Lecciones populares
de matemáticas

DIVISIÓN INEXACTA

A. A. Belski
L. A. Kaluzhnin

$$\alpha = \alpha \cdot 1$$
$$\alpha = (-\alpha)(-1)$$
$$\alpha = (-\alpha i) \cdot i$$
$$\alpha = (\alpha i) \cdot (-i)$$

Editorial MIR Moscú


ИЗДАТЕЛЬСТВО МИР

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ

БЕЛЬСКИЙ А.А., КАЛУЖНИН Л.А.

ДЕЛЕНИЕ С ОСТАТКОМ

ИЗДАТЕЛЬСКОЕ ОБЪЕДИНЕНИЕ
«ВИЩА ШКОЛА»

LECCIONES POPULARES DE MATEMATICAS

A. A. BELSKI Y L. A. KALUZHNIN

DIVISIÓN INEXACTA

TRADUCIDO DEL RUSO POR EL INGENIERO
ANTONIO MOLINA GARCIA

EDITORIAL MIR
MOSCÚ

Impreso en la URSS

На испанском языке

INDICE

CAPÍTULO I

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

Este teorema es bien conocido por los escolares, los cuales suelen emplearlo en los cálculos aritméticos (por ejemplo, para hallar el denominador común de las fracciones), sin darse cuenta a veces de que se trata de un teorema importante que requiere una demostración rigurosa y detallada. Nos referimos a lo siguiente: todo número entero sabemos descomponerlo en un producto de números primos. Por ejemplo,

$$420 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$$

Si el número es suficientemente grande, en obtener la descomposición correspondiente se tarda bastante tiempo, no obstante siempre obtenemos esta descomposición. Pero, ¿no será que hasta ahora hemos tenido suerte simplemente? ¿Estamos seguros de que cualquier número entero se puede representar siempre en forma de un producto de números primos? Esto es así, efectivamente, pero este hecho requiere ser demostrado. La primera parte del teorema fundamental constituye precisamente la afirmación que sigue:

Todo número entero puede representarse en forma de un producto de números primos.

La demostración de esta afirmación se da más adelante.

Antes de enunciar la segunda afirmación del teorema volveremos a referirnos al ejemplo de la descomposición del número 420 en factores primos. En la escuela este proceso se escribe así:

420	2
210	2
105	3
35	5
7	7
1	,

lo que da la descomposición (1). Pero, ¿no pueden existir, acaso, otros métodos de descomposición? Y si existen, ¿dan

el mismo resultado? Es natural, por ejemplo, intentar descomponer el número dado en el producto de dos números menores (sin que tengan que ser necesariamente primos entre sí), y después, cada uno de ellos, en un producto de números menores y así sucesivamente hasta llegar a números que ya no se puedan seguir descomponiendo, es decir, que sean primos. Sin embargo, después de dar el primer paso queda ya claro que este proceso no es unívoco. En efecto, para el número 420, tenemos:

$$420 = 20 \cdot 21, \quad 420 = 15 \cdot 28.$$

Por lo tanto es completamente natural que se nos plantee la pregunta: ¿será posible la existencia de números enteros que puedan descomponerse por diversos procedimientos en producto de números primos? No, resulta que no hay tales números, y la afirmación correspondiente, es decir, la afirmación de que la descomposición del número en un producto de factores primos es unívoca, constituye precisamente la segunda parte del teorema fundamental:

Si cierto número n se puede descomponer por dos procedimientos en productos de factores primos

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

estas descomposiciones coinciden con una exactitud de hasta el orden de los factores: ambas tienen el mismo número de factores, es decir, $k = l$, y cada factor que figure en la primera descomposición, figurará la misma cantidad de veces en la segunda[1].

La demostración de esta afirmación la damos con bastante detalle. Es más difícil que la demostración de la afirmación primera, ya que está relacionada con una serie de propiedades de la aritmética de los números enteros.

---

[1] Si se consideran números enteros cualesquiera (tanto positivos como negativos), debe entenderse por unicidad de la descomposición en factores primos el que las dos descomposiciones $n = p_1 p_2 \cdots p_k$ y $n = q_1 q_2 \cdots q_l$ pueden diferir no sólo en el orden de los factores, sino también en los signos de los factores correspondientes.

§ 1. DIVISIÓN INEXACTA Y MÁXIMO COMÚN DIVISOR (M.C.D.) DE DOS NÚMEROS

El punto de partida para nuestros razonamientos siguientes es la afirmación de la posibilidad de la "división inexacta o entera" en el campo de los números enteros. Esta afirmación se enuncia así:

TEOREMA 1. *Sean a y b números enteros y $b \neq 0$. Entonces existen tales números enteros q y r, siendo $0 \leqslant r < |b|$, que*

$$a = qb + r. \tag{1}$$

Los números q y r se determinan por a y b unívocamente, es decir, si

$$a = q_1 b + r_1 = q_2 b + r_2,$$

donde $0 \leqslant r_i < |b|$, $i = 1, 2$, será $q_1 = q_2$ y $r_1 = r_2$. Si en la igualdad (1) $r = 0$, esto quiere decir que el número a es divisible por el número b y respectivamente se escribe

$$b \mid a$$

Observación. Para dos números enteros a y b las expresiones "el número a es divisible por el número b", "el número a es múltiplo de b", "el número b es divisor del número a" o, finalmente, "el número b divide al número a" tienen el mismo sentido; nosotros emplearemos cada una de ellas.

Demostremos que la representación (1) es posible. Primeramente sea $b > 0$. Advertimos que para cada número racional τ (lo mismo, por otra parte, que para cualquier número real) existe un número entero t tal, que $t \leqslant \tau < t + 1$. En particular, supongamos que este número entero t, hallado para $\tau = \frac{a}{b}$, es

$$t \leqslant \frac{a}{b} < t + 1.$$

De aquí

$$bt \leqslant a < bt + b \quad \text{y} \quad 0 \leqslant a - bt < b.$$

Supongamos que $q = t$ y $r = a - bt$, en este caso $a = bq + r$ y entonces, como se deduce de la última desigualdad, $0 \leqslant r < b$.

Hemos obtenido la representación (1) para el caso en que $b > 0$.

Sea ahora $b < 0$; volvemos a advertir que existe un número entero t tal, que

$$t < \frac{a}{b} \leqslant t + 1.$$

Multiplicando esta desigualdad por b y teniendo en cuenta que $b < 0$, obtenemos: $b(t+1) \leqslant a < bt$, de donde $0 \leqslant a - b(t+1) < -b$. Supongamos que $q = t + 1$ y $r = a - b(t+1)$. Volvemos a obtener la representación (1): $a = bq + r$, donde $0 \leqslant r < -b$, es decir, $0 < r < |b|$.

Queda por demostrar la unicidad. Sea

$$a = q_1 b + r_1 = q_2 b + r_2.$$

Entonces $b(q_1 - q_2) = r_2 - r_1$. Como $0 \leqslant r_i < |b|$, la diferencia $r_2 - r_1$ será menor, en valor absoluto, que $|b|$ y, por consiguiente, la división por b es aquí posible únicamente con la condición de que $r_2 - r_1 = 0$. Pero si $r_1 = r_2$, será $q_1 b = q_2 b$ y, por lo tanto, $q_1 = q_2$.

El número q se llama *cociente entero* y el número r, resto de la división del número a por el número b.

Por medio del teorema 1 puede introducirse el concepto de máximo común divisor de dos números y demostrar una serie de sus propiedades.

DEFINICIÓN 1. *Si a y b son dos números enteros distintos de cero y si el número c es tal que $c|a$ y $c|b$, este c se llama divisor común de los números a y b.*

Advertimos que dos números cualesquiera tienen siempre divisores comunes: estos son los números 1 y -1. Si no existen otros divisores comunes, los números a y b se llaman PRIMOS ENTRE SÍ. De los números primos entre sí hablaremos más adelante.

DEFINICIÓN 2. *Un número d se llama máximo común divisor (m. c. d.) de los números a y b si:* 1) *d es divisor común de los números a y b y* 2) *d es divisible por cualquier otro divisor común de los números a y b.*

Así, por ejemplo, 6 es el m. c. d. de los números 18 y 30, ya que $6|18$ y $6|30$ y, por otra parte, 6 es divisible por todos los divisores comunes de estos números: $1, -1, 2, -2, 3, -3, 6, -6$.

De esta definición no se deduce directamente que siempre exista un m. c. d. de dos números a y b arbitrarios. Ahora demostraremos que esto es así efectivamente; para ello empleare-

mos la descomposición de los números a y b en sus factores primos.

TEOREMA 2. *Para cualquier par de números enteros, $a \neq 0$ y $b \neq 0$, existe un m. c. d.*

DEMOSTRACIÓN. Al mismo tiempo que los números a y b consideremos también todos los números posibles de forma $xa + yb$, donde x e y son unos números enteros cualesquiera. Los números de la forma

$$v = xa + yb \tag{2}$$

se llaman *combinaciones lineales* de los números a y b. Por ejemplo, para $a = 6$ y $b = 22$ serán combinaciones lineales los números $28 = 1 \cdot 6 + 1 \cdot 22$, $10 = (-2) \cdot 6 + 1 \cdot 22$, $-92 = 3 \cdot 6 + (-5) \cdot 22$, etc. En general, para unos números dados a y b existe una infinidad de números que son combinaciones lineales suyas. Designemos el conjunto de estos números por medio de M. Advertimos que el conjunto M contiene, en particular, a los mismos números a (cuando $x = 1$, $y = 0$) y b (cuando $x = 0$, $y = 1$), así como al número 0 (cuando $x = 0$, $y = 0$). Todos los números v del conjunto M son, evidentemente, números enteros. Si v pertenece a M, también $-v$ pertenece a M (si $v = xa + yb$, será $-v = (-x)a + (-y)b$). Señalaremos otra propiedad más de los números v pertenecientes a M, que vamos a utilizar: *todos estos números son divisibles por todos los divisores comunes de los números a y b.* En efecto, si $c \mid a$ y $c \mid b$ y suponiendo que $a = a' \cdot c$ y $b = b' \cdot c$, resultará que $v = xa + yb = xa'c + yb'c = (xa' + yb')c$, es decir, $c \mid v$. Supongamos ahora que $d \neq 0$ es el número mínimo, respecto del módulo, de todos los números pertenecientes a M distintos de cero.

Este número existe realmente en el conjunto M. Debe advertirse que en el conjunto M están comprendidos números no iguales a cero (por ejemplo, a o b) y que sus módulos son enteros positivos, es decir, números naturales. Pero una de las propiedades fundamentales de los números naturales, que de ordinario se considera como axioma (véase I. S. SOMINSKI, "Método de inducción matemática", pág. 9, observación. Ed. en ruso), consiste en que, en todo conjunto no vacío de números naturales siempre está contenido un número mínimo.

Demostremos que d es el m. c. d. de los números a y b. La propiedad 2) de la definición de m. c. d. la tiene, puesto que la poseen todos los números pertenecientes a M. Sólo hay que establecer que también posee la propiedad 1), es decir, que d es

divisor común de los números a y b. Demostremos que $d|a$. Como d pertenece a M, $d = sa + tb$, donde s y t son números enteros. Efectuamos la división inexacta de a por d, es decir, hallamos unos números q y r, $0 \leqslant r < |d|$, tales, que

$$a = qd + r.$$

Pero entonces el resto r también debe pertenecer al conjunto M. En efecto,

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + tb.$$

Recordemos ahora que d es el número mínimo, respecto del módulo, entre todos los distintos de cero del conjunto M, y que r es menor que $|d|$. Por consiguiente, $r = 0$ y $d|a$. De un modo análogo se demuestra que $d|b$. El teorema queda demostrado.

Hemos establecido la existencia del m. c. d. de los números enteros distintos de cero. De la demostración de este teorema se deduce el teorema siguiente:

TEOREMA 3. *El m. c. d. de los números a y b puede representarse en forma de combinación lineal de estos números.*

Se nos plantea la pregunta: ¿está determinado unívocamente el m. c. d. de los números a y b? La respuesta, naturalmente, es negativa: si el número d posee las propiedades 1) y 2) de la definición del m. c. d., también las tiene $-d$. Pero con esto queda agotada la multiformidad. Efectivamente, sean d y d' dos m. c. d. de los números a y b. Como d posee la propiedad 2) y d', la propiedad 1), $d'|d$. De un modo análogo $d|d'$. Así, $\alpha = \frac{d}{d'}$ y $\frac{d'}{d} = \frac{1}{d/d'} = \frac{1}{\alpha}$ son números enteros. Pero los únicos números enteros, cuyos recíprocos también son enteros, son 1 y -1. Así, pues, $\alpha = 1$ ó $\alpha = -1$, de donde $d' = d$ o $d' = -d$. Si en la definición de m. c. d. hubiera la condición de que este número debe ser positivo (lo que a veces resulta conveniente), podría decirse que el m. c. d. de dos números enteros distintos de cero existe y está definido unívocamente.

En adelante designaremos el m. c. d. de los números a y b por medio de (a, b), como se admite en la literatura sobre la teoría de los números.

Pasemos a considerar un par de números primos entre sí. Antes ya nos hemos encontrado con este concepto.

DEFINICIÓN 3. *Se dice que dos números enteros $a \neq 0$ y $b \neq 0$ son primos entre sí, cuando su m.c.d. es igual a 1.*

En otras palabras, puede decirse que números primos entre sí son aquellos cuyos únicos divisores comunes son los números 1 y -1.

De lo dicho anteriormente (teorema 3) se deduce que si $(a, b) = 1$, 1 puede representarse de la forma:

$$1 = sa + tb, \tag{3}$$

donde s y t son números enteros. Recíprocamente, si la igualdad (3) se cumple para los respectivos s y t, serán a y b primos entre sí. En efecto (véase la demostración del teorema 1), $d = (a, b)$ es el número mínimo, respecto del módulo, entre los números distintos de cero de la forma $xa + yb$. Por consiguiente, si (3) se cumple, $|d| \leqslant 1$ y $d \neq 0$, de manera que $d = \pm 1$.

De lo dicho se deduce directamente una propiedad importantísima de los números primos entre sí:

TEOREMA 4. *Si $a \mid bc$ y $(a, b) = 1$*, será $a \mid c$ (esta propiedad se lee así: *si un número a divide al producto de dos números y es primo con uno de los factores, divide al otro factor).*

Demostración. Como $(a, b) = 1$, podrán encontrarse unos números s y t tales, que

$$1 = sa + tb. \tag{4}$$

Multiplicando esta igualdad por c, tenemos:

$$c = (sc)a + t(bc).$$

Los dos sumandos del segundo miembro son divisibles por a, por consiguiente, c es divisible por a.

TEOREMA 5. *Si un número a es primo con los números b y c, también es primo con el producto bc.*

Demostración. Como $(a, b) = 1$, podrán encontrarse unos números enteros s y t que satisfagan la igualdad

$$1 = sa + tb.$$

Análogamente, como $(a, c) = 1$,

$$1 = ua + vc$$

para los respectivos u y v. Multiplicando miembro a miembro las dos últimas igualdades, obtenemos:

$$1 = (sa + tb)(ua + vc) = sua^2 + savc + tbua + tbvc =$$
$$= (sua + svc + tbu)a + (tv)(bc).$$

Sea $m = sua + svc + tbu$ y $n = tv$, entonces m y n son números enteros y

$$1 = ma + n(bc),$$

por consiguiente, a y b son primos entre sí.

La afirmación del teorema que acabamos de demostrar puede extenderse fácilmente a un número arbitrario de factores:

TEOREMA 6. *Si a es primo con los números $b_1, b_2, \ldots, b_k$, es también primo con el producto de $b_1, b_2, \ldots, b_k$.*

La demostración de este teorema se hace por el método de inducción matemática respecto al número k de factores.

§ 2. TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

TEOREMA. *Cualquier número entero, distinto de cero, puede representarse en forma de un producto de números primos, siendo esta representación única con una exactitud de hasta el orden de los factores y sus signos.*

Demostración. EXISTENCIA DE LA DESCOMPOSICION DE UN NÚMERO RACIONAL ENTERO EN UN PRODUCTO DE NUMEROS PRIMOS. Al principio nos limitaremos al caso de números enteros positivos.

Observación. El número 1, por muchas causas, no se considera primo, a pesar de que no puede descomponerse en un producto de números menores. Entonces se plantea la pregunta: ¿en qué sentido es justo para el número 1 el teorema recién indicado? O, de otra forma, ¿en qué sentido el número 1 puede representarse en forma de producto de números primos?

Nosotros consideraremos que $1 = 1$ es la descomposición del número 1 en un producto de números primos, siendo el número de factores del segundo miembro igual a cero. Esta convencionalidad recuerda la definición de la potencia nula, $a^0 = 1$ (el número de factores a es igual a cero). Un convenio semjante aceptamos también para el número -1.

Aplicamos el método de inducción matemática:

a) Para $n = 1$ la igualdad $1 = 1$ es la representación buscada: 1 es el producto de un conjunto vacío de números primos.

b) Supongamos que para todos los números positivos m menores que n ya ha sido demostrada la posibilidad de la descomposición en un producto de números primos. Demostremos entonces que para el número n también será posible esta

descomposición. Si n es un número primo,

$$n = n$$

es la descomposición buscada (un factor primo). Si n es un número compuesto, será un producto $n = n_1 \cdot n_2$ de dos números enteros n_1 y n_2, cada uno de los cuales será distinto de 1 y de n y, por consiguiente, $n_1 < n$ y $n_2 < n$. Pero entonces, por el supuesto de inducción, la posibilidad de descomposición de los números n_1 y n_2 en un producto de números primos ya ha sido establecida:

$$n_1 = p_1 \cdot p_2 \cdots p_r,$$
$$n_2 = q_1 \cdot q_2 \cdots q_s,$$

donde p_j y q_i son números primos. Tenemos que: $n = p_1 \cdot p_2 \cdots p_r \times q_1 \cdot q_2 \cdots q_s$, es decir, hemos obtenido la descomposición buscada del número n.

Supongamos que n es un número entero negativo, entonces $-n$ será un número positivo. Como ya hemos demostrado, $-n$ puede descomponerse en un producto de números primos:

$$-n = p_1 \cdot p_2 \cdots p_k,$$
$$\text{Entonces } n = (-1) p_1 \cdot p_2 \cdots p_k,$$

o, por ejemplo,

$$n = (-p_1) p_2 \cdots p_k$$

es la descomposición buscada del número n. Con esto queda demostrada la primera parte del teorema.

Observación. Existen muchas demostraciones de la unicidad de la descomposición. La que vamos a dar no es la más corta ni es muy simple. Pero tiene la ventaja de que se extiende directamente a una serie de otros campos, por ejemplo, al de los polinomios de una variable y al de los números complejos enteros.

DEMOSTRACIÓN DE LA UNICIDAD DE LA DESCOMPOSICIÓN DE UN NÚMERO RACIONAL ENTERO EN UN PRODUCTO DE FACTORES PRIMOS

Advertimos que, por la definición de número primo, dos números primos diferentes son primos entre sí. La demostración del carácter unívoco de la descomposición vamos a hacerla por el método de inducción matemática según el valor absoluto del número n.

a) Si $|n| = 1$, $n = \pm 1$ y $1 = 1$, $-1 = -1$, es decir, se efectúa la unicidad de la descomposición para los números 1 y -1.

b) Supongamos que la propiedad que se demuestra ha sido ya establecida para todos los números m en que $|m| < |n|$. Sean

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l$$

dos descomposiciones del número n en los productos de los números primos $p_1, p_2, \ldots, p_k$ y $q_1, q_2, \ldots, q_l$, respectivamente. Nosotros afirmamos que el número primo p_k se encuentra entre los números primos $q_1, \ldots, q_l$ o que puede ser opuesto a alguno de ellos. En efecto, si esto no fuera así, es decir, $p_k \neq q_i$, $i = 1, 2, \ldots, l$, sería p_k primo con todos los números q_i y, por consiguiente, de acuerdo con el teorema 6, sería primo con sus productos, o sea, con el número n. Pero esto es imposible, ya que $p_k | n$, es decir, $(p_k, n) = p_k$. Así, pues, p_k es igual a alguno de los números primos $\pm q_i$. Sea $p_k = q_l$ (en caso contrario esta igualdad podría conseguirse cambiando el orden de los factores q_i, y si a pesar de todo $p_k = -q_l$, cambiaríamos los signos de q_l y, respectivamente, de cualquier otro q_i).

Así, obtenemos:

$$n = p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k = q_1 \cdot q_2 \cdots q_{l-1} \cdot p_k,$$

de donde

$$m = \frac{n}{p_k} = p_1 \cdot p_2 \cdots p_{k-1} = q_1 \cdot q_2 \cdots q_{l-1}.$$

Pero $|m| < |n|$ y, por el supuesto de inducción, para m ya está demostrada la afirmación del teorema, es decir, $k - 1 = l - 1$. Las sucesiones $p_1, p_2, \ldots, p_{k-1}$ y $q_1, q_2, \ldots, q_{l-1}$ contienen, con una exactitud de hasta los signos, los mismos números primos, y los correspondientes números primos entran en ambas representaciones el mismo número de veces, y como $p_k = q_l$, esto es también justo para las sucesiones $p_1, p_2, \ldots, p_{k-1}, p_k$ y $q_1, q_2, \ldots, q_{l-1}, q_l$. El teorema queda demostrado.

§ 3. ALGORITMO DE EUCLIDES Y SOLUCIÓN DE LAS ECUACIONES DIOFÁNTICAS LINEALES CON DOS INCÓGNITAS

De acuerdo con el teorema 2, dos números enteros a y b tienen m. c. d. Veamos ahora uno de los procedimientos para hallar el m. c. d., el cual fue indicado ya por Euclides en sus "Elementos" y se llama ALGORITMO DE EUCLIDES. En este caso vamos a considerar que $|a| \geqslant |b|$.

PRIMER PASO. Efectuamos la división inexacta de a por b:

$$(1)\quad a = q_1 \cdot b + r_1,\ 0 \leqslant r_1 < |b|.$$

Si $r_1 = 0$, $b|a$ y $(a, b) = b$. Si $r_1 \neq 0$, hacemos lo siguiente:

SEGUNDO PASO. Dividimos b por r_1:

$$(2)\quad b = q_2 \cdot r_1 + r_2,\ 0 \leqslant r_2 \leqslant r_1.$$

Si $r_2 \neq 0$, pasamos al tercer paso:

TERCER PASO.

$$(3)\quad r_1 = q_3 \cdot r_2 + r_3,\ 0 \leqslant r_3 \leqslant r_2$$

y así sucesivamente. En cada paso el nuevo resto es menor que el resto del paso anterior:

$$|b| > r_1 > r_2 > \ \ldots$$

y en algún paso k-ésimo $(k < |b|)$ el resto será nulo: Paso k-ésimo:

$$r_{k-2} = q_{k1} r_{k-1}.$$

Demostremos que el último resto no igual a cero, r_{k-1}, es el m. c. d. buscado de los números a y b. Efectivamente, tenemos la cadena de igualdades:

$$(1)\quad a = q_1 \cdot b + r_1;$$

$$(2)\quad b = q_2 \cdot r_1 + r_2;$$

$$(3)\quad r_1 = q_3 \cdot r_2 + r_3;$$

$$\vdots \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(k-1)\quad r_{k-3} = q_{k-1} \cdot r_{k-2} + r_{k-1};$$

$$(k)\quad r_{k-2} = q_k \cdot r_{k-1}.$$

De la última igualdad se deduce que $r_{k-1}|r_{k-2}$, de la penúltima, que $r_{k-1}|r_{k-1}$ y $r_{k-1}|r_{k-2}$ y, por consiguiente, $r_{k-1}|r_{k-3}$,

y elevándose de este modo hacia las primeras igualdades, concluimos que $r_{k-1} \mid r_2, r_{k-1} \mid r_1, r_{k-1} \mid b$ y $r_{k-1} \mid a$. De aquí que r_{k-1} sea divisor común de los números a y b.

Supongamos ahora que $c|a$ y $c|b$. Entonces, de las igualdades (1), (2), ..., $(k-1)$ obtenemos sucesivamente: $c|r_1$, $c|r_2$, ..., $c|r_{k-1}$.

Por lo tanto, r_{k-1} es, en efecto, el m. c. d. de los números a y b.

Resolvamos el ejemplo siguiente: $a = 858$ y $b = 253$. Hallar el m. c. d. de estos números.

Tenemos:

(1) $858 = 3 \cdot 253 + 99$;

(2) $253 = 2 \cdot 99 + 55$;

(3) $99 = 1 \cdot 55 + 44$;

(4) $55 = 1 \cdot 44 + 11$;

(5) $44 = 4 \cdot 11$,

de donde $(858, 253) = 11$. Como vemos, valiéndose del algoritmo de Euclides, el m. c. d. de dos números se halla sin descomponer estos números en los factores primos.

En el teorema 3 establecimos que $(a, b) = d$ puede escribirse de la forma:

$$d = s \cdot a + t \cdot b,$$

pero en la demostración no se indicó cómo se hallan los respectivos números s y t. Esto se hace muy fácilmente aplicando el algoritmo de Euclides. No vamos a exponer esta solución en el caso general, sino que la analizaremos en el ejemplo que antes hemos puesto.

Así, pues, hay que hallar unos números enteros s y t tales que

$$11 = s \cdot 858 + t \cdot 253.$$

De las igualdades (4), (3), (2), (1) obtenemos sucesivamente que:

$11 = 55 + (-1) \cdot 44$,

$44 = 99 + (-1) \cdot 55$,

$55 = 253 + (-2) \cdot 99$,

$99 = 858 + (-5) \cdot 253 \cdot 17$

Sustituyendo ahora en la primera igualdad la expresión de 44

que da la segunda, después la de 55 que da la tercera y así sucesivamente, obtenemos:

$$11 = 55 + (-1)\cdot(99 + (-1)\cdot 55) = 2\cdot 55 + (-1)\cdot 99 =$$
$$= 2\cdot(253 + (-2)\cdot 99) +$$
$$+ (-1)\cdot 99 = 2\cdot 253 + (-5)\cdot 99 = 2\cdot 253 +$$
$$+ (-5)\cdot(858 + (-3)\cdot 253) =$$
$$= (-5)\cdot 858 + 17\cdot 253.$$

Por consiguiente, $s = -5$, $t = 17$.

Las igualdades que aparecen en el algoritmo de Euclides al hallar el m. c. d. de los números a y b permiten resolver en números enteros la ecuación de la forma

$$d = xa + yb,$$

donde $d = (a, b)$.

En general, una ecuación de la forma

$$xa + yb = c,$$

donde a, b, c son números enteros dados, para la cual hay que hallar la solución en números enteros de x, se llama *ecuación diofántica lineal* con dos incógnitas. Se llama lineal porque las incógnitas x e y figuran en ella en primera potencia. El término "diofántica" indica que los coeficientes de la ecuación son números enteros y que las soluciones también son números enteros.

Observación. "Diofántica" viene del nombre del matemático griego de la antigüedad Diofanto (250 d. n. e., aproximadamente), el cual, en su libro "Aritmética", estudió las ecuaciones indeterminadas con soluciones únicamente enteras; más adelante nos detendremos en las ecuaciones cuadráticas diofánticas.

Debe advertirse que ya sabemos resolver las ecuaciones lineales diofánticas del tipo

$$xa + yb = c. \qquad (1)$$

Pero tenemos que analizar el problema de todas las soluciones de esta ecuación más detalladamente. Indicaremos, para empezar, que no toda ecuación de este tipo tiene solución. En efecto, si la ecuación (1) tiene solución en números enteros, por ejemplo, $x = x_0$, $y = y_0$, es decir, $c = x_0 a + y_0 b$, y si $d = (a, b)$, como $d \mid a$ y $d \mid b$, el número d divide a los dos sumandos del segundo

miembro y, por consiguiente, divide también a c. De aquí hacemos la siguiente deducción:

Para que exista una solución entera de la ecuación (1) *es necesario que el segundo miembro de esta ecuación sea divisible por el m. c. d. de los números a y b.*

Por ejemplo la ecuación

$$9x + 15y = 7$$

no tiene solución numérica entera, ya que 7 no es divisible por $3 = (9, 15)$. Si, por el contrario, en la ecuación (1) $d|c$, ésta tiene solución en números enteros e incluso sabemos cómo hallarla. Efectivamente, sea $c = c' \cdot d$ y supongamos que s y t son unos números enteros tales, que

$$d = a \cdot s + b \cdot t.$$

Entonces

$$c = c' \cdot d = a(sc') + b(t \cdot c'),$$

es decir, $x_0 = sc'$ e $y_0 = t \cdot c'$ son la solución de la ecuación (1).

Resolvamos, por ejemplo, la ecuación diofántica

$$33 = 858x + 253y: \qquad (2)$$

Antes demostramos que

$$11 = 858 \cdot (-5) + 253 \cdot 17.$$

Multiplicando esta ecuación por 3 término a término, obtenemos

$$33 = 858 \cdot (-15) + 253 \cdot 51.$$

Así, $x = -15$ e $y = 51$ son la solución de la ecuación (2). Pero no debe pensarse que la solución hallada es única. En general, resulta que si una ecuación diofántica del tipo (1) tiene solución, dicha ecuación tiene infinitas soluciones. Ahora analicemos esta cuestión con más detalle: vamos a demostrar la afirmación enunciada y a hallar la forma general de todas las soluciones posibles de la ecuación (1).

Hallemos primero la forma general de la solución. Supongamos que la ecuación (1), además de la solución en números enteros x_0 e y_0, tiene también la solución x_1 e y_1. Entonces

$$c = ax_0 + by_0; \quad c = ax_1 + by_1.$$

Restando la segunda igualdad de la primera, obtenemos

$$a(x_0 - x_1) + b(y_0 - y_1) = 0,$$

o bien

$$a(x_0 - x_1) = b(y_1 - y_0). \tag{3}$$

Si $d = (a, b)$, obtenemos que $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, es decir,

$$a = a'd;$$
$$b = b'd.$$

Donde a' y b' son números primos entre sí. Simplificando por d la igualdad (3), llegamos a la igualdad

$$a'(x_0 - x_1) = b'(y_1 - y_0).$$

Pero como a' y b' son primos entre sí, $a' \mid (y_1 - y_0)$ y, análogamente, $b' \mid (x_0 - x_1)$. Suponiendo que

$$y_1 - y_0 = a'k_1;$$
$$x_0 - x_1 = b'k_2,$$

tenemos que: $a'b' \cdot k_1 = a'b' \cdot k_2$, de donde $k_1 = k_2 = k$. De este modo, en definitiva, obtenemos:

$$y_1 = y_0 + a'k = y_0 + \frac{a}{d}k; \tag{4}$$

$$x_1 = x_0 - b'k = x_0 - \frac{b}{d}k, \tag{5}$$

donde k es cierto número entero. Recíprocamente, es fácil comprobar que si x_0 e y_0 son una solución en números de la ecuación (1), todos los pares de números de la forma (4) y (5), cualquiera que sea el número entero k, darán soluciones de la ecuación (1). En efecto,

$$ax_1 + by_1 = a(x_0 - \frac{b}{d}k) + b(y_0 + \frac{a}{d}k) =$$

$$= ax_0 + by_0 + \left(-\frac{ab}{d}k + \frac{ab}{d}k\right) = c + 0 = c.$$

Así, pues, si x_0 e y_0 son soluciones en números enteros de la ecuación (1), todos los números de la forma $x_0 - \frac{b}{d}k$, $y_0 + \frac{a}{d}k$, donde k es un número entero cualquiera, serán también soluciones de esta ecuación (el número de dichas soluciones será infinito, siendo una para cada k), y otras soluciones no existen.

§ 4. NÚMEROS PITAGÓRICOS

El método por el cual hemos hallado la solución de la ecuación diofántica lineal con dos incógnitas, y principalmente la forma en que se dio la respuesta, se emplean para resolver el siguiente problema clásico:

Hallar todas las series de tres números enteros a, b, c, para las cuales

$$a^2 + b^2 = c^2. \tag{1}$$

Estas series de tres números se llaman PITAGÓRICAS, porque si a, b, c no son nulos y satisfacen la ecuación (1), siempre existe un triángulo rectángulo único cuyos lados son a, b, c. En efecto, si los segmentos a y b se toman sobre los lados que forman el ángulo recto, como muestra la fig. 1, y se unen sus extremos A y B, según el teorema de Pitágoras $AB^2 = a^2 + b^2 = c^2$, es de-

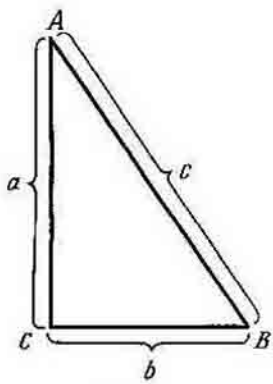

Fig. 1

cir, $AB = c$. La unicidad del triángulo ABC para los números a, b, c dados se deduce del criterio de igualdad de los triángulos respecto de sus tres lados. Examinemos, pues, detalladamente una serie de números pitagóricos a, b, c, suponiendo cumplida la igualdad (1).

Si $c = 0$, necesariamente $a = b = 0$. Por esto basta tomar únicamente el caso $c \neq 0$. De la igualdad (1) obtenemos:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1. \tag{2}$$

Supongamos que $\frac{a}{c} = x$ y $\frac{b}{c} = y$. Entonces la relación (2) toma la forma

$$x^2 + y^2 = 1. \tag{3}$$

Si podemos hallar todas las soluciones racionales (y no sólo enteras) de la ecuación (3), al mismo tiempo obtendremos la respuesta al problema de las series de números pitagóricos. Efectivamente, si (x, y) es la solución de la ecuación (3), cualquier serie de tres números $(\alpha x, \alpha y, \alpha)$ (donde α sea un número entero tal, que αx y αy también sean enteros) será pitagórica: la igualdad $\alpha^2 x^2 + \alpha^2 y^2 = \alpha^2$ se obtiene de (3) multiplicándola por α^2. Por esto veamos todas las soluciones racionales de la ecuación (3).

Ante todo, la ecuación (3) es equivalente a la ecuación

$$x^2 = 1 - y^2. \tag{3'}$$

Si del conjunto de todas las soluciones de esta ecuación se excluye la solución $x = 0$, $y = \pm 1$, todas las demás soluciones constituirán el conjunto de soluciones de la ecuación

$$\frac{x}{1-y} = \frac{1+y}{x}. \tag{4}$$

Sean

$$\frac{x}{1-y} = u, \quad \frac{1+y}{x} = v. \tag{5}$$

Los números u y v, evidentemente, serán también racionales, y x e y se expresarán por medio de ellos así:

$$x = \frac{2u}{uv+1}, \quad y = \frac{uv-1}{uv+1}. \tag{6}$$

(El lector puede comprobar fácilmente que las igualdades (6) son correctas, resolviendo el sistema (5) con respecto a x e y). La ecuación (4) en términos de u y v tiene una forma muy simple:

$$u = v. \tag{7}$$

De este modo, si $(x = x_0, y = y_0)$ es solución de la ecuación (4), será $(u_0 = \frac{x_0}{1 - y_0}, v_0 = \frac{1 + y_0}{x_0})$ solución de la ecuación (7) y, recíprocamente, si (u_0, v_0) es solución de la ecuación (7), será (véanse las fórmulas (6)) $(x_0 = \frac{2v_0}{u_0 v_0 + 1}, y_0 = \frac{u_0 y_0 - 1}{u_0 v_0 + 1})$ solución de la ecuación (4).

Pero todas las soluciones de la ecuación (7) se obtienen así: a las incógnitas u y v hay que atribuirles todos los valores racionales posibles iguales. Por consiguiente, todas las soluciones de la ecuación (4) vienen dadas por las fórmulas (6) cuando u y v son iguales a un mismo número t, pero racional arbitrario:

$$\begin{cases} x = \dfrac{2t}{t^2 + 1}, \\ y = \dfrac{t^2 - 1}{t^2 + 1}. \end{cases} \tag{8}$$

Supongamos que $t = \frac{m}{n}$ es una fracción irreducible. Entonces el sistema (8) toma la forma

$$\begin{cases} x = \dfrac{2mn}{m^2 + n^2}, \\ y = \dfrac{m^2 - n^2}{m^2 + n^2}. \end{cases} \tag{9}$$

Así son todos los números racionales x e y que satisfacen la ecuación (4). Sustituyendo m y n por valores enteros arbitrarios, simultaneamente no iguales a cero, obtenemos la solución de la

ecuación (4). Advertimos que si $m = 0$, $n = 1$ tenemos la solución: $x = 0$, $y = -1$, y si $m = 1$ y $n = 0$, la solución $x = 0$, $y = 1$. Estas dos soluciones fueron antes excluidas para poder efectuar correctamente las transformaciones, pero ahora, como puede verse, no se han perdido. Así, pues, cualesquiera que sean los enteros m y n, no iguales simultaneamente a cero, la serie de tres números enteros

$$2mn,\ m^2 - n^2,\ m^2 + n^2 \tag{10}$$

será pitagórica. Más aún, como ya dijimos, es pitagórica toda serie de tres números enteros

$$2\alpha mn,\ \alpha(m^2 - n^2),\ \alpha(m^2 + n^2) \tag{10'}$$

siendo α cualquier número racional admisible (en particular, $\alpha = 0$). Recordaremos que empezamos con la igualdad (1) y después, sucesivamente, pasamos de ella, mediante las igualdades (2)—(8), a la igualdad (9), es decir, a las igualdades

$$\frac{a}{c} = \frac{2mn}{m^2 + n^2}, \tag{9'}$$

$$\frac{b}{c} = \frac{m^2 - n^2}{m^2 + n^2}.$$

Supongamos que $a = 2mn\rho_1$, $b = (m^2 - n^2)\rho_2$, $c = (m^2 + n^2)\rho_3$, siendo ρ_1, ρ_2, ρ_3 ciertos números racionales. Entonces de la primera igualdad de (9') se deduce que $\frac{\rho_1}{\rho_2} = 1$, y de la segunda, que $-\frac{\rho_2}{\rho_3} = 1$, es decir, $a = 2mn\alpha$, $b = (m^2 - n^2)\alpha$, $c = (m^2 + n^2)\alpha$, siendo α cierto número racional.

Queda por aclarar cuál puede ser el denominador del número racional α. Como el número $2mn\alpha$ es entero, los divisores del denominador de α pueden ser únicamente los divisores de los números m, n y 2. Por otra parte, como $(m^2 - n^2)\alpha$ es un número entero, los divisores del denominador del número α deben ser divisores del número $m^2 - n^2$, y por esto entre ellos no hay divisores de los números m y n, ya que $(m, n) = 1$ por la condición. Por lo tanto, el número α es entero o racional con de-

nominador 2. En el útimo caso los números m y n son impares simultaneamente.

De este modo llegamos al teorema:

TEOREMA. *Una serie de tres números* (a, b, c) *es pitagórica si, y solamente si, tiene la forma* $(2\alpha mn, \alpha(m^2 - n^2), \alpha(m^2 + n^2))$, *donde* m *y* n *son números enteros primos entre sí y* α *es un número entero cualquiera; si* m *y* n *son impares, el número* α *no sólo puede ser entero, sino también un número de la forma* $\frac{p}{2}$, *siendo* p *un número impar.*

Por ejemplo, suponiendo $m = 2$, $n = 1$, $\alpha = 1$, obtenemos la serie de tres números pitagóricos 4, 3, 5, y con ella también las series pitagóricas de los mismos m y n, pero con otros α: (12, 9, 15); (20, 15, 25), etc.

En el antiguo Egipto las series de números pitagóricos se utilizaban para construir ángulos rectos. Si entre los números a, b, c existe la relación (1), el triángulo cuyos lados son a, b, c es un triángulo rectángulo. La construcción de un triángulo conociendo sus tres lados se efectúa fácilmente, valiéndose de un compás y una regla: tomando los extremos del segmento c como centros, se describen arcos con los radios a y b respectivamente, y su punto de intersección se une con los extremos del segmento c. En la práctica los segmentos a, b, c eran trozos de cuerda entre cuyas longitudes existía la misma relación que entre los números de una serie pitagórica cualquiera. Por ejemplo, 3:4:5.

EJERCICIOS

1. Hallar todos los números enteros x tales, que la expresión $x^3 + 2x + 7$, al ser dividida por 5, de 2 de resto.

2. Suponiendo que m es un número natural, $m > 1$, y que $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ es un polinomio con coeficientes enteros a_0, a_1, ..., a_n. Demostrar que, si x es un número entero, el resto de la división de $f(x)$ por m depende únicamente del resto del número x al ser dividido por m.

3. Demuéstrese que $d = \text{m.c.d.}\ (a, b)$ y $-d$ son los únicos divisores comunes de los números a y b, los cuales pueden representarse en forma de combinación lineal de los números a y b.

4. Demuéstrese que el número de pasos en el algoritmo de Euclides puede ser tan grande como se desee.

5. Hallar el m. c. d. (a, b) y representarlo en la forma $\alpha a + \beta b$ para: a) $a = 127$, $b = 211$; b) $a = 111\,111$, $b = 111$; c) $a = 191$, $b = 291$.
6. Demostrar que el m. c. d. $(a, b) = $ m. c. d. $(a, a + b) = $ m. c. d. $(a, a - b)$.
7. Hallar todas las soluciones en números enteros de las ecuaciones: a) $2x + 3y = 5$; 2) $10x + 2y = 5$; c) $121x + 1331y = 11$.
8. Demostrar que si p es un número primo, $\sqrt{p}$ es un número irracional.
9. Hallar todas las series de números pitagóricos a, b, c, para las cuales $|c| < 100$.

CAPÍTULO II

ARITMÉTICA DE LOS NÚMEROS GAUSIANOS

§ 1. NÚMEROS GAUSIANOS Y NÚMEROS GAUSIANOS ENTEROS

Los "números complejos enteros" o "números gausianos enteros", como suelen también llamarse en honor del gran matemático alemán K. F. GAUSS quien fue el primero que los estudió detalladamente, son la generalización natural de los números racionales enteros.

DEFINICIÓN. 1 *Se llama número gausiano entero el número complejo cuyas partes real e imaginaria son números racionales enteros. Dicho de otro modo, los números gausianos enteros son números complejos* α *de la forma*

$$\alpha = a + bi,$$

donde a y b son números racionales enteros. Además de los números gausianos enteros necesitaremos los números (simplemente) gausianos, es decir, los números complejos en los cuales las partes real e imaginaria son números racionales.

La relación entre los campos de los números gausianos y los números gausianos enteros es análoga a la relación entre los números racionales y los números racionales enteros. Más exactamente, se tienen en cuenta las afirmaciones siguientes, que en adelante emplearemos con frecuencia sin reserva especial y que el lector puede comprobar directamente sin dificultad:

II. *La suma, la diferencia, el producto y el cociente (en el caso en que el divisor no sea igual a cero) de dos números gausianos son también números gausianos* (esta propiedad se expresa

abreviadamente diciendo que los números gausianos forman un CAMPO).

III. *El cociente de dos números gausianos enteros es un número gausiano y, viceversa, todo número gausiano puede representarse como un cociente de dos números gausianos enteros.*

Esta afirmación requiere una breve explicación: supongamos que $\alpha = a + bi$ y $\beta = c + di$ son números gausianos enteros (es decir, a, b, c, d son números racionales enteros) y sea $\beta \neq 0$. Demostremos que $\gamma = \alpha/\beta$ es un número gausiano. En efecto,

$$\gamma = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd+bci-adi}{c^2+d^2} =$$

$$= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i.$$

Los números $\frac{ac+bd}{c^2+d^2}$ y $\frac{bc+ad}{c^2+d^2}$ (partes real e imaginaria del número γ) son números racionales y, por consiguiente, γ es un número gausiano.

Indicaremos por fin, que es evidente que todo número racional es gausiano (con parte imaginaria nula) y que todo número racional entero es un número gausiano entero.

Veamos la distribución de los números gausianos enteros en un plano complejo. Por definición los números gausianos enteros se representan mediante puntos cuyas coordenadas son números enteros (fig. 2). Se encuentran en los vértices de la red de cuadrados cuyo lado es igual a 1, la cual cubre el plano complejo.

En adelante no harán falta los conceptos de norma y módulo del número complejo. Se llama NORMA de un número complejo $\alpha = x + iy$ el número real no negativo $N(\alpha) = x^2 + y^2$; se denomina MÓDULO de un número complejo α (y se designa por $|\alpha|$) el número real $\sqrt{x^2+y^2}$. El módulo geométrico de un número complejo es la distancia, en el plano complejo, desde el origen de coordenadas al punto correspondiente. La norma $N(\alpha)$ del número α puede representarse como un producto, $N(\alpha) = \alpha \cdot \bar{\alpha}$, donde $\bar{\alpha}$ es el número complejo conjugado $x - iy$ del número α. También se considera conocida la propiedad multiplicativa de

la norma, es decir,

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta). \qquad (2)$$

Advertiremos inmediatamente que si α es un número gausiano, $N(\alpha)$ será un número racional no negativo, y si α es un número gausiano entero, $N(\alpha)$ será un número entero no negativo.

Observación. El módulo $|\alpha|$ de un número gausiano ya no será siempre un número racional, por esto, en adelante utilizaremos principalmente la norma y no el módulo.

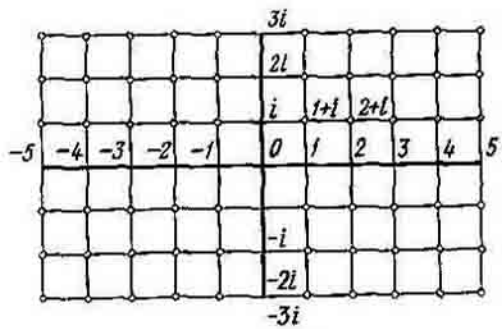

Fig. 2

Sin embargo, no todo número racional entero y positivo es norma de un número gausiano entero. En efecto, demostremos el teorema siguiente:

TEOREMA 1: *Un número racional entero y positivo c es norma de un número gausiano entero determinado si, y solamente si, el número c puede representarse en forma de suma de los cuadrados de dos números enteros.*

Demostración. Si $\alpha = a + bi$ es un número gausiano entero, $N(\alpha) = a^2 + b^2$ es la suma de los cuadrados de los números enteros a y b. Y al contrario, si $c = x^2 + y^2$, donde x e y son números racionales enteros, $c = N(x + yi)$, donde $x + iy$ es un número gausiano entero. El teorema queda demostrado.

No es difícil demostrar que no todo número entero positivo puede representarse en forma de suma de dos cuadrados. Así,

por ejemplo, si un número entero, positivo, impar t puede representarse en forma de suma de dos cuadrados de números enteros, al dividirlo por 4 da un resto igual a 1, es decir, es un número de la forma $t = 4k + 1$. Efectivamente, sea $t = x^2 + y^2$, entonces uno de los números, x por ejemplo, debe ser par, y el otro, y, impar. Supongamos que $x = 2m$ e $y = 2n + 1$. Por consiguiente, $x^2 = 4m^2$ e $y^2 = 4(n+n) + 1$ y, en definitiva, $t = 4(m^2 + n^2 + n) + 1$, lo que demuestra nuestra afirmación. Así, pues, los números 7, 11, 15 y otros no pueden representarse en forma de suma de dos cuadrados y, por lo tanto, no son normas de números gausianos.

La cuestión de qué números enteros pueden representarse en forma de suma de dos cuadrados o, lo que es lo mismo, qué números son normas de números gausianos enteros, la aclararemos como resultado del estudio de la aritmética de los números gausianos enteros.

Tanto en el campo (anillo) de los números racionales enteros, como en el de los números gausianos enteros, el interés fundamental recae sobre la cuestión de la divisibilidad.

Diremos que *el número gausiano entero* α *divide al número gausiano entero* β (*esto se escribe así:* $\alpha \mid \beta$), *si para cierto número gausiano entero* γ *se efectúa la igualdad*

$$\beta = \alpha \cdot \gamma. \tag{3}$$

Como de (3) se deduce que $N(\beta) = N(\alpha) \cdot N(\gamma)$, la condición necesaria para que $\alpha \mid \beta$ es la divisibilidad $N(\alpha) \mid N(\beta)$, donde $N(\alpha)$ y $N(\beta)$ son números racionales enteros.

En el caso de números racionales enteros sólo existen dos que dividen a todos ellos: $+1$ y -1; en el caso de números gausianos enteros hay cuatro de este tipo: $+1$, -1, $+i$, $-i$. En efecto,

$$\alpha = \alpha \cdot 1,$$
$$\alpha = (-\alpha)(-1),$$
$$\alpha = (-\alpha i) \cdot i,$$
$$\alpha = (\alpha i) \cdot (-i).$$

Entre los números gausianos enteros no existen otros con las propiedades dadas. Efectivamente, si cierto número gausiano entero ξ divide a todos los números gausianos enteros, en parti-

cular deberá dividir al número 1 (por esto dichos números se llaman *divisores de la unidad*). De $N(\xi) \mid 1$ se deduce que $N(\xi) = 1$. Si $\xi = x + iy$, será $x^2 + y^2 = 1$. Es evidente que esta ecuación tiene exactamente cuatro soluciones en números racionales enteros: $x = 1$, $y = 0$; $x = -1$, $y = 0$; $x = 0$, $y = 1$; $x = 0$, $y = -1$, las cuales corresponden a los números gausianos enteros $+1$, -1, i, $-i$.

Para los números gausianos enteros, de un modo análogo a como esto se hizo para los números racionales, se definen los conceptos de divisor común, máximo común divisor, números primos entre sí y números primos. Los primeros tres conceptos se definen textualmente lo mismo que en el caso de los números racionales enteros. Pero en la definición de número gausiano entero primo nos detendremos en más detalles.

DEFINICIÓN 2. *Un número gausiano π se llama primo si en cualquiera de sus descomposiciones $\pi = \tau \cdot \tau$ en un producto de dos números gausianos enteros uno de los factores (τ o τ) es divisor de la unidad (en este caso los números primos no se consideran divisores de la unidad).*

De otro modo esta propiedad puede expresarse así: *número gausiano primo π es un número gausiano entero, distinto de cero, tal, que su norma es mayor que la unidad y que él mismo no puede descomponerse en un producto de dos números gausianos enteros, cuyas normas sean menores que la del número π.*

De acuerdo con esta definición serán números gausianos primos, por ejemplo, los números $\pi_1 = 2 + i$. ($N(\pi_1) = 5$); $\pi_2 = 3 + 2i$, ($N(\pi_2) = 13$). En general, serán números gausianos primos todos aquellos cuyas normas sean números racionales primos. Más adelante veremos que los números gausianos primos no se agotan con estos ejemplos. Durante el curso de nuestras investigaciones describiremos todos los números gausianos primos. Pero ahora pasaremos a enunciar y demostrar el teorema fundamental de la aritmética de los números gausianos enteros:

TEOREMA. *Todo número gausiano entero $\alpha \neq 0$ puede descomponerse en un producto de números gausianos primos*

$$\alpha = \pi_1 \cdot \pi_2 \ldots \pi_k \tag{4}$$

(π_i son números gausianos primos que pueden no ser diferentes). Esta descomposición es unívoca en el siguiente sentido:

si

$$\alpha = \sigma_1 \cdot \sigma_2 \ldots \sigma_l \tag{5}$$

es otra descomposición del número α *en un producto de números gausianos primos* σ_j, *ambas descomposiciones tienen el mismo número de factores,* $k = l$, *y las descomposiciones (4)* y *(5) pueden diferir una de otra solamente en el orden de los factores y de los multiplicadores divisores de la unidad.*

Con respecto a la parte del enunciado que se refiere a la uniformidad de la descomposición, haremos otra advertencia. Si $\alpha = \pi_1 \cdot \pi_2 \cdot \pi_3$ es el producto de los números primos π_1, π_2, π_3, tendremos, por ejemplo, que $\alpha = (-\pi_3) \cdot (i\pi_2) \cdot (i\pi_1)$ es "otra" representación del número α en forma de producto de los números primos $-\pi_3$, $i\pi_2$, $i\pi_1$, diferentes de los números primos π_1, π_2, π_3. Sin embargo, es fácil darse cuenta de que cualquiera de los números $-\pi_3$, $i\pi_2$, $i\pi_1$ se obtiene multiplicando uno de los números π_1, π_2, π_3 por cierto divisor de la unidad, con lo que varía también el orden inicial de los números. Estas diferencias en la posición de un mismo número son permisibles. La segunda parte del enunciado del teorema afirma precisamente que con semejante género de diferentes descomposiciones queda agotada la multiplicidad de las representaciones. Esta circunstancia no se diferencia en nada de la situación que se da en la aritmética de los números racionales enteros. Pero se complica, porque en el caso de la aritmética de los números gausianos enteros disponemos de una cantidad mayor de divisores de la unidad.

Observación. La uniformidad de la descomposición con exactitud de hasta los signos de los factores, a que nos referimos en el caso de los números racionales enteros, significa precisamente uniformidad con exactitud de hasta los factores divisores de la unidad, ya que $+1$ y -1 son los únicos divisores de la unidad en este caso.

La afirmación de la uniformidad de la descomposición puede enunciarse más brevemente si se introduce el concepto de números gausianos enteros asociados.

DEFINICIÓN 3. *Dos números gausianos enteros se llaman asociados si difieren entre sí* en un factor igual a un divisor de la unidad, es decir, β, $-\beta$, $i\beta$, $-i\beta$ *serán números gausianos enteros asociados si* β *es un número gausiano entero arbitrario.*

Utilizando esta definición, la afirmación de la uniformidad en el teorema fundamental se enuncia así:

Si $\alpha = \pi_1 \cdot \pi_2 ... \pi_k$ y $\alpha = \sigma_1 \cdot \sigma_2 ... \sigma_l$, *siendo* π_i $(i = 1, 2, ..., k)$ *y* σ_j $(l = 1, 2, ..., l)$ *números primos,* $l = k$, *y los factores* σ_j *pueden transponerse de tal modo, que cada* σ_j *esté asociado con el número primo* π_i *respectivo.*

La demostración del teorema fundamental de la aritmética de los números gausianos enteros se hace lo mismo que la demostración de las afirmaciones respectivas para los números racionales enteros. Por esto no vamos a exponerla detalladamente, sino que recomendamos al lector que la haga él mismo.

La primera afirmación del teorema (acerca de la existencia de la descomposición) puede hacerse por inducción según la norma del número:

a) Si $N(\alpha) = 1$, entonces $\alpha = 1, -1, i, -i$, es decir, el número puede descomponerse en el producto de un conjunto vacío de números primos.

Observación. Con respecto a la "posibilidad de la descomposición" de los divisores de la unidad en un producto de factores primos, tomamos la misma posición que para ± 1 en el caso de los números racionales enteros.

b) Supongamos que $N(\alpha) = n$ y que para todos los números gausianos enteros de norma menor ya está demostrada la afirmación. Entonces o α es un número primo y todo esta demostrado, o $\alpha = \rho \cdot \tau$, donde $N(\rho) < n$ y $N(\tau) < n$. Por el supuesto de inducción, para ρ y τ existen las descomposiciones siguientes: $\rho = \pi_1 \cdot \pi_2 ... \pi_k$ y $\tau = \sigma_1 \cdot \sigma_2 ... \sigma_l$, entonces $\alpha = \pi_1 \cdot \pi_2 ... \pi_k \cdot \sigma_1 \cdot \sigma_2 ... \sigma_l$ será la descomposición para α.

La demostración de la afirmación de la uniformidad puede hacerse mediante el establecimiento de las propiedades del máximo común divisor y de los números primos entre sí en el campo de los números gausianos enteros. La llave para toda la demostración es la afirmación de la posibilidad de la división inexacta en el campo de los números gausianos enteros. Esta afirmación se enuncia así:

Supongamos que α, β $(\beta \neq 0)$ *son dos números gausianos enteros; en este caso existen también los números gausianos enteros* γ *y* ρ, *siendo* $N(\rho) < N(\beta)$, *tales que*

$$\alpha = \gamma \cdot \beta + \rho.$$

Observación. El número γ se llama COCIENTE y el ρ, RESTO de la división de α por β. En el teorema 1 de la pág. 8 estos conceptos se introdujeron para los números enteros ordinarios, en cuyo caso el resto no debe ser negativo ($r \geqslant 0$). Pero esta condición tiene poca importancia. Si renunciamos a ella y aceptamos únicamente la desigualdad $|r| < b$, la definición de cociente y de resto para los números gausianos será una generalización natural de la definición en la situación ordinaria.

La demostración se basa en un hecho geométrico muy simple: si P es un punto que se encuentra dentro de un cuadrado de lado a o en uno de sus lados, la distancia desde el punto P hasta el vértice más próximo será menor que a. En efecto, el punto más lejano de todos los vértices es el centro del cuadrado. Pero la distancia desde él hasta cualquier vértice es igual a $\frac{1}{\sqrt{2}}a < a$. Cualquier otro punto del cuadrado estará aún menos alejado del vértice más próximo.

De esta simple afirmación se deduce directamente que para cualquier punto τ del plano complejo puede hallarse un

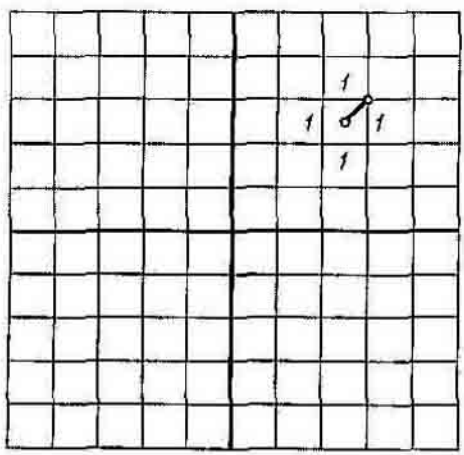

Fig. 3

punto γ de coordenadas enteras — punto que representará un número gausiano entero —, que diste de τ menos de 1 (fig. 3). Dicho de otro modo, para todo número complejo τ existe un número gausiano entero γ tal, que $N(\tau - \gamma) < 1$.

Hallemos γ para número $\tau = \frac{\alpha}{\beta}$ y supongamos que $\rho = \alpha - \gamma\beta$. Entonces ρ es un número gausiano entero,

$$N(\rho) = N(\beta) \cdot N\left(\frac{\alpha}{\beta} - \gamma\right) < N(\beta)$$
$$\alpha = \gamma\beta + \rho.$$

La afirmación queda demostrada.

Teniendo ya el teorema de la división inexacta, todas las demás propiedades pueden demostrarse del mismo modo que lo hicimos antes en el caso de los números racionales: 1) se demuestra la existencia del m. c. d. de dos números gausianos enteros α y β, como el número $\delta \neq 0$ cuya norma es la menor del conjunto de números que pueden representarse en la forma $\alpha\xi + \beta\eta$ (ξ y η son números gausianos enteros); 2) se introduce el concepto de números gausianos enteros primos entre sí y se demuestra el lema FUNDAMENTAL: *si α es primo con β_1 y α es primo con β_2, α es primo con $\beta_1 \cdot \beta_2$.* Después, ya con mucha facilidad, por inducción respecto a la norma, se demuestra la uniformidad de la descomposición en factores primos.

§ 2. NÚMEROS GAUSIANOS PRIMOS Y REPRESENTACIÓN DE LOS NÚMEROS RACIONALES ENTEROS EN FORMA DE SUMA DE DOS CUADRADOS

Pasemos ahora a la descripción de todos los números gausianos primos. Primeramente demostraremos varias afirmaciones auxiliares.

LEMA 1. *Todo número gausiano primo es divisor de un número racional primo.*

Observación. Un número racional primo es siempre un número gausiano entero, pero como número gausiano no es necesariamente primo, sino que puede dividirse en números gausianos enteros de norma menor. Así, por ejemplo, el número 2 es primo si se considera como número racional entero, pero no es primo si se considera como número gausiano entero. En efecto, en el campo de los números gausianos enteros, el número 2 permite la descomposición $2 = (1 + i)(1 - i)$ y ninguno de los factores $1 + i$ y $1 - i$ es divisor de la unidad. También es evidente que 5 no es primo en el campo de los números gausianos, ya que $5 = (2 + i) \cdot (2 - i)$.

Demostración. Efectivamente, como $N(\alpha) = \alpha \cdot \bar{\alpha}$, todo número gausiano entero divide a su norma: $\alpha | N(\alpha)$. Supongamos ahora que π es un número gausiano primo, entonces $\pi | N(\pi)$, y sea $N(\pi) = p_1 \cdot p_2 ... p_r$ la descomposición del número $N(\pi)$ en el producto de números racionales primos. Tenemos: $\pi | p_1 \cdot p_2 ... p_r$, por consiguiente, π divide a uno de los números primos p_i. En efecto, si el número gausiano primo π no dividiera a ninguno de los números p_i, sería primo con ellos y, por consiguiente, con su producto $N(\pi)$. Pero esto es imposible, ya que $\pi | N(\pi)$. Por lo tanto, el número π es divisor de uno de los números racionales enteros p_i. El lema queda demostrado.

LEMA 2. *La norma $N(\pi)$ del número gausiano primo π es un número racional primo o el cuadrado de un número racional primo.*

Demostración. Como ya sabemos, π divide a cierto número racional primo p. Supongamos que $p = \pi \cdot \gamma$. Pasemos a las normas: $N(\pi) \cdot N(\gamma) = p^2$. Son posibles solamente dos casos: 1) $N(\pi) = N(\gamma) = p$ y 2) $N(\pi) = p^2 = N(p)$, y $N(\gamma) = 1$. El lema queda demostrado.

El caso 2) significa que γ es divisor de la unidad y que es justa una de las siguientes igualdades: $\pi = p$, $\pi = -p$, $\pi = ip$, $\pi = -ip$. Por consiguiente, p es un número racional primo tal, que al mismo tiempo es también número gausiano primo. En el caso 1) γ es un número gausiano primo, ya que $N(\gamma) = p$. Puede afirmarse que $\gamma = \bar{\pi}$. En efecto, $N(\pi) = p = \pi \cdot \bar{\pi}$ y $\bar{\pi}$ es un número primo. Pero también tenemos que $p = \pi \cdot \gamma$, de manera que $\bar{\pi} = \gamma$.

En cambio, si p es un número racional primo tal, que no es número gausiano primo, se dividirá por cierto número gausiano primo, distinto de p, y al mismo tiempo, como hemos visto, $p = \pi \cdot \bar{\pi}$, es decir, p es un producto de dos números complejos, gausianos, primos, conjugados. En este caso p es la norma de un número gausiano entero y, por consiguiente, puede representarse en forma de suma de dos cudrados. Este número primo, si es impar (es decir, $p \neq 2$), será un número de la forma $4n + 1$. Puede demostrarse que todos los números primos de la forma $4n + 1$ pueden representarse en forma de suma de dos cuadrados, o sea, son normas de ciertos números gausianos enteros y, por lo tanto, no son gausianos primos y, consiguientemente, pertenecen a la clase de aquellos números racionales primos que pueden descomponerse en el producto de dos números gausianos primos conjugados entre sí. La demostración de esta

afirmación se da más adelante (cap. III, 3). Todos los números racionales primos distintos de los que tienen la forma $4n + 1$ y del número 2, es decir, los números de la forma $4n + 3$ y del número 2, es decir, los números de la forma $4n + 3$, constituyen pricisamente el conjunto de números racionales primos que siguen siendo primos en el campo de los números gausianos.

Una situación algo especial ocupa el número primo 2. Se ve fácilmente que

$$2 = i \cdot (1 - i)^2$$

$N(1 - i) = 2$. De este modo, 2 es divisible por el cuadrado del número gausiano primo $(1 - i)$.

Suponiendo sabido que todos los números primos de la forma $4n + 1$ pueden representarse en forma de suma de dos cuadrados, podemos ahora establecer cuáles son los números racionales enteros que pueden representarse en forma de esa suma. Como ya sabemos, para todo número t con tal propiedad, es necesario y suficiente que éste sea la norma de cierto número gausiano entero $\alpha: t = N(\alpha)$.

El número α se descompone en un producto de números gausianos primos:

$$\alpha = \pi_1 \cdot \pi_2 \ldots \pi_r. \tag{6}$$

Dividimos todos los números primos π_i $(i = 1, 2, \ldots, r)$ en dos clases: a la primera clase referimos aquellos números π_i cuyas normas son números primos, y a la segunda, respectivamente, los números cuyas normas son los cuadrados de números primos (puede ocurrir que una de las clases esté vacía, pero esto no influye en la marcha de nuestros razonamientos, sólo hay que tener en cuenta que todos los números a_i, o todos los b_k, en las descomposiciones (7) y (8) pueden ser ceros). Designamos los números de la primera clase por medio de $\sigma_j (j = 1, 2, \ldots, l)$, y todos los distintos números de la segunda clase, por medio de $\rho_k (k = 1, 2, \ldots, s)$. Tenemos: $N(\sigma_j) = p_j$, $N(\rho_k) = q_k^2$, donde p_j es un número primo de la forma $4n + 1$ ó 2, y q_k es un número primo de la forma $4n + 3$. Juntando los números primos iguales en el segundo miembro de la igualdad (6), escribimos este producto en forma de potencias de los números primos σ_j y ρ_k:

$$\alpha = \sigma_1^{a_1} \ldots \sigma_l^{a_l} \cdot \rho_1^{b_1} \ldots \rho_s^{b_s} \tag{7}$$

y, pasando a las normas, tenemos:

$$t = p_1^{a_1} \ldots p_l^{a_l} q_1^{2b_1} \ldots q_s^{2b_s}. \tag{8}$$

Vemos que los números q_k figuran en la descomposición del número con exponentes pares.

Al contrario, supongamos que el número t puede representarse en la forma (8), donde cada p_j es un número primo de la forma $4n + 1$ o el número 2, los q_k son números primos de la forma $4n + 3$ y $a_1, \ldots, a_l, b_1, \ldots, b_s$ son números enteros no negativos. Como cada p_j es la suma de dos cuadrados, puede elegirse σ_j de tal modo, que $N(\sigma_j) = p_j$. Suponiendo después que $\rho_k = q_k$ y, finalmente, que $\alpha = \sigma_1^{a_1} \ldots \sigma_l^{a_l} \rho_1 \ldots \rho_s^{b_s}$, obtenemos que $t = N(\alpha)$, es decir, t puede representarse en forma de suma de dos cuadrados. En definitiva tenemos el teorema siguiente:

TEOREMA 2. *Para que un número racional entero pueda representarse en forma de suma de dos cuadrados es necesario y suficiente que los números primos de la forma $4n + 3$ figuren con exponentes pares en la descomposición de dicho número en factores primos.*

Observación. Esta formulación abarca también el caso en que en la descomposición del número que se considera no existen números primos de la forma $4n + 3$, puesto que el número 0 también es par.

Como vemos, este teorema da el criterio para que la ecuación diofántica de segundo grado de la forma

$$x^2 + y^2 = t$$

tenga solución (en números enteros). En general, el estudio de las ecuaciones diofánticas de la forma

$$ax^2 + 2bxy + cy^2 = t$$

está relacionado íntimamente con las aritméticas de los campos de números análogos al campo de los números gausianos enteros.

En estas investigaciones resulta ser importante el siguiente hecho excepcional: el teorema de la uniformidad de la descomposición de los números en un producto de números primos no en todas estas aritméticas se cumple. Damos un ejemplo de tal "aritmética".

Consideremos los números complejos de la forma

$$\alpha = x + y\sqrt{-5}, \tag{1}$$

donde x e y son números racionales enteros. Se ve fácilmente que la suma, la diferencia y el producto de los números de la forma (1) son números de la misma forma. Designemos el conjunto de todos los números de la forma (1) por medio de Γ. Es evidente que Γ contiene todos los números racionales enteros (siendo $y = 0$). Lo mismo que en los casos de los números racionales enteros y gausianos enteros, puede hablarse de la divisibilidad en el caso Γ: α divide a β ($\alpha|\beta$), si $\frac{\beta}{\alpha}$ es un número de Γ, es decir, que puede representarse en la forma (1). Lo mismo que en el caso de los números gausianos enteros, en la cuestión de la divisibilidad desempeñan un papel importante las normas de los números de Γ:

$$N(\alpha) = N(x + y\sqrt{-5}) = (x + y\sqrt{-5})(x - y\sqrt{-5}) = x^2 + 5y^2.$$

De este modo, la norma de todo número de Γ es un número racional entero y, como $N(\xi \cdot \eta) = N(\xi) \cdot N(\eta)$, la condición necesaria (pero no suficiente en general) para que $\alpha|\beta$ es que $N(\alpha)|N(\beta)$.

Lo mismo que en el caso de los números gausianos enteros, se introduce naturalmente el concepto de divisores de la unidad y de números primos. Con respecto a los divisores de la unidad, el problema es aquí incluso más fácil que para los números gausianos enteros. Concretamente, son divisores de la unidad únicamente los números $+1$. En efecto, para los divisores de la unidad $\xi = u + v\sqrt{-5}$ debe cumplirse la condición $N(\xi) = u^2 + 5v^2 = 1$. Pero esta ecuación diofántica, evidentemente, no puede tener soluciones diferentes de $u = \pm 1$ y $v = 0$.

El hecho de que cada número de Γ pueda representarse en forma de producto de números primos de Γ se demuestra por inducción respecta a la norma, exactamente del mismo modo que en el caso de los números gausianos enteros. Pero aquí la afirmación de la uniformidad de esta descomposición ya no es correcta, como demostraremos en el ejemplo siguiente.

Demostraremos primero que los números $2 = 2 + 0 \cdot \sqrt{-5}$, $3 = 3 + 0 \cdot \sqrt{-5}$, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ son números primos en Γ. En efecto, $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. Si uno de estos números no fuera primo en Γ, podría dividirse únicamente por cierto número $\alpha = x + y\sqrt{-5}$ para el cual $N(\alpha) = x^2 + 5y^2 = 2$, o $N(\alpha) = x^2 + 5y^2 = 3$. Pero estos números no existen en Γ, ya que es evidente que las ecuaciones

$$x^2 + 5y^2 = 2$$

y

$$x^2 + 5y^2 = 3$$

no tienen solución en números enteros.

Así, pues, los cuatro números indicados son primos en Γ. Señalemos ahora la igualdad fácil de comprobar

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Esta igualdad muestra que el número 6 de Γ tiene dos representaciones distintas en forma de productos de números primos.

Con este hecho tropezó el matemático alemán E. KUMMER (1810 – 1893) cuando intentaba resolver el llamado gran teorema de Fermat. Después las dificultades surgidas en virtud del incumplimiento del teorema fundamental de la aritmética en ciertos campos de números, fueron vencidas eficazmente por el mismo Kummer y por otros matemáticos, como R. DEDEKIND, E. ZOLOTARIOV, L. KRONECKER y otros. En las matemáticas apareció un gran campo nuevo, la teoría de los números algebraicos.

EJERCICIOS

1. Efectuar la división inexacta del número gausiano entero a por el número gausiano entero b, si: a) $a = 2 + 3i$, $b = 1 - i$; b) $a = 1 + i$, $b = 2 + i$.
2. Descomponer en factores primos los números gausianos enteros: $1 + i$; $2 + 5i$; 5; 10.
3. ¿Pueden representarse en forma de suma de dos cuadrados de números racionales enteros los números: a) 197; b) 1472; c) 111 112?
4. Demuestre que para los números complejos de la forma $a + b\sqrt{-2}$, donde a y b son números racionales enteros, se cumple el teorema fundamental de la aritmética.
5. Demuestre que en el anillo de números de la forma $a \pm b\sqrt{-5}$, siendo a y b números racionales enteros, 7, $1+2\sqrt{-5}$ y $1-\sqrt{-5}$ son primos.

CAPÍTULO III

ARITMÉTICAS FINITAS

Las principales aplicaciones de la división inexacta las estudiamos demostrando el teorema fundamental de la aritmética y resolviendo ecuaciones diofánticas simples. Estudiemos ahora la construcción esencial relacionada con la división de los números enteros: las clases residuales.

La idea fundamental consiste en lo siguiente: los diversos restos de la división por un número natural dado n sólo son n: estos son los números $0, 1, 2, \ldots, n-1$. Por esto el conjunto infinito de los números enteros puede dividirse en un número finito (en n) de subconjuntos, en cada uno de los cuales entran los números que dan un mismo resto cuando se dividen por n. Estos subconjuntos se llaman *clases residuales respecto al módulo n*. Resulta que a ellas pueden trasladarse de forma natural las ope-

raciones ordinarias de la aritmética (multiplicación, suma, resta) y esto conduce a una nueva e interesante "aritmética" que se llama FINITA.

§ 1. CLASES RESIDUALES

Convengamos en que, si no se hacen indicaciones especiales, se entiende por "números" los "números enteros". Su conjunto es un "anillo" que en todas partes designaremos por Z.

DEFINICIÓN 1. *Los números x e y se llaman congruentes respecto a un módulo n, siendo n un número distinto de cero, si su diferencia $x-y$ es divisible por n.*

En este caso se escribe:

$$x \equiv y \,\text{mód}\,(n) \quad \text{o} \quad y \equiv x \,\text{mód}\,(n).$$

Para los números no congruentes respecto al módulo n se escribe:

$$x \not\equiv y \,\text{mód}\,(n) \quad o \quad y \not\equiv x \,\text{mod}\,(n).$$

Por ejemplo, $12 \equiv 15$ mód (3), porque $12 - 15 = -3$ es divisible por 3, y $21 \equiv 10$ mód (5), porque $21 - 10 = 11$ no es divisible por 5.

Sea $n = 3$. ¿Cómo es el conjunto de todos los números de Z congruentes con el número 5 respecto al módulo 3? En primer lugar, en este conjunto entra el mismo número $5 : 5 = 5$ mód (3). Después, si $x \equiv 5$ mód (3), $x - 5 = 3k$ para cierto k de Z, es decir, $x = 5 + 3k$. Al contrario, para cualquier k el número $x = 5 + 3k$ será congruente con 5 respecto al módulo 3, porque $x - 5 = 3k$, y éste es múltiplo de 3. Por consiguiente, dándole a k, en la fórmula $x = 5 + 3k$, todos los posibles valores en Z, obtenemos el conjunto de todos los números congruentes con 5 respecto al módulo 3. Este conjunto (lo designaremos por 5) es una progresión geométrica ordinaria, infinita a ambos lados y cuya diferencia es igual a 3; he aquí varios de sus términos consecutivos: para $k = -3, -2, -1, 0, 1, 2, 3$ tenemos

$$\ldots, -4, -1, 2, 5, 8, 11, \ldots$$

DEFINICIÓN 2. *El conjunto X de todos aquellos números de Z que son congruentes con el número x respecto al módulo n, se llama*

clase de restos del número x respecto al módulo n y se designa por uno de los tres procedimientos siguientes: x mód (n), *x o* $\bar{x}$, *si el número n se ha fijado.* Los números X se llaman *restos* del número x respecto al módulo n o *representantes* de la clase X.

De este modo, en el ejemplo anterior se definió la clase de restos 5 mód (3) del número 5 respecto al módulo 3. Es evidente que 8 mód (3) = 5 mód (3) y, en general, la clase de restos $x =$ mód (3) de cualquier representante x de 5 mód (3) es igual a **5.**

TEOREMA 1. *Sea* $x = qn + r$, *donde* $0 \leqslant r < n$. *Entonces* x mód $(n) = r$ mód (n).

Demostración. I *procedimiento.* Basta darse cuenta de que x mód (n) y r mód (n) es una misma progresión geométrica infinita a ambos lados $x + kn$ o $r + kn$ cuya diferencia es n, porque $x + kn = r + (k + q)n$.

II *procedimiento.* Cada número z congruente con x mód (n) es también congruente con r mód (n), porque si $z - x = kn$, será $z - r = z - x - qn = kn - qn = (k - q)n$. Y al contrario, si $z - r = kn$, será $z - x = r - x + qn = (k + q)n$.

El resto r de la división del número x por n se llama representante canónico de la clase x mód (n). En el ejemplo antes estudiado de la clase 5 mód (3), el representante canónico será, por consiguiente, el número 2.

COROLARIO. *Todas las clases residuales posibles respecto al módulo n son:*

0 mód (n), 1 mód (n), 2 mód (n), ..., $(n - 1)$ mód (n), es decir, **0, 1, 2, ..., n–1.**

En efecto, los números 0, 1, 2, ..., $n - 1$ constituyen el conjunto de todos los restos posibles de la división por n, por esto no puede haber otras clases residuales además de **0, 1, 2, ..., n–1.** Pero, entre estas clases, ¿no puede haber coincidentes? Si fuera $a = b$, siendo a y b distintos restos de la división por n, con cierto k entero se cumpliría la igualdad $a - b = kn$, y esto es imposible cuando $k \neq 0$, ya que $|a - b| < n$. y $|kn| \geqslant n$. Por consiguiente, $a = b$ y todas las clases **0, 1, 2, ..., n – 1** son distintas.

En adelante designaremos por medio de z_n el conjunto de clases de restos respecto al módulo n.

EJERCICIOS

1. Demostrar que si un número entero cualquiera a pertenece a dos clases de restos X e Y respecto al módulo n, será $X = Y$.

INDICACIÓN. Adviértase que si $x \equiv a$ mód (n) e $y \equiv a$ mód (n), será $x \equiv y$ mód (n) y, por consiguiente, x mód $(n) = y$ mód (n).

2. Demostrar que si $n = ml$, siendo m y l números naturales, cada clase de restos respecto al módulo m consta de l clases de restos respecto al módulo n.

3. Demostrar que Z_n y Z_{-n}, $n = 0$, son un mismo conjunto.

§ 2. ARITMÉTICA DE LAS CLASES RESIDUALES

Al estudiar la divisibilidad de los números enteros y de los gausianos enteros nos servimos de que éstos forman un anillo, es decir, de que la suma, la diferencia y el producto de dos números cualesquiera del conjunto considerado pertenecen a él y las operaciones citadas están subordinadas a las leyes habituales, conmutativa, asociativa y distributiva. Las propiedades del anillo de los números enteros constituyen la aritmética o, mejor dicho, la aritmética de los números enteros. En el capítulo anterior estudiamos la aritmética de los números gausianos enteros. Ahora vamos a introducir las operaciones aritméticas en el conjunto Z_n y daremos a conocer la aritmética de las clases residuales. Para concretar convendremos en que ne el concepto "respecto al módulo n" el número n es natural.

DEFINICIÓN 3. *La suma de dos clases de restos respecto al módulo* n—$\bar{x}$ e $\bar{y}$—*se llama clase* $\overline{x+y}$. En este caso se escribe:

$$\bar{x} + \bar{y} = \overline{x+y}.$$

Pero aquí puede asaltarnos una duda, ya que las clases $\bar{x}$ e $\bar{y}$ son conjuntos, incluso conjuntos infinitos. Los representantes x e y, mediante los cuales determinamos la suma $\bar{x} + \bar{y}$, tienen, dentro de sus clases, las mismas facultades que todos los demás representantes; por esto, si la definición 3 no entraña ningunas contradicciones, eligiendo en $\bar{x}$ e $\bar{y}$ otros representantes, por ejemplo, x' e y', en calidad de clase $\bar{x}' + \bar{y}'$ debemos obtener la misma clase $\overline{x+y}$, es decir, es necesario que se cumpla la igualdad $x' + y' = x + y$ (si fuera $x' + y' \neq x + y$, la definición entrañaría la contradicción siguiente: $\overline{x' + y'} = \overline{x' + y'} = \overline{x + y} = \overline{x+y}$, a pesar de que $x' + y' \neq x+y$). La comprobación de

la igualdad $\overline{x' + y'} = \overline{x + y}$ se llama en matemáticas *prueba de que la definicion es correcta.*

Efectivamente, sean r_x y r_y los restos de la división por n de los números x e y respectivamente. Entonces la clase $x + y$ consta de todos aquellos números que al ser divididos por n dan el mismo resto que $r_x + r_y$. Por otra parte, la clase $x' + y'$ consta de aquellos mismos números, porque los restos de la división por n de los números x' e y' son r_x y r_y. La corrección de la definición 3 queda demostrada.

Veamos varios ejemplos. Sea $n = 2$. Entonces las clases de restos sólo son dos: 0 y 1. Su suma es fácil de definir:

$$0 + 0 = 0,$$

$$1 + 0 = 0 + 1 = 1.$$

$$1 + 1 = 0.$$

Sin embargo, estos resultados conviene más definirlos en una tabla.

Tabla 1

	0	1
0	0	1
1	1	0

El resultado se lee así: supongamos que hay que hallar la suma **0 + 1**. En la columna de la izquierda se busca el primer sumando (es decir, **0**), y en la fila superior, el segundo (o sea, **1**). En la intersección de la fila en que se encuentra el primer sumando con la columna en que está el segundo, se indica la suma de los mismos: **1**. Esta tabla se llama tabla de sumar para Z_2.

Sea $n = 3$. En este caso las clases serán **0, 1** y **2**. La correspondiente tabla de sumar tiene la forma:

Tabla 2

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Al lector le será útil comprobar también las siguientes ta-

blas de sumar para $n = 7$ y $n = 10$:

Tabla 3

Tabla de sumar en Z_7

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
6	6	0	1	2	3	4	5

Tabla 4

Tabla da sumar en Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Así, pues, la suma de las clases de restos en Z_n se determinan por medio de la suma de los representantes de estas clases. Análogamente se determinan la resta y la multiplicación. He aquí leas definiciones exactas:

DEFINICIÓN 4. *La diferencia de dos clases de restos respecto a un módulo* n —$\bar{x}$ e $\bar{y}$— se llama clase $x - y$. En este caso se escribe:

$$\bar{x} - \bar{y} = x - y.$$

DEFINICIÓN 5. *El producto de dos clases de restos respecto a un módulo* n —$\bar{x}$ e $\bar{y}$—*se* llama clase $\overline{xy}$. En este caso se escribe:

$$\bar{x}\,\bar{y} = \overline{xy}, \text{ o } \bar{x} \cdot \bar{y} = \overline{xy}.$$

El lector es probable que se halla dado cuenta de que las definiciones 4 y 5, lo mismo que la 3, requieren la prueba de su corrección. La demostración de las igualdades respectivas $-x' - y' = x - y$ y $x'y' = xy$ no es difícil. La primera de ellas la dejamos para que sirva de ejercicio; la segunda se establece así. Tenemos: $x' = x + k_x n$ e $y' = y + k_y n$, donde k_x y k_y son números enteros. Entonces $x'y' = xy + n(xk_y + yk_x + k_x k_y n)$. *Por esto*

$$x'y' \equiv xy \text{ mód } (n).$$

Las tablas de sumar (véanse, por ejemplo, las tablas 1—4) son cómodas no sólo para determinar la suma, sino también para determinar la diferencia. Esto está relacionado con la sencilla observación siguiente: si $a = b - c$, entonces $b = a + c$. En efecto, sumemos a ambos miembros de la igualdad $a = b - c$ la clase c. Obtenemos:

$$a + c = (b - c) + c.$$

Es evidente que $\mathbf{b} - \mathbf{c} = \mathbf{b} + (-\mathbf{c})$ (tanto el uno como el otro son de la clase $(\mathbf{b} - \mathbf{c})$ mód (n)). Por esto $(\mathbf{b} - \mathbf{c}) + \mathbf{c} = (\mathbf{b} + (-\mathbf{c})) + \mathbf{c}$. No obstante, para tres clases cualesquiera $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ es justa la ley asociativa:

$$(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$$

(tanto el uno como el otro son de la clase $(x + y + z)$ mód (n)). Por esto $(\mathbf{b} + (-\mathbf{c})) + \mathbf{c} = \mathbf{b} + (-\mathbf{c} + \mathbf{c}) = \mathbf{b} + \mathbf{0} = \mathbf{b}$, de manera que $\mathbf{a} + \mathbf{c} = \mathbf{b}$.

Por consiguiente, para hallar en la tabla de sumar la diferencia $\mathbf{a} - \mathbf{b}$ basta encontrar en la columna de la izquierda es el sustrayendo $\mathbf{b}$, despues, en la misma fila de la tabla, se busca el minuendo a, y entonces la diferencia $a - b$ está indicada en la parte superior de la columna en que se encuentra $\mathbf{a}$. Así, por la tabla 3, es fácil hallar que 4 mód (7) $-$ 6 mód (7) $=$ 5 mód (7), o por la tabla 4, 4 mód (10) $-$ 6 mód (10) $=$ 8 mód (10) y 6 mód (10) $-$ 4 mód (10) $=$ 2 mód (10).

En cuanto a la multiplicación en Z_n, es conveniente definirla por tablas análogas a las de sumar, pero en vez de indicar la suma de las clases de restos, indicaremos en ellas su producto.

Tabla 5

Tabla de multiplicar en Z_2

	0	1
0	0	0
1	0	1

Tabla 6

Tabla de multiplicar en Z_3

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabla 7

Tabla de multiplicar en Z_7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tabla de multiplicar en Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Quedamos, pues, en que las clases residuales en Z_n pueden sumarse, restarse y multiplicarse. Las leyes conmutativa, asociativa y distributiva que actúan en la suma y multiplicación de los números se trasladan también a las clases de restos. Dejamos al lector la demostración de las igualdades respectivas. El conjunto Z_n, con la suma, resta y multiplicación que acabamos de introducir, es lo que se llama *anillo de las clases de restas respecto al módulo n*. Los elementos **0** y **1** de Z_n es natural que se llamen cero y uno del anillo Z_n.

Finamente, refirámonos a la división en el anillo Z_n. Sean $a = a \text{ mód } (n)$ y $b = b \text{ mód } (n)$; se dice que la clase b divide a la clase a (y se escribe $\mathbf{b} \mid \mathbf{a}$), si existe una clase $\mathbf{c} - c$ mód (n) tal, que $a = b \cdot c$. Por ejemplo, si $n = 10$ (véase tabla 8), la clase **2** divide a la clase **4** y la clase **4** divide a la clase **6**. Si $\mathbf{b} \mid \mathbf{a}$, se dice también que **b** es divisor de la clase **a**.

En el anillo de los números enteros Z todos los números son divisores de 0, porque $x \cdot 0 = 0$ para cualquier x, y única-

mente 1 y -1 son divisores del número 1. Naturalmente, en el anillo Z_n también todas las clases x dividen a 0, y las clases **1** y $-$ **1** dividen a **1**. Pero a diferencia del anillo Z, aquí, para una u otra n pueden establecerse varias propiedades específicas no propias de Z.

Así, en el anillo Z la igualdad $xy = 0$ sólo es posible cuando por lo menos uno de los elementos x o y es igual a 0. Pero en el anillo Z_{10} tenemos que $2 \cdot 5 = 0$, aunque $2 \neq 0$ y $5 \neq 0$! En el anillo son divisores del número 1 solamente 1 y -1, mientras que en el anillo Z_{10} a la clase **1** la dividen a la vez cuatro elementos: **1**, **3**, **7**, **9**, porque $\mathbf{1} = 1 \cdot 1 = 3 \cdot 7 = 7 \cdot 3 = 9 \cdot 9$. Finalmente, en el anillo Z pueden efectuarse simplificaciones sin vacilar (es decir, puede garantizarse que de la igualdad $ax = ay$ y la condición $a \neq 0$ se deduce la igualdad de los números $x = y$), y en el anillo Z_n, no; por ejemplo, en Z_{10}, de la igualdad $2 \cdot 7 = 2 \cdot 2$ y la condición $2 \neq 0$ no se deduce que $7 = 2$.

Ahora demostraremos el teorema fundamental en este plano, acerca de los anillos Z_n. Introduciremos dos términos:

Una clase $\mathbf{x}$ *del anillo* Z_n se *llama divisora de cero si* $\mathbf{x} \neq \mathbf{0}$ *y existe en* Z_n *una clase* $\mathbf{y} \neq \mathbf{0}$ tal, que $\mathbf{xy} = \mathbf{0}$.

Una clase x *de* Z_n *se llama divisora de la unidad si existe en* Z_n *una clase* y *tal, que* $x \cdot y = 1$.

Los divisores de la unidad se llaman también ELEMENTOS INVERTIBLES.

TEOREMA 2. (1) *Una clase* $\mathbf{x}$ *del anillo* $\mathbf{Z_n}$ *es divisora de la unidad si, y solamente si, los números* x *y* n *son primos entre sí.*

(2) *Una clase* $\mathbf{x}$ *del anillo* $\mathbf{Z_n}$ *es divisora de la unidad si, y colamente si, no es divisora de cero.*

Conviene advertir que el máximo común divisor de los números x y n no depende de la elección que se haga del representante de la clase x. En efecto, si $x' = x$ mód (n), será $x' = x + kn$ y todo divisor común de x y n (en particular, el máximo) será divisor común de x' y n. Pero esto $(x, n) \mid (x', n)$ y, como es natural, al contrario: $(x', n) \mid (x, n)$. Por lo tanto, la formulación del teorema 2 en la parte (1) es correcta.

Demostración (1) Sean x y n primos entre sí. Según el teorema 3, capítulo I, esto significa que $xs + nt = 1$ para ciertos s y t de Z. Pero entonces, pasando a los restos respecto al módulo n, obtenemos:

$$\mathbf{xs} + \mathbf{nt} = \mathbf{1}$$

o bien

$$(xs) \text{ mód } (n) + (nt) \text{ mód } (n) = 1 \text{ mód } (n),$$

es decir, $\mathbf{xs} = \mathbf{1}$, pues que $\mathbf{nt} = \mathbf{0t} = \mathbf{0}$ y es invertible en Z^n.

Al contrario, sea $\mathbf{xs} = \mathbf{1}$ en Z para cierta clase **s**. Entonces $xs - 1 \equiv$ mód (n), es decir, $xs - 1 = k \cdot n$ y, por consiguiente, x y n son primos entre sí.

(2) Supongamos que **x** no es divisor de cero. Consideremos el máximo común divisor d de los números x y n. Sea

$$d = xs + nt$$

para ciertos s y t enteros y $n = d \cdot n'$. Si $d = 1$, de lo demostrado antes, x es inversible en $\mathbf{Z}_n$. Si $d = 1$, $\mathbf{n'} = \mathbf{0}$ y, además, para $x = x' \cdot d$

$$xn' = x'd \cdot n' = x' \cdot n = \mathbf{0} \qquad (1)$$

y x es divisor de cero en contradicción con lo propuesto. Por consiguiente, $d = 1$ y **x** es inversible en $\mathbf{Z}_n$.

Al contrario, sea **x** inversible en $\mathbf{Z}_n$, es decir, $\mathbf{xy} = \mathbf{1}$ para cierto y de $\mathbf{Z}_n$. Si fuera $\mathbf{xz} = \mathbf{0}$ para $\mathbf{z} \neq \mathbf{0}$, de la última igualdad se deduciría que $\mathbf{yxz} = \mathbf{y0} = \mathbf{0}$, es decir, $\mathbf{(yx)z} = \mathbf{0}$ ó $\mathbf{1} \cdot z = \mathbf{0}$, pero $z \neq \mathbf{0}$ por la suposición hecha. El teorema queda demostrado.

COROLARIO 1. *Una clase* **x** *de* $\mathbf{Z}_n$, $\mathbf{x} = \mathbf{0}$, *es divisora de cero si, y solamente si, los números* x *y* n *no son primos entre sí.*

COROLARIO 2. *En un anillo* Z_p, *donde* p *es un número primo, no existen divisores de cero.*

En efecto, cada uno de los números $1, 2, \ldots, p - 1$ son primos con p, si p es primo; por esto las clases $\mathbf{1}, \mathbf{2}, \ldots, p - \mathbf{1}$ son inversibles en Z_p.

Para terminar este párrafo daremos dos teoremas más dedicados a los hechos "singulares" de la aritmética finita.

TEOREMA 3. *Si* p *es un número primo y* $a = a$ *mód* (p) *y* $b = b$ *mód* (p), *será* $(a + b)^p = a^p + b^p$.

Demostración. Recordaremos en primer lugar que para unos números cualesquiera x e y el binomio $(x + y)^p$ se desarrolla de acuerdo con la siguiente fórmula de Newton:

$$(x + y)^p = x^p + C_p^1 x^{p-1} y + \ldots + C_p^k x^{p-k} y^k + \ldots + C_p^{p-1} x y^{p-1} + y^p.$$

donde

$$C_p^k = \frac{p(p-1)...(p-k+1)}{1 \cdot 2...k}, \quad k = 1, 2, ..., p-1.$$

El coeficiente binomial C_p^k, cualquiera que sea k, es divisible por p, porque p, por ser primo, es primo con cada uno de los números 1, 2, ..., k si $k < p$. Por consiguiente, la diferencia $(x + y)^p - x^p - y^p$ se representa en forma de una suma de números en que cada uno de ellos es divisible por p; por esto $(x + y)^p \equiv (x^p + y^p)$ mód (p), de donde para $x = a$ e $y = b$ se obtiene lo que necesitábamos

$$(a + b)^p = a^p + b^p.$$

No menos interesante es el hecho siguiente, conocido con el nombre de "pequeño teorema de Fermat":

TEOREMA 4. *Si p es un número primo y $x = x$ mód (p), será $x^p = x$.*

Demostración. Si $x = 0$, la afirmación es evidente. Supongamos que $x \neq 0$. Esto significa que el número x no es divisible por p, y como p es primo, los números x y p son primos entre sí. Por consiguiente, las clases x, $2x$, ..., $(p-1)x$ son distintas de dos en dos: la igualdad $lx = kx$ significaría que $l = k$ (por el teorema 2 de este capítulo el elemento x es inversible, y si $xy = 1$, multiplicando ambas partes de la igualdad $lx = kx$ por y, obtenemos que $l = k$), pero esto es imposible si $0 < l, k < p$ y $l \neq k$. Por lo tanto, x, $2x$, ..., $(p-1)x$ es la representación en cierto orden de las clases **1**, **2**, ..., $p-1$, y por esto el producto $x \cdot 2x \cdot ... \cdot (p-1)x$ es igual a $\mathbf{1} \cdot \mathbf{2} \cdot ... \cdot (p-\mathbf{1})$, es decir, $\mathbf{1} \cdot \mathbf{2} \cdot ... \cdot (p-\mathbf{1})x^{p-1} = \mathbf{1} \cdot \mathbf{2} \cdot ... \cdot (p-\mathbf{1})$. Por consiguiente, si la última igualdad se simplifica por $\mathbf{1} \cdot \mathbf{2} \cdot ... \cdot (p-\mathbf{1})$, se obtiene $x^{p-1} = \mathbf{1}$, o después de multiplicarla por x, tenemos $x^p = x$. El teorema queda demostrado.

El conjunto de las clases no nulas de restos **1**, **2**, ..., $p-\mathbf{1}$ respecto al módulo p primo posee muchas propiedades interesantes. Una de ellas consiste en lo siguiente: entre estas clases siempre hay una clase a tal, que cualquiera otra clase es cierta potencia suya, es decir, para cualquiera otra clase x existe una clase natural t tal, que $a^t = x$.

EJERCICIOS

1. Por la tabla 7 hallar para cada x de Z_7 una clase recíproca (es decir, una y tal, que $xy = 1$).

2. Demostrar que si la clase x del anillo Z_n es invertible, existe exactamente una clase y para la cual $xy = 1$ (si se supone lo contrario, es decir, la existencia de la igualdad $1 = xy_1 = xy_2$, hay que multiplicar también la última de ellas por y_1 o por y_2).

3. Demostrar que por el elemento $a \neq 0$ del anillo Z_n puede simplificarse (es decir, garantizar que de $ax = ay$ se deduce que $x = y$) si, y solamente si, a es divisor de la unidad.

INDICACIÓN. La suficiencia de esta condición es casi evidente y su necesidad debe establecerse por reducción al absurdo: si a no es divisor de la unidad, $ab = 0$ para cierto $b \neq 0$ de Z_n; después de esto hay que representar b en forma de $x - y$ para algunos $x \neq y$ de Z_n y considerar la igualdad $a(x - y) = 0$.

4. Hacer las tablas de sumar y de multiplicar para Z_8 y hallar en este anillo todos los divisores de cero y todos los divisores de la unidad.

5. Sea N un número natural arbitrario y r un número igual a la cantidad de números primos con N de la serie $1, 2, ..., N-1$. Demostrar que para cualquier número entero a, primo con N, en el anillo Z_n se efectúa la igualdad $a^r = 1$ (teorema de Euler).

§ 3. ECUACIONES Y RESTOS DIOFÁNTICOS

Ahora ya podemos comenzar el estudio de las ecuaciones diofánticas de tipo más general que el que consideramos en el capítulo I.

Primero introduciremos el concepto de polinomio en números enteros de n variables. Diremos que $x_1, x_2, ..., x_n$ son variables independientes si cada una de ellas toma valores en números enteros independientemente de todas las demás. Se llama MONOMIO de las variables $x_1, x_2, ..., x_n$ toda expresión de la forma

$$ax_1^{m_1} x_2^{m_2} ... x_n^{m_n}, \qquad (1)$$

donde $m_1, m_2, ..., m_n$ son números enteros no negativos, y a es un número entero arbitrario que se llama COEFICIENTE DEL MONOMIO. Si en lugar de cada una de las letras $x_1, x_2, ..., x_n$ se pone en el monomio números concretos, por ejemplo, $x_1 = a_1, x_2 = a_2, ..., x_n = a_n$ dicho monomio se convertirá en un número entero determinado $a \cdot a_1^{m_1} a_2^{m_2} ... a_n^{m_n}$.

Dos monomios de las mismas variables $ax_1^{m_1} x_2^{m_2} ... x_n^{m_n}$ y $bx_1^{k_1} x_2^{k_2} ... x_n^{k_n}$ pueden "multiplicarse" y de nuevo se obtiene un

monomio según la regla siguiente:

$$(ax_1^{m1} x_2^{m2} \ldots x_n^{mn})(bx_1^{k1} x_2^{k2} \ldots x_n^{kn}) = abx_1^{m1+k_1} x_2^{m2+k_2} \ldots x_n^{mn+k_n}. \quad (2)$$

Está claro que la igualdad (2) seguirá siendo justa si $x_1, x_2, \ldots, x_n$ se sustituyen por valores numéricos concretos.

Convengamos también en cómo hay que "sumar" los monomios: por suma de dos monomios $ax_1^{m1} x_2^{m2} \ldots x_n^{mn}$ y $bx_1^{k1} x_2^{k2} \ldots x_n^{kn}$ entenderemos la expresión

$$ax_1^{m1} \cdot x_2^{m2} \ldots x_n^{mn} + bx_1^{k1} x_2^{k2} \ldots x_n^{kn},$$

que para valores enteros concretos de $x_1, x_2, \ldots, x_n$, por ejemplo, $x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n$, toma el valor numérico entero $aa_1^{m1} a_2^{m2} \ldots a_n^{mn} + ba_1^{k2} a_2^{k2} \ldots a_n^{kn}$. Después de esto no es difícil determinar la suma de un número finito cualquiera de monomios de las variables $x_1, x_2, \ldots, x_n$.

DEFINICIÓN 6. *Se llama polinomio en números enteros de las variables $x_1, x_2, \ldots, x_n$ una suma cualquiera de un número finito de monomios de las variables $x_1, x_2, \ldots, x_n$. Los coeficientes de los monomios sumandos se llaman coeficientes del polinomio. Al polinomio de n variables lo designaremos por $f(x_1, x_2, \ldots, x_n)$.*

Así, por ejemplo, $f(x_1, x_2) = x_1 + x_2$ es un polinomio de dos variables; sus coeficientes son iguales a la unidad; para el polinomio $g(x_1, x_2) = x_1^2 + 2x_1x_2 + x_2^2$ es característico, claro está, que todos sus valores (es decir, los números que se obtienen al sustituir x_1 y x_2 por números enteros concretos) son cuadrados, porque

$$g(x_1, x_2) = (x_1 + x_2)^2.$$

Es indudable que la frecuente repetición de las palabras "en números enteros" en toda la construcción que hemos hecho se debe a la concreción de nuestros fines; hemos construido un polinomio de n variables $x_1, x_2, \ldots, x_n$, que para valores en números enteros de las últimas toma valores en números enteros. Pero podríamos hablar también de polinomios reales o complejos de n variables, sólo que en este caso los coeficientes de los monomios deberían tomarse reales o complejos, respectivamente, y, de un modo análogo, los valores de las variables $x_1, x_2, \ldots, x_n$. Es más, puede construirse (y esto lo vamos a necesitar) un polinomio de n variables $x_1, x_2, \ldots, x_n$, cuyos coeficientes sean clases de restos respecto a un módulo m fijado y cuyas variables tomen los valores de Z_m. A este polinomio le llamare-

mos (a difirencia del polinomio en números enteros) *polinomio sobre el anillo de clases de restos respecto al módulo m.*

Veamos la relación *que existe entre los polinomios en números enteros y los polinomios sobre el anillo de clases de restos. Supongamos que* $f(x_1, x_2, ..., x_n)$ es un polinomio en números enteros de n variables y m es un número entero positivo. Demos a las variables $x_1, x_2, ..., x_n$ unos valores numéricos cualesquiera, por ejemplo, $x_1 = a_1, x_2 = a_2, ..., x_n = a_n$, entonces el polinomio se transforma en el número $f(a_1, a_2, ..., a_n)$. Designemos ahora por $f(x_1, x_2, ..., x_n)$ el polinomio sobre el anillo de clases de restos respecto al módulo m que se obtiene de $f(x_1, x_2, ..., x_n)$ sustituyendo los coeficientes por sus clases de restos respecto al módulo m. Entonces, como se deduce del 2,

$$f(a_1, a_2, ..., a_n) = f(\bar{a}_1, \bar{a}_2, ..., \bar{a}_n),$$

donde $f(a_1, a_2, ..., a_n) = f(a_1, a_2, ..., a_n)$ mód (m) y $\bar{a}_i = a_i$ mód m) $(i = 1, 2, ..., n)$. Al polinomio $f(x_1, x_2, ..., x_n)$ le llamaremos REDUCCIÓN DEL polinomio $x_2, ..., x_n)$ respecto al módulo m.

Por ejemplo, si $m=9$, $n=2$ y $f(x_1, x_2) = (15x_1^3 + 9x_1^2x_2 + 8x_1x_2 + 11x_2^2$, será $\bar{f}(x_1, x_2) = 6x_1^3 + 0x_1^2x_2 + 8x_1x_2 + 2x_2^2 = 6x_1^3 + 8x_1x_2 + 2x_2^2$.

DEFINICIÓN 7 *Se llama ecuación diofántica de n variables la ecuación de la forma*

$$f(x_1, x_2, ..., x_n) = 0, \tag{3}$$

donde $f(x_1, x_2, .., x_n)$ es un polinomio en números enteros de n variables y $x_1, x_2, ..., x_n$ toman únicamente valores enteros.

Si $x_1 = a_1, x_2 = a_2, ..., x_n = a_n$ son la solución de la ecuación diofántica (3), es decir, $f(a_1, a_2, ..., a_n) = 0$, será

$$\bar{f}(\bar{a}_1, \bar{a}_2, ..., \bar{a}_n) = \bar{0} \tag{4}$$

para la reducción respecto a un módulo cualquiera m. Por consiguiente, si con cualquier m la igualdad (4) no se cumple para todos los restos posibles $\bar{a}_1, \bar{a}_2, ..., \bar{a}_n$ respecto al módulo m, la ecuación (3) no tiene solución. En otras palabras, es correcto el teorema siguiente:

TEOREMA 5. *La condición necesaria para que tenga solución la ecuación* (3) *es que pueda cumplirse la igualdad* (4) *para todos los módulos m y cualesquiera restos* $\bar{a}_i = a_i$ mód (m), $i = 1, 2, ..., n$.

EJEMPLO 1. Hallar todas las soluciones de la ecuación diofántica

$$x^2 + 21xy + 14y^2 - 3 = 0.$$

La reducción respecto al módulo 7 de esta ecuación tiene la forma

$$x^2 \equiv \overline{3}.$$

Pero entre las clases de restos $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$ respecto al módulo 7 sólo son cuadrados las clases $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{4}$, esto se verifica directamente; $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{2}$, $\overline{4}^2 = \overline{2}$, $\overline{5}^2 = \overline{4}$ y $\overline{6}^2 = \overline{1}$; por esto la igualdad $x^2 = \overline{3}$ no se cumple nunca y la ecuación dada no tiene soluciones.

2. Hallar todas las soluciones de la ecuación diofántica

$$15x^2 - 7y^2 = 9.$$

Supongamos que $x = m$, $y = n$ son la solución. Del examen de la divisibilidad por 3 y por 9 se deduce que m^2 y n^2 son divisibles por 9; al mismo tiempo los cocientes de la división también serán n cuadrados, lo que se obtiene fácilmente del teorema fundamental de la aritmética. Así, pues, $m^2 = 9m_1^2$ y $n^2 = 9n_1^2$. La ecuación dada se reduce ahora a la forma

$$15m_1^2 - 7n_1^2 = 1,$$

y la reducción con respecto al módulo 5 da

$$-2n_1^2 = \overline{1}.$$

Teniendo en cuenta que $-\overline{2}\,\overline{2} = -\overline{4} = \overline{1}$, obtenemos

$$\overline{n}_1^2 = \overline{2}.$$

Pero entre los restos respecto al módulo 5 sólo son cuadrados $\overline{0}$, $\overline{1}$ y $\overline{4}$. Por esto la ecuación dada no tiene solución.

Es natural que se nos plantee la pregunta: ¿es suficiente la condición de solubilidad de la reducción de la ecuación diofántica dada respecto a todos los módulos posibles para que dicha ecuación tenga solución? En el caso general la respuesta a esta pregunta es negativa. Puede demostrarse que, por ejemplo, la ecuación diofántica

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0,$$

que, evidentemente, no tiene soluciones (porque ni 13, ni 17, ni 221 son cuadrados en el anillo Z), al reducirse respecto a un módulo m cualquiera adquiere solución entre las clases de restos respectivas. Pero nuestros conocimientos para este fin son ahora insuficientes: se necesita una descripción detallada de los subconjuntos de cuadrados que hay en el anillo de clases de restos respecto al módulo m. He aquí cómo se obtiene por lo menos cuando los m son primos.

Supongamos que p es un número primo distinto de 2 (y, por consiguiente, impar) y $-\frac{p-}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}$ son todos los elementos de Z_p. Si cada

uno de estos se eleva al cuadrado, se obtienen no más de $\frac{p-1}{2}$ elementos diferentes no nulos: porque todos ellos están contenidos en el conjunto

$$1=(-1)^2,$$
$$2^2=(-1)^2,$$
$$\cdot\ \cdot$$
$$\cdot\ \cdot$$
$$\cdot\ \cdot$$
$$\left(\frac{p-1}{2}\right)^2=\left(-\frac{p-1}{2}\right)^2$$

Además, todos los cuadrados $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ son diferentes dos a dos: si fuera $\alpha^2=\beta^2$, necesariamente sería $(\alpha-\beta)\times(\alpha+\beta)=0$, y o bien $\alpha=\beta$ (porque en Z_p no hay divisores de cero), o bien $\alpha=-\beta$; la primera es imposible, ya que α y β son diferentes por la condición, la segunda está excluida, porque α y β son elementos distintos del conjunto $1, 2, \ldots, \frac{p-1}{2}$. Por consiguiente, en Z_p hay exactamente $\frac{p-1}{2}$ cuadrados no nulos.

¿Cuándo se encuentra entre estos elementos -1? Según el pequeño teorema de Fermat $a^{p-1}=1$ para todos los $a\neq 0$ de Z_p. Si a es un cuadrado, es decir, $a=b^2$ para cierto b, será $a^{\frac{p-1}{2}}=(b^2)^{\frac{p-1}{2}}=b^{p-1}=1$. En general, $x^{\frac{p-1}{2}}$ es igual a 1 ó -1 en dependencia de que x sea o no sea cuadrado. En efecto, si x es un cuadrado, como ya hemos visto, esto es así; en cambio, si x no es un cuadrado, $x^{\frac{p-1}{2}}=r$, pero ya $r^2=1$, ó $r^2-1=0$. Esto último, en virtud de la correlación $r^2-1=(r-1)(r+1)$ y la ausencia en Z_p de divisores de cero, sólo es posible cuando $r=1$ ó $r=-1$. Si fuera $r=1$, el polinomio $z^{\frac{p-1}{2}}-1$ sobre Z_p se anularía más que para $\frac{p-1}{2}$ valores de z. Sin embargo, esto no es posible por la siguiente causa:

Supongamos que $f(z)=a_0z^n+\ldots+a_n$ es un polinomio arbitrario sobre Z_p y $f(c)=0$ para cierto c de Z_p; entonces necesariamente $f(z)=(z-c)g(z)$ para cierto polinomio $g(z)$ sobre Z_p. En efecto, procedemos a la inducción respecto al número n, llamado GRADO del polinomio $f(z)$ tiene la forma a_0z+a_1 y como $f(c)=0$, *es decir*, $a_0c+a_1=0$, necesariamente $f(z)=a_0z-a_0c$. Por consiguiente, $f(z)=(z-c)a_0$. Supongamos que la proposición ha demostrada para todos los grados menores que n. El polinomio $g_1(z)=f(z)-a_0z^{n-1}(z-c)$ es de grado menor que n y, evidentemente, se anula para $z=c$. Por esto, de acuerdo con el supuesto de inducción, $g_1(z)=(z-c)g_2(z)$ y, por consiguiente, $f(z)=g_1(z)+a_0z^{n-1}(z-c)=(z-c)(a_0z^{n-1}+g_2(z))$. La afirmación queda demostrada. De ella se deduce que si $c_1, \ldots, c_k$ son diversos elementos de Z_p, para los que $f(c_1)=\ldots=f(c_k)=0$, será $f(z)=(z-c_1)\ldots(z-c_k)g(z)$. Hay que razonar lo mismo que antes, separando primero en $f(z)$ el factor $z-c_1$ obteniéndose $f(z)=(z-c_1)g_1(z)$ y, por lo tanto, $g_1(c_2)=0$, después $z-c_2$ en $g_1(z)$ y así sucesivamente. Como en la multiplicación los exponentes de los polinomios se su-

man, en la expresión $f(z) = (z - c_1)...(z - c_k)g(z)$ no puede haber en el segundo miembro factores de la forma $(z - c_i)$ mayores que el grado del polinomio $f(z)$. He aquí por qué el polinomio $z^{p-1} - 1$, citado en el párrafo precedente, no puede ser mayor que los $\frac{p-1}{2}$ valores de z para los cuales su valor es igual a 0.

Por consiguiente, $x^{\frac{p-1}{2}} = -1$. De aquí se saca una conclusión importante en principio: el elemento x de Z_p es cuadrado si, y solamente si, $x^{\frac{p-1}{2}} = 1$, y no es un cuadrado si, y solamente si, $x^{\frac{p-1}{2}} = -1$. Por lo tanto, -1 es un cuadrado cuando $(-1)^{\frac{p-1}{2}} = 1$, y no es un cuadrado cuando $-1)^{\frac{p-1}{2}} = -1$. *El número* p es impar; por consiguiente, o bien $p = 4k+1$, o bien $p = 4k-1$. En el primer caso necesariamente $(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$ y (-1) es un cuadrado; en el segundo caso necesariamente $(-1)^{\frac{p-1}{2}} = (-1)^{2k-1} = -1$ y -1 no es un cuadrado. Otra afirmación: si x e y de Z_p no son cuadrados, necesariamente xy será un cuadrado (demuéstrelo independientemente).

En la ecuación diofántica $(x^2-13)(x^2-17)(x^2-221) = 0$ vemos que $221 = 13 \cdot 17$; por consiguiente, en la reducción con respecto a un módulo primero esta ecuación tiene solución (aunque una de las clases $13 \cdot 17$ ó $13 \cdot 17$ es un cuadrado).

Ahora puede demostrarse la afirmación enunciada ya en el cap. II: todo número primo p de la forma $p = 4k + 1$, donde k es entero, es norma de un número gausiano entero (y, por lo tanto, puede representarse en la forma de suma de dos cuadrados enteros): $p = x^2 + y^2$. La demostración la haremos por inducción respecto a p. Si $p = 5$ (este es el más pequeño de los p de la forma $4k+1$) la afirmación es evidente: $5 = 2^2 + 1^2$. Supongamos que la afirmación está demostrada para todos los números primos de la forma $4k+1$ menores que el número primo p de esta misma forma: $p = 4k + 1$. En el anillo Z_p la clase -1 es un cuadrado (esto fue demostrado antes), es decir, $x^2 + 1 = 0$ para cierta x de Z_p. Esto significa que en el anillo de números enteros Z, $x^2 + y^2 = lp$, donde x e y son números enteros y donde la clase de restos del mismo número y es la clase 1. Como todos los cuadrados que hay en Z_p se obtienen de la serie $0^2, 1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$, puede considerarse que $0 < x, y < \frac{p}{2}$ y, por consiguiente, $l < p$. Desde luego, vamos a considerar que x e y son números enteros primos entre sí (en el caso contrario simplificaríamos la igualdad $x^2 + y^2 = lp$ por sus divisores comunes).

Supongamos que $l = p_1 \cdot p_2 ... p_r$ es la descomposición de l en factores primos en el anillo Z. Como $(x, y) = 1$ y $x^2 + y^2$ es divisible por p_j $(j = 1, 2, ..., r)$, la clase -1 mód (p_j) es un cuadrado en Z_{p_j}, será $p_j = 4m_j + 1$ para cierto entero m_j $(j = 1, 2, ..., r)$. Y como $p_j < p$, por el supuesto de inducción

$$p_j = x_j^2 + y_j^2 = (x_j + iy_j)(x_j + i)_j) = t^{(j)}, \ \bar{t}^{(j)},$$

donde $t^{(j)}, \bar{t}^{(j)}$ son factores primos en el anillo de los números gausianos enteros, y, como de ordinario, $a + bi = a - bi$ es un número conjugado

Por consiguiente,

$$(x+iy)(x-iy) = pt^{(1)}\ldots t^{(r)}\bar{t}^{(1)}\ldots\bar{t}^{(r)}.$$

En el segundo miembro de esta igualdad tenemos un producto de números gausianos primos. Aplicando el hecho de que el teorema fundamental de la aritmética es justo en el anillo de los números gausianos, simplificamos los dos miembros de la última igualdad por los números primos $t^{(1)}$, $\bar{t}^{(1)}$, ..., $t^{(r)}$, $\bar{t}^{(r)}$, y como resultado obtenemos la representación del número entero primo p en forma de producto de números gausianos conjugados. El teorema queda demostrado.

El estudio de las ecuaciones sobre los anillos de clases de restos tiene gran importancia en la teoría de los números precisamente porque permite en muchos casos "prever" el resultado de la resolución de algunos problemas diofánticos.

Terminaremos este capítulo con un ejemplo de estudio de las resoluciones de una ecuación diofántica particular:

$$f(x,\ y) = ax^2 + 2bxy + cy^2 = 0.$$

Convengamos en designar con el símbolo $f_p(x,\ y)$ la reducción del polinomio $f(x,\ y)$ respecto al módulo p.

TEOREMA 6. Sea $p \neq 2$ un número primo. La ecuación $f_p(x,\ y) = 0$

tiene solución distinta de $x = y0 = 0$ mód (p) *si, y solamente si,* $\bar{b}^2 - \bar{a}\cdot\bar{c} = (b^2 - ac)$ mód (p) *es un cuadrado en el anillo* Z_p.

Demostración. Sea $\bar{b} - \bar{ac} = \bar{z}^2$ y supongamos que $a \neq \neq 0$. Como entre las clases no nulas de restos respecto a un módulo primo es posible la división, de las transformaciones algebraicas puede resultar la igualdad siguiente:

$$\bar{a}x^2 - \bar{2}\bar{b}xy + \bar{c}y^2 = \bar{a}\left(x - \frac{-\bar{b}+\bar{z}}{\bar{a}}y\right)\left(x - \frac{-\bar{b}-\bar{z}}{\bar{a}}y\right)$$

(de su corrección es posible convencerse directamente, basándose en las definiciones de las operaciones con monomios). Por consiguiente, basta hallar las soluciones de la ecuación:

$$\left(x - \frac{\bar{z}-\bar{b}}{\bar{a}}y\right)\left(x + \frac{\bar{b}+\bar{z}}{\bar{a}}y\right) = 0.$$

Estas soluciones, en virtud de la ausencia de divisores de cero en el anillo de las clases de restos respecto a un número primo, se definen por dos igualdades independientes:

$$x = \frac{-\bar{b}+\bar{z}}{\bar{a}}y \quad \text{y} \quad x = \frac{-\bar{b}-\bar{z}}{\bar{a}}y.$$

Si $\bar{a}=\bar{0}$ y $\bar{c} \neq \bar{0}$, todo lo dicho anteriormente se traslada fácilmente a este caso. Si, en cambio, $\bar{a}=\bar{c}=\bar{0}$, la solución no nula de la ecuación dada será, por ejemplo, $x=\bar{1}$, $y=\bar{0}$.

Al contrario, sean $x=\bar{x}$, $y=\bar{y}$ la solución, siendo $x \neq 0$ o $\bar{y} \neq 0$. Si $\bar{a}=\bar{c}=\bar{0}$, la afirmación es evidente: $\bar{b}^2$ es un cuadrado. Sea $\bar{a} \neq \bar{0}$. Entonces

$$\bar{0}=\bar{a}\bar{x}^2+2\bar{b}\bar{x}\bar{y}+\bar{c}\bar{y}^2=\bar{a}^2\left(\bar{x}^2+\frac{\overline{2b}}{\bar{a}}\bar{x}\bar{y}+\frac{\bar{c}}{\bar{a}}\bar{y}^2\right)=$$

$$=\bar{a}\left(\left(\bar{x}+\frac{\bar{b}}{\bar{a}}\bar{y}\right)^2-\frac{\bar{b}^2-\bar{a}\bar{c}}{\bar{a}^2}\bar{y}^2\right).$$

Por consiguiente,

$$\left(\bar{x}+\frac{\bar{b}}{\bar{a}}\bar{y}\right)^2=\frac{\bar{b}^2-\bar{a}\bar{c}}{\bar{a}^2}\bar{y}^2.$$

Como $\bar{a} \neq \bar{0}$, la clase $\bar{y}$ es distinta de 0; si fuera $\bar{y}=0$, también sería $\bar{x}=0$ y esto contradice la condición. Por consiguiente,

$$\bar{b}^2-\bar{a}\cdot\bar{c}=\frac{\bar{a}^2}{\bar{y}^2}\left(\bar{x}+\frac{\bar{b}}{\bar{a}}\bar{y}\right)^2=\left[\frac{\bar{a}}{\bar{y}}\left(\bar{x}+\frac{\bar{b}}{\bar{a}}\bar{y}\right)\right]^2.$$

El teorema queda demostrado.

En la condición se supuso que $p \neq 2$. Pero esto se hizo no porque siendo $p=2$ el teorema sea incorrecto: en este caso su afirmación es trivial, porque la solución de $\bar{f}_2(x, y)$ es igual a $\bar{a}x^2+\bar{c}y^2$ y ambas clases de rectos respecto al módulo 2 son cuadrados y, al mismo tiempo, la eucación $\bar{a}x^2+\bar{c}y^2=\bar{0}$ tiene necesariamente soluciones; esto se establece simplemente seleccionando tódos los valores posibles del polinomio $\bar{f}_2(x, y)$.

CAPÍTULO IV

SISTEMAS DE NUMERACIÓN

Cuando escribimos los números, empleamos generalmente diez símbolos: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Estos símbolos se llaman *cifras decimales*. En este capítulo vamos a estudiar el papel que desempeña el número 10 en la escritura tradicional de los nú-

meros y describiremos los posibles procedimientos de sustituir el "diez" por otros números naturales. En nuestro tiempo ha adquirido una importancia especial la forma de escritura en la cual el papel de diez lo desempeña el dos: en las calculadoras o computadoras electrónicas no se emplea el sistema decimal, sino el sistema de escritura llamado BINARIO.

§ 1. SISTEMA DECIMAL DE NUMERACIÓN

Se entiende por sistema decimal de numeración todo el sistema de números, escritos de la forma ordinaria valiéndose de las cifrás decimales cuyos símbolos son 0, 1, 2, ..., 9, cada uno de los cuales designa a cierto número entero no negativo. Los sistemas de escritura de este tipo se llaman "posicionales" y en ellos la cifra indica distintos números en dependencia del lugar que ocupa en la escritura. Naturalmente, en vez de estos diez símbolos podían haberse tomado otros. pero si estos otros fueran de nuevo diez y se utilizaran de un modo análogo a las cifras tradicionales, el sistema de números debería llamarse también decimal.

¿En qué consiste el papel del número diez? Nosotros escribimos los números valiéndonos de todos los restos posibles de la división por 10; precisamente como restos de la división por 10 se comportan las cifras decimales en todas las operaciones aritméticas con números. En efecto, descifremos la notación decimal de un número:

Supongamos primeramente que N es un número natural. Del algoritmo de la división inexacta se deduce que $N = 10q_0 + r_0$, donde $0 \leqslant r_0 \leqslant 9$ y $0 \leqslant q_0 \leqslant N$ (si, por ejemplo, $N = 6$, será $q_0 = 0$ y $r_0 = 6$). Si el cociente $q_0 > 0$, de un modo exactamente igual, $q_0 = 10q_1 + r_1$, siendo $0 \leqslant r_1 \leqslant 9$ y

$$N = 10q_0 + r_0 = 10^2 q_1 + 10r_1 + r_0.$$

Si $q_1 > 0$, este proceso puede continuarse, obteniéndose

$$N = 10^3 q_2 + 10^2 r_2 + 10r_1 + r_0.$$

El cociente q_2 será menor que q_1, y q_1 menor que q_0, el cual será a su vez menor que N. Por esto, al cabo de un número fini-

to de pasos n obtenemos que $q_n = 0$ y

$$N = 10^n r_n + 10^{n-1} r_{n-1} + \ldots + 10 r_1 + r_0, \qquad (1)$$

donde $r_0, \ldots, r_n$ son números enteros no negativos y no superiores a 9. La expresión (1), obtenida de un modo totalmente concreto del número N, se llama representación decimal (o descomposición decimal) del número N.

Debe advertirse que si existiera una segunda expresión

$$N = 10^{n'} r'_{n'} + 10^{n'-1} r'_{n'-1} + \ldots + 10 r'_1 + r'_0, \qquad (1')$$

obtenida por algún otro procedimiento, y en la cual $r'_{n'}, \ldots, r'_0$ fueran números NO NEGATIVOS enteros Y no superiores a 9, resultaría que $n' = n$ y $r' = r_i$ para $i = 1, 2, \ldots, n$. Efectivamente, el resto de la división por 10 del número N está determinado unívocamente y, como se deduce de las representaciones (1) y (1'), es igual a r_0 y r'_0. Por esto $r_0 = r'_0$. La igualdad de los números r_1 y r'_1 se obtiene de la unicidad del resto de la división por 10 del número $\dfrac{N - r_0}{10}$. Damos al lector la posibilidad de que termine la demostración él mismo.

Si se admite que el símbolo $a_n a_{n-1} \ldots a_0$ designa las cifras decimales $a_n, a_{n-1}, \ldots, a_0$ escritas unas a continuación de otras, está claro que el número N, escrito en cifras decimales, tendrá la forma:

$$N = \overline{r_n r_{n-1} \ldots r_0}.$$

Con la representación (1) están ligados no pocos hechos interesantes. He aquí algunos de ellos:

TEOREMA 1. *La diferencia entre un número y la suma de sus cifras es divisible por* 9.

Demostración. Supongamos que se da el número N representado en la forma (1). Entonces

$$N - (r_0 + \ldots + r_n) = 10^n r_n + 10^{n-1} r_{n-1} + \ldots + 10 r_1 + r_0 -$$
$$- r_n - r_{n-1} - \ldots - r_1 - r_0 =$$
$$= (10^n - 1) r_n + (10^{n-1} - 1) r_{n-1} + \ldots + (10 - 1) r_1.$$

Pero 10 mód (9) = 1 mód (9), de manera que también 10^n mód (9) = 1 mód (9), en virtud de lo cual N mód (9) = $(r_n + \ldots + r_0)$

mód (9) y, por consiguiente, $N - (r_n + \ldots + r_0) \equiv 0$ mód (9). La afirmación queda demostrada.

COROLARIO. *Si la suma de las cifras de un número N es divisible por 9, dicho número también es divisible por 9.*

Al contrario, si un número es divisible por 9, la suma de sus cifras también es múltiplo de 9.

En efecto, si M es la suma de las cifras del número N y es divisible por 9, de $N \equiv M$ mod (9) se decuce que $N \equiv 0$ mód (9). Análogamente, si $N \equiv 0$ mód (9), de $N \equiv M$ mód (9) se deduce que también $M \equiv 0$ mód (9).

Exactamente del mismo modo se enuncia y demuestra la condición de divisibilidad por 3.

TEOREMA 2. *Si la diferencia entre la suma de las cifras de un número N situadas en los lugares pares y la suma de las cifras de este mismo número situadas en los lugares impares es divisible por* 11, *el número N es divisible por* 11. El recíproco también es correcto: *si el número N es múltiplo de* 11, *la diferencia entre las sumas de las cifras antes indicadas es divisible por* 11.

Demostración. Advertimos que $10^{2k} \equiv 1$ mód (11) y $10^{2k+1} \equiv 10$ mód (11). Por esto, pasando de la expresión (1) a los restos respecto al módulo 11, obtenemos:

$$N \equiv r_0 + 10n_1 + r_2 + 10r_3 \ldots \text{mód (11)},$$

de donde

$$N \equiv (r_0 + r_2 + \ldots) + 10(r_1 + r_3 + \ldots) \text{ mód (11)}.$$

Si $(r_0 + r_2 + \ldots) \equiv (r_1 + r_3 + \ldots)$ mód (11), será, naturalmente, $N \equiv (r_1 + r_3 + \ldots) + 10(r_1 + r_3 + \ldots)$ mod $(11) \equiv 0$ mód (11). Al contrario, si $N \equiv 0$ mód (11), teniendo en cuenta la congruencia $10 \equiv -1$ mód (11), obtenemos:

$$(r_0 + r_2 + \ldots) + 10(r_1 + r_3 + \ldots) \equiv 0 \text{ mód (11)}$$

y

$$(r_0 + r_2 + \ldots) - (r_1 + r_3 + \ldots) \equiv 0 \text{ mód (11)}.$$

Como vemos, en la escritura decimal de un número natural, las cifras se encuentran en un orden completamente riguroso como restos de la división por 10. Todo número entero se escribe exactamente del mismo modo, pero antes de escribir un número negativo se pone el signo menos.

Pasemos a los números racionales, es decir, a las fracciones de la forma $R = \dfrac{N}{M}$, donde, para empezar, consideraremos que

N y M son números naturales, y luego estudiaremos también los números racionales negativos. Nuestro fin inmediato es obtener para este número una descomposición de la forma (1) que coincida con ella para $M = 1$.

Vamos a considerar que la fracción $R = \frac{N}{M}$ es propia, es decir, $N < M$. En el caso contrario podríamos separar la parte entera, cuya representación decimal ya se ha descrito, y después analizar la fracción propia.

Sea $10N - q_1 M + a_1$, donde $0 \leqslant a_1 < M$. Entonces $0 \leqslant q_1 < 9$, porque $10N < 10M$ y

$$R = \frac{N}{M} = \frac{10N}{10M} = \frac{q_1 M + a_1}{10M} = 10^{-1} q_1 + 10^{-1} \frac{a_1}{M}.$$

Si $a_1 = 0$, la representación decimal de R tiene la forma:

$$R = 10^{-1} q_1. \tag{2}$$

Si $a_1 \neq 0$, análogamente,

$$\frac{a_1}{M} = 10^{-1} q_2 + 10^{-1} \frac{a_2}{M},$$

donde otra vez $0 \leqslant q_2 \leqslant 9$ y $0 \leqslant a_2 < M$. Si $a_2 = 0$ la representación decimal de R tiene la forma:

$$R = 10^{-1} q_1 + 10^{-2} q_2.$$

Si $a_2 \neq 0$,

$$\frac{a_2}{M} = 10^{-1} q_3 + 10^{-1} \frac{a_3}{M},$$

donde $0 \leqslant q_3 \leqslant 9$ y $0 \leqslant a_3 < M$ y así sucesivamente.

Pueden ocurrir dos casos: o bien en uno de los pasos el resto se anula y obtenemos una fracción decimal finita

$$R = 0,\ \overline{q_{-1} q_{-2} \ldots\ q_{-k}} = q_{-1} 10^{-1} + q_{-2} 10^{-2} + \ldots + q_{-k} 10^{-k},$$

o bien a_k no se anula nunca. Pero como los restos de la división por el número M son únicamente M, los restos a_k (y, por consiguiente, los cocientes q_k) comienzan a repetirse, es decir, obte-

nemos una fracción decimal periódica infinita:

$$R = 10^{-1}q_{-1} + 10^{-2}q_{-2} + \ldots + 10^{-k}q_{-k} + \ldots$$

Estudiemos este caso más detalladamente para establecer la longitud del período. Supongamos que la tabla para el cálculo de los restos tiene la forma:

$$\begin{aligned} 10a_0 &= Mq_1 + a_1, \\ 10a_1 &= Mq_2 + a_2, \\ &\ldots\ldots\ldots \\ 10a_{k-2} &= Mq_{k-1} + a_{k-1}, \\ 10a_{k-1} &= Mq_k + a_0. \end{aligned} \tag{4}$$

Aquí, para simplificar, la numeración de las letras se ha elegido de tal modo que la primera cifra del período (es decir, cierto cociente q_i, obtenido en el proceso antes discrito) tenga el número 1, en la última fila de la tabla, de nuevo, por segunda vez, aparece el resto a_0, con el cual se inició la enumeración en (4). Recordaremos que los restos $a_0, a_1, \ldots, a_{k-1}$ son todos distintos de cero, lo que, naturalmente, no puede decirse de las cifras q_i. Esquemáticamente, el trozo correspondiente a la fracción decimal tiene la forma:

$$0, \overline{\ldots q_1 q_2 \ldots q_{k-1} q_k \ldots}$$

Una vez que escribamos la cifra q_k, la siguiente cifra calculada volverá a ser q_1; por consiguiente, el período de la fracción empieza con la cifra q_1 y termina en q_k. En total, el número de cifras es k. Consideremos (4) respecto al módulo M:

$$\begin{aligned} 10a_0 &\equiv a_1, \\ 10a_1 &\equiv a_2, \\ &\ldots\ldots\ldots \\ 10a_{k-2} &\equiv a_{k-1}, \\ 10a_{k-1} &\equiv a_0; \end{aligned} \tag{5}$$

sustituyendo la a_1 de la segunda congruencia por la a_1 de la primera, la a_2 de la tercera por la a_2 de la segunda y así sucesivamente, obtenemos:

$$10^k a_0 \equiv a_0$$

Pueden ocurrir dos casos: $(10, M) = 1$ y $(10, M) \neq 1$. En el primer caso, en la igualdad $10N = Mq + a$, donde $0 \leqslant a < M$, los números a y M son primos entre sí, porque cualquier divisor común de ellos, al ser primo con 10, debe dividir también a N, y $(N, M) = 1$ por la condición. Por consiguiente, para $(10, M) = 1$ todos los restos a_i son primos con M y, en particular, $(a_0, M) = 1$. Esto significa que la clase a_0 mód (M) es invertible y, por esto

$$10^k \equiv 1 \text{ mód } (M).$$

El número k, para el cual $10^k \equiv 1$ mód (M), es el menor entre los números naturales n para los que $10^n \equiv 1$ mód (M). En efecto, si fuera $10^n \equiv 1$ mód (M) para $n < k$, de las congruencias (5) se deduciría que

$$a_n \equiv 10^n a_0 \equiv a_0 \text{ mód } (M).$$

Pero a_n y a_0 son restos de la división por M, por lo que la congruencia $a_n \equiv a_0$ mód (M) significa la igualdad $a_n = a_0$ y esto contradice al hecho de que todos los restos $a_0, a_1, \ldots, a_{k-1}$ son distintos dos a dos (en esto se fundaron las igualdades (4)).

Estudiemos el caso $(10, M) \neq 1$. Sea $M = 2^r 5^s M'$, donde ya $(10, M') = 1$. Entonces $R = \dfrac{N}{M} = \dfrac{N}{2^r 5^s M'}$; multiplicamos el numerador y el denominador de la fracción R por tales potencias de dos y de cinco, que el denominador tome la forma $10^l M'$ (por ejemplo, $\dfrac{29}{140} = \dfrac{29}{2^2 \cdot 5 \cdot 7} = \dfrac{2^0 \cdot 5 \cdot 29}{10^2 \cdot 7} = \dfrac{145}{10^2 \cdot 7}$). Obtenemos: $R = 10^{-l} \dfrac{N'}{M'}$, donde $(M', N') = 1$ y $(M', 10) = 1$. Por lo demostrado, el período de la fracción $R' = \dfrac{N'}{M'}$ es igual a aquel número natural mínimo k para el cual $10^k \equiv 1$ mód (M'). Pero el período de la fracción $R = 10^{-l} \cdot R'$ es el mismo, sólo que empieza l signos más a la derecha.

Hemos demostrado el siguiente teorema:

TEOREMA 3. *Sea* $R = \dfrac{N}{M}$ *y* $M = 2^r 5^s M'$, *donde* $(N, M) = 1$ *y* $(10, M') = 1$. *En este caso el período de la fracción es igual al número natural mínimo* k *para el cual*

$$10^k \equiv 1 \text{ mód } (M').$$

Antes de describir la reconstrucción de las cifras decimales de las fracciones racionales, basada, como en el caso de los números naturales, en la descomposición decimal

$$R = r_{-1} \cdot 10^{-1} + \ ... + \ r_{-n} \cdot 10^{-n} + \ ..., \qquad (6)$$

donde $0 \leqslant r_{-i} \leqslant 9$, indicaremos la siguiente circunstancia, en virtud de la cual se introducirá la uniformidad de la representación (6):

$$10^{-s} = 9 \cdot 10^{-s-1} + 9 \cdot 10^{-s-2} + \ ... \ + 9 \cdot 10^{-s-n} + \ ...$$

(es decir, 0, 0 ... 0 1 = 0, 0 ... 0 9 9 ... 9 ...).

Demostración. De acuerdo con la regla de sumación de una progresión geométrica infinitamente decreciente, tenemos

$$9 \cdot 10^{-s-1} + 9 \cdot 10^{-s-2} + ... = \\ = 9 \cdot 10^{-s} \times \\ \times (10^{-1} + 10^{-2} + ...) = \\ = 9 \cdot 10^{-s} \cdot \frac{10^{-1}}{1 - 10^{-1}} = 10^{-s}.$$

Por esto es natural suponer que en todas partes, en vez del "nueve período", pueda escribirse la unidad en el orden que precede al período, es decir,

$$0, \overline{r_{-1} ... r_{-k}\ 9\ 9} \ ... = 0, \overline{r_{-1} ... r_{-k}} + 0, \underbrace{0 \ ... \ 0\ 1}_{k}.$$

La reconstrucción de las cifras decimales de la fracción R puede definirse ahora así.

Sea

$$R = r_{-1} \cdot 10^{-1} + r_{-2} \cdot 10^{-2} + \ ... \ + r_{-k} \cdot 10^{-k} + \ ...$$

Entonces r_{-1} es la parte entera del número $10R$, r_{-2} es la parte entera del número $10(10R - r_{-1})$ y así sucesivamente. r_{-k} es la parte entera del número

$$10^{k}R - 10^{-k-1} r_{-1} - ... - 10 r_{-k+1}.$$

Veamos ahora en unos ejemplos el resultado obtenido. Sea $R = \frac{2}{3}$. La longitud del período l de esta fracción en la repre-

sentación decimal es igual al menor de tales números k, que $10^k \equiv 1$ mód (3). Es evidente que $l = 1$. El período mismo es fácil de determinar: $R = 0,\ 666\ \ldots$

He aquí un ejemplo de fracción con período más largo en la representación decimal: $R_l = \frac{1}{7}$. Aquí la mejor forma de buscar el número mínimo l, para el cual $10^l \equiv 1$ mód (7), es la siguiente. Para facilitar las anotaciones vamos a omitir el símbolo mód (7). En el anillo Z_7 tenemos: $10 \equiv 3$. Por esto, $10^n \equiv 3^n$ y, por consiguiente,

$$3^1 \equiv 3,$$
$$3^2 \equiv 2,$$
$$3^3 \equiv 3 \cdot 2 \equiv 6,$$
$$3^4 \equiv 3 \cdot 6 \equiv 4,$$
$$3^5 \equiv 3 \cdot 4 \equiv 5,$$
$$3^6 \equiv 3 \cdot 5 \equiv 1.$$

Así, pues, la longitud del período l es igual a 6.

EJERCICIOS

1. Hallar la longitud del período de la fracción $R = \frac{1}{23}$ en la representación decimal.

Respuesta. La longitud del período es igual a 22.

2. Demostrar que existen fracciones decimales con períodos de longitud tan grande como se quiera.

INDICACIÓN. Supongamos que N es un número natural arbitrario. Escribamos la fracción decimal R en varios pasos de acuerdo con la regla siguiente: 1er paso, 0,10; 2º paso, 0,101100; 3er paso, 0,101100111000, ... y así sucesivamente hasta que el número de cifras de la parte fraccionaria no supere N. Después de esto añadimos a la fracción obtenida su parte fraccionaria una vez, otra, y así sucesivamente. La fracción infinita obtenida será, desde luego, periódica. Queda por demostrar únicamente que su período es igual a la parte que se añade.

Resumiendo, puede decirse que todo número racional se escribe en forma de fracción, finita o infinita, pero necesariamente decimal periódica (cuya parte entera puede ser igual a 0 o distinta de él). Sin duda, también es correcta la afirmación

recíproca: toda fracción decimal finita o infinita, pero periódica, es un número racional. Para la fracción finita esta afirmación es simplemente evidente, y para la periódica se demuestra así. La fracción periódica dada puede representarse en forma de suma de una fracción decimal finita y de una fracción de la forma:

$$\rho = 0, \underbrace{0 \ldots 0}_{s} \overline{q_1 \ldots q_n q_1 \ldots q_n},$$

donde $\overline{q_1 \ldots q_n}$ es el período. Como ya se dijo, el primer sumando (es decir, la fracción finita) es un número racional; en cuanto al segundo, suponiendo que $\overline{q_1 \ldots q_n} = q$, lo representaremos de la forma:

$$\rho = q \cdot 10^{-n-s} + q \cdot 10^{-2n-s} + q \cdot 10^{-3n-s} + \ldots =$$
$$= q \cdot 10^{-s}(10^{-n} + 10^{-2n} + 10^{-3n} + \ldots).$$

De acuerdo con la regla de sumación de una progresión geométrica infinitamente decreciente, tenemos

$$10^{-n} + 10^{-2n} + \ldots = \frac{10^{-n}}{1 - 10^{-n}} = \frac{1}{10^n - 1}.$$

De este modo, ρ es un número racional y, por lo tanto, también es racional la fracción dada.

Finalmente, vamos a ocuparnos de los números irracionales, denominación por la cual se suele entender las fracciones decimales no periódicas infinitas. La reconstrucción de las cifras decimales de estos números se hace en dos etapas: primero se reconstruyen las cifras de la parte entera (según la regla descrita para los números enteros) y después las cifras de la parte fraccionaria.

Así, un número real arbitrario R (que consideraremos no negativo) se escribe, en el sistema decimal de numeración, de la forma

$$R = 10^n a_n + \ldots + 10a_1 + a_0 + 10^{-1}a_{-1} + \ldots + 10^{-k}a_{-k} + \ldots, \quad (7)$$

donde $a_n, \ldots, a_1, a_0, a_{-1}, \ldots, a_{-k}$ son cifras decirmales. Teniendo en cuenta la observación hecha en la pág. 67, la representación (7) del número R es única. A (7) le llamaremos representación decimal (o descomposición decimal) del número R.

Suponiendo que P y Q son números reales escritos en la forma (7) y, como de ordinario, $P \geqslant Q$, $Q \geqslant 0$. Describamos la descomposición (7) del número $P + Q$. Hablando en rigor, la descomposición del número $P + Q$ puede obtenerse únicamente "elevando gradualmente la exactitud con que se dan" los sumandos P y Q. Pero como nosotros no nos proponemos ahora desarrollar la aritmética de los números reales, sino que queremos solamente ilustrar el comportamiento de las cifras al sumarse, será suficiente considerar que P y Q son fracciones decimales finitas:

$$P = 10^n p_n + \ldots + 10^r p_r + \ldots + p_0 + 10^{-1} p_{-1} + \ldots + \\ + 10^{-m} p_{-m},$$

$$Q = 10^l q_l + \ldots + 10^r q_r + \ldots + q_0 + 10^{-1} q_{-1} + \ldots + \\ + 10^{-m} q_{-m}, \tag{8}$$

(entre las cifras están p_{-m} y q_{-m} aunque una no es igual a 0).

En la descomposición (7) del número $P + Q$ para 10^{-k}, $k > m$, figuran cifras nulas. Para 10^{-m} figura el resto de la división por 10 del número $p_{-m} + q_{-m}$; supongamos que $p_{-m} + q_{-m} = 10a_{-m} + b_{-m}$, $0 \leqslant b_{-m} \leqslant 9$. Entonces, para 10^{-m+1} figura el resto de la división por 10 del número $p_{-m+1} + q_{-m+1}$, sumado con el cociente a_{-m} y reducido otra vez respecto al módulo 10, y así sucesivamente. Las cifras p_r y q_r resultan, de este modo, subordinadas a la suma aritmética de los restos respecto al módulo 10.

Pasemos a la representación decimal del número $P - Q$, sin tener en cuenta que P y Q están dados en la forma (8), pero, en cambio, suponiendo conocido el proceso de adición en el caso general.

Sean $10^n \leqslant Q < 10^{n+1}$ y $Q = 10^{n+1} - Q'$. Por lo tanto, $P - Q = -10^{n+1} + P + Q'$ y la descomposición decimal del número $P - Q$ es fácil de obtener de la descomposición decimal del número $P + Q'$. En efecto, supongamos que a_{n+1} es la cifra del número $P + Q'$ que figura en la descomposición (7) para 10^{n+1}. Si $a_{n+1} \geqslant 1$, la respuesta es evidente. Si $a_{n+1} = 0$, hay que analizar dos casos: $10^{n+1} > P + Q'$ y $10^{n+1} < P + Q'$. En el primer caso el número $P + Q' - 10^{n+1}$ es negativo y su escritura decimal se obtiene basándose en la representación

$$10^{n+1} = 9 \cdot 10^n + 9 \cdot 10^{n-1} + \ldots + 9 \cdot 10 + 9 + 9 \cdot 10^{-1} + \\ + 9 \cdot 10^{-2} + 9 \cdot 10^{-3} + \ldots \qquad (9)$$

El número $P + Q'$ puede restarse de esta representación simplemente de orden en orden y después, si es necesario, se utiliza la observación hecha en la pág. 67. En cuanto al caso $10^{n+1} < P + Q'$ y $a_{n+1} = 0$, se analiza así. Supongamos que a_{n+k} es la cifra distinta de cero inmediata por la izquierda a a_{n+1} (esta cifra existe en virtud de la desigualdad $10^{n+1} < P + Q'$). Entonces, en vez del sumando $a_{n+k} \cdot 10^{n+k}$ puede escribirse una suma de dos sumandos: $(a_{n+k} - 1)\, 10^{n+k}$ y 10^{n-k}, pero 10^{n+k} se representa en una forma análoga a (9). Después de esto la escritura decimal del número $P + Q' - 10^{n+k}$ se obtiene de acuerdo con las reglas indicadas para la adición.

En el ejemplo de estas dos operaciones aritméticas fundamentales con los números, vemos ya que las cifras decimales se comportan como restos de la división por 10. La multiplicación y la división de los números reales en la escritura decimal se definen basándose en las operaciones de adición y sustracción, por lo que las cifras vuelven a resultar subordinadas a la aritmética de los restos respecto al módulo 10.

§ 2. SISTEMA DE NUMERACIÓN *N*-ARIO

Por el párrafo precedente podemos darnos cuenta de que el número y el procedimiento según el cual se escribe (fórmula (7)), están relacionados principalmente sólo por la tradición. Nosotros empezamos por el algoritmo de cálculo de las cifras decimales tomando un número natural arbitrario N, y no por cómo se ha escrito este número.

Sustituyamos ahora el diez por otro número natural N fijado arbitrariamente y repitamos, por lo menos en los rasgos importantes, la construcción del párrafo anterior.

En primer lugar hacen falta las cifras, o sea, todos los restos posibles de la división por N, es decir, los números $0, 1, \ldots, N - 1$. A propósito, si $N = 1$ (porque éste también es un número natural), 0 será la única cifra; desde luego, si sólo se dispone de una cifra es imposible escribir el conjunto infinito de los números. Por esto supondremos que $N \geqslant 2$.

Sea A un número natural arbitrario. Escribámoslo por medio de los restos de su división por N, es decir, mediante los números 0, 1, ..., $N-1$. Para esto dividiremos inexactamente A por N:

$$A = Nq_0 + r_0, \quad 0 \leqslant r_0 < N.$$

Si $q_0 = 0$, la igualdad

$$A = r_0$$

será la representación N-aria buscada del número A. Pero si $q_0 \neq 0$, dividiremos inexactamente q_0 por N:

$$q_0 = Nq_1 + r_1, \quad 0 \leqslant r_1 < N.$$

Entonces

$$A = N'q_1 + Nr_1 + r_0.$$

Si $q_1 = 0$, la representación N-aria buscada del número A será

$$A = r_1 N + r_0.$$

Si, por el contrario $q_1 \neq 0$, el proceso debe continuarse. Como q_1 es menor que q_0, y q_0 es nenor que A, los cocientes q_0, q_1, etc. irán disminuyendo sin dejar de ser números enteros no negativos; por consiguiente, en cierta etapa obtendremos un cociente q_k nulo y, al mismo tiempo, la representación N-aria del número natural A:

$$A = r_k N^k + r_{k-1} N^{k-1} + \ \ldots \ + r_1 N + r_0, \qquad (10)$$

donde $r_0, r_1, \ldots, r_{k-1}, r_k$ son números enteros no negativos, no superiores a $N-1$; a estos números hemos convenido en llamarles cifras N-arias.

La representación (10) del número natural A es única, es decir, no depende del procedimiento descrito de cálculo de las cifras $r_0, r_1, \ldots, r_{k-1}, r_k$. Si fuera

$$A = r'_{k'} N^{k'} + r'_{k'-1} N^{k'-1} + \ \ldots \ + r'_1 N + r'_0 \qquad (10')$$

y $r'_{k'}, r'_{k'-1}, \ldots, r'_1, r'_0$ fueran números enteros no negativos, no superiores a $N-1$, r'_0 y r_0 coincidirían como restos de la división por N del número A, r_1 y r_1, como restos de dividir por N el número $\dfrac{A - r_0}{N}$ y así sucesivamente.

EJERCICIOS

1. Escribir el número $A = 722$ en el sistema binario.

Las cifras del sistema binario son los números 0 y 1. Tenemos que escribir, por consiguiente, $A = 722$ por medio de los números 0 y 1. Para que sea más fácil calcular los restos $r_0, r_1, \ldots, r_k$, vamos a llenar sucesivamente una tabla de dos columnas: en la de la izquierda figurarán los cocientes $q_0, q_1, \ldots, q_k$, y en la de la derecha, los restos $r_0, r_1, \ldots, r_k$. Así,

722	0
361	

es decir, $r_0 = 0$, el cociente q_0 es igual a 361. Segundo paso:

722	0
361	1
180	

o sea, $r_1 = 1$ y $q_1 = 180$. Tercer paso:

722	0
361	1
180	0
90	

es decir, $r_1 = 0$, $q_1 = 90$. Después:

722	0
361	1
180	0
90	0
45	1
22	0
11	1
5	1
2	0
1	1
0	

(11)

Por lo tanto, en el sistema binario, el número 722 se escribe así: «1011010010» (la columna de la derecha de la tabla (11) debe hacerse girar 90° alrededor de su base, en el sentido de las agujas del reloj, con lo que se obtiene la respuesta). Y he aquí la descomposición (10) en este caso:

$$722 = 0\cdot 2^0 + 1\cdot 2^1 + 0\cdot 2^2 + 0\cdot 2^3 + 1\cdot 2^4 + 0\cdot 2^5 + 1\cdot 2^6 + 1\cdot 2^7 + 0\cdot 2^8 + 1\cdot 2^9 = 2^9 + 2^7 + 2^6 + 2^4 + 2.$$

2. Escribir el número $A = 722$ en el sistema duodecimal ($N = 12$).

Las cifras serán los números 0, 1, 2, ..., 11. El cálculo de los restos $r_0, r_1, \ldots,$

y de los cocientes $q_0, q_1 \ldots$ también conviene representarlo en forma de tabla (11).

$$\begin{array}{r|l} 722 & 2 \\ 60 & 0 \\ 5 & 5 \\ 0 & \end{array} \qquad (11')$$

Por consiguiente, en el sistema duodecimal, el número 722 tiene la forma "502", es decir,

$$722 = 2 \cdot 12^0 + 0 \cdot 12 + 5 \cdot 12^2 = 5 \cdot 12^2 + 2.$$

3. Escribir el número $A = 722$ en el sistema de base 722 ($N = 722$). La tabla (11), en este caso, es así:

$$\begin{array}{r|l} 722 & 0 \\ 1 & 1 \\ 0 & \end{array}$$

Por lo tanto, el número 722 en este sistema tiene la forma: "10", es decir, $722 = 0 \cdot 722^0 + 1 \cdot 722$. Para no confundir la notación "10" con el número 10, la escribiremos $\bar{1}\,\bar{0}$, indicando que $\bar{1}$ y $\bar{0}$ se consideran como restos respecto del módulo 722.

Es curioso el hecho siguiente:

En el sistema N-ario, el número N se escribe como $\bar{1}\bar{0}$.

Está claro que para escribir un número A en el sistema decimal partiendo de su representación en el sistema N-ario hay que hacerlo sobre la base de la igualdad (10), es decir, realizando una serie de multiplicaciones y adiciones, y no divisiones inexactas. Esto puede explicarse por el hecho de que en cualquier caso operamos con números escritos en el sistema decimal tradicional, ya que no tenemos cifras especiales para ningún otro sistema. Por ejemplo, el número binario $\bar{1}0\bar{1}\bar{1}0\bar{1}0\bar{0}\bar{1}\bar{0}$ es, naturalmente, el habitual $2 + 2^4 + 2^6 + 2^7 + 2^9 = 722$. Pero si quisiéramos obtener la notación de este número en el sistema decimal por medio del proceso de división inexacta, anteriormente descrito, tendríamos que dividir $1011010\bar{0}\bar{1}\bar{0}$ por el número 10, que en el sistema binario tiene la forma $1\bar{0}\bar{1}\bar{0}$. Para que quede claro damos la tabla correspondiente del cálculo de los restos de la división por $1\bar{0}\bar{1}\bar{0}$.

restos de la división por $\overline{1010}$.

$$\begin{array}{r|l} \overline{10110100010} & \overline{1010} \\ \overline{1010} & \overline{10110100010} \\ \hline \overline{1010} & \\ \overline{1010} & \\ \hline \overline{010} & \end{array}$$

Por consiguiente, el cociente es igual a $\overline{1001000}$, y el resto $\overline{10}$. La siguiente etapa es:

$$\begin{array}{r|l} \overline{1001000} & \overline{1010} \\ \overline{1010} & \overline{111} \\ \hline \overline{10000} & \\ \overline{1010} & \\ \hline \overline{1100} & \\ \overline{1010} & \\ \hline \overline{10} & \end{array}$$

El cociente, en este caso, es igual a $\overline{111}$, y el resto, $\overline{10}$. Finalmente, juntamos todo esto en la tabla tradicional de restos y cocientes:

$$\begin{array}{r|l} \overline{10110100010} & \overline{10} \\ \overline{1001000} & \overline{10} \\ \overline{111} & \overline{111} \\ \overline{0} & \end{array}$$

La notación $\overline{111}\ \overline{10}\ \overline{10}$ significa, naturalmente, 722, sólo que las cifras, en este caso, están escritas en el sistema binario (de esto son prueba las rayitas diacríticas superpuestas).

Este ejemplo, que muestra el procedimiento de conversión de un número del sistema binario al sistema decimal, testimonia que las operaciones aritméticas ordinarias con los números pueden efectuarse en el sistema en el cual están escritos, sin recurrir al sistema decimal.

Generalicemos ahora nuestros razonamientos.

Sean $A=\overline{a}_n\overline{a}_{n-1}\dots\overline{a}_1\overline{a}_0$ y $B=\overline{b}_m\overline{b}_{m-1}\dots\overline{b}_1\overline{b}_0$ dos números

naturales escritos en el sistema N-ario (de modo que $\bar{a}_n, \ldots, \bar{a}_0$, $\bar{b}_m, \ldots, \bar{b}_0$, son cifras N-arias). Para escribir la suma $A+B$, lo más conveniente es efectuar la adición "en columna":

$$\begin{array}{r} \bar{a}_n\bar{a}_{n-1}\ldots a_1 a_0 \\ + \\ \bar{b}_m \ldots \bar{b}_1\bar{b}_0 \\ \hline \end{array} \qquad (12)$$

Sumando $\bar{a}_0 + \bar{b}_0$ obtenemos $Nd_0 + c_0$, donde $0 \leqslant c_0 < N-1$ y $0 \leqslant d_0 \leqslant 1$; por esto, debajo de $\bar{a}_0$ y $\bar{b}_0$ en la notación (12) deberá escribirse $\bar{c}_0$. Después se suman $\bar{a}_1$, $\bar{b}_1$ y $\bar{d}_0$, y se vuelve a representar la suma en la forma $Nd_1 + c_1$; debajo de $\bar{a}_1$ y $\bar{b}_1$ en (12) escribimos $\bar{c}_1$, y así sucesivamente.

Ejemplo. Sean $N=3$, $A=\overline{2111001}$ y $B=\overline{2010212}$. Hallar la suma de A y B

$$\begin{array}{r} \overline{2111001} \\ + \\ \overline{2010212} \\ \hline \overline{11121220} \end{array}$$

Pasemos a la resta. Aquí hay que determinar ante todo qué número es mayor: A o B. Si $n > m$, como se deduce de la representación (10), $A > B$; si, por el contrario, $n < m$, será, como es natural, $A < B$. Si $n = m$ hay que comparar $\bar{a}_n$ y $\bar{b}_n$. Si $\bar{a}_n > \bar{b}_n$, será $A > B$, si $\bar{a}_n < \bar{b}_n$, será $A < B$. Si $\bar{a}_n = \bar{b}_n$ hay que comparar $\bar{a}_{n-1}$ y $\bar{b}_{n-1}$ y así sucesivamente. Si se establece que $\bar{a}_n = \bar{b}_n$, $\bar{a}_{n-1} = \bar{b}_{n-1}, \ldots, \bar{a}_1 = \bar{b}_1, \bar{a}_0 = \bar{b}_0$ resulta que $A = B$. Por ejemplo, para $N = 2$ el número 101101001001 es mayor que el número 101101000111

Para calcular la diferencia $A - B$ hay que resolver primero cuál de las desigualdades tiene lugar: $A \geqslant B$ o $A < B$. Si es la segunda, hay que buscar la diferencia $B - A$ y después poner delante de la respuesta el signo menos. Vamos a considerar que $A \geqslant B$. El cálculo de la diferencia $A - B$ también es más conveniente hacerlo "en columna"

$$\begin{array}{r} \bar{a}_n\bar{a}_{n-1}\ldots\bar{a}_2\bar{a}_1\bar{a}_0 \\ - \\ \bar{b}_m \ldots \bar{b}_2\bar{b}_1\bar{b}_0 \\ \hline \end{array}$$

sobreentendiendo que cada una de las filas es la notación

abreviada de la parte derecha de la fórmula (10). Si $\bar{a}_0 \geqslant \bar{b}_0$, debajo de $\bar{a}_0$ y $\bar{b}_0$ escribiremos la cifra N-aria $\bar{c}_0 = a_0 - b_0$. Si $a_0 < b_0$ y $a_1 > 0$, "tomamos" de a_1 "una unidad" y suponemos que $c_0 = N + a_0 - b_0$. Después de esto, desde luego, figurará en la tabla, en vez de $\bar{a}_1$, la cifra $\bar{a}_1 - 1$. Si $a_1 = 0$ y $a_2 > 0$, hay que "tomar la unidad" de a_2, es decir, representar el número de la forma:

$$A = \ldots + (a_2 - 1)N^2 + N^2 + a_0 =$$
$$= \ldots + (a_2 - 1)N^2 + N^2 - N + N + q_0 =$$
$$= \ldots + (a_2 - 1)N^2 + (N-1)N + N + a_0.$$

Entonces $c_0 = N + a_0 - b_0$ y c_1 —cifra que se encuentra debajo de a_1 y b_1— será igual a $N - 1 - b_1$. Si también $a_2 = 0$, pero $a_3 < 0$, hay que repetir estos razonamientos, representando A de la forma

$$A = \ldots + a_3 N^3 + a_0 = \ldots + (a_3 - 1)N^3 + N^3 + a_0 =$$
$$= + (a_3 - 1)N^3 + N^3 - N^2 + N^2 - N + N + a_0 =$$
$$= + (a_3 - 1)N^3 + (N-1)N^2 + (N-1)N + N + a_0,$$

si $a_3 = 0$ el lector se figurará ya, evidentemente, lo que hay que hacer.

Ejemplo. Sean $N = 8$, $A = \overline{724135}$ y $B = \overline{2635410}$. Hallar $A - B$. Como $B > 0$,

$$\begin{array}{r} \overline{2635410} \\ - \\ \overline{724135} \\ \hline \overline{1711253} \end{array}$$

Respuesta: $-\overline{1711253}$

Hemos estudiado la adición y la sustracción de los números naturales en el sistema N-ario. Como la multiplicación y la división inexacta se basan en la adición y la sustracción, tenemos todo lo necesario para efectuar estas operaciones en el sistema N-ario.

Pasemos a las fracciones:

$$R = r_{-1} \cdot 10^{-1} + r_{-2} \cdot 10^{-2} + \ldots$$

Su reconstrucción en signos decimales fue descrita en el pá-

rrafo anterior. Nuestro fin inmediato es representar la fracción indicada R en la forma

$$R = a_{-1}N^{-1} + a_{-2}N^{-2} + \ldots,$$

donde $a_{-1}, a_{-2}, \ldots$ son cifras N-arias. Evidentemente, a_{-1} es la parte entera del número NR (está claro que $a_{-1} < N$, ya que $R < 1$ y, por lo tanto, $NR < N$; de aquí que a_{-1} sea una cifra N-aria). Análogamente, a_2 es la parte entera del número $N(NR - a_{-1})$, es decir, $N^2R - Na_{-1}$ y, en general, a_{-k} es la parte entera del número

$$N^{-k}R - N^{k-1}a_{-1} - N^{k-2}a_{-2} - \ldots - Na_{-k+1}.$$

Ejemplo. Escribir la fracción $R = 0{,}0875$ en el sistema de base nueve ($N = 9$).

Los resultados del cálculo también aquí conviene inscribirlos en una tabla de dos columnas: a la izquierda se indicarán las fracciones y a la derecha, las partes enteras de sus productos por el número $N = 9$. Así,

0875	0
7875	7
0875	0
7875	7
0875	

Por consiguiente, en el sistema de base nueve, la fracción decimal finita $R = 0{,}0875$ es una fracción periódica infinita

$$\overline{0{,}0707}$$

la longitud de cuyo período es igual a 2, el número natural menor de aquellos números n para los cuales $9^n \equiv 1$ mód (M), donde M —denominador de la fracción R representada en forma racional (es decir, $R = \frac{7}{80}$ y $M = 80$)— es primo con el número 9.

La transformación de una fracción decimal finita en periódica infinita de otro sistema de notación merece especial atención. En primer lugar, advertimos que si el número racional $R = \frac{A}{B}$, $(A, B) = 1$ es una fracción decimal periódica infinita, en el sistema B-ario esta fracción será ya finita. De acuerdo con el teorema 3 del § 1, la longitud del periodo de la fracción R en el sistema decimal hay que determinarla así: se representa B en la forma $2^r \cdot 5^s \cdot B'$, donde $(10, B') = 1$, y después se halla un número natural n tal, que para él $10^n \equiv 1$ mód (B'). Tiene lugar el siguiente teorema:

TEOREMA 4. *Supongamos que* $N \geqslant 2$ *es un número natural y* $R = \frac{A}{B}$, *un número racional en notación no reducible. Sea* $B = B'B''$ *una representación tal del número B, que* $(B', N) = 1$ *y cada divisor primo del factor B'' divide a N. Entonces el período de la fracción N-aria que representa al número R es igual al menor de los números naturales n tales, que* $N^n \equiv 1$ *mód* (B').

Proponemos al lector que demuestre de por sí este teorema, basándose en la demostración del teorema 3.

De este modo, un número racional, en cualquier sistema N-ario, será una fracción periódica finita o infinita; un número irracional, en cambio, en cualquier sistema, se representará como una fracción no periódica, porque si fuera posible representarlo, aunque sólo fuera en un sistema, por una fracción periódica, las transformaciones análogas a las realizadas en la pág 70 nos conducirían a la representación de este número en forma de relación entre dos números enteros, cosa imposible a causa de la irracionalidad.

La suma y la resta de las fracciones finitas N-arias conviene hacerlas en "columnas" como las de los números enteros.

Examinemos ahora los caracteres de divisibilidad. El teorema 1 de este capítulo contiene precisamente aquella información que eficazmente se puede extender al caso del sistema N-ario:

TEOREMA 5. *La diferencia entre un número natural A y la suma de sus cifras N-arias es divisible por* $N - 1$.

Para demostrarlo basta utilizar la representación (10), de la cual se deduce que

$$A - M = r_k(N^k - 1) + r_{k-1}(N^{k-1} - 1) + \ \ldots \ + r_1(N - 1),$$

donde $M = r_0 + \ \ldots \ + r_k$.

Pero

$$N^s - 1 = (N - 1)(N^{s-1} + N^{s-2} + \ \ldots \ + N + 1),$$

de donde se deduce lo requerido.

He aquí por qué el número A es divisible por un divisor cualquiera del número $N - 1$ si, y solamente si, la suma de las cifras N-arias del número A es múltiplo de este divisor. Por ejemplo, disponiendo de la representación octal de cualquier

número A, es fácil conocer si éste es divisible por 7: hay que sumar las cifras y determinar si la suma es múltiplo de 7. Así, el número 76125, dado en el sistema octal, es, naturalmente, divisible por 7 (porque la suma de sus cifras es igual a 21). En el sistema decimal este número se escribe así: 31829.

Cuando $N = 2$, lo que acabamos de decir se convierte en trivial, porque $N - 1 = 1$. Por esto, en el sentido del teorema 5, el sistema binario no es conveniente: en este caso para comprobar una u otra divisibilidad, es mejor efectuar la correspondiente división inexacta o pasar a otro sistema, donde será más fácil obtener la respuesta.

§ 3. SISTEMAS N-ARIO Y N^k-ARIO

Estos sistemas para $N = 2$ han adquirido gran importancia en virtud de su empleo en las calculadoras electrónicas. Cada número binario se escribe por medio de dos cifras solamente: 0 y 1. Como un tubo electrónico ordinario puede encontrarse en uno de los dos estados: conectado o desconectado, si se conviene en considerar que el primer estado es la reproducción del cero, y el segundo, la reproducción de la unidad, con un juego de n tubos podrá reproducirse cualquier número binario de n cifras. En este principio se basa el funcionamiento de las computadoras electrónicas: el número se introduce en ellas según el sistema binario y después se somete a determinadas operaciones aritméticas.

Al analizar los ejemplos de notación binaria de un número en el párrafo anterior, el lector se habrá dado cuenta probablemente de que incluso un número pequeño requiere para su representación una cantidad bastante grande de signos binarios; así, el número 722 en el sistema binario tiene diez cifras. Por esto es natural que los números se representen según el referido sistema únicamente en el instante de introducirlos en la computadora, y hasta dicho momento se escriban en un sistema tal, que, primero, para su representación se necesiten menos signos y, segundo, su paso al sistema binario sea más directo que, por ejemplo, del sistema decimal.

Supongamos, por ejemplo, que $A = 30213$ es un número en el sistema cuaternario. ¿Cómo escribirlo en el sistema binario?

Utilicemos la representación (10):

$$A = 3\cdot 4^4 + 2\cdot 4^2 + 1\cdot 4 + 3 = (2+1)\cdot 2^8 + 2\cdot 2^4 + \\ + 1\cdot 2^2 + (2+1) = \\ = 2^9 + 2^8 + 2^5 + 2^2 + 2 + 1.$$

Por consiguiente, $A = 1100100111$ es su notación en el sistema binario. En otras palabras, hemos escrito cada cifra cuaternaria del número A con cifras binarias y hemos obtenido la respuesta. Esto puede comprobarse fácilmente partiendo de la respuesta.

Hagamos los razonamientos correspondientes en forma general. Sea

$$A = a_{2n}\cdot 2^{2n} + a_{2n-1}2^{2n-1} + \ldots + a_3\cdot 2^3 + a_2\cdot 2^2 + a_1\cdot 2 + \\ + a_0, \qquad (12)$$

donde, posiblemente, $a_{2n} = 0$ (porque necesitamos que el número de cifras sea par) y $a_0, a_1, \ldots, a_{2n-1}, a_{2n}$ son cifras binarias, es decir, números 0 y 1. El número $a_1\cdot 2 + a_0$ no supera a 3, y, por esto, sirve de cifra cuaternaria. Consideremos el siguiente par de sumandos: $a_3\cdot 2^3 + a_2\cdot 2^2 = (a_3\cdot 2 + a_2)2^2$, es decir, es una cifra cuaternaria multiplicada por 4. La pareja siguiente será una cifra cuaternaria multiplicada por $2^4 = 4$ y así sucesivamente.

Utilizando una representación análoga a la (12), es fácil deducir la siguiente regla.

Regla. *Para pasar de la notación N-aria de un número natural A a la notación en el sistema N^k-ario hay que dividir las cifras N-arias del número A en grupos de k cifras de derecha a izquierda y, una vez hecho esto, escribir cada uno de los grupos por medio de una cifra N^k-aria. La transformación inversa se hace así: cada cifra N^k-aria del número A hay que escribirla en el sistema N-ario por medio de cifras N-arias, entonces se obtiene la representación N-aria de A.*

Observación. Todo número entero no negativo $M < N^k$ (es decir, toda cifra N^k-aria) se escribe con no más de kN cifras N-arias, porque N^k en el sistema N-ario es $\underbrace{100\ldots0}_{k \text{ ceros}}$. En este caso se supone que si para M hacen falta $l < k$ cifras N-arias. delante de la notación N-aria se escriben $k-l$ ceros. Esto está en completa conformidad con la representación (10).

En vez de la demostración, que se hace fácilmente después de introducir las designaciones correspondientes, damos dos ejemplos que ilustran esta regla.

Sea $A = \overline{975}$ un número en el sistema de base 27. Representarlo en el sistema ternario. Tenemos que el $\overline{9}$ de base 27 es el $\overline{100}$ de base 3; el $\overline{7}$ de base 27 es el $\overline{021}$ de base 3, y el $\overline{5}$ de base 27 es el $\overline{012}$ de base 3. De este modo el número $\overline{975}$ de base 27 se escribe en el sistema ternario así: $\overline{100021012}$.

Sea $A = \overline{781015109}$ un número en el sistema de base 16. Escribámoslo en el sistema de base 256. Tenemos que $\overline{109}$ en el sistema de base 16 equivale a $\overline{169}$ en el sistema de base 256; $\overline{1015}$ de base 16 equivale a $\overline{175}$ de base 256, y $\overline{78}$ de base 16 equivale a $\overline{120}$ de base 256. Por consiguiente, el número A, en el sistema de base 256, se escribe así: $\overline{120\ 175\ 169}$.

BIBLIOGRAFÍA

1. ХИНЧИН А.Я. Элементы теории чисел. ЭЭМ, кн. I, Арифметика. М., Гостехиздат, 1951.
(A.YA. JINCHIN, "Elementos de la teoría de los números". Enciclopedia de Matemáticas elementales, libro I, Aritmética)
2. МАРКУШЕВИЧ А.И. Деление с остатком в арифметике и в алгебре. Сер. «Педагогическая библиотека учителя». Изд. Академии педагогических наук РСФСР, 1949.
(A.I. MARKUSHÉVICH, "División inexacta en aritmética y en álgebra"; Serie "Biblioteca pedagógica del maestro".)
3. ДЭВЕНПОРТ Г. Высшая арифметика. М., «Наука», 1965.
(G. DAVENPORT, "Aritmética superior".)
4. I.M. VINOGRÀDOV, "Fundamentos de la teoría de los números". Moscú, Mir, 1971.
5. АРНОЛЬД И.В. Теоретическая арифметика. М., Учпедгиз, 1939.
(I.V. ARNOLD, "Aritmética teórica".)
6. БУХШТАБ А.А. Теория чисел. М., «Просвещение». 1966.
(A.A. BUJSHTAB, "Teoría de los números".)
7. HASSE H. Zahlentheorie, Berlin (RDA), 1950.
8. N.N. VOROBIOV, "Criterios de divisibilidad". Serie "Lecciones populares de matemáticas". Moscú, Mir, 1975.
9. S.V. FOMÍN, "Sistemas de numeración". Serie "Lecciones populares de matemáticas". Moscú, Mir, 1975.
10. ДЫНКИН Е.Б., УСПЕНСКИЙ В.А. «Математические беседы». М—Л., Гостехиздат, 1952.
(E.B. DINKIN Y V.A. USPIENSKI, "Charlas matemáticas".

Lecciones populares de matemáticas

En esta pequeña obra se tratan algunos problemas interesantes de la teoría de los números. Se da la demostración del teorema de la unicidad de la descomposición en factores primos, se estudian el algoritmo de Euclides, las ecuaciones diofánticas, la aritmética de los números complejos enteros y las clases residuales, la representación de los números en los diversos sistemas posicionales, etc.

Este libro está dedicado a los alumnos de las escuelas especiales físico-matemáticas. Será de utilidad a los profesores de matemáticas de los centros de enseñanza media y a los alumnos de los últimos grados de dicha enseñanza

Editorial MIR **Moscú**