc.

γ) Sea p un divisor primo de a. Hallemos t de la condición $b+mt \equiv 0$ (mód. p). Sea p^δ la máxima potencia de p que divide a $(a, b+mt)$, y sea $a=a_1p^\delta$. Se tiene

$$a_1x \equiv \frac{b+mt}{p^\delta} \text{ (mód. } m\text{)}.$$

Si $a_1 > 1$, repetimos una operación análoga con esta nueva congruencia, etc.

El método indicado es cómodo en el caso en que el número a posea factores primos no muy grandes.

3. Haciendo $t=[\tau]$, escribimos las congruencias

$$a\cdot 0 \equiv 0 \text{ (mód. } m\text{)},$$
$$a\cdot 1 \equiv y_1 \text{ (mód. } m\text{)},$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$a\cdot t \equiv y_t \text{ (mód. } m\text{)},$$
$$a\cdot 0 \equiv m \text{ (mód. } m\text{)}.$$

Colocando estas congruencias en orden de crecimiento de sus segundos miembros (compárese con la pregunta 4, a, cap. II) y restando término a término cada congruencia (a excepción de la última) de la que le sigue, se obtienen $t+1$ congruencias de la forma $az \equiv u$ (mód. m); $0 < |z| \leqslant \tau$. En este caso, al menos en una congruencia será $0 < u < \frac{m}{\tau}$.

En efecto, u admite $t+1 > \tau$ valores, estos valores son positivos, y su suma es igual a m.

4, a, α) Se deduce de la definición de fracción simbólica.

β) Aquí se puede hacer $b_0=b+mt$, donde t se define por la condición $b+mt \equiv 0$ (mód. a); entonces, satisface a la congruencia $ax \equiv b$ el número entero, representado por la fracción ordinaria $\frac{b_0}{a}$.

γ) Se tiene (b_0 es un múltiplo de a, d_0 es un múltiplo de c)

$$\frac{b}{a}+\frac{d}{c} \equiv \frac{b_0}{c}+\frac{d_0}{c} = \frac{b_0c+ad_0}{ac} \equiv \frac{bc+ad}{ac}.$$

δ) Se tiene

$$\frac{b}{a}\cdot\frac{d}{c} \equiv \frac{b_0}{a}\cdot\frac{d_0}{c} = \frac{b_0d_0}{ac} \equiv \frac{bd}{ac}.$$

b, α) Se tiene (las congruencias se toman respecto del módulo p)

$$\binom{p-1}{a} = \frac{(p-1)(p-2)\ldots(p-a)}{1\cdot 2\ldots a} \equiv \frac{(-1)^a 1\cdot 2\ldots a}{1\cdot 2\ldots a} \equiv (-1)^a.$$

La pregunta 2, b se resuelve más fácilmente así:

$$\frac{b}{a} \equiv \frac{b(-1)^{a-1}(p-1)\dots(p-(a-1))}{1\cdot 2\dots(a-1)\,a} \text{ (mód. } p).$$

β) Se tiene

$$\frac{2^p-2}{p} \equiv 1+\frac{p-1}{1\cdot 2}+\frac{(p-1)(p-2)}{1\cdot 2\cdot 3}+\dots$$
$$\dots+\frac{(p-1)(p-2)\dots(p-(p-2))}{1\cdot 2\dots(p-1)} \text{ (mód. } p).$$

5, a. Entre los números s, $s+1$, . . ., $s+n-1$, ningún par puede tener simultáneamente divisores comunes con d. Los productos $s(s+1)\dots(s+n-1)$ pueden ser reunidos en $n^{\varkappa}$ clases según la cantidad de modos con que el número d pueda dividirse en n factores primos entre sí, teniendo en cuenta el orden de estos últimos (pregunta 11, b, cap. II). Sea $d = u_1u_2\dots u_n$ una de tales divisiones. La cantidad de productos con la condición $s \equiv 0$ (mód. u_1), $s+1 \equiv 0$ (mód. u_2), . . ., $s+n-1 \equiv 0$ (mód. u_n) es igual a $\frac{a}{b}$. Por lo tanto, el número buscado es igual a $n^{\varkappa}\frac{a}{d}$.

b. El número indicado es igual a

$$\sum_{d \setminus a} \mu(d)\, S_d; \quad S_d = \frac{n^{\varkappa}a}{d},$$

donde $\varkappa$ es igual a la cantidad de divisores primos del número d. Pero, se tiene

$$\sum_{d \setminus a} \mu(d)\frac{n^{\varkappa}a}{d} = a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\dots\left(1-\frac{n}{p_k}\right).$$

6, a. Todos los valores de x que satisfacen a la primera congruencia vienen dados por la igualdad $x = b_1 + m_1t$, donde t es entero. Para elegir entre éstos aquellos que satisfacen también a la segunda congruencia, hay que limitarse solamente a aquellos valores de t que satisfacen a la congruencia

$$m_1t \equiv b_2 - b_1 \text{ (mód. } m_2).$$

Pero esta congruencia es resoluble cuando, y sólo cuando, $b_2 - b_1$ es múltiplo de d. Además, cuando ésta es resoluble, el conjunto de valores t que la satisfacen se determina por una igualdad de la forma $t = t_0 + \frac{m_2}{d}t'$, donde t' es entero; el conjunto de valores x que satisface

al sistema considerado en la pregunta se determina por la igualdad

$$x = b_1 + m_1\left(t_0 + \frac{m^2}{d}t'\right) = x_{1,2} + m_{1,2}t';$$

$$x_{1,2} = b_1 + m_1 t_0.$$

b. Si el sistema

$$x \equiv b_1 \text{ (mód. } m_1\text{)}, \quad x \equiv b_2 \text{ (mód. } m_2\text{)}$$

es resoluble, el conjunto de valores x que le satisface se expresa por una congruencia de la forma $x \equiv x_{1,2}$ (mód. $m_{1,2}$). Si el sistema

$$x \equiv x_{1,2} \text{ (mód. } m_{1,2}\text{)}, \quad x \equiv b_3 \text{ (mód. } m_3\text{)}$$

es resoluble, el conjunto de valores x que le satisface se expresa por una congruencia de la forma $x \equiv x_{1,2,3}$ (mód. $m_{1,2,3}$). Si el sistema

$$x \equiv x_{1,2,3} \text{ (mód. } m_{1,2,3}\text{)}, \quad x \equiv b_4 \text{ (mód. } m_4\text{)}$$

es resoluble, el conjunto de valores x que le satisface se expresa por una congruencia de la forma $x \equiv x_{1,2,3,4}$ (mód. $m_{1,2,3,4}$), etc.

7, α) Al sustituir x por $-x$ (en virtud de lo cual x' se sustituye por $-x'$) el valor de la suma $\left(\frac{a,\ b}{m}\right)$ no varía.

β) Cuando x recorre el sistema reducido de restos respecto del módulo m, x' también recorre el sistema reducido de restos respecto del módulo m.

γ) Haciendo $x \equiv hz$ (mód. m), resulta

$$\left(\frac{a,\ bh}{m}\right) = \sum_z e^{2\pi i \frac{ahz+bz'}{m}} = \left(\frac{ah,\ b}{m}\right).$$

δ) Se tiene

$$\left(\frac{a_1,\ 1}{m_1}\right)\left(\frac{a_2,\ 1}{m_2}\right) = \sum_x \sum_y e^{2\pi i \frac{a_1 m_2 x + a_2 m_1 y + m_2 x' + m_1 y'}{m_1 m_2}}$$

Haciendo $m_2x' + m_1y' = z'$, se tiene

$$(a_1m_2x + a_2m_1y)(m_2x' + m_1y') \equiv a_1m_2^2 + a_2m_1^2 \text{ (mód. } m_1m_2\text{)},$$

$$\left(\frac{a_1,\ 1}{m_1}\right)\left(\frac{a_2,\ 1}{m_2}\right) = \left(\frac{m_2^2a_1 + m_1^2a_2,\ 1}{m_1m_2}\right),$$

lo cual demuestra la propiedad indicada para el caso de dos factores. La generalización para el caso de más de dos factores es trivial.

8. La congruencia

$$a_0x^n + a_1x^{n-1} + \ldots + a_n - a_0(x - x_1)(x - x_2) \ldots (x - x_n) \equiv 0 \text{ (mód. } p\text{)}$$

admite n soluciones. Su grado es inferior a n. Por consiguiente, todos sus coeficientes son múltiplos de p, lo cual se expresa mediante las congruencias indicadas en la pregunta.

9, a. Si $p > 3$, para cada x tomado de la sucesión 2, 3, . . ., $p - 2$, hallamos en esta sucesión un número correspondiente x', distinto del mismo x, que cumple la condición $xx' \equiv 1$ (mód. p); en efecto, si fuese $x = x'$ resultaría que $(x - 1)(x + 1) \equiv 0$ (mód. p); $x \equiv 1$ o $x \equiv p - 1$. Por consiguiente,

$$2 \cdot 3 \ldots (p - 2) \equiv 1 \text{ (mód. } p); \quad 1 \cdot 2 \ldots (p - 1) \equiv -1 \text{ (mód } p).$$

b. Sea $P > 2$. Suponiendo que P posee un divisor u que cumple la condición $1 < u < P$, se tendría que $1 \cdot 2 \ldots (P - 1) + 1 \equiv 1$ (mód. u).

10. a. Hallamos un número h que cumpla la condición $a_0 h \equiv 1$ (mód. m). La congruencia dada equivale a la que sigue:

$$x^n + a_1 h x^{n-1} + \ldots + a_n h \equiv 0 \text{ (mód. } m).$$

b. Sea $Q(x)$ el cociente y $R(x)$ el residuo de la división de $x^p - x$ por $f(x)$. Todos los coeficientes de $Q(x)$ y $R(x)$ son enteros. $Q(x)$ es de grado $p - n$, $R(x)$ es de grado inferior a n,

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

Supongamos que la congruencia $f(x) \equiv 0$ (mód. p) posee n soluciones. Estas mismas soluciones son también soluciones de la congruencia $R(x) \equiv 0$ (mód. p). Por lo tanto, todos los coeficientes de $R(x)$ son múltiplos de p.

Recíprocamente, supongamos que todos los coeficientes de $R(x)$ son múltiplos de p. Entonces $f(x)\, Q(x)$ es múltiplo de p para los mismos valores de x que $x^p - x$; por lo tanto, la suma de los números de soluciones de las congruencias

$$f(x) \equiv 0 \text{ (mód. } p), \quad Q(x) \equiv 0 \text{ (mód. } p)$$

no es menor que p. Supongamos que la primera admite α soluciones y la segunda β soluciones. De

$$\alpha \leqslant n, \ \beta \leqslant p - n, \ p \leqslant \alpha + \beta$$

deducimos que $\alpha = n$, $\beta = p - n$.

c. Elevando término a término la congruencia dada a la potencia $\frac{p-1}{n}$, nos convencemos de que la condición indicada es necesaria Supongamos que se cumple esta condición; de

$$x^p - x = x\left(x^{p-1} - A^{\frac{p-1}{n}} + A^{\frac{p-1}{n}} - 1\right)$$

se deduce que el residuo de la división de $x^p - x$ por $x^n - A$ es igual a $\left(A^{\frac{p-1}{n}} - 1\right)x$, donde $A^{\frac{p-1}{n}} - 1$ es múltiplo de p.

11. De $x_0^n \equiv A$ (mód. m), $y^n \equiv 1$ (mód. m) se deduce que $(x_0 y)^n \equiv A$(mód. m); ahora bien, los productos $x_0 y$ que corresponden a valores de y incongruentes (respecto del módulo m), son incongruentes. De $x_0^n \equiv A$ (mód. m), $x^n \equiv A$ (mód. m) se deduce que $x^n \equiv x_0^n$ (mód. m) y, determinando y de la condición $x \equiv y x_0$ (mód. m), se tiene

$$y^n \equiv 1 \text{ (mód. } m\text{)}.$$

Respuestas a las preguntas del capítulo V

1. La congruencia indicada es equivalente a la siguiente: $(2ax + b)^2 \equiv b^2 - 4ac$ (mód. m). Para cada solución $z \equiv z_0$ (mód. m) de la congruencia $z^2 \equiv b^2 - 4ac$ (mód. m) hallamos de $2ax + b \equiv z_0$ (mód. m) una solución correspondiente de la congruencia indicada.

2, a. Si $\left(\frac{a}{p}\right) = 1$, se tiene $a^{2m+1} \equiv 1$ (mód. p), $(a^{m+1})^2 \equiv a$ (mód. p), $x \equiv \pm a^{m+1}$ (mód. p).

b. Si $\left(\frac{a}{p}\right) = 1$, se tiene $a^{4m+2} \equiv 1$ (mód. p), $a^{2m+1} \equiv \pm 1$ (mód. p), $a^{2m+2} \equiv \pm a$ (mód. p).

Como $\left(\frac{2}{p}\right) = -1$, también se tiene $2^{4m+2} \equiv -1$ (mód. p). Por lo tanto, para un s que toma uno de los valores 0; 1, resulta

$$a^{2m+2}\, 2^{(4m+2)s} \equiv a \text{ (mód. } p\text{)}, \quad x \equiv \pm a^{m+1}\, 2^{(2m+1)s} \text{ (mód. } p\text{)}.$$

c. Sea $p = 2^k h + 1$, donde $k \geqslant 3$ y h es impar, $\left(\frac{a}{p}\right) = 1$. Se tiene

$$a^{2^{k-1}h} \equiv 1 \text{ (mód. } p\text{)}, \quad a^{2^{k-2}h} \equiv \pm 1 \text{ (mód. } p\text{)},$$

$$N^{2^{k-1}h} \equiv -1 \text{ (mód. } p\text{)}$$

Por consiguiente, para cierto entero no negativo s_2, se obtiene

$$a^{2^{k-2}h} N^{s_2 2^{k-1}} \equiv 1 \text{(mód. } p\text{)} \quad a^{2^{k-3}h} N^{s_2 2^{k-2}} \equiv \pm 1 \text{ (mód. } p\text{)};$$

de aquí, para cierto entero negativo s_3, se obtiene

$$a^{2^{k-3}h} N^{s_3 2^{k-2}} \equiv 1 \text{ (mód. } p\text{)}, \quad a^{2^{k-4}h} N^{s_3 2^{k-3}} \equiv \pm 1 \text{ (mód. } p\text{)},$$

etc.; finalmente, se obtiene

$$a^h N^{2^s k} \equiv 1 \text{ (mód. } p\text{)}, \quad x \equiv \pm a^{\frac{h+1}{2}} N^{s k} \text{ (mód. } p\text{)}.$$

d. Se tiene

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

3, a. Las condiciones de resolubilidad de las congruencias (1) y (2) se deducen trivialmente (**f**, § 2 y **k**, § 2). La congruencia (3) es resoluble cuando, y sólo cuando, $\left(\frac{-3}{p}\right)=1$. Pero $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$ y

$$\left(\frac{p}{3}\right)=\begin{cases}1, \text{ si } p \text{ es de la forma } 6m+1,\\ -1, \text{ si } p \text{ es de la forma } 6m+5.\end{cases}$$

b. Cualesquiera que sean los primos distintos $p_1, p_2, \ldots, p_k$ de la forma $4m+1$, el divisor primo mínimo p del número $(2p_1p_2\ldots p_k)^2+1$ es distinto de $p_1, p_2, \ldots, p_k$ y, como $(2p_1p_2\ldots p_k)^2+1\equiv 0$ (mód. p), es de la forma $4m+1$.

c. Cualesquiera que sean los primos distintos $p_1, p_2, \ldots, p_k$ de la forma $6m+1$, el divisor primo mínimo p del número $(2p_1p_2\ldots p_k)^2+3$ es distinto de $p_1, p_2, \ldots, p_k$ y, como $(2p_1p_2\ldots p_k)^2+3\equiv 0$ (mód. p), es de la forma $6m+1$.

4. En el primer conjunto hay números que son congruentes con $1\cdot 1, 2\cdot 2, \ldots, \frac{p-1}{2}\,\frac{p-1}{2}$, o sea, con todos los restos cuadráticos del sistema completo; según la condición, un número que pertenece al segundo conjunto es un no-resto cuadrático. Pero al segundo conjunto pertenecen todos los productos de este no-resto por todos los restos, es decir, pertenecen todos los no-restos cuadráticos.

5, a. Supongamos que en el sistema de numeración de base p

$$a=a_{\alpha-1}p^{\alpha-1}+\ldots+a_1p+a_0$$

y que la solución buscada (el resto mínimo no negativo) es

$$x=x_{\alpha-1}p^{\alpha-1}+\ldots+x_1p+x_0. \qquad (1)$$

Formemos la tabla:

$a_{\alpha-1}$	...	a_4	a_3	a_2	a_1	a_0
$2x_0x_{\alpha-1}$	...	$2x_0x_4$	$2x_0x_3$	$2x_0x_2$	$2x_0x_1$	x_0^2
$2x_1x_{\alpha-2}$	...	$2x_1x_3$	$2x_1x_2$	x_1^2		
$2x_2x_{\alpha-3}$	...	x_2^2				
...						

donde en la columna bajo a_s figuran los números cuya suma engendra el coeficiente de p^s en el desarrollo del cuadrado del segundo miembro (1) según las potencias de p. Hallamos x_0 de la condición

$$x_0^2 \equiv a_0 \text{ (mód. } p).$$

Haciendo $\frac{x_0^2 - a_0}{p} = p_1$, obtenemos x_1 de la condición

$$p_1 + 2x_0x_1 \equiv a_1 \text{ (mód. } p).$$

Haciendo $\frac{p_1 + 2x_0x_1 - a_1}{p} = p_2$, obtenemos x_2 de la condición

$$p_2 + 2x_0x_2 + x_1^2 \equiv a_2 \text{ (mód. } p),$$

etc. Como $(x_0, p) = 1$, para el número x_0 dado, los números $x_1, x_2, \ldots, x_{\alpha-1}$ se determinan univocamente.

b. Aquí

$$a = a_{\alpha-1}2^{\alpha-1} + \ldots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0,$$
$$x = x_{\alpha-1}2^{\alpha-1} + \ldots + x_3 2^3 + x_2 2^2 + x_1 2 + x_0.$$

y se tiene la tabla siguiente:

$a_{\alpha-1}$	...	a_4	a_3	a_2	a_1	a_0
$x_0x_{\alpha-2}$	...	x_0x_3	x_0x_2	x_0x_1		x_0^2
$x_1x_{\alpha-3}$	...	x_1x_2		x_1^2		
$x_2x_{\alpha-4}$	...	x_2^2				
...	...					

Consideremos solamente el caso $\alpha \geqslant 3$. Como $(a, 2) = 1$, tiene que ser necesariamente $a_0 = 1$. Por lo tanto, $x_0 = 1$. Luego tiene que ser necesariamente $a_1 = 0$ y, como $x_0x_1 + x_1^2 = x_1 + x_1^2 \equiv 0$ (mód. 2), tiene que ser necesariamente $a_2 = 0$. Para x_1 son posibles dos valores: 0 y 1. Los números $x_2, x_3, \ldots, x_{\alpha-2}$ se determinan univocamente, y para $x_{\alpha-1}$ son posibles dos valores: 0 y 1. Por lo tanto, si $\alpha \geqslant 3$ tiene que ser necesariamente $a \equiv 1$ (mód. 8), y entonces la congruencia indicada admite 4 soluciones.

6. Evidentemente, P y Q son enteros, y Q es congruente respecto del módulo p con el número que se obtiene al sustituir a por z^2, para lo cual es suficiente sustituir $\sqrt{a}$ por z. Por lo tanto, $Q \equiv 2^{\alpha-1}z^{\alpha-1}$ (mód. p); por consiguiente, $(Q, p) = 1$ y Q' verdaderamente se puede determinar de la congruencia $QQ' \equiv 1$ (mód. p^α). Se tiene

$$P^2 - aQ^2 = (z+\sqrt{a})^\alpha (z-\sqrt{a})^\alpha = (z^2-a)^\alpha \equiv 0 \text{ (mód. } p^\alpha),$$

de donde

$$(PQ')^2 \equiv a\,(QQ')^2 \equiv a \text{ (mód. } p^\alpha).$$

7. Sea $m = 2^\alpha p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ la descomposición canónica del número m. Entonces m se expresa de 2^k maneras en la forma $m = 2^\alpha ab$, donde $(a, b) = 1$.

Supongamos que $\alpha = 0$. De $(x-1)(x+1) \equiv 0$ (mód. m) se deduce que para ciertos a y b.

$$x \equiv 1 \text{ (mód. } a); \qquad x \equiv -1 \text{ (mód. } b).$$

Resolviendo este sistema se obtiene $x \equiv x_0$ (mód. m). Por lo tanto, la congruencia indicada tiene 2^k soluciones.

Supongamos que $\alpha = 1$. Para ciertos a y b

$$x \equiv 1 \text{ (mód. } 2a); \qquad x \equiv -1 \text{ (mód. } 2b).$$

Resolviendo este sistema se obtiene $x \equiv x_0$ (mód. m). Por lo tanto, la congruencia indicada tiene 2^k soluciones.

Supongamos que $\alpha = 2$. Para ciertos a y b

$$x \equiv 1 \text{ (mód. } 2a); \qquad x \equiv -1 \text{ (mód. } 2b).$$

Resolviendo este sistema se obtiene $x \equiv x_0 \left(\text{mód. } \frac{m}{2}\right)$. Por lo tanto, la congruencia indicada tiene 2^{k+1} soluciones.

Supongamos que $\alpha \geqslant 3$. Para ciertos a y b tiene que verificarse uno de los sistemas

$$x \equiv 1 \text{ (mód. } 2a); \qquad x \equiv -1 \text{ (mód. } 2^{\alpha-1}b);$$

$$x \equiv 1 \text{ (mód. } 2^{\alpha-1}a); \qquad x \equiv -1 \text{ (mód. } 2b).$$

Resolviendo uno de estos sistemas se obtiene $x \equiv x_0 \left(\text{mod}\frac{m}{2}\right)$. Por lo tanto, la congruencia indicada tiene 2^{k+2} soluciones.

8. a. Determinando x de la congruencia $xx' \equiv 1$ (mód. p), se tiene

$$\sum_{x=1}^{p-1}\left(\frac{x(x+k)}{p}\right) = \sum_{x=1}^{p-1}\frac{(xx'(xx'+kx')}{p}\Big) = \sum_{x=1}^{p-1}\left(\frac{1+kx'}{p}\right).$$

Evidentemente, $1+kx'$ recorre todos los restos del sistema completo, a excepción de 1. De aquí se deduce el teorema indicado.

b. La igualdad en cuestión se deduce de la igualdad

$$T=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)\right)\left(1+\eta\left(\frac{x+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)+\eta\left(\frac{x+1}{p}\right)+\varepsilon\eta\left(\frac{x(x+1)}{p}\right)\right).$$

c. Supongamos que δ denota la cantidad de valores de y que son iguales a cero (por consiguiente, $\delta=0$ ó $\delta=1$). Se tiene

$$S^2\leqslant X\sum_{y_1}\sum_{y}S_{y_1,\,y};\ S_{y_1,\,y}=\sum_{x=0}^{p-1}\left(\frac{(xy+k)(xy_1+k)}{p}\right).$$

Ahora hallamos que:

$S_{y_1,\,y}=p$, si $y_1=y=0$;

$S_{y_1,\,y}=0$, si solamente uno de los números y_1 e y es igual a cero;

$S_{y_1,\,y}=p-1=p-\left(\frac{y_1y}{p}\right)$, si $y_1=y>0$;

$S_{y_1,\,y}=-\left(\frac{y_1y}{p}\right)$ en los demás casos.

Por lo tanto,

$$S^2\leqslant X\left(p\delta+p(Y-\delta)-\left(\sum_{y>0}\left(\frac{y}{p}\right)\right)^2\right)\leqslant XYp.$$

d. α) Se tiene

$$S=\sum_{x=0}^{p-1}\sum_{z_1=0}^{Q-1}\sum_{z=0}^{Q-1}\left(\frac{(x+z_1)(x+z)}{p}\right).$$

Para $z_1=z$, la sumación respecto de x da $p-1$. Para z_1 distinto de z, la sumación respecto de x (pregunta a) da -1. Por lo tanto, $S=pQ-Q^2$.

β) Según el teorema de la pregunta α), se tiene

$$T(Q^{0,5+0,5\lambda})^2\leqslant S<pQ;\quad T<pQ^{-\lambda}.$$

γ) Si $p\leqslant 5$, el teorema es trivial. Si $p>5$, aplicamos el teorema de la pregunta α). Suponiendo que en la sucesión indicada en la pregunta

no hay no-restos cuadráticos, llegamos a la conclusión que $S_x = Q$ para $x = M,\ M+1,\ \ldots,\ M+Q$. Por lo tanto ($Q^2 + 2Q$ y $Q^2 + 2Q + 1$ no son iguales a p, puesto que son compuestos), hallamos

$$(Q+1)\,Q^2 \leqslant (p-Q)\,Q, \quad Q^2 + 2Q < p, \quad (Q+1)^2 < p,$$

lo cual es imposible.

9, a. Si m se expresa en la forma (1), la solución

$$z \equiv z_0 \pmod{m} \tag{5}$$

de la congruencia $x \equiv zy \pmod{m}$ también es solución de la congruencia (2). Diremos que la expresión indicada está ligada con la solución (5) de la congruencia (2).

Con cada solución (5) de la congruencia (2) está ligada no menos de una expresión (1). En efecto, tomando $\tau = \sqrt{m}$, se tiene

$$\frac{z_0}{m} = \frac{P}{Q} + \frac{\theta}{Q\sqrt{m}}; \quad (P, Q) = 1,\ 0 < Q \leqslant \sqrt{m}, \quad |\theta| < 1.$$

Por lo tanto, $z_0 Q = mP + r$, donde $|r| < \sqrt{m}$. Luego, de (2) se deduce que $|r|^2 + Q^2 \equiv 0 \pmod{m}$. De aquí y de $0 < |r|^2 + Q^2 < 2m$ se obtiene

$$m = |r|^2 + Q^2. \tag{6}$$

Ahora bien, $(|r|, Q) = 1$, puesto que

$$1 = \frac{r^2 + Q^2}{m} = \frac{(z_0 Q - mP)\,z_0 Q - rmP + Q^2}{m} \equiv -rP \pmod{Q}.$$

Si $|r| = r$, $r \equiv z_0 Q \pmod{m}$, la expresión (6) está ligada con la solución (5). Si $|r| = -r$, como $z_0^2 Q \equiv z_0 r \pmod{m}$, $Q \equiv z_0 |r| \pmod{m}$, la expresión $m = Q^2 + |r|^2$ está ligada con la solución (5). Con cada solución (5) está ligada no más de una expresión (1). En efecto, si dos expresiones del número m en la forma (1), $m = x^2 + y^2$ y $m = x_1^2 + y_1^2$, están ligadas con una solución (5), entonces, de $x \equiv z_0 y \pmod{m}$, $x_1 \equiv z_0 y_1 \pmod{m}$ se deduce que $xy_1 \equiv x_1 y \pmod{m}$. Por lo tanto, $xy_1 = x_1 y$, y como $(x, y) = (x_1, y_1) = 1$, resulta que $x = x_1$, $y = y_1$.

b. Si p se expresa en la forma (3), la solución

$$z \equiv z_0 \pmod{p} \tag{7}$$

de la congruencia $x \equiv zy \pmod{p}$ también es solución de la congruencia (4). Diremos que la expresión indicada está ligada con la solución (7) de la congruencia (4).

Conociendo la solución (7) de la congruencia (4), hallamos no menos de una expresión (3). En efecto, tomado $\tau = \sqrt{p}$, se tiene

$$\frac{z_0}{p} = \frac{P}{Q} + \frac{\theta}{Q\sqrt{p}}; \quad (P, Q) = 1, \ 0 < Q \leqslant \sqrt{p}, \ |\theta| < 1.$$

Por lo tanto, $z_0 Q \equiv r \pmod{p}$, donde $|r| < \sqrt{p}$. Luego, de (4) se deduce que $|r|^3 + aQ^3 \equiv 0 \pmod{p}$. De aquí y de $0 < |r|^3 + aQ^3 < (1 + a)p$ se deduce que, si $a = 2$, tiene que ser $|r|^3 + 2Q^3 = p$ ó $|r|^3 + 2Q^3 = 2p$. En el último caso $|r|$ es par, $|r| = 2r_1$, $p = Q^3 + 2r_1^3$. Si $a = 3$, tiene que ser $|r|^3 + 3Q^3 = p$, ó $|r|^3 + 3Q^3 = 2p$, ó $|r|^3 + 3Q^3 = 3p$. El segundo caso es imposible, pues, respecto del módulo 4 el primer miembro es congruente con 0, mientras que el segundo miembro es congruente con 2. En el tercer caso, $|r|$ es múltiplo de 3, $|r| = 3r_1$, $p = Q^3 + 3r_1^3$.

Suponiendo que dos expresiones del número p en la forma (3), $p = x^3 + ay^3$ y $p = x_1^3 + ay_1^3$, están ligadas con una misma solución de la congruencia (4), hallamos que $x = x_1$, $y = y_1$. Suponiendo que estas expresiones están ligadas con soluciones distintas de la congruencia (4), hallamos que $x \equiv zy \pmod{p}$, $x_1 \equiv -zy_1 \pmod{p}$, de donde $xy_1 + x_1 y \equiv 0 \pmod{p}$, lo cual es imposible, puesto que

$$0 < (xy_1 + x_1 y)^3 \leqslant (x^3 + y^3)(x_1^3 + y_1^3) < p^3$$

c, α) Los términos de la suma $S(k)$ con $x = x_1$ y $x = -x_1$ son iguales.

β) Se tiene

$$S(kt^2) = \sum_{x=0}^{p-1} \left(\frac{xt\,(x^2t^2 + kt^2)}{p} \right) = \left(\frac{t}{p} \right) S(k).$$

γ) Haciendo $p - 1 = 2p_1$, se tiene

$$p_1 (S(r))^2 + p_1 (S(n))^2 = \sum_{t=1}^{p_1} (S(rt^2))^2 + \sum_{t=1}^{p_1} (S(nt^2))^2 =$$

$$= \sum_{k=0}^{p-1} S(k)^2 = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \sum_{k=0}^{p-1} \left(\frac{xy\,(x^2 + k)\,(y^2 + k)}{p} \right).$$

Si y no es igual a x o a $p - x$, el resultado de la sumación respecto de k es igual a $-\left(\frac{xy}{p}\right)$; si $y = x$ o $y = p - x$ éste es igual a $(p-1) \times \left(\frac{xy}{p}\right)$. Por lo tanto,

$$p_1 (S(r))^2 + p_1 (S(n))^2 = 4pp_1. \quad p = \left(\frac{1}{2} S(r) \right)^2 + \left(\frac{1}{2} S(n) \right)^2$$

10, a. Se tiene

$$X^2-DY^2=(x_1+y_1\sqrt{D})(x_2\pm y_2\sqrt{D})(x_1-$$
$$-y_1\sqrt{D})(x_2\pm y_2\sqrt{D})=k^2.$$

b. Tomando cualquier τ_1 que cumpla la condición $\tau_1>1$, hallamos unos enteros x_1, y_1 que cumplen la condición $|y_1\sqrt{D}-x_1|<\frac{1}{\tau_1}$, $0\leqslant y_1\leqslant\tau_1$, de donde, multiplicando término a término por $y_1\sqrt{D}+x_1<2y_1\sqrt{D}+1$, obtenemos $|x_1^2-Dy_1^2|<2\sqrt{D}+1$. Tomando $\tau_2>\tau_1$ de modo que sea $|y_1\sqrt{D}-x_1|>\frac{1}{\tau_2}$, hallamos unos nuevos enteros x_2, y_2 que cumplen la condición $|x_2^2-Dy_2^2|<2\sqrt{D}+1$, etc. De aquí se deduce que en el intervalo $-2\sqrt{D}-1<k<2\sqrt{D}+1$ existe un entero k, distinto de cero, tal que entre los pares x_1, y_1; x_2, y_2;... hay un conjunto infinito de pares x, y que cumplen la condición $x^2-Dy^2=k$; entre estos últimos siempre habrá dos pares ξ_1, η_1 y ξ_2, η_2 que satisfacen a la condición $\xi_1\equiv\xi_2$ (mód. $|k|$), $\eta_1\equiv\eta_2$ (mód. $|k|$). Determinando los enteros ξ_0, η_0 mediante la igualdad

$$\xi_0+\eta_0\sqrt{D}=(\xi_1+\eta_1\sqrt{D})(\xi_2-\eta_2\sqrt{D}),$$ se tiene (pregunta a)

$$\xi_0^2-D\eta_0^2=|k|^2,\ \xi_0\equiv\xi_1^2-D\eta_1^2\equiv 0\ (\text{mód. }|k|);$$
$$\eta_0\equiv-\xi_1\eta_1+\xi_1\eta_1\equiv 0\ (\text{mód. }|k|).$$

Por lo tanto, $\xi_0=\xi|k|$, $\eta_0=\eta|k|$, donde ξ y η son enteros y $\xi^2-D\eta^2=1$.

c. Los números x, y que se determinan por la igualdad (2) satisfacen (pregunta a) a la ecuación (1).

Suponiendo que existe un par de enteros positivos x, y que satisfacen a la ecuación (1), pero distinto de los pares que se determinan por la igualdad (2), para cierto $r=1, 2, \ldots$ tendremos

$$(x_0+y_0\sqrt{D})^r<x+y\sqrt{D}<(x_0+y_0\sqrt{D})^{r+1}.$$

De aquí, dividiendo término a término por $(x_0+y_0\sqrt{D})^r$, obtenemos

$$1<X+Y\sqrt{D}<x_0+y_0\sqrt{D}, \tag{3}$$

donde (pregunta a) X e Y son enteros que se determinan por la igualdad

$$X+Y\sqrt{D}=\frac{x+y\sqrt{D}}{(x_0+y_0\sqrt{D})^r}=(x+y\sqrt{D})(x_0-y_0\sqrt{D})^r$$

y satisfacen a la ecuación

$$X^2-DY^2=1. \tag{4}$$

Pero de (4) se deducen las desigualdades $0<X-Y\sqrt{D}<1$, las cuales, junto con la primera desigualdad (3), muestran que X e Y son positivos. Por lo tanto, la segunda desigualdad (3) contradice a la difinición de los números x_0, y_0.

11, a, α) Se tiene

$$|U_{a,\,p}|^2=U_{a,\,p}\overline{U}_{a,\,p}=\sum_{t=1}^{p-1}\sum_{x=1}^{p-1}\left(\frac{t}{p}\right)e^{2\pi i\frac{ax(t-1)}{p}}.$$

Para $t=1$ la sumación respecto de x da $p-1$; para $t>1$ resulta $-\left(\frac{t}{p}\right)$. Por lo tanto

$$|U_{a,\,p}|^2=p-1-\sum_{t=2}^{p-1}\left(\frac{t}{p}\right)=p,\ |U_{a,\,p}|=\sqrt{p}.$$

o sea

$$|U_{a,\,p}|^2=U_{a,\,p}\overline{U}_{a,\,p}=\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x+t}{p}\right)\left(\frac{x}{p}\right)e^{2\pi i\frac{at}{p}}.$$

Para $t=0$ la sumación respecto de x da $p-1$; para $t>0$ resulta $-e^{2\pi i\frac{at}{p}}$. Por lo tanto

$$|U_{a,\,p}|^2=p-1-\sum_{t=1}^{p-1}e^{2\pi i\frac{at}{p}}=p,\quad |U_{a,\,p}|=\sqrt{p}.$$

β) Si $(a,\,p)=p$ el teorema es evidente. Si $(a,\,p)=1$ éste se deduce de

$$U_{a,\,p}=\left(\frac{a}{p}\right)\sum_{x=1}^{p-1}\left(\frac{ax}{p}\right)e^{2\pi i\frac{ax}{p}}=\left(\frac{a}{p}\right)U_{1,\,p}.$$

b, α) Supongamos que r recorre los restos cuadráticos, y n los no-restos cuadráticos, comprendidos en el sistema completo de restos. Se tiene

$$S_{a,\,p}=1+2\sum_{r}e^{2\pi i\frac{ar}{p}}.$$

Restando de aquí término a término

$$0=1+\sum_{r}e^{2\pi i\frac{ar}{p}}+\sum_{n}e^{2\pi i\frac{an}{p}}$$

se obtiene la igualdad indicada.

β) Se tiene

$$|S_{a,m}|^2 = \sum_{t=0}^{m-1} \sum_{x=0}^{m-1} e^{2\pi i \frac{a(t^2+2tx)}{m}}.$$

Para un t dado la sumación respecto de x da $me^{2\pi i \frac{at^2}{m}}$ ó 0, según que *sea divisible* $2t$ *por* m *o no. Si* m *es impar, se tiene*

$$|S_{a,m}|^2 = me^{2\pi i \frac{a \cdot 0^2}{m}} = m.$$

Si m es par, $m = 2m_1$, se tiene

$$|S_{a,m}|^2 = m\left(e^{2\pi i \frac{a \cdot 0^2}{m}} + e^{2\pi i \frac{a \cdot m_1^2}{m}}\right).$$

Aquí el segundo miembro es igual a cero si m_1 es impar y es igual a $2m$ si m_1 es par.

γ) Para cualquier entero b, se tiene

$$|S_{A,m}| = \left| \sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2+2Abx}{m}} \right|,$$

de donde, eligiendo b de la condición $2Ab \equiv a$ (mód. m), se obtiene (pregunta β) el resultado indicado.

12, a, α) Se tiene

$$m \sum_{z}{}' \Phi(z) = \sum_{z} \sum_{s=M}^{M+Q-1} \sum_{a=0}^{m-1} \Phi(z)\, e^{2\pi i \frac{a(z-s)}{m}}.$$

La parte de la suma del segundo miembro que corresponde a $a = 0$, es igual a $Q \sum_{z} \Phi(z)$; la parte que corresponde a los valores restantes de a es en valor absoluto (pregunta 11, c, cap. III)

$$< \Delta \sum_{a=1}^{m-1} \left| \sum_{s=M}^{M+Q-1} e^{2\pi i \frac{as}{m}} \right| < \Delta m (\ln m - \delta).$$

β) Es suficiente demostrar que la suma

$$T = \sum_{z} \sum_{y=0}^{l} \sum_{y_1=0}^{l} \sum_{a=0}^{m-1} e^{2\pi i \frac{a(z-N-y+y_1)}{m}},$$

la cual es igual al producto de m por el número de soluciones de la congruencia $z \equiv N - y + y_1$ (mód. m), es positiva. Pero la parte de esta suma que corresponde a $a = 0$, es igual a

$$Zh^2; \quad h = l + 1.$$

La parte que corresponde a un valor $a > 0$ dado, es en valor absoluto menor que

$$\Delta_0 \min\left(h^2, \frac{1}{4\left(\frac{a}{m}\right)^2}\right).$$

Por consiguiente, la parte que corresponde a todos los valores positivos a, es en valor absoluto menor que

$$2\Delta_0 \sum_{a=1}^{\infty} \min\left(h^2, \frac{m^2}{4a^2}\right) < 2\Delta_0 \left(\int_0^{\frac{m}{2h}} h^2\, d\alpha + \int_{\frac{m}{2h}}^{\infty} \frac{m^2}{4a^2}\, d\alpha\right) = 2\Delta_0 mh.$$

Por lo tanto,

$$T > Zh^2 - 2\Delta_0 mh > 0.$$

b, α) Se deduce del teorema de la pregunta 11, a, α) y del teorema de la pregunta a.

β) La desigualdad de la pregunta α) da $R - N = \theta\sqrt{p}\ln p$. Además, es obvio que $R + N = Q$.

γ) Del teorema de la pregunta 11, b, β) se deduce que se cumplen las condiciones del teorema de la pregunta a, α) si se hace $m = p$, $\Phi(z) = 1$ $\Delta = \sqrt{p}$, y z recorre los valores $z = x^2$; $x = 0, 1, \ldots, p-1$. Pero entre los valores de z hay uno que es congruente respecto del módulo p con 0 y sendos pares que son congruentes respecto del módulo p con cada resto cuadrático del sistema completo. Por lo tanto,

$$\sum_z{}' \Phi(z) = 2R, \qquad \sum_z \Phi(z) = p$$

y se obtiene

$$2R = \frac{Q}{p}p + \theta\sqrt{p}\ln p.$$

δ) Se deduce del teorema de la pregunta 11, b, γ) y del teorema de la pregunta a, α).

ε) Del teorema de la pregunta δ) se deduce que se cumplen las condiciones del teorema de la pregunta a, α) si se hace $m = p$, $\Phi(z) = 1$, $\Delta = \sqrt{p}\ln p$, y z recorre los valores $z = Ax^2$; $x = M_0, M_0 + 1, \ldots, M_0 + Q_0 - 1$. Por lo tanto,

$$\sum_z{}' \Phi(z) = T, \qquad \sum_z \Phi(z) = Q_0,$$

de donde se deduce la fórmula indicada en la pregunta.

c. La parte de la suma que contiene los términos con $\left(\frac{\alpha}{p}\right)=1$, es igual a $p(R^2+N^2)$, la parte restante es igual a $-2pRN$. Por lo tanto, toda la suma es igual a $p(R-N)^2$.
La parte de la suma que contiene los términos con $a=0$, es igual a 0. La parte restante es en valor absoluto menor (pregunta **11, c, cap. III**),

$$\sum_{a=1}^{p-1}\left|\sum_{x=M}^{M+Q-1} e^{2\pi i\frac{ax}{p}}\right|\sum_{\alpha=1}^{p-1}\left|\sum_{y=M}^{M+Q-1} e^{2\pi i\frac{a\alpha y}{p}}\right|<p^2(\ln p)^2.$$

Por consiguiente,

$$p(R-N)^2<p^2(\ln p)^2, \quad |R-N|<\sqrt{p}\ln p.$$

Respuestas a las preguntas del capítulo VI

1, a. Si q es un número primo impar y $a^p \equiv 1$ (mód. q), entonces a respecto del módulo q pertenece a uno de los exponentes $\delta = 1$; p. Si $\delta = 1$, se tiene $a \equiv 1$ (mód. q), si $\delta = p$, se tiene $q - 1 = 2px$; x es entero.
b. Si q es un número primo impar y $a^p + 1 \equiv 0$ (mód. q), entonces $a^{2p} \equiv 1$ (mód. q). Por lo tanto, respecto del módulo q el número a pertenece a uno de los exponentes $\delta = 1, 2, p, 2p$. Los casos $\delta = 1$; p son imposibles. Si $\delta = 2$, se tiene $a^2 \equiv 1$ (mód. q), $a + 1 \equiv 0$ (mód. q). Si $\delta = 2p$, se tiene $q - 1 = 2px$; x es entero.
c. Son primos de la forma $2px + 1$, por ejemplo, los divisores primos del número $2^p - 1$. Sean $p_1, p_2, \ldots, p_k$ cualesquiera k números primos de la forma $2px + 1$; el número $(p_1, p_2, \ldots p_k)^p - 1$ posee un divisor primo de la forma $2px + 1$, distinto de $p_1, p_2, \ldots, p_k$
d. Si q es primo y $2^{2^n} + 1 \equiv 0$ (mód. q), entonces $2^{2^{n+1}} \equiv 1$ (mód. q). Por lo tanto, respecto del módulo q el número 2 pertenece al exponente 2^{n+1} y, por consiguiente, $q - 1 = 2^{n+1}x$; x es entero.
2. Evidentemente, respecto del módulo $a^n - 1$ el número a pertenece al exponente n. Por lo tanto, n es un divisor de $\varphi(a^n - 1)$.
3, a. Supongamos que después de realizar la k-ésima operación se obtiene la sucesión inicial. Evidentemente, la k-ésima operación es equivalente a la siguiente: en la sucesión

$$1, 2, \ldots, n-1, n, n, n-1, \ldots, 2, 1, 1, \ldots$$
$$\ldots, n-1, n, n, n-1, \ldots, 2, 1, 2, \ldots$$

se toman los números que ocupan los lugares $1, 1 + 2^k, 1 + 2 \cdot 2^k$..
Por lo tanto, en la sucesión inicial, en el $1 + 2^k$ lugar tiene que estar

el número 2. Por consiguiente, la condición indicada en la pregunta es necesaria. Pero ésta también es suficiente, puesto que al cumplirse se tienen las siguientes congruencias respecto del módulo $2n-1$:

$$1 \equiv 1, \quad 1+2^h \equiv 0, \quad 1+2\cdot 2^h \equiv -1, \ \ldots$$

o bien

$$1 \equiv 1, \quad 1+2^h \equiv 2, \quad 1+2\cdot 2^h \equiv 3, \ \ldots$$

b. La solución es análoga a la solución de la pregunta **a.**

4. La solución de la congruencia $x^\delta \equiv 1$ (mód. p) pertenece a un exponente de la forma $\frac{\delta}{\delta'}$, donde δ' es un divisor de δ. Aquí δ' es un múltiplo de d cuando, y sólo cuando, $x^{\frac{\delta}{d}} \equiv 1$ (mód. p). Escribiendo todos los δ valores de δ' y tomando $f=1$, obtenemos $S' = \sum_{d \setminus \delta} \mu(d)\, S_d$, donde S' es el número buscado y $S_d = \frac{\delta}{d}$.

5, a. Aquí (§ 3; ejemplo **c**, § 5) tiene que ser $\left(\frac{g}{2^n+1}\right) = -1$. Esta condición se cumple para $g=3$.

b. Aquí no tiene que ser $\left(\frac{g}{2p+1}\right) = 1$, $g^2 \equiv 1$ (mód. $2p+1$). Esta condición se cumple para los valores indicados de g.

c. Aquí no tiene que ser $\left(\frac{g}{4p+1}\right) = 1$, $g^4 \equiv 1$ (mód. $4p+1$). Esta condición se cumple para $g=2$.

d. Aquí no tiene que ser $\left(\frac{g}{2^np+1}\right) = 1$, $g^{2^n} \equiv 1$ (mód. 2^np+1). Esta condición se cumple para $g=3$.

6, a, α) Si n es múltiplo de $p-1$, el teorema es evidente. Supongamos que n no es divisible por $p-1$. Los números $1, 2, \ldots, p-1$, sin tener en cuenta el orden que siguen, son congruentes respecto del módulo p con los números $g, 2g, \ldots, (p-1)g$, donde g es una raíz primitiva respecto del módulo p. Por lo tanto,

$$S_n \equiv g^n S_n \text{ (mód. } p), \quad S_n \equiv 0 \text{ (mód. } p).$$

β) Se tiene

$$\sum_{x=1}^{p-1} \left(\frac{x(x^2+1)}{p}\right) \equiv \sum_{x=1}^{p-1} x^{\frac{p-1}{2}} (x^2+1)^{\frac{p-1}{2}} \text{ (mód. } p),$$

de donde (pregunta **α**)) se obtiene el resultado indicado.

b. Si $p>2$, se tiene

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

7, a. Se tiene $g_1^{\operatorname{ind}_{g_1} a} \equiv a$ (mód. p). $\operatorname{ind}_{g_1} a \operatorname{ind}_g g_1 \equiv \operatorname{ind}_g a$ (mód. $p-1$), $\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a$ (mód. $p-1$).

b. De $\operatorname{ind}_g a \equiv s$ (mód. n). $\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a$ (mód. $p-1$) se deduce que $\operatorname{ind}_{g_1} a \equiv \alpha s \equiv s_1$ (mód. n).

8. Sea $(n, p-1)=1$. Hallando u de la condición $nu \equiv 1$ (mód. $p-1$), obtenemos la solución $x \equiv a^u$ (mód. p).

Supongamos que n es primo, $p-1=n^\alpha t$, α es un entero positivo, $(t, n)=1$. Si la congruencia es posible, se tiene $a^{n^{\alpha-1}t} \equiv 1$ (mód. p); si $\alpha > 1$, entonces, observando que $z \equiv g^{n^{\alpha-1}tr}$ (mód. p), $r=0, 1, \ldots, n-1$, son todas las soluciones de la congruencia $z^n \equiv 1$ (mód. p), para cierto $r_1=0, 1, \ldots, n-1$, se tiene

$$a^{n^{\alpha-2}t} g^{n^{\alpha-1}tr_1} \equiv 1 \text{ (mód. } p);$$

si $\alpha > 2$, para cierto $r_2=0, 1, \ldots, n-1$, se tiene

$$a^{n^{\alpha-3}t} g^{n^{\alpha-2}tr_1+n^{\alpha-1}tr_2} \equiv 1 \text{ (mód. } p),$$

etc.; finalmente, para cierto $r_{\alpha-1}=0, 1, \ldots, n-1$, se tiene

$$a^t g^{ntr_1+n^2tr_2+\ldots+n^{\alpha-1}tr_{\alpha-1}} \equiv 1 \text{ (mód. } p).$$

Hallando u y v de la condición $tu-nv=-1$, se obtienen n soluciones:

$$x \equiv a^v g^{ut(r_1+nr_2+\ldots+n^{\alpha-2}r_{\alpha-1})+n^{\alpha-1}tr} \text{ (mód. } p);$$
$$r=0, 1, \ldots n-1.$$

Supongamos que el número primo n_1 es un divisor de $(n, p-1)$, $n=n_1n_2$, $n_2>1$. Para cada solución de la congruencia $y^{n_1} \equiv a$ (mód. p) buscamos una solución correspondiente de la congruencia $x^{n_2} \equiv y$ (mód. p).

9, a. Del modo indicado se obtienen $cc_0c_1 \ldots c_k = \varphi(m)$ caracteres. Supongamos que para dos caracteres $\chi_1(a)$ y $\chi_2(a)$ son distintos entre sí los valores R' y R'' de alguna de las raíces $R, R_0, R_1, \ldots, R_k$; para el número a_1, cuyos índices son todos iguales a 0, a excepción de uno, correspondiente a los valores indicados R' y R'', e igual a 1, se tiene

$$\chi_1(a_1)=R', \quad \chi_2(a_1)=R''.$$

b, α) Se tiene $\chi(1)=R^0 \ldots R_k^0=1$.

β) Sean $\gamma', \ldots, \gamma_k'$; $\gamma'', \ldots, \gamma_k''$ los sistemas de índices de los números a_1 y a_2; entonces $\gamma'+\gamma'', \ldots, \gamma_k'+\gamma_k''$ es el sistema de índices del número a_1a_2 (c, § 7).

γ) Si $a_1 \equiv a_2$ (mód. m), los índices de los números a_1 y a_2 son congruentes entre sí respecto de los módulos $c, \ldots, c_k$.

c. La propiedad indicada se deduce de

$$\sum_{\alpha=0}^{m-1} \chi(a) = \sum_{\gamma=0}^{c-1} R^{\gamma} \ldots \sum_{\gamma_k=0}^{c_k-1} R_k^{\gamma_k}.$$

d. La propiedad indicada se deduce de

$$\sum_{\chi} \chi(a) = \sum_{R} R^{\gamma} \ldots \sum_{R_k} R_k^{\gamma_k}.$$

e. Supongamos que $\psi(a_1)$ no es igual a 0; de la igualdad $\psi(a_1) = \psi(a_1)\psi(1)$ se deduce que: $\psi(1)=1$. Por otra parte $\psi(a)$ es diferente de 0 si $(a, m)=1$; en efecto, determinando a' de la condición $aa' \equiv 1$ (mód. m), obtenemos $\psi(a)\psi(a')=1$.

Si $(a_1, m)=1$, se tiene

$$\sum_{a}{}' \frac{\chi(a)}{\psi(a)} = \sum_{a}{}' \frac{\chi(a_1a)}{\psi(a_1a)} = \frac{\chi(a_1)}{\psi(a_1)} \sum_{a}{}' \frac{\chi(a)}{\psi(a)};$$

por lo cual, o $\sum_{a}{}' \frac{\chi(a)}{\psi(a)} = 0$ o bien $\psi(a_1) = \chi(a_1)$ para todos los valores de a_1. Pero la primera proposición no puede verificarse para todos los χ, pues en caso contrario sería $H=0$, mientras que $H=\varphi(m)$ ya que, sumando para un valor dado a respecto de todos los caracteres, se tiene

$$\sum_{\chi} \frac{\chi(a)}{\psi(a)} = \begin{cases} \varphi(m), & \text{si } a \equiv 1 \text{ (mód. } m), \\ 0 & \text{en caso contrario.} \end{cases}$$

f. α) Si $R', \ldots, R_k$ y $R'', \ldots, R_k''$ son los valores de $R, \ldots, R_k$, correspondientes a los caracteres $\chi_1(a)$ y $\chi_2(a)$: entonces $\chi_1(a)\ \chi_2(a)$ es el carácter cuyos valores correspondientes son $R'R'', \ldots, R_k'R_k''$.

β) Cuando $R, \ldots, R_k$ recorren todas las raíces de las correspondientes ecuaciones, $R'R, \ldots, R_k'R_k$ recorren en cierto orden las mismas raíces.

γ) Determinando l' de la condición $ll' \equiv 1$ (mód. m), se tiene

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \sum_{\chi} \frac{\chi(al')}{\chi(ll')} = \sum_{\chi} \chi(al').$$

lo cual es igual a $\varphi(m)$ o a 0, según que sea $a \equiv l$ (mód. m) o no.

10, a, α) Determinando x' mediante la congruencia $xx' \equiv 1$ (mód. p), se tiene

$$\sum_{x=1}^{p-1} e^{2\pi i \frac{l \operatorname{ind}(x+h) - l \operatorname{ind} x}{n}} = \sum_{x=1}^{-1} e^{2\pi i \frac{l \operatorname{ind}(1+hx')}{n}} = -1.$$

β) Se tiene

$$S = \sum_{x=0}^{p-1} \sum_{z_1=0}^{Q-1} \sum_{z=0}^{Q-1} e^{2\pi i \frac{l \operatorname{ind}(x+z_1) - l \operatorname{ind}(x+z)}{n}}.$$

Si $z_1 = z$ la sumación respecto de x da $p-1$, si z_1 no es igual a z la sumación respecto de x (pregunta α)) da -1. Por lo tanto,

$$S = Q(p-1) - Q(Q-1) = (p-Q)Q.$$

11, a, α) Se tiene

$$|U_{a,p}|^2 = \sum_{t=1}^{p-1} \sum_{x=1}^{p-1} e^{2\pi i \frac{h \operatorname{ind} t}{n}} e^{2\pi i \frac{a(t-1)x}{p}} =$$

$$= p - 1 - \sum_{t=2}^{p-1} e^{2\pi i \frac{h \operatorname{ind} t}{n}} = p.$$

β) Si $(a, p) = p$, el teorema es evidente. Si $(a, p) = 1$, el teorema se deduce de

$$U_{a,p} = e^{2\pi i \frac{-h \operatorname{ind} a}{n}} \sum_{x=1}^{p-1} e^{2\pi i \frac{h \operatorname{ind} ax}{n}} e^{2\pi i \frac{ax}{p}} = e^{2\pi i \frac{-h \operatorname{ind} a}{n}} U_{1,p}.$$

γ) Evidentemente, A y B son enteros y $|S|^2 = A^2 + B^2$. Para ciertos ε, ε', ε'' que cumplen la condición $|\varepsilon| = |\varepsilon'| = \varepsilon'' | = 1$, se tiene (pregunta β))

$$S = \frac{1}{\varepsilon \sqrt{p}\, \varepsilon \sqrt{p}} \sum_{z_1=1}^{p-1} \sum_{z=1}^{p-1} \sum_{x=0}^{p-1} e^{2\pi i \frac{\operatorname{ind} z_1 + \operatorname{ind} z}{4}} e^{2\pi i \frac{z_1 x + z(x+1)}{p}}.$$

Si $z_1 + z$ no es igual a p, la sumación respecto de x da cero. Por lo tanto

$$S = \varepsilon' \sum_{z=1}^{p-1} \left(\frac{z}{p}\right) e^{2\pi i \frac{z}{p}} = \varepsilon'' \sqrt{p}, \quad |S|^2 = p.$$

δ) Se tiene

$$S = \frac{1}{n} \sum_{x=1}^{p-1} \sum_{h=0}^{n-1} e^{2\pi i \frac{h(\operatorname{ind} x - s)}{n}} e^{2\pi i \frac{x}{p}}$$

La parte de esta expresión que corresponde a $k=0$, es igual a $-\frac{1}{n}$. La parte que corresponde a todos los valores positivos de k es en valor absoluto menor que (pregunta α))

$$\left(1-\frac{1}{n}\right)\sqrt{p}.$$

b. α) Para un valor de z dado, la congruencia $x^n \equiv z$ (mód. p) es posible solamente cuando ind z es divisible por δ, teniendo en este caso δ soluciones. Por lo tanto

$$S_{a,\,p}=1+\delta\sum_{z_0} e^{2\pi i\,\frac{az_0}{p}}=\delta\left(\frac{1}{\delta}+\sum_{z_0} e^{2\pi i\,\frac{az_0}{p}}\right),$$

donde z_0 recorre los números del sistema reducido de restos respecto del módulo p que cumplen la condición ind $z \equiv 0$ (mód. δ). Por lo tanto (pregunta a, δ))

$$S_{a,\,p}<\delta\left(1-\frac{1}{\delta}\right)\sqrt{p}=(\delta-1)\sqrt{p}.$$

β) Haciendo

$$x=u+p^{s-1}v;\ u=0,\ \ldots,\ p^{s-1}-1,\ v=0,\ \ldots,\ p-1,$$

se tiene

$$e^{2\pi i\,\frac{ax^n}{p^s}}=e^{2\pi i a\,(u^n p^{-s}+nu^{n-1}p^{-1}v)}.$$

Si $(u,\ p)=1$ la sumación respecto de v da cero. Por lo tanto

$$S_{a,\,p^s}=\sum_{x_0=0}^{p^{s-1}-1} e^{2\pi i a p^{n-s}x_0^n}=p^{s-1},\quad S'_{a,\,p^s}=0.$$

γ) Sea p^τ la máxima potencia de p que divide a n. Se tiene $s \geqslant \tau+3$. Haciendo

$$x=u+p^{s-1-\tau}v,\quad u=0,\ \ldots,\ p^{s-1-\tau}-1,\quad v=0,\ \ldots,\ p^{\tau+1}-1,$$

obtenemos

$$e^{2\pi i\,\frac{ax^n}{p^s}}=e^{2\pi i a\,(u^n p^{-s}+nu^{n-1}p^{-\tau-1}v)}.$$

Si $(u,\ p)=1$ la sumación respecto de v da cero. Por lo tanto

$$S_{a,\,p^s}=\sum_{x_0=0}^{p^{s-1}} e^{2\pi i\,\frac{ax_0^n}{p^{s-n}}}=p^{n-1}S_{a,\,p^{s-n}},\quad S'_{a,\,p^s}=0$$

δ) Sea $m=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ la *descomposición canónica del número* m. Haciendo

$$T_{a,m}=m^{-1+\nu}S_{a,m};\quad \nu=\frac{1}{n},\quad m=M_1p_1^{\alpha_1}=\dots=M_kp_k^{\alpha_k}$$

y determinando $a_1,\dots,a_k$ de la condición

$$a\equiv M_1a_1+\dots+M_ka_k\ (\text{mód. } m),$$

se tiene (pregunta 12, d, cap. III)

$$T_{a,m}=T_{a_1,p_1^{\alpha_1}}\dots T_{a_k,p^{\alpha_k}}.$$

Pero, si $s=1$, se tiene

$$|T_{a,p^s}|<p^{-1+\nu}n\sqrt{p}\leqslant np^{-\frac{1}{6}}.$$

Si $1<s\leqslant n$, $(n,p)=1$, se tiene

$$|T_{a,p^s}|=p^{-s+s\nu}p^{s-1}\leqslant 1.$$

Si $1<s\leqslant n$, $(n,p)=p$, se tiene

$$|T_{a,p^s}|\leqslant p^{-s+s\nu}p^s\leqslant p\leqslant n.$$

El caso $s>n$, en virtud de que $T_{a,p^s}=p^{-s+s\nu}p^{n-1}S_{a,p^{s-n}}=T_{a,p^{s-n}}$ *se reduce al caso* $s\leqslant n$. *Por lo tanto*

$$|T_{a,m}|\leqslant C=n^{ns+n},$$

de donde se deduce la desigualdad indicada en la pregunta.

12, a. Se deduce del teorema de la pregunta 11, a, α) y del teorema de la pregunta 12, a, α) cap. V.

b, α) Se tiene

$$Tn=\sum_{x=M}^{M+Q-1}\sum_{k=0}^{n-1}e^{2\pi i\frac{k(\operatorname{ind}x-s)}{n}}.$$

Para $k=0$, sumando respecto de x, resulta Q; para $k>0$ resulta un número cuyo módulo es menor que $\sqrt{p}\ln p$. *De aquí se deduce la* fórmula indicada en la pregunta.

β) Se deduce del teorema de la pregunta 12, a, β) cap. V y del teorema de la pregunta 11, a, δ).

c. Tomando $f(x)=1$, si x recorre los valores $x=\operatorname{ind}M$, $\operatorname{ind}(M+1),\dots,\operatorname{ind}(M+Q-1)$, *resulta (pregunta* 17, a, *cap.* II) $S'=\sum_{d\mid p-1}\mu(d)S_d$.

Aquí S' es el número de valores de x que cumplen la condición $(x,p-1)=1$;

por lo tanto, $S'=H$. Por otra parte, S_d es el número de valores de x que son múltiplos de d, es decir, es el número de restos de grado d que hay en la sucesión $M,\ M+1,\ \ldots,\ M+Q-1$. Por consiguiente,

$$H=\sum_{d\backslash p-1}\mu(d)\left(\frac{Q}{d}+\theta_d\sqrt{p}\ln p\right);\quad |\theta_d|<1,\quad \theta_1=0.$$

d. Del teorema de la pregunta **a** se deduce que se cumplen las condiciones de la pregunta **12, a, α)** cap. **V**, si se hace $m=p-1$, $\Phi(z)=1$, $\Delta=\sqrt{p}\ln p$, y z recorre los valores $z=\operatorname{ind} x$; $x=M,\ M+1,\ \ldots$ $\ldots,\ M+Q-1$. Entonces se obtiene (Q_1 en lugar de Q)

$$\sum_z{}'\,\Phi(z)=J,\qquad \sum_z\Phi(z)=Q,\quad J=\frac{Q_1}{p-1}Q+\theta\sqrt{p}\,(\ln p)^2.$$

13. Supongamos que no hay no-restos no superiores a h. La cantidad de no-restos de grado n que hay entre los números

$$1,\ \ldots,\ Q;\quad Q=[\sqrt{p}\,(\ln p)^2]$$

se puede acotar de dos modos:
Partiendo de la fórmula de la pregunta **12, b** y teniendo en cuenta que pueden ser no-restos solamente los números que son divisibles por números primos mayores que h. Resulta

$$1-\frac{1}{n}<\ln\frac{\frac{1}{2}\ln p+2\ln\ln p}{\frac{1}{c}\ln p+2\ln\ln p}+O\frac{1}{\ln p}.$$

$$0<\ln\frac{1+4\dfrac{\ln\ln p}{\ln p}}{1+2c\dfrac{\ln\ln p}{\ln p}}+O\left(\frac{1}{\ln p}\right).$$

La imposibilidad de la última desigualdad para todos los números p suficientemente grandes demuestra el teorema.
14, a. Se tiene

$$|S|^2\leqslant X\sum_{x=0}^{m-1}\sum_{y_1=0}^{m-1}\sum_{y=0}^{m-1}\rho(y_1)\overline{\rho(y)}\,e^{2\pi i\frac{ax(y_1-y)}{m}}.$$

Para valores dados de y_1 e y, la sumación respecto de x da $Xm\,|\rho(y)|^2$ o cero, según que sea $y_1=y$ o no. Por lo tanto

$$|S|^2\leqslant XYm,\quad |S|\leqslant\sqrt{XYm}.$$

b, α) Se tiene

$$S=\frac{1}{\varphi(m)}\sum_{u}\sum_{v}\chi(u)\,\chi(v)\,e^{2\pi i\frac{au^n+v^n}{m}},$$

donde u y v recorren los sistemas reducidos de restos respecto del módulo m. De aquí que

$$S=\frac{1}{\varphi(m)}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\nu(x)\,\rho(y)\,e^{2\pi i\frac{axy}{m}};$$

$$\nu(x)=\sum_{u^n\equiv x\,(\text{mód. }m)}\chi(u),\qquad \rho(y)=\sum_{v^n\equiv y\,(\text{mód. }m)}\chi(v).$$

Pero, se tiene (pregunta 11, cap. IV)

$$\sum_{x=0}^{m-1}|\nu(x)|^2\leqslant K\varphi(m),\qquad \sum_{y=0}^{m-1}|\rho(y)|^2\leqslant K\varphi(m).$$

Por lo tanto (pregunta a)

$$|S|\leqslant\frac{1}{\varphi(m)}\sqrt{K\varphi(m)\,K\varphi(m)\,m}=K\sqrt{m}.$$

β) Sea $m=2^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k}$ la descomposición canónica del número m. La congruencia $x^n\equiv 1$ (mód. m) es equivalente al sistema

$$x^n\equiv 1\ (\text{mód. }2^{\alpha}),\quad x^n\equiv 1\ (\text{mód. }p_1^{\alpha_1}),\ \dots,\ x^n\equiv 1\ (\text{mód. }p_k^{\alpha_k}).$$

Sean $\gamma(x)$ y $\gamma_0(x)$ los índices del número x respecto del módulo 2^{α} (g, § 6). La congruencia $x^n\equiv 1$ (mód. 2^{α}) es equivalente al sistema $n\gamma(x)\equiv 0$ (mód. c), $n\gamma_0(x)\equiv 0$ (mód. c_0). La primera congruencia de este sistema posee no más de 2 soluciones; la segunda posee no más de n soluciones. Por lo tanto, la congruencia $x^n\equiv 1$ (mód. 2^{α}) posee no más de $2n$ soluciones. Según b, § 5, cada una de las congruencias $x^n\equiv 1$ (mód. $p_1^{\alpha_1}$), ..., $x^n\equiv 1$ (mód. $p_k^{\alpha_k}$) posee no más de n soluciones. Por consiguiente,

$$K\leqslant 2\,(\tau(m))^{\frac{\ln n}{\ln 2}};\quad K=O(m^{\varepsilon}).$$

c, α) Fácilmente se observa que s recorre

$$U=(p-1)\left(1+\frac{1}{q_2}\right)\dots\left(1+\frac{1}{q_k}\right)^{2^{-k}}$$

valores, y s' recorre

$$V=(p-1)\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_k}\right)^{2^{-k}}$$

valores. Además, cuando t, para unos valores dados de s y s', recorre el sistema reducido de restos respecto del módulo $p-1$, el producto $(s+s')t$ también recorre el sistema reducido de restos respecto del módulo $p-1$. Por lo tanto, $W=UVS$. Pero, en virtud del teorema de la pregunta a, se tiene $|S_t|<\sqrt{UVp}$ y, por consiguiente, $W=\varphi(p-1)\sqrt{UVp}$. Comparando las dos expresiones halladas para W, se obtiene

$$S<\varphi(p-1)\sqrt{\frac{p}{UV}}=\frac{\varphi(p-1)}{p-1}\frac{2^k\sqrt{p}}{\sqrt{\left(1-\frac{1}{q_1^2}\right)\dots\left(1-\frac{1}{q_k^2}\right)}}<$$

$$<\frac{9}{8}\frac{\varphi(p-1)}{p-1}2^k\sqrt{p}.$$

β) Se deduce del teorema de la pregunta 12, a, α) cap. V y del teorema de la pregunta α).

γ) Se deduce del teorema de la pregunta 12, a, β) cap. V y del teorema de la pregunta α).

15, a. Se tiene

$$|S|^2=\sum_{t=1}^{p-1}\sum_{x=1}^{p-1}e^{2\pi i\frac{a(t^n-1)x^n+b(t-1)x}{p}}.$$

En el caso $t^n\equiv 1$ (mód. p), la sumación respecto de x da $p-1$ si $t=1$ y -1 si $t>1$. En el caso contrario, tomando $z(t-1)^{-1}$ en lugar de x la parte de la suma doble que corresponde al valor t elegido la expresamos en la forma

$$\sum_{x=1}^{p-1}e^{2\pi i\frac{a(t^n-1)(t-1)^{-n}x^n+bx}{p}}.$$

Por lo tanto

$$|S|^2\leqslant p-1+\Big|\sum_{u=1}^{p-1}\sum_{v=1}^{p-1}\nu(u)\rho(v)e^{2\pi i\frac{au+v}{p}}\Big|,$$

donde $\nu(u)$ no es superior al número de soluciones de la congruencia $(t^n-1)(t-1)^{-n}\equiv u$ (mód. p) con la condición $t>1$, y $|\rho(v)|$ no es superior al número de soluciones de la congruencia $x^n\equiv v$ (mód. p).

Por lo tanto, $v(u) \leqslant 2n_1$, $|\rho(v)| \leqslant n_1$,

$$\sum_{u=1}^{p-1} (v(u))^2 \leqslant (p-1)\,2n_1, \qquad \sum_{v=1}^{p-1} |\rho(v)|^2 \leqslant (p-1)\,n_1.$$

Aplicando el teorema de la pregunta **14, a,** obtenemos

$$|S|^2 \leqslant p-1+\sqrt{(p-1)\,2n_1\,(p-1)\,n_1 p} < 2n_1 p^{\frac{3}{2}}.$$

b, α) Se deduce del teorema de la pregunta **a** *y del teorema de la* **pregunta 12, a, α) cap. V.**

β) Del teorema de la pregunta α) se deduce que se cumplen las condiciones del teorema de la pregunta 12, a, α) cap. V si se hace $m=p$, $\Phi(z)=1$, $\Delta=\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}\ln p$, y z recorre los valores $z=Ax^n$; $x=M_0$, M_0+1, ..., M_0+Q_0-1. Por lo tanto

$$\sum_z{}' \Phi(z)=T, \qquad \sum_z \Phi(z)=Q_0,$$

de donde se deduce la fórmula indicada en la pregunta.

c, α) Supongamos que $\gamma \equiv 4a\gamma_1$ (mód. p). Se tiene (pregunta 11, a, cap. V)

$$\left(\frac{a}{p}\right) S=\sum_{x=0}^{p-1}\left(\frac{4a^2x^2+4abx+4ac}{p}\right) e^{2\pi i\,\frac{4a\gamma_1 x}{p}} =$$

$$=\frac{1}{U_{1,p}}\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)\sum_{x=0}^{p-1} e^{2\pi i\,\frac{z(4a^2x^2+4abx+4ac+4a\gamma_1 xz^{-1})}{p}} =$$

$$=\sum_{z=1}^{p-1} e^{2\pi i\,\frac{-(b^2-4ac)z-2b\gamma_1-\gamma_1^2 z^{-1}}{p}}$$

La última suma es en valor absoluto (pregunta **a**) $<\frac{3}{2}p^{\frac{3}{4}}$.

β) Se deduce del teorema de la pregunta α) y del teorema de la pregunta 12, a, α) cap. V.

Respuestas a los ejercicios numéricos

Respuestas a los ejercicios del capítulo I

1, a. 17. b. 23

2, a. α) $\delta_4 = \frac{15}{11}$; β) $\alpha = \frac{19}{14} + \frac{\theta}{14 \cdot 20}$.

b. α) $\delta_6 = \frac{80}{59}$; β) $\alpha = \frac{1002}{739} + \frac{\theta}{739 \cdot 1000}$.

3. En total se obtienen 22 fracciones.

5, a. $2^6 \cdot 3^5 \cdot 11^3$. b. $2^3 \cdot 3^3 \cdot 5^4 \cdot 7^3 \cdot 11^3 \cdot 17 \cdot 23 \cdot 37$.

Respuestas a los ejercicios del capítulo II

1, a. 1312.

b. $2^{118} \cdot 3^{50} \cdot 5^{31} \cdot 7^{19} \cdot 11^{15} \cdot 13^9 \cdot 17^7 \cdot 19^6 \cdot 23^5 \cdot 29^4 \cdot 31^4 \cdot 37^3 \cdot 41^3 \cdot 43^2 \times$
$\times 47^2 \cdot 53^2 \cdot 59^2 \cdot 61^2 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113$.

2, a. $\tau\,(5600) = 36$; $S\,(5600) = 15\,624$.

b. $\tau\,(116\,424) = 96$; $S\,(116\,424) = 410\,400$.

3. La suma de todos los valores es igual a 1.

4. α) 1152; β) 466 400.

5. La suma de todos los valores es igual a 774.

Respuestas a los ejercicios del capítulo III

1, a. 70. b. Es divisible.

2, a. $3^3 \cdot 5^2 \cdot 11^2 \cdot 2\,999$. b. $7 \cdot 13 \cdot 37 \cdot 73 \cdot 101 \cdot 137 \cdot 17 \cdot 19 \cdot 257$.

Respuestas a los ejercicios del capítulo IV

1, a. $x \equiv 81$ (mód. 337). b. $x \equiv 200$; 751; 1302; 1853; 2404 (mód. 2755).
2, b. $x \equiv 1630$ (*mód.* 2413).
3. $x \equiv 94 + 111\,t$; $y \equiv 39 + 47\,t$, donde t es un entero arbitrario.
4, a. $x \equiv 170b_1 + 52b_2$ (mód. 221);
$x \equiv 131$ (mód. 221); $x \equiv 110$ (mód. 221); $x \equiv 89$ (mód. 221).
b. $x \equiv 11\,151b_1 + 11\,800b_2 + 16\,875b_3$ (mód. 39 825).
5, a. $x \equiv 91$ (mód. 120). b. $x \equiv 8479$ (mód. 15 015).
6. $x \equiv 100$ (mód. 143); $y \equiv 111$ (mód. 143)
7, a. $3x^4 + 2x^3 + 3x^2 + 2x \equiv 0$ (mód. 5).
b. $x^5 + 5x^4 + 3x^3 + 3x + 2 \equiv 0$ (mód. 7).
8. $x^6 + 4x^5 + 22x^4 + 76x^3 + 70x^2 + 52x + 39 \equiv 0$ (mód. 101).
9, a. $x \equiv 16$ (mód. 27). b. $x \equiv 22$; 53 (mód. 64)
10, a. $x \equiv 113$ (mód. 125).
b. $x \equiv 43$, 123, 168, 248, 293, 373, 418, 498, 543, 623, (mód. 625).
11, a. $x \equiv 2, 5, 11, 17, 20, 26$ (*mód. 30*).
b. $x \equiv 76$, 22, 176, 122 (mód. 225).

Respuestas a los ejercicios del capítulo V

1, a. 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
b. 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35.
2, a. α) 0; β) 2. b. α) 0; β) 2.
3, a. α) 0; β) 2. b.α) 0; β) 2.
4, a. α) $x \equiv \pm 9$ (mód. 19); β) $x \equiv \pm 11$ (mód. 29);
γ) $x \equiv \pm 14$ (mód. 97).
b. α) $x \equiv \pm 66$ (mód. 311); β) $x \equiv \pm 130$ (mód. 277);
γ) $x \equiv \pm 94$ (mód. 353).
5, a. $x \equiv \pm 72$ (mód. 125). b. $x \equiv \pm 127$ (mód. 243).
6, a. $x \equiv 13, 19, 45, 51$ (mód. 64). b. $x \equiv 41, 87, 169, 215$ (mód. 256)

Respuestas a los ejercicios del capítulo VI

1, a. 6. b. 18.
2, a. 3, 3, 3. b. 5, 5, 5. c. 7.
5, a. α) 0; β) 1; γ) 3. b. α) 0; β) 1; γ) 10.
6, a. α) $x \equiv 40$; 27 (mód. 67). β) $x \equiv 33$ (mód. 67).
γ) $x \equiv 8$, 36, 28, 59, 31, 39 (mód. 67).
b. α) $x \equiv 17$ (mód. 73). β) $x \equiv 50$, 12, 35, 23, 61, 38 (mód. 73).
γ) $x \equiv 3$, 24, 46 (mód. 73).

7, a. α) 0; β) 4. b. α) 0; β) 7.
8, a. α) $x \equiv 54$ (mód. 101). β) $x \equiv 53, 86, 90, 66, 8$ (mód. 101).
b. $x \equiv 59, 11, 39$ (mód. 109).
9, a. α) 1, 4, 5, 6, 7, 9, 11, 16, 17; β) 1, 7, 8, 11, 12, 18.
b. α) 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36;
β) 1, 7, 9, 10, 12, 16, 26, 33, 34.
10, a. α) 7, 37; β) 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.
b. α) 3, 27, 41, 52;
β) 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59

TABLAS DE INDICES

NUMERO PRIMO 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

NUMERO PRIMO 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

NUMERO PRIMO 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

NUMERO PRIMO 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

NUMERO PRIMO 13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

NUMERO PRIMO 17

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

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

NUMERO PRIMO 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

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

NUMERO PRIMO 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

NUMERO PRIMO 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

NUMERO PRIMO 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

NUMERO PRIMO 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

NUMERO PRIMO 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

NUMERO PRIMO 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

NUMERO PRIMO 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

NUMERO PRIMO 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

NUMERO PRIMO 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

NUMERO PRIMO 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

NUMERO PRIMO 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

NUMERO PRIMO 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

NUMERO PRIMO 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

NUMERO PRIMO 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	12	33
7	20	60	22	66	40	41	44	53		

NUMERO PRIMO 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

NUMERO PRIMO 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

NUMERO PRIMO 97

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

TABLA
de los números primos <4070 y sus raíces primitivas mínimas

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1789	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

Continuación

p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	3	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3851	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	7	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	2	3881	13
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2647	3	2927	5	3299	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	5	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

INDICE ALFABÉTICO DE MATERIAS

INDICE

RESPUESTAS A LOS EJERCICIOS NUMERICOS