Universidad Autónoma de Guerrero

Escuela Superior de Matemáticas No. 2

El algoritmo de Euclides y la ecuación diofántica lineal en dos variables

T E S I S

que para obtener el título de

Lic. en Matemática Educativa

presenta:

Ricardo Mandujano Zamora

Asesor:

Dr. José Hernández Santiago

Cd. Altamirano, Gro., México, enero de 2026.

Índice general

Prefacio **1**

1. El máximo común divisor de dos números enteros **5**

1.1. Definición y primeros ejemplos 5

1.2. El algoritmo de la división en $\mathbb{Z}$ 6

1.3. Otras formas de pensar el máximo común divisor 8

1.3.1. El algoritmo de Euclides 9

1.3.2. La representación de (a, b) como una combinación lineal de a y b 12

1.4. Eficiencia del algoritmo de Euclides 15

2. La ecuación diofántica lineal en dos variables **19**

2.1. Planteamiento 19

2.2. Dos teoremas 19

2.2.1. Existencia y estructura de las soluciones 20

3. Ejemplos varios **27**

3.1. Propósito 27

3.2. Ejemplos 27

3.3. Fuentes 36

Bibliografía **39**

Prefacio

Son dos los temas que se abordan en este trabajo: el primero de ellos es el cálculo del máximo común divisor de dos números enteros mediante el algoritmo de Euclides y, el segundo, es la resolución de las ecuaciones del tipo

$$aX + bY = c \tag{1}$$

donde a y b son números enteros distintos de cero y c es algún otro número entero. A una ecuación de ese tipo se le conoce como *ecuación diofántica lineal en dos variables* y resolverla consiste precisamente en determinar todos los pares ordenados $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ tales que $ax+by = c$ (al conjunto conformado por todos esos pares ordenados se le conoce como el conjunto de soluciones de la ecuación diofántica (1)).

Algunas de las razones por las que consideramos pertinente desarrollar una tesina sobre estos temas son las siguientes:

- La noción de máximo común divisor tiene un papel señero en la aritmética (cf. [3, p. 818], [4, p. 231] o [2, p. 85]).
- Un buen entendimiento y manejo de los teoremas principales en torno al máximo común divisor son necesarios para incursionar en tópicos más avanzados que, en cierta medida, surgieron al *extender* la relación de divisibilidad en $\mathbb{Z}$ a contextos más amplios (ver, por ejemplo, [7, pp. 125-129]).
- Aunque el estudio del máximo común divisor y sus aplicaciones había estado fuera de los planes de estudio de la educación media superior por varios años, uno de los lineamientos de la Nueva Escuela Mexicana para la enseñanza en dicho nivel es precisamente el de "revisar algunos elementos disciplinares de la aritmética como la divisibilidad (propiedades y algunos criterios), máximo común divisor y mínimo común múltiplo"(cf. [5, p. 47]): tal revisión está contemplada para la unidad de aprendizaje curricular Pensamiento Matemático 2 (Pensamiento aritmético, algebraico y geométrico) a impartirse en el segundo semestre de la educación media superior y,

según lo que se lee en esa misma página de [5], el objetivo básico de tal medida es incidir en "el desarrollo de las habilidades de pensamiento matemático [del estudiantado]". Es de añadir que, desde nuestra perspectiva, la intención de la Nueva Escuela Mexicana de volver a dar cabida al desarrollo del pensamiento aritmético en la currícula de educación media superior es laudable pero bastante tardía. En otros puntos del orbe, la conclusión de que la aritmética representa una excelente opción para mejorar la enseñanza de las matemáticas se había alcanzando desde hace varias décadas. Por ejemplo, alrededor de 1990, E. R. Gentile (1928-1991) ya comentaba en [2, p. iv] que "la fuerza [de la aritmética en la enseñanza] radica en la posibilidad de plantear problemas de todo tipo de complejidad. El resolverlos es el ejercicio específico del aprendizaje. La aritmética es una ciencia cotidiana, capaz de atraer a cualquier persona que posea sólo un poco de curiosidad". Sobre esa misma tónica, es digno de mención el exhorto del gran G. H. Hardy (1877-1947) que aparece en la última sección del artículo [3]:

> «The elementary theory of numbers should be one of the very best subjects for early mathematical instruction. It demands very little previous knowledge; its subject matter is tangible and familiar; the processes of reasoning which it employs are simple, general and few; and it is unique among the mathematical sciences in its appeal to natural human curiosity. A month's intelligent instruction in the theory of numbers ought to be twice as instructive, twice as useful, and at least ten times as entertaining as the same amount of "calculus for engineers". It is after all only a minority of us who are going to spend our lives in engineering workshops, and there is no particular reason why most of us should feel any overpowering interest in machines; nor is it in the least likely that, on those occasions when machines are of real importance to us, we shall require the power of dealing with them by methods more elaborate than the simplest rule of thumb. It is not engineering mathematics that is wanted for the understanding of modern physics, and still less is it wanted by most of us for the ordinary needs of life; we do not actually drive cars by solving differential equations. There may be a case for subordinating mathematics to the linguistic and literary studies which are so much more obviously useful to ordinary men, but there is none for sacrificing a splendid subject to meet a quite imaginary need.»

En la luz de estos considerandos, al desarrollar este trabajo no sólo hemos tenido en mente el resarcir algunas deficiencias de nuestra formación durante la educación media superior y la licenciatura sino que también hemos procurado legar un escrito que pueda servir de apoyo a

toda persona interesada en ampliar su entendimiento del máximo común divisor, el algoritmo de Euclides y la aplicación de éste en la resolución de las ecuaciones diofánticas lineales en dos variables.

La tesina consta de tres capítulos. El capítulo 1 inicia con la definición del máximo común divisor de dos número enteros no ambos cero y, a lo largo del capítulo, paulatinamente se van desglosando los resultados primordiales en torno a ese concepto. Uno de los teoremas más importantes del capítulo es el teorema 1.2: este teorema asevera que si a y b son dos números enteros no ambos cero, entonces el máximo común divisor de a y b siempre se puede expresar como una combinación lineal de a y b con coeficientes enteros. Dada su relevancia en la investigación de diversas situaciones que implícita o explícitamente involucran al máximo común divisor de dos números enteros, algunos autores denominan a ese teorema 1.2 como *la sugerencia universal en aritmética* (cf. [1, p. 42] o [2, p. 85]). En nuestra obra, dicha relevancia quedará de manifiesto en el capítulo 2 cuando se establezcan los dos teoremas clave sobre el conjunto de soluciones de la ecuación diofántica lineal $aX + bY = c$ (donde c es un número entero).

Naturalmente, el algoritmo de Euclides es otro hecho de capital importancia que se desarrolla en el capítulo 1: no sólo explicamos su funcionamiento general de forma detallada (ver la pág. 10 de ese capítulo) sino que también explicamos cómo es que el algoritmo de Euclides se aplica para expresar el máximo común divisor de dos números no ambos cero como combinación lineal de ellos con coeficientes enteros. El capítulo 1 termina con un teorema debido al matemático francés Pierre-Joseph-Étienne Finck (1797-1870) sobre el número de pasos necesarios para calcular el máximo común divisor de dos números enteros positivos mediante el algoritmo de Euclides. Cabe señalar que la demostración del teorema de Finck que presentamos en este trabajo es una versión corregida de la propuesta en [8, p. 69].

El tema del capítulo 2 del trabajo es la ecuación diofántica lineal en dos variables. Si a y b son números enteros distintos de cero y c es algún otro número entero, consideremos la ecuación diofántica lineal

$$aX + bY = c.$$

Las dos preguntas que sobre una ecuación de ese tipo se abordan y responden en el capítulo 2 son: i) ¿cómo se determina si la ecuación tiene alguna solución? ii) Cuando se conoce algún par ordenado $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ tal que $aX + bY = c$, ¿es posible determinar el resto de soluciones de la ecuación? Es en la subsección 2.2.1 (Existencia y estructura de las soluciones) que se presentan las respuestas a ambas interrogantes; como es de esperarse, la teoría ahí presentada es ilustrada

con varios ejemplos.

En el capítulo 3 presentamos una recopilación de diez problemas que pueden resolverse planteando una ecuación diofántica lineal en dos variables y analizando el respectivo conjunto de soluciones. Como lo mencionamos al inicio de ese capítulo, en el análisis de cada uno de esos problemas–antes de invocar los teoremas clave que se demostraron en la subsección 2.2.1–es necesario aplicar competencias matemáticas básicas tales como el identificar datos e incógnitas en un planteamiento dado y vincularlos a través de ecuaciones. Por lo anterior y, en vista de que algunos de esos problemas admiten soluciones distintas a las que exponemos, consideramos que este capítulo brinda un compendio de problemas idóneos para el desarrollo o consolidación de habilidades de pensamiento aritmético y/o algebraico (lo cual está en total sintonía con las ideas y anhelos de la Nueva Escuela Mexicana en lo que a la enseñanza de las matemáticas se refiere).

Consideramos prudente concluir este prefacio con algunos comentarios sobre el estilo general de la obra. En primer lugar, hemos procurado que el texto sea prácticamente autocontenido y que lo únicos requisitos necesarios para leerlo sea un manejo de la simbología de la teoría de conjuntos y del álgebra básica (como la del libro de A. Baldor). Posiblemente sólo hay un ingrediente que va más allá de lo previamente mencionado y que se usa en varias partes del capítulo 1: *el principio del buen orden de los números naturales* (p. b. o.). Ese principio afirma que todo subconjunto no vacío de $\mathbb{N}$ tiene un elemento mínimo; decidimos no remitir su enunciación a una sección de preliminares pues, aparte de que creemos que el principio es susceptible de ser contemplado como autoevidente en la *praxis*, la aritmética de $\mathbb{N}$ puede desarrollarse formalmente contemplando al p. b. o. como axioma. Otra cuestión que hemos procurado cuidar al trabajar en esta tesina es el balance entre la **teoría** discutida, los **ejemplos** y la **resolución de problemas**: al igual que E. R. Gentile, también somos de la idea de que "esos tres aspectos forman el triángulo de coherencia de toda enseñanza eficaz" (cf. [2, p. iv]). Esperamos que la atención que prestamos a las referidas cuestiones de estilo redunde en un documento de lectura amena o, al menos, digerible.

Capítulo 1

El máximo común divisor de dos números enteros

1.1. Definición y primeros ejemplos

Definición 1.1. *Sean m y n números enteros no ambos cero. El máximo común divisor de m y n es el mayor de los números enteros que dividen tanto a m como a n.*

Habitualmente el máximo común divisor de los números enteros m y n se denota por (m, n) o por $\text{mcd}(m, n)$.

Ejemplos.

a) A partir de la definición, calculemos el máximo común divisor de 6 y 14. Puesto que el conjunto de los divisores de 6 es $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ y el conjunto de los divisores de 14 es $\{\pm 1, \pm 2, \pm 7, \pm 14\}$, entonces los números enteros que dividen tanto a 6 como a 14 son justamente los elementos de $\{\pm 1, \pm 2, \pm 3, \pm 6\} \cap \{\pm 1, \pm 2, \pm 7, \pm 14\}$ y, en consecuencia,

$$(6, 14) = \text{máx}\,(\{\pm 1, \pm 2, \pm 3, \pm 6\} \cap \{\pm 1, \pm 2, \pm 7, \pm 14\}) = 2.$$

b) Calculemos ahora el máximo común divisor de 22 y 242. En este caso, el conjunto de los divisores de 22 es $\{\pm 1, \pm 2, \pm 11, \pm 22\}$ mientras que el conjunto de los divisores de 242 es $\{\pm 1, \pm 2, \pm 11, \pm 22, \pm 121, \pm 242\}$. Por consiguiente:

$$(22, 242) = \text{máx}\,(\{\pm 1, \pm 2, \pm 11, \pm 22\} \cap \{\pm 1, \pm 2, \pm 11, \pm 22, \pm 121, \pm 242\}) = 22.$$

La pregunta sobre la existencia de maneras alternativas para determinar el máximo común divisor de dos números dados surge de forma natural. En la sección que sigue dilucidaremos el teorema clave en la fundamentación del procedimiento clásico para el cálculo del máximo común divisor (*i.e.*, **el algoritmo de Euclides**). Por ahora, y a modo de cierre de esta sección, presentamos un ejemplo de una situación en la que eventualmente se calcula el máximo común divisor de dos números enteros.

Problema 1.1. *En una bodega hay dos contenedores: en uno hay* 80 *litros de jugo de naranja y en el otro hay* 36 *litros de jugo de piña. Para su transporte se requiere guardar el jugo en el menor número de envases iguales. ¿Cuál es la capacidad máxima que pueden tener los envases para que no sobre jugo?*

Solución. Para que no sobre jugo al mover el líquido de los contenedores a los envases es necesario que la capacidad x de los envases sea un divisor de 80 y de 36. Como se desea que los envases sean de la mayor capacidad posible entonces

$$x = (36, 80).$$

Puesto que el conjunto de divisores de 36 es $\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm9, \pm12, \pm18, \pm36\}$ mientras que el conjunto de divisores de 80 es $\{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm16, \pm20, \pm40, \pm80\}$, concluimos que

$$\begin{aligned} x &= \text{máx}\,(\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm9, \pm12, \pm18, \pm36\} \cap \{\pm1, \pm2, \pm4, \pm5, \pm8, \pm10, \pm16, \pm20, \pm40, \pm80\}) \\ &= 4. \end{aligned}$$

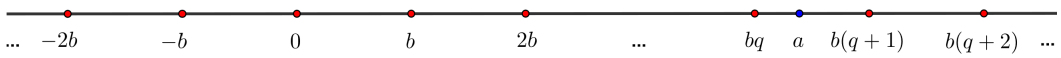
■

1.2. El algoritmo de la división en $\mathbb{Z}$

Teorema 1.1. *Supóngase que a y b son números enteros y que $b > 0$. Existen números enteros q y r, **únicos**, tales que*

$$a = bq + r \qquad y \qquad 0 \leq r < b.$$

Demostración. Podemos guiarnos de la idea que se aplica al hacer la división "usual" de dos números enteros: consideramos la sucesión de múltiplos del número b y expresamos como $b(q + 1)$ al mínimo de ellos que sobrepasa al número a. Para fijar ideas, considere el diagrama siguiente:



Se cumple que

$$bq \leq a < b(q+1)$$

y, consiguientemente, si se hace $r = a - bq$ se colige que

$$a = bq + r \tag{1.1}$$

y que

$$0 \leq a - bq = r < b. \tag{1.2}$$

Para establecer la unicidad de q y r, suponemos que q' y r' son números enteros tales que

$$a = bq' + r' \tag{1.3}$$

y

$$0 \leq r' < b. \tag{1.4}$$

De (1.2) y (1.4) se desprende que $-b < r' - r < b$. Por otro lado, de (1.1) y (1.3) se obtiene que $b(q - q') = r' - r$. Así entonces, $r' - r$ es un múltiplo de b en el intervalo $(-b, b)$: esto sólo puede cumplirse cuando $r' = r$. Con esta información, podemos regresar a (1.1) y (1.3) para establecer que $q = q'$. ∎

Al número q del teorema previo se le llama el *cociente* de la división de a entre b y al número r se le denomina el *resto* (o *residuo*) de la división de a entre b. Como es de esperarse, hay una versión del teorema anterior para el caso en que $b < 0$.

Corolario 1.1. *Supóngase que a y b son números enteros y que $b < 0$. Existen números enteros q y r, **únicos**, tales que*

$$a = bq + r \qquad y \qquad 0 \leq r < |b|.$$

Demostración. Se tiene que $-b > 0$ y, por el teorema 1.1, existen números enteros q y r tales que

$$a = (-b)q + r$$

donde $0 \leq r < (-b) = |b|$. Reescribiendo la igualdad anterior en la forma

$$a = b(-q) + r$$

tenemos la primera parte del aserto. La verificación de la unicidad de q y r se puede efectuar siguiendo la demostración del teorema 1.1, *mutatis mutandis*. ∎

1.3. Otras formas de pensar el máximo común divisor

Ya habiendo discutido el algoritmo de la división y su demostración, estamos en condiciones de establecer uno de los resultados centrales de este capítulo.

Teorema 1.2. *Supóngase que a y b son números enteros no ambos cero. Siempre es posible encontrar números x_0 y y_0 tales que*

$$(a, b) = ax_0 + by_0.$$

En la demostración de este teorema y en lo posterior estaremos empleando la simbología usual para la relación de divisibilidad en los números enteros. Recuérdese que si m y n son números enteros entonces $m \mid n$ se lee como "m divide a n" o "n es divisible por m" e indica que $n = m\kappa$ para algún número entero κ.

Demostración del Teorema 1.2. Consideremos al conjunto $C = \{ax + by : (x, y) \in \mathbb{Z} \times \mathbb{Z}\} \cap \mathbb{Z}^+$. No resulta difícil convencerse de que C es un subconjunto no vacío de $\mathbb{Z}^+$. Llamemos d al elemento mínimo de C y supongamos que $d = ax_0 + by_0$ donde x_0 y y_0 son números enteros. Afirmamos que $d = (a, b)$. Para establecer esta igualdad es menester verificar tres cosas:

i) $d \mid a$.

ii) $d \mid b$.

iii) Si c es otro divisor común de a y b, entonces $c \leq d$.

Para demostrar i) aplicamos el algoritmo de la división en $\mathbb{Z}$. Existen números enteros q y r tales que

$$a = dq + r \tag{1.5}$$

donde $0 \leq r < d$. Si fuera el caso que $d \nmid a$, entonces r sería distinto de 0 y de (1.5) se tendría que

$$\begin{aligned} r &= a - dq \\ &= a - (ax_0 + by_0)q \\ &= a(1 - x_0q) + b(-y_0q); \end{aligned}$$

es decir, ¡r sería un elemento de C **menor que** d! Esto es un absurdo pues d es el elemento mínimo de C. Por lo tanto, $d \mid a$.

Procediendo de manera análoga se puede probar el inciso ii. Finalmente, si c es otro divisor común de a y b entonces c es un divisor de cualquier combinación lineal de a y b con coeficientes enteros; esto implica en particular que $c \mid (ax_0 + by_0)$ o bien que $c \mid d$. La desigualdad entre c y d es consecuencia de la relación de divisibilidad entre ellos: en efecto, $d = |c|Q$ para algún número entero positivo Q y, por consiguiente, $d = |c|Q \geq |c| \geq c$. ∎

1.3.1. El algoritmo de Euclides

Ya tenemos todos los ingredientes necesarios para discutir el procedimiento clásico para el cálculo del máximo común divisor de dos números enteros; éste será útil no sólo para calcular el máximo común divisor sino también para expresar tal cantidad como una combinación lineal, con coeficientes enteros, de los números considerados. Un hecho que juega un papel significativo en lo que sigue es que cuando se tienen dos números enteros a y b, distintos de cero, que satisfacen $b \mid a$ entonces $(a, b) = |b|$. Por otro lado, la clave para poner en marcha el algoritmo la brinda el resultado que enunciamos y demostramos a continuación.

Teorema 1.3. *Supóngase que a y b son números enteros distintos de cero y supóngase que q y r son aquellos números enteros tales $a = bq + r$ y $0 \leq r < |b|$. Se cumple entonces que*

$$(a, b) = (b, r).$$

Demostración. Consideremos la siguiente notación: si $\kappa \in \mathbb{Z}$, entonces $\mathcal{D}_\kappa$ denota al conjunto de divisores del número κ. Es relativamente claro que el conjunto de los divisores comunes de a y b es $\mathcal{D}_a \cap \mathcal{D}_b$ y que el conjunto de los divisores comunes de b y r es $\mathcal{D}_b \cap \mathcal{D}_r$. La igualdad que deseamos demostrar es una consecuencia inmediata de la igualdad $\mathcal{D}_a \cap \mathcal{D}_b = \mathcal{D}_b \cap \mathcal{D}_r$, la cual puede establecerse por el argumento (conjuntista) estándar:

- Si $z \in \mathcal{D}_a \cap \mathcal{D}_b$, entonces $z \mid a$ y $z \mid b$ y, en consecuencia, z divide a cualquier combinación lineal de a y b con coeficientes enteros; en particular, $z \mid r$ pues $r = a - bq$. Se tiene así que $z \in \mathcal{D}_b \cap \mathcal{D}_r$.
- Si $z \in \mathcal{D}_b \cap \mathcal{D}_r$, entonces $z \mid b$ y $z \mid r$ y, en consecuencia, z divide a cualquier combinación lineal de b y r con coeficientes enteros; en particular, $z \mid a$ pues $a = bq + r$. Se ha obtenido así que $z \in \mathcal{D}_a \cap \mathcal{D}_b$.

∎

Sean a y b números enteros. Sin pérdida de generalidad podemos suponer que $b > 0$. Por el algoritmo de la división en $\mathbb{Z}$, existen números enteros q_1 y r_1 tales que

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

Si $r_1 = 0$, entonces $b \mid a$ y $(a, b) = b$. Si ese no fuera el caso, aplicando nuevamente el algoritmo de la división en $\mathbb{Z}$ podemos garantizar la existencia de números enteros q_2 y r_2 tales que

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1$$

Si $r_2 = 0$, entonces el teorema 1.3 nos permite concluir que $(a, b) = (b, r_1) = r_1$. Si $r_2 \neq 0$, dividimos ahora r_1 entre r_2 y obtenemos números enteros q_3 y r_3 tales que

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2$$

Nuevamente, si $r_3 = 0$, entonces $(a, b) = (b, r_1) = (r_1, r_2) = r_2$. Si $r_3 \neq 0$, entonces invocando el algoritmo de la división una vez más podemos garantizar la existencia de números enteros q_4 y r_4 tales que

$$r_2 = r_3q_4 + r_4, \quad 0 \leq r_4 < r_3$$

Si $r_4 = 0$ entonces $(a, b) = (b_1, r_1) = (r_1, r_2) = (r_2, r_3) = r_3$. En caso contrario, podemos reiterar el proceso e ir obteniendo enteros $q_1, q_2, q_3, q_4, \ldots, q_{n-1}, q_n$ y $r_1, r_2, r_3, r_4, \ldots, r_{n-3}, r_{n-2}, r_{n-1}, r_n$ tales que

$$\begin{cases} a & = & bq_1 + r_1, & 0 \leq r_1 < b \\ b & = & r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ r_2 & = & r_3q_4 + r_4, & 0 \leq r_4 < r_3 \\ & \vdots & & \\ r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} & = & r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \end{cases}$$

Puesto que los restos $r_1, r_2, r_3, r_4, \ldots, r_n$ son mayores o iguales a 0 y **decrecientes** (esto es, $r_1 > r_2 > r_3 > r_4 > \ldots$), entonces **uno de ellos será igual a** 0. Si pensamos que r_n es el primer resto que resulta ser igual a 0, entonces $r_{n-1} \mid r_{n-2}$ y

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = (r_3, r_4) = \ldots = (r_{n-2}, r_{n-1}) = r_{n-1}.$$

A este procedimiento para calcular el máximo común divisor de dos números enteros es a lo que se le denomina **el algoritmo de Euclides**. ¡Nótese que, en el algoritmo, la pareja inicial

de números enteros de la cual se requiere el máximo común divisor se va reemplazando por otras parejas de números enteros que se obtienen de sucesivas aplicaciones del algoritmo de la división en $\mathbb{Z}$ y el proceso termina cuando se llega a una pareja de números en la que uno de ellos divide al otro!

Ejemplos.

a) Calculemos el máximo común divisor de 39 y 666 mediante el algoritmo de Euclides. Tenemos en primer lugar que

$$666 = 39(17) + 3.$$

Al dividir 39 entre 3 se obtiene

$$39 = 3(13) + 0.$$

Puesto que se ha llegado a un resto igual a 0 concluimos que

$$(666, 39) = (39, 3) = 3.$$

b) Calculemos ahora el máximo común divisor de 94 y 18. Al hacer las divisiones indicadas en el algoritmo de Euclides obtenemos:

$$\begin{aligned} 94 &= 18(5) + 4 \\ 18 &= 4(4) + 2 \\ 4 &= 2(2) + 0. \end{aligned}$$

Se tiene así que

$$(94, 18) = (18, 4) = (4, 2) = 2.$$

c) Calculemos ahora el máximo común divisor de 21 y 13. Haciendo las divisiones sucesivas obtenemos:

$$\begin{aligned} 21 &= 13(1) + 8 \\ 13 &= 8(1) + 5 \\ 8 &= 5(1) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0. \end{aligned}$$

Puesto que el último resto distinto de cero que apareció en el proceso es 1 concluimos que

$$(21, 13) = (13, 8) = (8, 5) = (5, 3) = (3, 2) = (2, 1) = 1.$$

Al igual que lo hemos hecho en los tres incisos anteriores, a lo largo de esta obra nos estaremos apegando a la **convención** de escribir entre paréntesis los cocientes que se obtienen en las distintas divisiones que se realizan en el algoritmo de Euclides.

NOTAS

La *aparición* del algoritmo de Euclides se puede rastrear hasta las proposiciones I y II del libro VII de *Los elementos* de Euclides. B. Mazur explica en [4, p. 233] la razón por la cual se requirieron dos proposiciones de *Los elementos* para tratar el algoritmo:

«... dado que Euclides hacía distinción entre "la unidad" (lo que ahora conocemos como el número 1) y los números para denotar pluralidades (i.e., números mayores que 1), él separó el caso en el que la salida del algoritmo es una unidad del caso en el que salida del algoritmo es un número mayor o igual a 2. El primer caso es discutido en Eucl. VII-1 mientras que el segundo caso es el tema de Eucl. VII-2.»

Del algoritmo de Euclides, el gran D. Knuth escribió alguna vez: «... Podríamos decir que es el abuelo de todos los algoritmos pues es el algoritmo no trivial más antiguo que ha subsistido hasta nuestros días.»

1.3.2. La representación de (a, b) como una combinación lineal de a y b

Consideremos los números enteros a y b y supongamos que $b > 0$. El algoritmo de Euclides no sólo permite determinar (a, b) sino que también ayuda a expresar ese número como una combinación lineal de a y b con coeficientes enteros. En el capítulo dos quedará de manifiesto la utilidad de una combinación de ese estilo en diversas investigaciones aritméticas.

Ilustraremos a continuación el procedimiento para expresar (a, b) como combinación lineal de a y b con coeficientes enteros. Primero consideremos el caso en el que, al aplicar el algoritmo de Euclides, se efectúan dos divisiones:

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1q_2 + r_2, & r_2 = 0 \end{cases}$$

En este caso se cumple que $(a,b) = (b,r_1) = r_1$ y que el máximo común divisor de a y b se puede escribir como una combinación lineal de a y b con coeficientes enteros:

$$r_1 = a(1) + b(-q_1).$$

Supongamos ahora que, al calcular (a,b) mediante el algoritmo de Euclides, se llevan a cabo tres divisiones. En este caso, el cálculo del máximo común divisor queda como se indica en el siguiente esquema:

$$\begin{cases} a &= bq_1 + r_1, & 0 < r_1 < b \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & r_3 = 0. \end{cases}$$

Tenemos así que $(a,b) = (b,r_1) = (r_1,r_2) = r_2$. Para expresar r_2 como combinación lineal de a y b primero despejamos a r_2 de la segunda igualdad y obtenemos

$$r_2 = b - r_1q_2. \tag{1.6}$$

Después de esto, despejamos r_1 de la primera igualdad y la información así obtenida la introducimos en (1.6):

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a(-q_2) + b(1 + q_1q_2).$$

¡Se ha expresado así a (a,b) como combinación lineal de a y b con coeficientes enteros!

Detallaremos a continuación el procedimiento para obtener la combinación lineal cuando el algoritmo de Euclides determina el máximo común divisor de a y b en cuatro divisiones:

$$\begin{cases} a &= bq_1 + r_1, & 0 < r_1 < b \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ r_2 &= r_3q_4 + r_4, & r_4 = 0. \end{cases}$$

Se tiene aquí que $(a,b) = (b,r_1) = (r_1,r_2) = (r_2,r_3) = r_3$. Como hemos visto en los casos anteriores, la idea en lo que sigue es ir despejando y sustituyendo los restos del penúltimo hacia arriba. Lo que obtenemos es:

$$\begin{aligned} r_3 &= r_1 - r_2q_3 \\ &= r_1 - (b - r_1q_2)q_3 \\ &= (a - bq_1) - (b - (a - bq_1)q_2)q_3 \\ &= a - bq_1 - bq_3 + (a - bq_1)q_2q_3 \\ &= a(1 + q_2q_3) - bq_1 - bq_3 - bq_1q_2q_3 \\ &= a(1 + q_2q_3) + b(-q_1 - q_3 - q_1q_2q_3). \end{aligned}$$

De los ejemplos discutidos es aparente que el algoritmo de Euclides permite representar a (a, b) como una combinación lineal de a y b, con coeficientes enteros, independientemente del número de divisiones requeridas al aplicar el algoritmo. Por ejemplo, sabiendo que cuando se realizan cuatro divisiones en el algoritmo de Euclides es posible obtener la combinación lineal con coeficientes enteros, para llegar a la combinación lineal con coeficientes enteros en el caso de haberse realizado cinco divisiones se puede proceder así: en primer lugar tenemos que el esquema obtenido al aplicar el algoritmo de Euclides es del tipo

$$\begin{cases} a &= bq_1 + r_1, & 0 < r_1 < b \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ r_2 &= r_3q_4 + r_4, & 0 < r_4 < r_3 \\ r_3 &= r_4q_5 + r_5, & r_5 = 0 \end{cases}$$

De esto se sigue que el cálculo de (b, r_1) se logra con cuatro divisiones; al hacer el despeje de restos (de r_4 hacia arriba) llegaremos a que $r_4 = by_0 + r_1z_0$ para algunos números enteros y_0 y z_0. De esto y de la igualdad $a = bq_1 + r_1$ se desprende que

$$r_4 = by_0 + r_1z_0 = by_0 + (a - bq_1)z_0 = az_0 + b(y_0 - q_1z_0),$$

lo cual ya es una combinación lineal de a y b, con coeficientes enteros, que coincide con (a, b).

Ejemplos numéricos.

a) Calculemos el máximo común divisor de 2023 y 49 y expresemóslo como una combinación lineal de 2023 y 49 con coeficientes enteros. Aplicando el algoritmo de Euclides se tiene que:

$$\begin{aligned} 2023 &= 49(41) + 14 \\ 49 &= 14(3) + 7 \\ 14 &= 7(2) + 0. \end{aligned}$$

De esto se sigue que $(2023, 49) = 7$; para obtener la combinación lineal despejamos los restos del penúltimo al primero y reducimos términos semejantes:

$$\begin{aligned} 7 &= 49 - 14(3) \\ &= 49 - (2023 - 49(41))(3) \\ &= 49(124) + 2023(-3). \end{aligned}$$

b) Expresemos ahora $(97, 47)$ como una combinación lineal de 97 y 47 con coeficientes enteros. Primero aplicamos el algoritmo de Euclides:

$$\begin{aligned} 97 &= 47(2) + 3 \\ 47 &= 3(15) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0. \end{aligned}$$

Tenemos así que $(97, 47) = 1$. Al hacer el despeje de restos se llega a que

$$1 = 3 - 2 = 3 - (47 - 3(15)) = (97 - 47(2)) - 47 + (97 - 47(2))(15) = 97(16) + 47(-33).$$

1.4. Eficiencia del algoritmo de Euclides

Cuando se tiene un algoritmo para llevar a cabo una tarea dada, una pregunta que surge de modo natural es la de cuántos *pasos* se requieren para que el algoritmo complete esa tarea. En el caso específico del algoritmo de Euclides, la pregunta puede plantearse de la siguiente manera: si a y b son números enteros no ambos cero, ¿a lo más cuántas divisiones deben realizarse para dar con el máximo común divisor de a y b ? Si suponemos que $a \geq b > 0$, entonces en el algoritmo de Euclides se llega al primer resto igual a 0 a lo más en b pasos; no obstante, veremos en esta sección que el algoritmo de Euclides es más eficiente que lo que predice esa burda observación anterior.

Teorema 1.4. *Sean a y b números enteros. Supongamos que $a \geq b > 0$ y que al calcular el máximo común divisor de a y b mediante el algoritmo de Euclides obtenemos el siguiente esquema:*

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2 \\ r_2 = r_3q_4 + r_4, & 0 < r_4 < r_3 \\ \quad\vdots & \\ r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} = r_{n-1}q_n + r_n, & r_n = 0 \end{cases}$$

Hagamos $r_{-1} = a$ y $r_0 = b$. Se cumple que

$$r_{i+1} < \frac{1}{2} r_{i-1}$$

para cada $i \in \{0, 1, 2, \ldots, n-1\}$.

Demostración. Sea $i \in \{0, 1, 2, \ldots, n-1\}$. Si $r_i < \frac{1}{2} r_{i-1}$, entonces de las desigualdades para los restos se obtiene que

$$r_{i+1} < r_i < \frac{1}{2} r_{i-1}.$$

Supongamos ahora que $r_i \geq \frac{1}{2} r_{i-1}$. En vista de que el algoritmo de Euclides indica que $r_{i-1} = r_i q_{i+1} + r_{i+1}$ obtenemos que

$$r_{i+1} = r_{i-1} - r_i q_{i+1} \leq r_{i-1} - \frac{1}{2} r_{i-1} q_{i+1} = r_{i-1}\left(1 - \frac{1}{2} q_{i+1}\right). \tag{1.7}$$

Como $a \geq b > 0$, los cocientes $q_1, q_2, \ldots, q_n$ son mayores que 0; de esto y 1.7 se concluye que

$$r_{i+1} \leq r_{i-1}\left(1 - \frac{1}{2} q_{i+1}\right) \leq \frac{1}{2} r_{i-1}$$

que es justo a lo que queríamos llegar. ∎

Teorema 1.5. *Sean a y b números enteros tales que $a \geq b > 0$. Se cumple que el algoritmo de Euclides para calcular (a, b) termina en a lo más $2\log_2 b + 1$ pasos, donde cada paso es una aplicación del algoritmo de la división en $\mathbb{Z}$.*

Demostración. Supongamos que al calcular (a, b) mediante el algoritmo de Euclides obtenemos las n igualdades que se listan enseguida:

$$\begin{cases} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2 q_3 + r_3, & 0 < r_3 < r_2 \\ r_2 = r_3 q_4 + r_4, & 0 < r_4 < r_3 \\ \vdots & \\ r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} = r_{n-1} q_n + r_n, & r_n = 0 \end{cases}$$

Sin pérdida de generalidad podemos suponer que $n > 1$. El teorema 1.4 nos permite garantizar que si $2i$ es un número par del intervalo $[1, n]$ entonces

$$r_{2i} < \frac{1}{2} r_{2i-2} < \frac{1}{2^2} r_{2i-4} < \frac{1}{2^3} r_{2i-6} < \ldots < \frac{1}{2^i} r_{2i-2i} = \frac{1}{2^i} b.$$

En consecuencia, tan pronto como $(i+1) \geq \log_2 b$ se llega a que $2^{i+1} \geq 2^{\log_2 b} = b$ y a que $r_{2i} < 2$: como r_{2i} es un número entero mayor que o igual a cero se sigue que $r_{2i} = 0$ o $r_{2i} = 1$. En el primer caso tenemos que $n \leq 2i$ mientras que, en el segundo caso, lo que se tiene es que $n \leq 2i + 1$. Puesto que[1]

$$2(i+1) \geq 2\log_2 b$$

entonces

$$2i + 1 \quad \geq \quad 2\lfloor \log_2 b \rfloor + 2\{\log_2 b\} - 1 \tag{1.8}$$

y

$$2i \geq 2\lfloor \log_2 b \rfloor + 2\{\log_2 b\} - 2; \tag{1.9}$$

la desigualdad en (1.8) implica que el número impar $2i + 1$ es mayor o igual a $2\lfloor \log_2 b \rfloor + 1$ y la desigualdad en (1.9) indica que el número par $2i$ es mayor o igual a $2\lfloor \log_2 b \rfloor - 2$. De todas las consideraciones anteriores se colige que

$$n \leq 2\lfloor \log_2 b \rfloor + 1 \leq 2\log_2 b + 1$$

y la demostración termina. ∎

NOTAS

Para saber más de la historia de los teoremas relacionados con la eficiencia del algoritmo de Euclides, el artículo [6] es una referencia obligada. De acuerdo con las investigaciones de Shallit, el teorema sobre la eficiencia del algoritmo de Euclides que se acaba de demostar se debe al francés Pierre-Joseph-Étienne Finck (1797-1870). Hay un teorema del matemático francés Gabriel Lamé (1795-1870) que asevera que si a y b son números enteros y $a > b > 0$, entonces el total de pasos al calcular (a, b), mediante el algoritmo de Euclides, es a lo más 5 veces el número de dígitos en la representación decimal del número b; aunque este teorema es más fino que el de Finck y suele citarse más, Shallit explica en su artículo que el teorema de Finck fue publicado antes que el teorema de Lamé (1842 vs. 1844) y que incluso el teorema de Lamé es susceptible de refinamiento (para más detalles sobres estos puntos en específico, ver [6, p. 414]).

[1] En lo que sigue, $\lfloor x \rfloor$ y $\{x\}$ denotan, respectivamente, la parte entera y la parte decimal del número real x. Cualquier duda sobre las propiedades básicas de ambas funciones se puede disipar al consultar el cap. 10 de [1].

Capítulo 2

La ecuación diofántica lineal en dos variables

2.1. Planteamiento

Sean a y b números enteros distintos de cero y sea c un tercer número entero. En este capítulo estudiaremos la ecuación

$$aX + bY = c. \tag{2.1}$$

Decimos que el par ordenado $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de esa ecuación si $ax + by = c$. A una ecuación como (2.1) se le conoce como *ecuación diofántica lineal en dos variables* y son dos las preguntas que en torno a ello estaremos discutiendo en este capítulo:

i) ¿Cómo determinar si una ecuación de esa índole tiene soluciones?

ii) Cuando la ecuación tiene solución, ¿es posible describir explícitamente el conjunto conformado por todas sus soluciones?

2.2. Dos teoremas

Sean a y b números enteros no ambos cero. De acuerdo con el teorema 1.2 sabemos que $(a, b) = ax + by$ para algunos números enteros x y y. En la demostración de los dos teoremas básicos concernientes a la ecuación diofántica lineal en dos variables serán relevantes los dos corolarios del teorema 1.2 que se presentan a continuación.

Corolario 2.1. *(La regla de oro de la aritmética) Sean a y b números enteros no ambos cero y* ***coprimos*** *(i.e.,* $(a, b) = 1$*). Si c es un número entero tal que* $a \mid bc$*, entonces* $a \mid c$*.*

Demostración. Como $(a, b) = 1$, entonces

$$1 = ax + by \tag{2.2}$$

para algunos números enteros x y y. Por otro lado, del supuesto de que bc es divisible por a se tiene que

$$bc = ad \tag{2.3}$$

para algún número entero d. Luego, si multiplicamos ambos miembros de (2.2) por c se obtiene:

$$c = acx + bcy;$$

de esto y de (2.3) se llega a que

$$\begin{aligned} c &= acx + ady \\ &= a(cx + dy) \end{aligned}$$

lo cual indica que $a \mid c$. ∎

Corolario 2.2. *Sean a y b números enteros no ambos cero. Se cumple que*

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

Demostración. De acuerdo con el teorema 1.2,

$$(a, b) = ax + by$$

para algunos números enteros x y y. Dividiendo ambos miembros de esta igualdad entre (a, b) se obtiene que

$$1 = \frac{a}{(a,b)}x + \frac{b}{(a,b)}y.$$

De esto se sigue que si d es un número entero que divide tanto a $\frac{a}{(a,b)}$ como a $\frac{b}{(a,b)}$ entonces $d \mid 1$: en consecuencia, el máximo común divisor de esos números tiene que ser exactamente igual a uno. ∎

2.2.1. Existencia y estructura de las soluciones

Teorema 2.1. *Sean a y b números enteros no ambos cero y sea c algún otro número entero. La ecuación diofántica*

$$aX + bY = c$$

tiene soluciones $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ si y sólo si $(a, b) \mid c$.

Demostración. Supongamos que $(x, y) \in \mathbb{Z}\times\mathbb{Z}$ es una solución de la ecuación diofántica $aX+bY = c$. Se cumple entonces que

$$ax + by = c. \tag{2.4}$$

Como (a, b) divide a b y a simultáneamente, entonces (a, b) divide a cualquier combinación lineal de a y b con coeficientes enteros: en particular, $(a, b) \mid c$ pues, de acuerdo con (2.4), c es un ejemplo de una combinación lineal de a y b con coeficientes enteros.

Supongamos ahora que $(a, b) \mid c$. Además, pensemos que

$$(a, b) = ax_0 + by_0 \tag{2.5}$$

para algunos números enteros x_0 y y_0 y que $z \in \mathbb{Z}$ es tal que

$$c = (a, b)z. \tag{2.6}$$

Multiplicando ambos miembros de (2.5) por z llegamos a que

$$(a, b)z = (ax_0 + by_0)z$$

lo cual se puede reescribir como

$$c = a(x_0z) + b(y_0z);$$

es claro que la igualdad anterior indica que la ecuación diofántica $aX+bY = c$ admite soluciones en números enteros. ∎

Ejemplos.

a) La ecuación $2X+6Y = 19$ no admite soluciones en números enteros pues el máximo común divisor de 2 y 6 es 2 y $2 \nmid 19$. La no solubilidad de una ecuación tan específica como ésta también se puede establecer notando que 19 es un número impar pero que $2X + 6Y$ es un número par para cualesquiera números enteros X y Y. Nótese que en este razonamiento

está encapsulada parte de la esencia del criterio en 2.1: ¡para que una igualdad como $2X + 6Y = 19$ tenga cabida (siendo X y Y números enteros), entonces cualquier número entero que divida a la expresión en la izquierda tiene que dividir al número en la derecha!

b) La ecuación $6X + 15Y = 36$ sí admite soluciones $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ pues $(6, 15) = 3$ y $3 \mid 36$. Un ejemplo de una solución a esta ecuación diofántica es $(x = 1, y = 2)$; otro ejemplo de una solución a la ecuación es $(x = 6, y = 0)$. Ya que se ha establecido la solubilidad de la ecuación surge el problema de describir a cabalidad el conjunto de soluciones de la misma: en el teorema que viene a continuación se presenta la solución a dicho problema en su formulación general.

Teorema 2.2. *Sean a y b números enteros distintos de cero y sea c algún otro número entero. Supongamos que $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de la ecuación diofántica*

$$aX + bY = c. \tag{2.7}$$

Si $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ es otra solución de la ecuación, entonces

$$\begin{cases} x &= x_0 + \frac{b}{(a,b)}t \\ y &= y_0 - \frac{a}{(a,b)}t \end{cases}$$

para algún número entero t.

Demostración. Se tiene que $ax + by = c$ y que $ax_0 + by_0 = c$. De esto se sigue que $ax + by = ax_0 + by_0$, lo cual se puede reescribir como

$$a(x - x_0) = b(y_0 - y).$$

Diviendo ambos lados de esta igualdad entre (a, b) obtenemos que

$$\frac{a}{(a,b)}(x - x_0) = \frac{b}{(a,b)}(y_0 - y). \tag{2.8}$$

Esta igualdad indica que $\frac{a}{(a,b)}$ es un divisor de $\frac{b}{(a,b)}(y_0 - y)$; puesto que $\frac{a}{(a,b)}$ y $\frac{b}{(a,b)}$ son coprimos (ver el corolario 2.2), la regla de oro de la aritmética nos permite garantizar que $\frac{a}{(a,b)}$ divide a $y_0 - y$. Así pues,

$$y_0 - y = \frac{a}{(a,b)}t \tag{2.9}$$

para algún número entero t. De lo anterior se desprende que $y = y_0 - \frac{a}{(a,b)}t$, que es justamente a lo que deseábamos llegar (en lo que a y respecta). Para obtener la fórmula para x combinamos

la información en (2.8) y (2.9): se obtiene que

$$a(x - x_0) = b\left(\frac{a}{(a,b)}t\right)$$

o bien que

$$x = x_0 + \frac{b}{(a,b)}t$$

y la demostración termina. ∎

En el teorema 2.2 se ha explicado cómo determinar completamente el conjunto de soluciones de una ecuación diofántica lineal en dos variables cuando se conoce una solución particular de ella. Para dar con una solución particular de la ecuación se puede proceder como en la demostración del teorema 2.1: enseguida detallamos el proceso para la ecuación $aX + bY = c$ en donde a y b son números enteros distintos de 0 y c es algún número entero tal que $(a, b) \mid c$:

◇ Con ayuda del algoritmo de Euclides determinamos números enteros x y y tales que $(a, b) = ax + by$.

◇ Multiplicando ambos lados de la igualdad anterior por $\frac{c}{(a,b)}$ llegamos a que

$$c = a\left(\frac{cx}{(a,b)}\right) + b\left(\frac{cy}{(a,b)}\right).$$

◇ De lo anterior se colige que $\left(x_0 = \frac{cx}{(a,b)}, y_0 = \frac{cy}{(a,b)}\right)$ es una solución particular de la ecuación diofántica $aX + bY = c$.

Ejemplos.

a) Determinemos el conjunto de soluciones de la ecuación diofántica $6X + 15Y = 36$. Dado que

$$\begin{aligned} 15 &= 6(2) + 3 \\ 6 &= 3(2) + 0, \end{aligned} \tag{2.10}$$

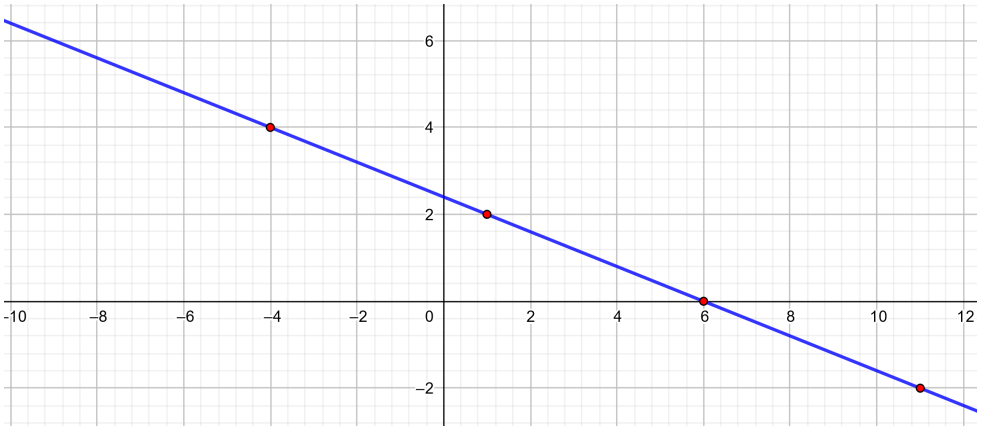
se sigue que $(15, 6) = (6, 3) = 3$; al ser 3 un divisor de 36 tenemos que la ecuación diofántica dada sí admite soluciones en números enteros. Para obtener una solución particular de la ecuación recurrimos a (2.10). De esa igualdad se obtiene que $3 = 6(-2) + 15(1)$; luego, si multiplicamos ambos lados por $\frac{36}{3} = 12$, se llega a que

$$36 = 6(-24) + 15(12).$$

Esto indica que $(x_0 = -24, y_0 = 12)$ es una solución particular de la ecuación diofántica $6X + 15Y = 36$. El teorema 2.2 nos permite concluir que el conjunto conformado por todas las soluciones de la ecuación es

$$\mathcal{S} = \{(\underbrace{-24 + 5t}_{x}, \underbrace{12 - 2t}_{y}) : t \in \mathbb{Z}\}.$$

Puesto que, geométricamente, $6X + 15Y = 36$ es una recta en el plano (con pendiente igual a $-6/15$ y ordenada al origen igual a $36/15$) entonces $\mathcal{S}$ consiste de todos los puntos de coordenadas enteras sobre esa recta.



En la figura, la recta $6X + 15Y = 36$ aparece en azul y, en rojo, se muestran cuatro de los puntos de coordenadas enteras sobre ella (cada punto es un elemento de $\mathcal{S}$). ¡Nótese que los puntos de coordenadas enteras están regularmente espaciados sobre la recta!

b) Determinemos ahora el conjunto de soluciones de la ecuación diofántica $245X + 198Y = 9$. Primero determinamos el máximo común divisor de los coeficientes 245 y 198 mediante el algoritmo de Euclides. Se obtiene que:

$$\begin{aligned} 245 &= 198(1) + 47 \\ 198 &= 47(4) + 10 \\ 47 &= 10(4) + 7 \\ 10 &= 7(1) + 3 \\ 7 &= 3(2) + 1 \\ 3 &= 1(3) + 0. \end{aligned}$$

Estas igualdades indican que $(245, 198) = 1$ y, además, permiten expresar ese máximo común divisor como una combinación lineal de 245 y 198 con coeficientes enteros; para hacerlo, todo es cuestión de ir despejando y sustituyendo los restos (distintos de cero) del último al primero:

$$\begin{aligned} 1 &= 7 - 3(2) \\ &= 7 - (10 - 7)(2) \\ &= 7(3) - 10(2) \\ &= (47 - 10(4))(3) - 10(2) \\ &= 47(3) - 10(14) \\ &= 47(3) - (198 - 47(4))(14) \\ &= 47(59) - 198(14) \\ &= (245 - 198)(59) - 198(14) \\ &= 245(59) + 198(-73). \end{aligned}$$

De esto se sigue que una solución particular de la ecuación diofántica $245X + 198Y = 9$ es $(x_0 = 531, y_0 = -657)$. En la luz del teorema 2.2 podemos concluir entonces que el conjunto de soluciones de la ecuación diofántica dada es

$$\mathcal{S} = \{(531 + 198t, -657 - 245t) : t \in \mathbb{Z}\}.$$

Al igual que en el inciso anterior es posible ubicar al conjunto $\mathcal{S}$ en el plano cartesiano pero, en esta ocasión, esa parte del análisis (por así decirlo) queda para que el lector interesado ponga a prueba su entendimiento de lo que hasta este momento hemos discutido.

NOTAS

Sobre la ecuación diofántica lineal en dos variables, A. Weil comenta en [7, p. 7] lo siguiente:

«El método general para resolverla lo brinda [implícitamente] el algoritmo de Euclides... Sin embargo, si no tomamos en cuenta las contribuciones de la civilización china, la primera descripción explícita de la solución general ocurre en la parte matemática del tratado astronómico conocido como *Āryabhaṭīya* el cual se remonta al siglo V d.C. A la solución allí expuesta se le llamó "la solución por el método *kuṭṭaka*" en algunos escritos posteriores: dado que *kuṭṭaka* se traduce como "pulverizador", la denominación no suena del todo fuera de lugar y hasta trae a

la mente el "descenso infinito" de Pierre de Fermat (1601-1665). Puesto que la astronomía hindú de los siglos V-VI d.C. se basa en gran medida en contribuciones griegas, surge la tentación de atribuirle el mismo origen al método *kuṭṭaka* pero sería difícil validar una hipótesis tal.

Después, en 1621, Claude Gaspar Bachet de Méziriac (1581-1638), ignorando por completo las contribuciones de sus predecesores de la India y también las respectivas conexiones con el libro VII de *Los elementos*, se atribuyó la solución general de la ecuación diofántica lineal en dos variables en sus comentarios a la *Aritmética* de Diofanto de Alejandría (s. III d.C.). Bachet mencionó que su solución sería publicada después en un libro de "elementos" de la aritmética pero, como tal obra nunca salió, la insertaría en la segunda edición de sus *Problèmes plaisants et délectables* (Lyon 1624) y sería en ese tomo en el cual la aprenderían Fermat y John Wallis (1616-1703); no obstante, tanto Fermat como Wallis seguramente tenían bien presentes *Los elementos* como para no caer en la cuenta que todo ello ya estaba en Euclides...»

Capítulo 3

Ejemplos varios

3.1. Propósito

En los problemas que trataremos a continuación no sólo se ilustra la teoría desarrollada en el capítulo anterior sino que también se ponen a prueba algunas competencias algebraicas básicas tales como el planteamiento de ecuaciones con dos variables, la eliminación de una variable en un sistema de dos ecuaciones lineales y la resolución de inecuaciones de primer grado.

3.2. Ejemplos

Ejemplo 1. Un granjero gasta $ 1000 en comprar 100 animales de 3 tipos diferentes. Cada vaca le cuesta $ 20, cada cerdo $ 12 y cada oveja $ 8. Si se sabe que el granjero compró al menos 10 animales de cada especie, ¿cuántos animales de cada especie compró?

Solución. Denotemos con x al número de vacas adquiridas por el granjero, con y al número de cerdos y con z al número de ovejas. Del planteamiento del problema se desprende que las incógnitas satisfacen

$$\begin{cases} x + y + z = 100 \\ 20x + 12y + 8z = 1000 \end{cases}$$

Si multiplicamos ambos lados de la primera ecuación por -8 y la ecuación así obtenida la sumamos lado a lado con la segunda ecuación del sistema obtenemos la ecuación diofántica lineal

$$12x + 4y = 200,$$

la cual es equivalente a

$$3x + y = 50. \tag{3.1}$$

Como $(3, 1) = 1$ y $1 \mid 50$, esta ecuación admite soluciones en números enteros. Una solución particular de la ecuación es $(x_0 = 0, y_0 = 50)$. Luego, el conjunto de soluciones de 3.1 es

$$\mathcal{S} = \{(\underbrace{t}_{x}, \underbrace{50 - 3t}_{y}) : t \in \mathbb{Z}\}.$$

Puesto que tanto x como y deben ser mayores o iguales a 10, entonces el parámetro t debe cumplir las desigualdades

$$t \geq 10 \quad \text{y} \quad 50 - 3t \geq 10.$$

De esto se sigue que t sólo puede ser igual a 10, 11, 12 o 13. Cada una de esta opciones para t da una posible respuesta al problema; los distintos totales que pudo haber adquirido el granjero se desglosan en la tabla que se muestra a continuación:

t	x (vacas)	y (cerdos)	z (ovejas)
10	10	20	70
11	11	17	72
12	12	14	74
13	13	11	76

Ejemplo 2. La asociación "Defendamos El Cerro Chuperio" tiene 50 integrantes. El sábado cada uno de los integrantes presentes plantó 17 árboles y el domingo cada uno de los integrantes presentes plantó 20 árboles. En total se plantaron 1545 árboles. ¿Cuántos de los miembros de la asociación faltaron el sábado y cuántos faltaron el domingo?

Solución. Denotemos con x al número de personas que asistieron el sábado y con y al número de personas que asistieron el domingo. Considerando la condición sobre el número de árboles que fueron plantados en total obtenemos la ecuación:

$$17x + 20y = 1545. \tag{3.2}$$

Aplicando el algoritmo de Euclides procedemos a calcular el máximo común divisor de 17 y

20:

$$\begin{aligned} 20 &= 17(1) + 3 \\ 17 &= 3(5) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0. \end{aligned}$$

De la penúltima igualdad se obtiene que $1 = (17, 20)$ y entonces podemos garantizar que la ecuación 3.2 admite soluciones en números enteros. Para obtener una solución particular de la ecuación empezamos por recurrir al algoritmo de Euclides para expresar el máximo común divisor de 17 y 20 como combinación lineal de ellos con coeficientes enteros: llegamos a que $1 = 17(-7) + 20(6)$ y de esto se sigue que

$$1545 = 17(-10815) + 20(9270).$$

Así pues, $(x_0 = -10815, y_0 = 9270)$ es una solución particular de 3.2; consecuentemente, el conjunto de soluciones de la ecuación es

$$\mathcal{S} = \{(-10815 + 20t, 9270 - 17t) : t \in \mathbb{Z}\}$$

Puesto que la asociación tiene 50 integrantes, se requiere que el parámetro t satisfaga las desigualdades

$$-10815 + 20t \leq 50 \quad \text{y} \quad 9270 - 17t \leq 50.$$

De la primera desigualdad se obtiene que $t \leq 543.25$, mientras que de la segunda desigualdad se llega a que $t \geq 542.35$. Tenemos así que $x = -10815 + 20(543) = 45$ y $y = 9270 - 17(543) = 39$; por lo tanto, el sábado faltaron 5 miembros de la asociación y el domingo faltaron 11 miembros.

Ejemplo 3. Una compañía compró cierto número de reliquias falsas a $ 17 cada una y vendió algunas de ellas a $ 49 cada una. Si la cantidad comprada originalmente es mayor que 50 y menor que 100 y la compañía tuvo una ganancia de $ 245, ¿cuántas reliquias faltan por vender?

Solución. Denotemos con x al número de reliquias adquiridas por la compañía y con y al número de reliquias vendidas. Estas incógnitas están vinculadas por la ecuación

$$49y - 17x = 245.$$

Puesto que $(49, -17) = 1$, la ecuación tiene soluciones en números enteros. Para obtener una solución particular, recurrimos al algoritmo de Euclides; dado que

$$\begin{aligned} 49 &= (-17)(-2) + 15 \\ -17 &= 15(-2) + 13 \\ 15 &= 13(1) + 2 \\ 13 &= 2(6) + 1 \\ 2 &= 1(2) + 0, \end{aligned}$$

se sigue que

$$\begin{aligned} 1 &= 13 - 2(6) \\ &= 13 - (15 - 13)(6) \\ &= 13(7) - 15(6) \\ &= (-17 + 15(2))(7) - 15(6) \\ &= -17(7) + 15(8) \\ &= -17(7) + (49 - 17(2))(8) \\ &= -17(23) + 49(8). \end{aligned}$$

Esto indica que $(x_0 = 23(245), y_0 = 8(245))$ es una solución particular de la ecuación diofántica que estamos analizando; por lo tanto, el conjunto de soluciones de ella es

$$\mathcal{S} = \{(5635 + 49t, 1960 + 17t) : t \in \mathbb{Z}\}.$$

La condición $50 < x < 100$ indica que el parámetro t debe satisfacer las desigualdades

$$50 < 5635 + 49t < 100.$$

El único número entero t que satisface ambas desigualdades es $t = -113$. De esto se sigue que $x = 5635 + 49(-113) = 98$ y que $y = 1960 + 17(-113) = 39$. Se concluye que la compañía aún tiene $98 - 39 = 59$ reliquias por vender.

Ejemplo 4. En un cine cobran 18 dólares a los mayores de edad y 7.50 dólares a los menores de edad. En una función se recaudaron 900 dólares y asistieron más mayores de edad que menores de edad. ¿Cuáles fueron los posibles números de asistencia a esa función?

Solución. Denotemos con x al número de personas que son mayores de edad y que asistieron a la función y denotemos con y al número de personas que son menores de edad y que asistieron a la función. Las incógnitas están vinculadas por la ecuación $18x + 7.50y = 900$ y por las desigualdades $x > y \geq 0$. La ecuación es equivalente con

$$12x + 5y = 600. \tag{3.3}$$

Mediante el algoritmo de Euclides calculamos $(12, 5)$ y lo expresamos como combinación lineal de 12 y 5: dado que

$$\begin{aligned} 12 &= 5(2) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 1(2) + 0, \end{aligned}$$

se obtiene que $(12, 5) = 1$ y que

$$\begin{aligned} 1 &= 5 - 2(2) \\ &= 5 - (12 - 5(2))(2) \\ &= 12(-2) + 5(5); \end{aligned}$$

en consecuencia, una solución particular a 3.3 es $(x_0 = -1200, y_0 = 3000)$. Tenemos así que el conjunto de soluciones de la ecuación diofántica que estamos considerando es

$$\mathcal{S} = \{(-1200 + 5t, 3000 - 12t) : t \in \mathbb{Z}\}.$$

Como las incógnitas en este problema deben satisfacer $x > y \geq 0$, el parámetro t cumple que

$$-1200 + 5t > 3000 - 12t \geq 0.$$

De la desigualdad de más a la izquierda se sigue que $t > 4200/17 \approx 247.06$; de la desigualdad en la derecha se obtiene que $t \leq 3000/12 = 250$. Como t ha de ser un número entero, entonces $t = 248$, $t = 249$ o $t = 250$. Cada una de estas posibilidades para t da una respuesta válida; concentramos las tres en la siguiente tabla:

t	x (mayores de edad)	y (menores de edad)
248	40	24
249	45	12
250	50	0

Ejemplo 5. Estando a la orilla de un río, ¿cómo mediría 14 litros de agua cuando se tiene un recipiente con una capacidad de 3 litros y un recipiente con una capacidad de 19 litros?

Solución. Suponiendo que los 14 litros deben quedar en algún contenedor adicional, el problema se relaciona con el estudio del conjunto de soluciones de la ecuación diofántica

$$19x + 3y = 14. \tag{3.4}$$

La ecuación admite soluciones en números enteros pues $(19, 3) = 1$. Además, en vista de que

$$\begin{aligned} 19 &= 3(6) + 1 \\ 3 &= 1(3) + 0, \end{aligned}$$

se tiene que $1 = 19(1) + 3(-6)$ y que, por ende, $(x_0 = 14, y_0 = -84)$ es una solución particular de 3.4. Esto dice que una forma de quedarnos con 14 litros en el contenedor adicional es virtiendo 14 veces el recipiente de 19 litros y extrayendo después 84 veces el recipiente de 3 litros de él. Esa no es la única manera de llegar a los 14 litros. El conjunto de soluciones de la ecuación diofántica que estamos analizando es $\mathcal{S} = \{(14 + 3t, -84 - 19t) : t \in \mathbb{Z}\}$. En la siguiente tabla presentamos otras formas de hacer la medición de los 14 litros:

t	x	y
-1	11	-65
-2	8	-46
-3	5	-27
-4	2	-8
-5	-1	11

La solución en la penúltima fila de la tabla brinda una forma muy breve de hacer la medición de los 14 litros: ¡virtiendo 2 veces el recipiente de 19 litros y extrayendo después 8 veces el recipiente de 3 litros!

Ejemplo 6. Por 5 rublos se compraron 100 unidades de diferentes frutas. Sus precios son los siguientes: cada sandía cuesta 50 kopeks, cada manzana cuesta 10 kopeks y cada ciruela cuesta 1 kopek. ¿Cuántas piezas de cada fruta se compraron?

Solución. Denotemos con x al número de sandías compradas, con y al número de manzanas compradas y con z al número de ciruelas que se compraron. Estas incógnitas satisfacen el sistema de ecuaciones:

$$\begin{cases} x + \quad y + z = 100 \\ 50x + 10y + z = 500 \end{cases}$$

De estas dos ecuaciones se obtiene la ecuación diofántica

$$49x + 9y \quad = \quad 400. \tag{3.5}$$

Como $(49, 9) = 1$ y $1 \mid 400$, es claro que la ecuación admite soluciones en números enteros. En vista de que

$$\begin{aligned} 49 &= 9(5) + 4 \\ 9 &= 4(2) + 1 \\ 4 &= 1(4) + 0, \end{aligned}$$

tenemos que $1 = 9 - 4(2) = 9 - (49 - 9(5))(2) = 49(-2) + 9(11)$; de esto se desprende que $(x_0 = -800, y_0 = 4400)$ es una solución particular de 3.5. El conjunto de soluciones de ésta es

$$\mathcal{S} = \{(-800 + 9t, 4400 - 49t) \colon t \in \mathbb{Z}\}.$$

Puesto que necesitamos las soluciones de 3.5 en las que tanto x como y son números enteros no negativos, entonces el parámetro t debe satisfacer

$$t \geq 800/9 \quad \text{y} \quad 4400/49 \geq t.$$

El único número $t \in \mathbb{Z}$ que cumple ambas desigualdades es $t = 89$. Concluimos que el número de sandías compradas fue $x = -800 + 9(89) = 1$, que el número de manzanas compradas fue $y = 4400 - 49(89) = 39$ y que el número de ciruelas compradas fue $z = 60$.

Ejemplo 7. Una bufanda cuesta 19 rublos pero el comprador no tiene más que billetes de 3 rublos y la cajera sólo de 5. ¿Puede en estas condiciones abonarse el importe de la compra?

Solución. Este problema se conecta con la ecuación diofántica

$$3x + 5y = 19. \tag{3.6}$$

Como $(5,3) = 1$ y $1 = 3(2)+5(-1)$, una solución particular de la ecuación 3.6 es $(x_0 = 38, y_0 = -19)$. En consecuencia, el conjunto de soluciones es

$$\mathcal{S} = \{(38 + 5t, -19 - 3t) : t \in \mathbb{Z}\}.$$

Con $t = -6$ tenemos la solución $(x = 8, y = -1)$, la cual proporciona la respuesta más concisa posible a la pregunta planteada: una forma de abonar el importe de la compra es dando 8 billetes de 3 rublos y recibiendo como cambio 1 billete de 5 rublos de parte de la cajera.

Ejemplo 8. Sean a y b números enteros positivos y coprimos. Suponga que c es algún otro número entero. Demuestre que la recta de ecuación $ax + by = c$ pasa por un punto de coordenadas enteras del plano cuya ordenada pertenece al intervalo $[0, a-1]$.

Solución. Como $(a,b) \mid c$, la ecuación diofántica $aX + bY = c$ tiene soluciones en números enteros. Pensemos que (x_0, y_0) es una solución particular de $aX + bY = c$. Puesto que las ordenadas de la soluciones de esa ecuación son del tipo $y_0 - at$ (donde t es un número entero), el problema se reduce a establecer que, para algún $t \in \mathbb{Z}$, se cumple que $0 \leq y_0 - at \leq a - 1$.

Si tomamos t como el cociente que se obtiene al dividir y_0 entre a y r es el resto de esa división, entonces $y_0 - at = r$ y las desigualdades $0 \leq y_0 - at \leq a - 1$ son inmediatas del algoritmo de la división en $\mathbb{Z}$.

Ejemplo 9. Sean a y b números enteros positivos y coprimos. Demuestre que $c = ab - a - b$ es el mayor número entero para el cual la ecuación

$$aX + bY = c$$

no admite soluciones en números enteros no negativos X y Y.

Solución. Primero demostraremos que para $c = ab - a - b$ la ecuación no tiene soluciones en números enteros no negativos. Supongamos lo contrario; es decir, supongamos que existen números enteros no negativos x y y tales que

$$ax + by = ab - a - b.$$

De esta igualdad se sigue que

$$a(x + 1) + b(y + 1) = ab; \tag{3.7}$$

lo cual a su vez implica que $a \mid b(y+1)$ y que $b \mid a(x+1)$. Como a y b son coprimos, el colorario 2.1 aplica y nos lleva a que $a \mid (y+1)$ y $b \mid (x+1)$; tomando esto en cuenta y la igualdad 3.7 se desprende que

$$ab \geq ab + ab = 2ab,$$

lo cual es un absurdo. Así pues, la ecuación diofántica $aX + bY = c$ no admite soluciones en números enteros no negativos cuando $c = ab - a - b$.

Supongamos ahora que N es un número entero mayor que $ab - a - b$. Mostraremos que la ecuación diofántica $aX + bY = N$ admite soluciones en números enteros no negativos. De acuerdo con el **Ejemplo 8**, la ecuación $aX + bY = N$ tiene una solución $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \times \mathbb{Z}$ en la que $0 \leq \mathbf{y} \leq a - 1$. Afirmamos que en esa solución se cumple que $\mathbf{x} \geq 0$: en efecto, en vista de que

$$\begin{aligned} a\mathbf{x} &= N - b\mathbf{y} \\ &> ab - a - b - b(a-1) \\ &= -a, \end{aligned}$$

tenemos que $\mathbf{x} > -1$ y, consiguientemente, que $\mathbf{x} \geq 0$. Se cumple pues que $(\mathbf{x}, \mathbf{y})$ es una solución en números enteros no negativos de $aX + bY = N$ y la demostración termina.

Ejemplo 10. En Piedradura hay billetes de 3 y 5 piedrólares. Demuestre que con suficientes billetes de esas denominaciones es posible pagar cualquier monto de 8 o más piedrólares sin que se requiera vuelto.

Solución. Este problema se puede abordar de distintas maneras. Dado que $(3)(5) - 3 - 5 = 7$, la conclusión deseada se puede obtener fácilmente a partir del resultado en el ejemplo anterior; de hecho, el problema también se puede establecer mediante inducción matemática. A continuación presentaremos una solución en la que sólo se apela al algoritmo de la división.

En vista de que

$$\begin{aligned} 8 &= 3(1) + 5(1) \\ 9 &= 3(3) + 5(0) \\ 10 &= 3(0) + 5(2) \\ 11 &= 3(2) + 5(1) \\ 12 &= 3(4), \end{aligned}$$

en lo sucesivo podemos suponer que el monto $\mathcal{M}$ a pagar es de 13 o más piedrólares. Por el algoritmo de la división en $\mathbb{Z}$ sabemos que $\mathcal{M}$ deja resto 0, 1 o 2 en la división por 3.

Si $\mathcal{M}$ deja resto 0, entonces

$$\mathcal{M} = 3q$$

para algún número entero $q \geq 5$; esto indica que, en este caso, el monto se puede pagar usando puros billetes de 3 piedrólares.

Si $\mathcal{M}$ deja resto 1, entonces $\mathcal{M} = 3q + 1$ para algún número entero $q \geq 4$. Luego, al notarse que

$$\mathcal{M} = 3q + 1 = 3(q - 3) + 5(2)$$

se colige que, en este caso, el monto se puede pagar usando $q - 3$ billetes de 3 piedrólares y dos billetes de 5 piedrólares.

Finalmente, si $\mathcal{M}$ deja resto 2, entonces $\mathcal{M} = 3q + 2$ para algún número entero $q > 3$. Luego, al tenerse que

$$\mathcal{M} = 3q + 2 = 3(q - 1) + 5(1)$$

se concluye que, en este caso, el monto se puede pagar al desembolsar $q - 1$ billetes de 3 piedrólares y un billete de 5 piedrólares.

Puesto que los tres casos considerados engloban todas las posibilidades para un monto (entero) $\mathcal{M} \geq 13$, la demostración termina.

3.3. Fuentes

Comentamos a continuación de dónde retomamos algunos de los problemas que discutimos en la sección anterior. Infortunadamente, no pudimos asociar dos ellos con alguna referencia específica.

- Ejemplo 1:

J. A. de la Peña. *Álgebra en todas partes.* Colección La ciencia para todos, no. 166; Fondo de Cultura Económica, México, 1999, pp. 74-75.

- Ejemplo 3:

A. J. Pettofrezzo & D. R. Byrkit. *Introducción a la teoría de los números.* Editorial Prentice-Hall Internacional, 1972, p. 51.

- Ejemplo 4:

E. R. Gentile. *Aritmética elemental en la formación matemática.* UBA y Consejo Nacional de Investigaciones Científicas y Universitarias, Buenos Aires, Argentina, 1991, p. 17.

- Ejemplo 6:

Ya. I. Perelman. *Algebra can be fun.* Translated from the 13th Russian edition by G. Yankovsky, Mir Publishers, Moscow, 1979, pp. 124-126.

- Ejemplo 7:

Ya. I. Perelman. *Algebra can be fun.* Translated from the 13th Russian edition by G. Yankovsky, Mir Publishers, Moscow, 1979, pp. 116-120.

El resultado en el Ejemplo 9 se atribuye al matemático inglés James Joseph Sylvester (1814-1897); para más detalles sobre la historia y ramificaciones de este ejemplo se recomienda consultar el siguiente artículo:

J. L. Ramírez Alfonsín. *El problema diofántico de Frobenius.* La Gaceta de la Real Sociedad Matemática Española, vol. 16 (2013), no. 1. pp. 117-129.

El Ejemplo 8 es un paso intermedio que aparece en algunas demostraciones del teorema de Sylvester; para que la demostración de dicho teorema quedara más clara, nosotros decidimos abordar ese paso por separado.

- Ejemplo 10:

I. S. Sominski. *El método de la inducción matemática.* Editorial Limusa, 1972, p. 30.

Bibliografía

[1] E. R. Gentile, *Aritmética elemental*. UBA y Consejo Nacional de Investigaciones Científicas y Técnicas. Buenos Aires, Argentina, 1985.

[2] E. R. Gentile, *Aritmética elemental en la formación matemática*. UBA y Consejo Nacional de Investigaciones Científicas y Técnicas. Buenos Aires, Argentina, 1991.

[3] G. H. Hardy, *An introduction to the theory of numbers*. Bulletin of the Amer. Math. Soc, **35** (1929), no. 6, pp. 778-818.

[4] B. Mazur, *How did Theaetetus prove his theorem?* The envisioned life: essays in the honor of Eva Brann. Paul Dry Books, 2007, pp. 227-250.

[5] Secretaria de Educación Pública (México), *Progresiones de aprendizaje del recurso sociocognitivo de Pensamiento Matemático*. Recurso en línea: `http://desarrolloprofesionaldocente.sems.gob.mx/convocatoria1_2023/docs/Documento%20progresiones%20-%20Pensamiento%20matem%C3%A1tico.pdf` (Consultado por última vez: 02-05-2023).

[6] J. Shallit, *Origins of the analysis of the Euclidean algorithm*. Historia Mathematica, **24** (1994), pp. 401-419.

[7] A. Weil, *Number theory: an approach through history, from Hammurapi to Legendre*. Birkhäuser Verlag, 1983.

[8] F. Zaldívar, *Introducción a la teoría de números*. Fondo de Cultura Económica (Colec. Sección de Obras de Ciencia y Tecnología), México, D. F., 2012.