COLECCIÓN **CÁTEDRA**

MAT



# TEORÍA DE NÚMEROS EN LA FORMACIÓN DOCENTE

Sara Scaglia
Marcela Götte

ediciones UNL

# Teoría de números en la formación docente

UNIVERSIDAD
NACIONAL DEL LITORAL

ediciones UNL





—

Sugerencias y comentarios
editorial@unl.edu.ar
www.unl.edu.ar/editorial

Scaglia, Sara
Teoría de números en la formación docente /
Sara Scaglia ; Marcela Götte.
1a ed. – Santa Fe : Ediciones UNL, 2025.
Libro digital, PDF/A – (cátedra)

Archivo Digital: descarga y online
ISBN 978–987–749–505–8

1. Matemática. 2. Educación Superior. 3.
Números. I. Götte, Marcela II. Título
CDD 510.711

———————



Se diagramó y compuso
en Ediciones UNL.

Queda hecho el depósito
que marca la ley 11723.


# Teoría de números en la formación docente

*Sara Scaglia*
*Marcela Götte*

ediciones UNL
CÁTEDRA

# Agradecimientos

Agradecemos a la Dra. Liliana Nitti y a la Mg. Eleonora Cerati los comentarios realizados a una primera versión de este libro, que han permitido aclarar algunas ideas y profundizar las reflexiones en torno a otras.

Asimismo, agradecemos a Juan Bautista Götte por sus ocurrentes caricaturas de matemáticos famosos, que proporcionan un toque de humor a los comentarios históricos.

Por último, agradecemos especialmente a nuestras/os estudiantes de Matemática Discreta I del Profesorado en Matemática de la Facultad de Humanidades y Ciencias de la Universidad Nacional del Litoral la posibilidad de disfrutar de momentos estimulantes y enriquecedores de intercambio.

*Las autoras*

# Índice

**INTRODUCCIÓN** / 9

**1. SITUACIONES PARA INTRODUCIR CONCEPTOS DE DIVISIBILIDAD** / 15
**2. APORTES PARA LA ENSEÑANZA DE DIVISIBILIDAD** / 27
**3. DIVISIBILIDAD EN LOS ENTEROS** / 35
3.1 Conceptos básicos de divisibilidad / 35
3.2 Números primos y números compuestos / 36
3.3 Algoritmo de la división / 37
3.4 Máximo común divisor y algoritmo de Euclides / 38
3.5 Mínimo común múltiplo / 42
3.6 Ecuaciones diofánticas / 43
3.7 El teorema fundamental de la aritmética / 46

**4. SITUACIONES PARA PROFUNDIZAR CONCEPTOS DE DIVISIBILIDAD** / 49
**5. SITUACIONES PARA INTRODUCIR CONCEPTOS DE CONGRUENCIA** / 53
**6. APORTES PARA LA ENSEÑANZA DE CONGRUENCIA** / 61
**7. CONGRUENCIAS EN LOS ENTEROS** / 69
7.1 Conceptos básicos de congruencia / 69
7.2 Congruencia como relación de equivalencia / 71
7.3 Criterios de divisibilidad / 72
7.4 Ecuación lineal de congruencia / 73
7.5 Sistemas de ecuaciones lineales de congruencias / 76
7.6 Teorema chino del resto / 79
7.7 Sistema de restos / 80
7.8 Pequeño teorema de Fermat / 80
7.9 Teorema de Euler-Fermat / 81

**8 SITUACIONES PARA PROFUNDIZAR CONCEPTOS DE CONGRUENCIA** / 83
**REFERENCIAS BIBLIOGRÁFICAS** / 87
**SOBRE LAS AUTORAS** / 89

# Introducción

Este libro tiene la finalidad de compartir nuestras experiencias en torno a la enseñanza de la aritmética o teoría de números en la formación de profesores/as de matemática.

Este campo de la matemática se ocupa del estudio de las propiedades de los números naturales y enteros (Gentile, 1985). Las propiedades de los números naturales relacionadas con la divisibilidad fueron estudiadas desde tiempos remotos. Algunas fueron conocidas por los chinos (500 a. C.) y posteriormente Euclides (300 a. C.) realizó el primer estudio sistemático de la teoría de números. Los resultados que se generaron en ese entonces no tenían aplicaciones concretas. Transcurridos más de dos milenios, esas propiedades constituyen la base para el desarrollo de conocimientos que son esenciales en la sociedad actual para dar respuesta a dos tipos de problemas: la confidencialidad en la transmisión de información y la integridad en la transmisión y el almacenamiento de información (Canavelli, 2011).

La propuesta que compartimos en estas páginas proviene de nuestra experiencia en la formación de profesores/as de matemática. No obstante, consideramos que muchas situaciones, conceptos y propiedades que se trabajan en esta obra pueden adaptarse para su inclusión en la escolaridad obligatoria. En efecto, en los Núcleos de Aprendizaje Prioritarios (NAP) en vigencia en nuestro país para el primer ciclo de la educación secundaria, se propone la exploración y el enunciado de propiedades ligadas a la divisibilidad y la producción y el análisis de afirmaciones sobre los criterios de divisibilidad en el conjunto de los números naturales (Ministerio de Educación, 2013).

Las orientaciones curriculares apuntan, además, al desarrollo de ciertas habilidades que se vinculan específicamente con el quehacer matemá-

tico tales como la resolución de problemas, la producción de modelos matemáticos, la producción de conjeturas, el análisis de su campo de validez y la utilización de distintas representaciones para dar cuenta de los conocimientos matemáticos (Ministerio de Educación, 2013). En el mismo sentido, Itzcovich (2007) reconoce que durante la escolaridad obligatoria la matemática para las/os estudiantes queda definida según el tipo de experiencias que les hagamos transitar en relación con los conceptos matemáticos e identifica algunas características principales del trabajo matemático, entre las cuales figuran las habilidades mencionadas al inicio de este párrafo.

En sintonía con las recomendaciones anteriores, durante el estudio de un determinado campo de la matemática, además de la familiarización con los conceptos, estrategias y propiedades del campo, nos interesa hacer hincapié en las características del trabajo matemático, que se consideran tan importantes como las nociones específicas. De Lorenzo (1998) sostiene que la imagen más difundida de la matemática asume a esta disciplina como exacta y verdadera, fosilizada en libros de texto que presentan definiciones precisas como puntos de partida, demostraciones completas y únicas de cada propiedad, promoviendo la idea de que se trata de una disciplina acabada, en la que no queda nada por hacer. Frente a esta imagen, el autor contrapone la idea de la matemática como «un trabajo, un producto y una producción de la especie humana» (De Lorenzo, 1998:16). Señala que «el Hacer matemático no es un saber ya plenamente cristalizado, sino un saber vivo, en constante proceso» (16).

En relación con el contenido de este libro, consideramos que la aritmética proporciona un espacio fecundo para iniciarse en el hacer matemático en el sentido en que lo propone De Lorenzo (1998), a la vez que admite una organización de sus principales definiciones y propiedades siguiendo un esquema prototípico del sistema axiomático deductivo, propio de la disciplina. Ambos aspectos son considerados y retomados en este libro. Gentile (2012a) afirma que matemáticos como Hilbert y Hardy han reconocido la potencialidad de la aritmética para el entrenamiento matemático inicial, dado que «es única en cuanto a campo de experimentación de la imaginación» (Gentile, 2012:9). Como indica este autor, en este campo de la matemática es posible plantear problemas de todo tipo de complejidad. Conjeturas relevantes que tuvieron en vilo durante muchos siglos a algunos de los matemáticos más destacados e incluso otras aún no resueltas hasta el momento de la publicación de esta obra (como la

conjetura de Goldbach) admiten una formulación relativamente sencilla en términos de nociones aritméticas.

Una lectura básica del índice de cualquier libro de texto de aritmética permite vislumbrar las huellas que dejaron muchos matemáticos (algunos de tiempos remotos) en este dominio de la matemática. Denominaciones como el «algoritmo de Euclides», las «ecuaciones diofánticas», el «pequeño Teorema de Fermat», el «Teorema de Euler–Fermat» son algunas de ellas. En la figura 1 mostramos las épocas aproximadas en que vivieron algunos de los matemáticos que vamos a mencionar en este trabajo (Boyer, 1986).

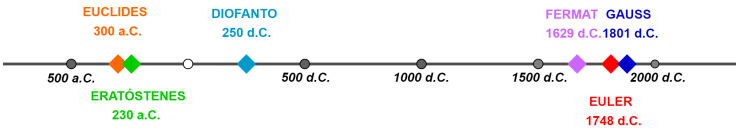



Figura 1. Ubicación temporal aproximada de algunos de los matemáticos mencionados

Nos interesa llamar la atención sobre esta cuestión, porque muchas veces estudiamos matemática pensando que los teoremas, sus demostraciones, determinadas estrategias de resolución, tienen una existencia independiente (y previa) a los seres humanos. Esta posición es coherente con la concepción platonista de la matemática (Davis y Hersh, 1988), según la cual, los objetos matemáticos son reales y existen de modo independiente del conocimiento que tengamos de ellos. No son creados sino descubiertos por los matemáticos. El estudio que proponemos de la aritmética, en consonancia con las afirmaciones anteriores de De Lorenzo (1998) pretende discutir esa creencia, que según Coriat (1997) se puso en duda a partir del siglo XIX, como consecuencia de la aparición de geometrías para las que no se conocían aplicaciones en el mundo real. Las matemáticas comenzaron a pensarse como un juego «cuya única meta–regla, inamovible, es la de “no hacer trampas”: ser coherentes con los axiomas admitidos y aceptar los resultados que se deriven de éstos» (181). Según este autor, al aceptar el papel motor de la cultura en el desarrollo de la disciplina, no se necesita un absoluto mental o divino al que haya que referirse para sancionar un nuevo conocimiento matemático. Por esa razón, se alude al término invención para hacer referencia a este enfoque, que concibe las matemáticas como un juego o una cuestión de conversación. En línea con esta nueva interpretación, consideramos la

matemática como un producto cultural, porque las concepciones de la sociedad en un momento histórico particular permean las producciones matemáticas, y social, porque estas son el resultado de la interacción entre personas que se reconocen como pertenecientes a una misma comunidad (Sadovsky, 2005).

A partir de estas consideraciones, nuestra propuesta para el estudio de la aritmética se organiza en torno a dos grandes temáticas: divisibilidad y congruencias. Para cada una se destinan cuatro capítulos que describimos a continuación.

En los capítulos primero y quinto, planteamos los enunciados de situaciones con las que se espera problematizar conceptos vinculados con divisibilidad y congruencias (respectivamente). Entre las situaciones problemáticas se incluyen datos históricos sobre matemáticos que abordaron algunas de las nociones aritméticas estudiadas y que ayudan a reconocer los resultados presentados como un acervo de conocimientos que se fue construyendo a lo largo de los siglos.

En los capítulos segundo y sexto desarrollamos comentarios sobre cada situación problematizadora incluida en el capítulo previo. Estos comentarios apuntan a reflexionar sobre el trabajo matemático que es posible desplegar en torno a cada una (Itzcovich, 2007): la resolución de problemas en los que intervienen las nociones que se espera estudiar y que proporcionan estrategias óptimas (en el sentido de económicas y potentes) para su resolución; la construcción de modelos que permiten expresar situaciones mediante sistemas teórico–matemáticos con la finalidad de producir nuevos conocimientos sobre esa situación (Chevallard, 1989); la elaboración y validación de conjeturas que establecen relaciones entre las nociones estudiadas y la determinación de su campo de validez; la exploración de las situaciones a partir de distintas representaciones. Algunas situaciones tienen la finalidad de reflexionar en torno a la producción de definiciones, dado que asumimos, como De Villiers (2009), que la construcción de definiciones constituye una actividad matemática no menos importante que la elaboración de deducciones a partir de definiciones dadas.

Con la finalidad de favorecer el recorrido de esta propuesta y ser coherentes con la decisión adoptada en relación con valorar el trabajo matemático tanto como su resultado, los capítulos segundo y sexto incluyen recomendaciones respecto de cómo secuenciar las situaciones problematizadoras del capítulo previo, con el desarrollo matemático

del capítulo posterior. No obstante, se trata solo de sugerencias, dado que reconocemos que cada lector/a docente deberá construir su propio recorrido, a la luz de los propósitos que persigue en su proyecto de enseñanza y de las características de sus estudiantes. Asimismo, pensamos que los comentarios de ningún modo agotan las cuestiones en torno a las cuales reflexionar en la formación del profesorado.

En cuanto al modo de organizar el trabajo en el aula, es altamente recomendable que las situaciones sean abordadas en grupos pequeños, para luego proponer una discusión y puesta en común de las estrategias que se hayan puesto en juego en cada grupo. Como sostiene Sadovsky (2005:61), «elaborar conocimiento en colaboración con otros da en general lugar a un intercambio que permite profundizar las ideas que están en juego en un cierto momento». No obstante, el/la docente decidirá en qué situaciones conviene proponer un trabajo autónomo e independiente por parte de cada estudiante y en cuáles puede resultar más rico proponer de entrada un trabajo grupal, reconociendo también la «posibilidad de que la clase pueda constituirse en un ámbito que aloje el trabajo privado de los alumnos, que no ingresará a la esfera pública, que no será compartido» (Sadovsky, 2005:62).

Los capítulos tercero y séptimo contienen un desarrollo deductivo en torno a temas aritméticos elementales vinculados con divisibilidad y congruencias (respectivamente). Como sostiene De Lorenzo (1998), constituyen posibles organizaciones estáticas de este campo de la matemática. Por esa razón, ha supuesto la selección de definiciones y de demostraciones únicas para cada propiedad. Como destaca Gentile (2012a), la aritmética constituye una opción excelente para mostrar «una verdadera Teoría, clara y coherente, como un edificio que se puede visualizar en su totalidad» (Gentile, 2012a:10). Como libros de consulta y fuentes para nuestra elección tomamos las obras de Becker, Pietrocola y Sánchez (2001), Gentile (1985, 2012a, 2012b) y Grimaldi (1998).

Los capítulos cuarto y octavo incluyen una selección de situaciones problemáticas que permiten profundizar el estudio y proporcionan la oportunidad de que las/os estudiantes realicen un trabajo autónomo en torno a los conceptos aritméticos abordados en sendos capítulos previos. Para la elaboración de esas situaciones consultamos las obras de Becker, Pietrocola y Sánchez (2001), Gentile (1985, 2012a, 2012b) y Grimaldi (1998).

Esperamos que el/la lector/a disfrute durante el estudio de la teoría de números en la misma medida en que las autoras del libro lo hemos hecho durante su enseñanza en la formación de profesoras/es.

Sara y Marcela

# Capítulo 1

# Situaciones para introducir conceptos de divisibilidad

**SITUACIÓN 1**

En el año 1994, Molinos Río de la Plata difundió una promoción para que participen los consumidores de sus productos en todo el país. La figura 2 es una fotografía del volante original utilizado para su difusión.

Las bases completas del concurso se incluyen en la figura 3, fotografía del reverso del volante original. A continuación, se transcriben algunos puntos de interés para su análisis:

«2- En todos los envases o etiquetas de los productos encontrará la mención de la cantidad de puntos. También podrá encontrar puntos adicionales en el dorso de algunas etiquetas y tarjetas válidas por puntos adicionales (de aquí en más *tarjetas*) en el interior de algunos envases. (…)

3- Quienes obtengan envases y/o etiquetas de los productos, y/o tarjetas, con indicación de puntos que sumen exactamente —ni más, ni menos— las cantidades de puntos que se establecen en la cláusula 4 de estas bases se harán acreedores a los premios allí especificados.

4- Los participantes que acumulen exactamente 2500 (dos mil quinientos) puntos ganarán un departamento de tres (3) ambientes. Los que acumulen exactamente 1000 (un mil) puntos ganarán un departamento de dos (2) ambientes. Los que logren acumular exactamente 500 (quinientos) puntos habrán ganado un departamento de un (1) ambiente».


Figura 2. Volante utilizado para promocionar el concurso

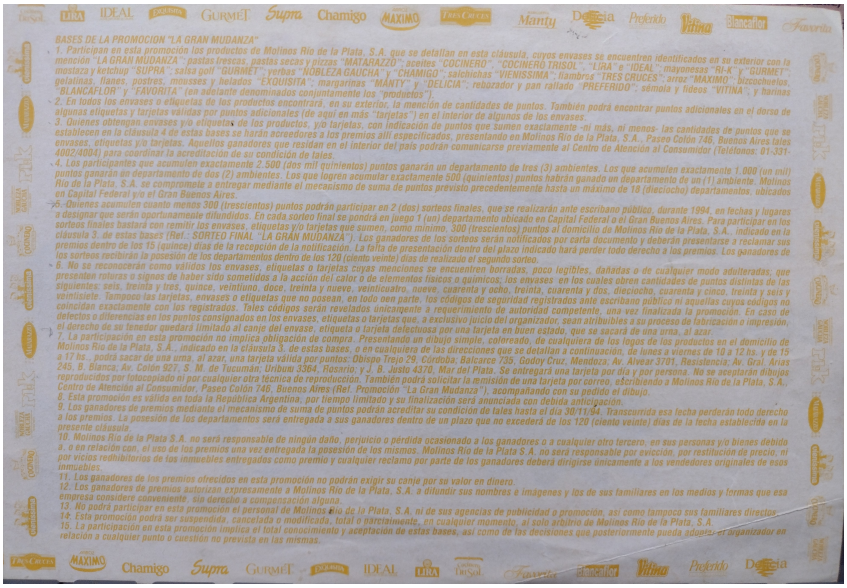



Figura 3. Reverso del volante (bases del concurso)

«6- No se reconocerán como válidos los envases, etiquetas o tarjetas cuyas menciones se encuentran borradas, poco legibles, dañadas o de cualquier modo adulteradas; que presenten roturas o signos de haber sido sometidas a la acción del calor o de elementos físicos o químicos; los envases en los cuales obren cantidades de puntos distintas de las siguientes: seis, treinta y tres, quince, veintiuno, doce, treinta y nueve, veinticuatro, nueve, cuarenta y ocho, treinta, cuarenta y dos, dieciocho, cuarenta y cinco, treinta y seis y veintisiete».

Juan y Rafael empezaron a reunir etiquetas, pero Ana, que estudia matemáticas, les dijo que «no se gasten», que ese concurso es un fraude. Elabora una justificación matemática que los conduzca a aceptar o rechazar el comentario de Ana.

**SITUACIÓN 2**

¿Tienen primer elemento o elemento mínimo los siguientes conjuntos?

$A = \{x/\ x \in N\ y\ x > 5\}$

$B = \{x/x \in Q\ y\ x > 5\}$

$C = \{x/x \in R\ y\ x > 5\}$

$D = \{x/x \in N\ y\ 2 < x < 10\}$

$E = \{x/x \in Q\ y\ 2 < x < 10\}$

$F = \{x/x \in R\ y\ 2 < x < 10\}$

Compara los conjuntos y las respuestas. Intenta plantear alguna conclusión.

**SITUACIÓN 3**

1. Responde:
   a) ¿Es -3 divisor de 15?
   b) ¿Es 7 divisor de 23?
   c) ¿Es 8 divisor de -30?
2. Justifica todas tus respuestas.
3. ¿Cómo definirías que $b$ es divisor de $a$, siendo $a$ y $b$ números enteros?
4. ¿Pueden tomar $a$ y $b$ cualquier valor entero? ¿Por qué?
5. Analiza las expresiones: *ser divisor de* y *ser múltiplo de*. ¿Se vinculan de algún modo? Explica.

**SITUACIÓN 4**

1. «Sea $a$ entero y $a \neq 0$ entonces $a|0$» ¿Es verdadera o falsa esta afirmación?
2. ¿Qué podemos decir de $a$ y $b$ si $a|b$ y $b|a$ para $a$ y $b$ enteros?
3. Analiza la veracidad de las siguientes afirmaciones:

   a) Si $m$ entero no nulo es divisor del entero $n$, es divisor de cualquier múltiplo de $n$.

   b) Si $m$ entero no nulo es divisor de $n$ (entero), $m$ es divisor de $n + 10$.

   c) Si $m$ entero no nulo es divisor de los enteros $p$ y $q$, entonces $m$ es divisor de $pr + qs$, para cualesquiera $r$ y $s$ enteros.

   d) Sean $m$ y $n$ enteros no nulos tales que $m|p$ y $n|p$ para $p$ entero, entonces $m + n|p$.

**SITUACIÓN 5**

Analiza si cada enunciado sobre el conjunto de números enteros es verdadero o falso. Si es verdadero, demuéstralo. Si es falso, modifica el antecedente o el consecuente (pero no los dos al mismo tiempo) para que resulte un enunciado verdadero. Demuestra el enunciado resultante y, cuando sea necesario, delimita su dominio de validez.

a) Si $a|b$ y $c|b$ entonces $a|c$.

b) Si $a|b$ entonces $a|b + t$, para $t$ entero cualesquiera.

c) Si $a|b$ y $a|c$, entonces $a|bx + cy$, para $x$ e $y$ enteros cualesquiera.

d) Si $n$ es par, entonces $8|(n^2-1)$.

**SITUACIÓN 6**

1. Plantea tres ejemplos de números primos.
2. Plantea tres ejemplos de números compuestos.
3. Plantea definiciones para número primo y número compuesto.

**SITUACIÓN 7**

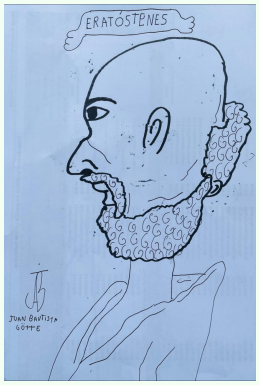
1. Te invitamos a ver la primera parte (los primeros 10 minutos) del primer programa «Alterados por Pi», disponible en https://www.youtube.com/watch?v=MjYrmDl_KtE.
2. Luego de verlo:

a) Selecciona alguna frase que te haya sorprendido y comenta por qué te sorprendió.

b) Reflexiona sobre la pregunta: ¿para qué se usan los números primos?

**Nota histórica: Eratóstenes de Cirene (250 a.C.)**

Fue un matemático que también se desempeñó como bibliotecario de la Universidad de Alejandría. Vivió entre 276 a. C. y 194 a. C. Un resultado muy importante de este matemático fue la determinación con bastante pertinencia del diámetro de la Tierra (Boyer, 1986).




En aritmética adquirió cierta «fama» la criba de Eratóstenes, que consiste en un procedimiento para determinar los números primos menores que un natural dado. Te proponemos que indagues en el modo en que funciona este método.

**SITUACIÓN 8**

Conjetura: ¿cuántos números primos existen? Intenta proporcionar argumentos a favor de tu conjetura.
En los *Elementos* de Euclides se incluye una proposición que aborda esta pregunta. Te pedimos que explores en libros de aritmética una posible respuesta para compartir en la próxima clase.

**SITUACIÓN 9**

Se tiene un edificio de cuatro pisos con las habitaciones numerados como en la tabla 1. ¿En qué piso localizas la habitación Nº 98? Justifica la respuesta.
En general, escribe mediante una expresión matemática los números que identifican las habitaciones en cada piso.

Tabla 1

| | | | | | | |
|---|---|---|---|---|---|---|
| P3 | 3 | 7 | 11 | 15 | 19 | ... |
| P2 | 2 | 6 | 10 | 14 | 18 | ... |
| P1 | 1 | 5 | 9 | 13 | 17 | ... |
| PB | 0 | 4 | 8 | 12 | 16 | ... |

**SITUACIÓN 10**

Observa la tabla 2 [1]:

Tabla 2

| FILA | COLUMNA 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| | ... | ... | ... | ... | ... | ... |
| -2 → | -12 | -11 | -10 | -9 | -8 | -7 |
| -1 → | -6 | -5 | -4 | -3 | -2 | -1 |
| 0 → | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 → | 6 | 7 | 8 | 9 | 10 | 11 |
| 2 → | 12 | 13 | 14 | 15 | 16 | 17 |
| 3 → | 18 | 19 | 20 | 21 | 22 | 23 |
| 4 → | 24 | 25 | 26 | 27 | 28 | 29 |
| 5 → | 30 | 31 | 32 | 33 | 34 | 35 |
| 6 → | 36 | 37 | 38 | 39 | 40 | 41 |
| | ... | ... | ... | ... | ... | ... |

a) Plantea dos números mayores que 1000 que se encuentren en la misma columna que el 130.

b) Escribe una expresión general para los números que se ubican en la columna 3.

c) Escribe una expresión general para los números que se ubican en la fila 145 y en la fila -28 de la tabla.

d) Escribe una expresión general para un número que se encuentra en la fila a y en la columna r de la tabla.

e) Se va hacer otra tabla con un criterio similar pero con 7 columnas. ¿En qué fila y columna estará el 126? Para esta segunda tabla, qué número se ubica en la fila 8 y columna 4?

f) Escribe una expresión general para indicar un número entero si se tiene una tabla de b columnas.

[1] Adaptado de Sadovsky (2005).

**SITUACIÓN 11**

En una bodega hay 3 toneles de vino cuyas capacidades son: 250 litros, 360 litros, y 540 litros. Su contenido se quiere envasar en cierto número de barriles iguales. Calcula las capacidades máximas de estos barriles para que en ellos se pueda envasar el vino contenido en cada uno de los toneles.

**SITUACIÓN 12**

Sean $a$ y $b$ enteros positivos no simultáneamente nulos. Supongamos (sin pérdida de generalidad) que $a > b$. ¿Qué relación existe entre $mcd(a, b)$ y $mcd(a - b, b)$? Justifica. Expresa en forma coloquial la propiedad resultante.

**SITUACIÓN 13**

Analiza las siguientes afirmaciones:

Si un número entero $a$ no nulo divide al producto $b.c$, para $b$ y $c$ enteros, entonces $a$ divide a $b$ o $a$ divide a $c$.

i. $a = 2; b = 10; c = 5$

ii. $a = 3; b = 3; c = 4$

iii. $a = 5; b = 2; c = 30$

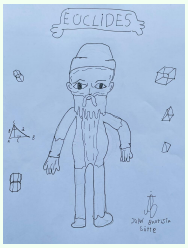
a) ¿Se puede afirmar que la proposición anterior es verdadera? ¿Por qué?

b) Expresa en símbolos la proposición.

c) Si es verdadera, demuéstrala, si es falsa, modifica el antecedente o el consecuente para que resulte verdadera.

**Nota histórica: Euclides de Alejandría**

La obra cumbre de este matemático que vivió alrededor de 300 a. C. es los *Elementos*. Según Boyer (1986) se trata de un texto introductorio (un libro de texto, diríamos) que cubría toda la aritmética, la geometría sintética (de puntos, rectas, planos, círculos y esferas) y el álgebra, este último no con el sentido simbólico moderno, sino con un «ropaje geométrico» (Boyer, 1986:145).




En lo que respecta a aritmética, veamos a continuación algunas definiciones prestando atención al lenguaje utilizado:
«Una unidad es aquello en virtud de lo cual cada una de las cosas que hay es llamada una» (Euclides, 1996:111); «Un número es una pluralidad compuesta de unidades» (112); «Un número es parte de un número, el menor del mayor, cuando mide al mayor» (113); «Y el mayor es múltiplo del menor cuando es medido por el menor» (113); «Un número primo es el medido por la sola unidad (116)»; «Números primos entre sí son los medidos por la sola unidad como medida común» (116) y «Número compuesto es el medido por algún número» (119).
1) ¿Qué significan los términos «parte» y «mide» en el vocabulario actual?
En las proposiciones 1 y 2 del libro VII incluye un resultado muy importante: el algoritmo de Euclides. Consiste en un método para calcular el $mcd(a, b)$ para a y b enteros positivos. Te invitamos a ver el siguiente video:
https://www.youtube.com/watch?v=9yOkoRU5mDs
Explica cómo funciona el método.
2) Expresa y demuestra en el vocabulario que utilizamos hoy la proposición 30 del libro VII de los *Elementos* (Euclides, 1996): «Si dos números, al multiplicarse entre sí, hacen algún (número) y algún número primo mide a su producto, también medirá a uno de los iniciales» (Euclides, 1996:152).

**SITUACIÓN 14**

«Moda discreta[2]» lanzó una promoción para las personas amantes de la moda en sus redes sociales. En un posteo de Instagram (figura 4) publicaron que con la compra de remeras y pantalones se puede ganar un viaje a París. Lucía quiere participar en la promoción, pero su hermana le dijo que no gaste dinero, que debe ser un fraude. Elabora una justificación matemática que le permita a Lucía decidir si se trata o no de un fraude.


Figura 4. Moda discreta

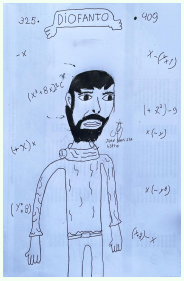
**SITUACIÓN 15**

Un coleccionista de obras de arte ha adquirido varias obras entre pinturas y dibujos. Las pinturas le han costado 649 euros cada una y los dibujos 132 euros. Cuando el coleccionista llega a la casa, no sabe si ha gastado 2716 euros o 2761 euros. ¿Cuánto ha gastado exactamente?

[2]Adaptado de Alassia *et al.* (2023).

## Nota histórica: Diofanto de Alejandría

No existe certeza respecto del siglo en que vivió Diofanto (Boyer, 1986). Se estima que alrededor de 250 d. C. Su obra más importante es *Arithmetica*, que incluye la resolución exacta de ecuaciones determinadas e indeterminadas. Según Boyer (1986), contiene 150 problemas resueltos en términos de ejemplos numéricos concretos y específicos. Encontramos en los libros de historia alguna disparidad sobre esta información, puesto que Kline (1999) sostiene que se trata de 189 problemas. Es interesante hacer notar que toda esta producción se realiza con una limitación importante en la notación: faltan símbolos especiales para las operaciones, relaciones y para la notación exponencial. En la figura 5 mostramos un ejemplo de su escritura, con la traducción correspondiente a los símbolos que usamos hoy en día.




$$SS2\ C3\ x5\ M\ S4\ u6$$
$$2x^4 + 3x^3 - 4x^2 + 5x - 6$$

S: cuadrado
C: cubo
x: incógnita
M: menos
u: unidad

Figura 5. La escritura de Diofanto y su interpretación actual (Boyer, 1986)

2) Es el creador de la rama del álgebra llamada «análisis diofántico», que se ocupa de las resoluciones de ecuaciones indeterminadas. Te proponemos conocer mediante un ejemplo un método utilizado por Diofanto para resolver problemas. El problema es el siguiente: calcular dos números tales que su suma sea 20 y la suma de sus cuadrados sea 208. Veamos la resolución de Diofanto:

**Nota histórica: Diofanto de Alejandría (continuación)**

Representa los números desconocidos por

$$10 + x$$
$$10 - x$$
$$(10 + x)^2 + (10 - x)^2 = 208$$
$$100 + 20x + x^2 + 100 - 20x + x^2 = 208$$
$$2x^2 = 8$$
$$x^2 = 4$$

Respuestas de Diofanto: 8 y 12.

Aplica ahora ese método para resolver el siguiente problema: **Calcular dos números tales que su suma es 10 y la suma de sus cubos es 370.**

A continuación, presentamos algunas *reglas* seguidas por Diofanto en el método usado en el ejemplo:

• «Siempre que dos números tengan que satisfacer dos condiciones, se deben elegir dichos números indeterminados de tal manera que una de las dos condiciones se verifique automáticamente» (Boyer, 1986:240–241).

• En lugar de plantear un sistema de dos ecuaciones, opera con las condiciones de modo que aparezca una única incógnita.

• Encuentra siempre una única solución.

• Le interesan soluciones racionales exactas.

Para finalizar estas notas, te presentamos un problema incluido en la Arithmetica (II–8): **Dividir un cuadrado dado en dos cuadrados.** Este problema es muy importante, porque Fermat enuncia su famosa conjetura cuando intenta generalizar este resultado. Lo que abre un nuevo capítulo para indagar en la historia: ¿cuál es la 'famosa' conjetura de Fermat? ¿Está demostrada?

**SITUACIÓN 16**[3]

Si 66 x 40 = 2640, ¿es posible decidir, sin hacer la división, si 2640 es divisible por 40, 60, 33, 3, 4, 9 y 12?

**SITUACIÓN 17**

¿Es $2^8$ divisor de 2024? Justifica la respuesta.

[3]Tomado de Sessa y Cambriglia (2011).

**SITUACIÓN 18**

Juan y Pedro son deportistas olímpicos y deben acudir en forma periódica a controles médicos rutinarios con el traumatólogo. Juan asiste cada 38 días y Pedro cada 20 días. Hoy coincidieron en la consulta del médico.

a) ¿Dentro de cuántos días volverán a coincidir?

b) ¿Cómo se puede caracterizar unívocamente (desde las relaciones aritméticas) al resultado obtenido en a) en función de los números dados en el enunciado?

**SITUACIÓN 19**

Según Gentile (2012), un curso de Aritmética debe seguir el siguiente esquema:


Figura 6. Esquema para un posible desarrollo de Aritmética (Gentile, 2012:84)

Analiza el esquema y compara con el desarrollo propuesto en el capítulo 3 para el estudio de la divisibilidad. Explicita las razones por las cuales el desarrollo es pertinente. ¿Es posible afirmar que para demostrar cada una de las propiedades se cuenta con los resultados previos necesarios?

# Capítulo 2
# Aportes para la enseñanza de divisibilidad

**SITUACIÓN 1**. *Comentarios*

Esta situación se elabora en torno a una promoción que tuvo lugar en nuestro país y que proporciona un contexto pertinente para la introducción del estudio de propiedades de la relación de divisor. En la formación de profesores/as, la utilizamos como punto de partida para iniciar el estudio de la divisibilidad, previo a la definición 3.1.

El pedido de justificación matemática puede pasar, según se considere oportuno, por la utilización de un resultado o propiedad matemática que permita tomar una decisión. Esto da lugar al enunciado de una conjetura y su posterior demostración. Un posible enunciado de la conjetura es: la suma de múltiplos de 3 da como resultado un múltiplo de 3. También se puede aprovechar la situación para avanzar en el grado de generalidad: ¿esto vale para cualquier número natural o entero? En Rougier y Scaglia (2012) se documenta el trabajo realizado en una clase de formación inicial de profesores/as de matemática en torno al contexto presentado. Resulta de interés el modo en que el intercambio entre estudiantes y docente favorece la ampliación del dominio de validez de la conjetura inicial. Las conjeturas que se formulan y prueban son las siguientes:

- La suma de dos múltiplos de 3 es un múltiplo de 3.
- La sumatoria de dos múltiplos de n da como resultado otro múltiplo de n, con n que pertenece a los enteros.
- La sumatoria de k múltiplos de n es igual a un múltiplo de n, para n entero y k natural.

La última constituye un resultado matemático que permite afirmar que no es posible ganar el concurso reuniendo puntos contenidos en los envases de los productos. El único modo de obtener algunas de las tres cantidades de puntos mencionadas requerirían el uso de números que no son múltiplos de 3.

El estudio de esta situación problemática puede aprovecharse también para proponer el siguiente interrogante: ¿qué ideas matemáticas hemos utilizado para abordar la situación? Entre las posibles respuestas surgirán probablemente los términos divisor, múltiplo, divisible, por ejemplo. Se

trata de conceptos matemáticos con los que el estudiantado puede estar familiarizado, razón por la cual resulta viable solicitar la producción de una definición. Esto da pie para abordar una primera reflexión en torno a las características de las definiciones, reconociendo que estas constituyen condiciones necesarias y suficientes. Pensamos que este hecho merece plantearse dado que es muy común que las definiciones se presenten como una implicación: «si un número *b* es divisor de un número *a*, entonces…». Como afirma Grimaldi (1998) una definición debe interpretarse correctamente como una bicondicional (es decir, una proposición compuesta de la forma si y solo si), aunque usualmente se presente como una implicación.

**SITUACIÓN 2**. *Comentarios*
La comparación entre subconjuntos de los conjuntos de números **N**, **Q** y **R** se propone con la finalidad de reflexionar en torno al Principio del Buen Orden (PBO). Por tanto, se sugiere que la situación se proponga antes de su abordaje. La conclusión que se solicita puede asumir algún enunciado compatible con el principio. Es posible que el estudiantado esté familiarizado con la propiedad de densidad del orden de **Q** y **R** (este último conjunto numérico, además, cumple con la propiedad de completitud). En relación con el PBO, en el desarrollo matemático que planteamos en el Capítulo 3 lo asumimos como un axioma, es decir, una afirmación que consideramos verdadera sin necesidad de demostración. Grimaldi (1998) utiliza el PBO en la demostración del principio de inducción matemática y afirma que es posible utilizar este último para demostrar el PBO. Este planteo puede utilizarse para reflexionar sobre el hecho de que la construcción de una teoría matemática completa supone hacer elecciones y que no hay un único modo de presentar la teoría en función de las elecciones realizadas.

**SITUACIÓN 3**. *Comentarios*
Esta situación puede utilizarse para producir la definición de divisor (Definición 3.1) y comparar esta noción con la de múltiplo. La definición surge a partir de la consideración de algunos casos (ejemplos y no ejemplos), por lo que asumimos un proceso inductivo en su construcción.

**SITUACIÓN 4**. *Comentarios*
Los enunciados de esta situación se proponen con la intención de que el estudiantado explore relaciones de la relación de divisor, algunas de las cuales se expresan en los teoremas 3.1 a 3.7. La sugerencia es que se resuelva la situación en forma previa a la lectura de dichos teoremas. Balacheff (2000) sostiene que uno de los obstáculos en el aprendizaje de la demostración radica en que la enseñanza «despoja a los estudiantes de la responsabilidad de la verdad» (Balacheff, 2000:5), por ejemplo, mediante consignas en las que se les pide que demuestren o muestren determinados resultados. El autor sostiene que en ese tipo de consignas, el enunciado se considera verdadero y lo que se tiene que descubrir es una demostración. La exploración que se propone en esta

situación tiene la finalidad de promover un trabajo matemático que invite al estudiantado a asumir la responsabilidad de contrastar cada conjetura.

**SITUACIÓN 5**. *Comentarios*

Esta situación persigue, como la anterior, la exploración de enunciados con el fin de determinar su veracidad. Aquí, además, la solicitud de reformulación de los enunciados falsos posiciona al estudiante en la tarea de reformular conjeturas y anticipar posibles relaciones. Compartimos a continuación dos reformulaciones del enunciado d). Este enunciado es falso, como se justifica mediante un contraejemplo. Por ejemplo, para n= 6 =2.3, se constata que 8 no es divisor de $6^2 - 1 = 35$, pues no existe entero k que cumpla que 35= 8.k. Las resoluciones que presentamos a continuación fueron realizadas por un estudiante de profesorado en el pizarrón.

*Primera reformulación del enunciado*

Si $n$ es impar, entonces $8|(n^2 - 1)$.

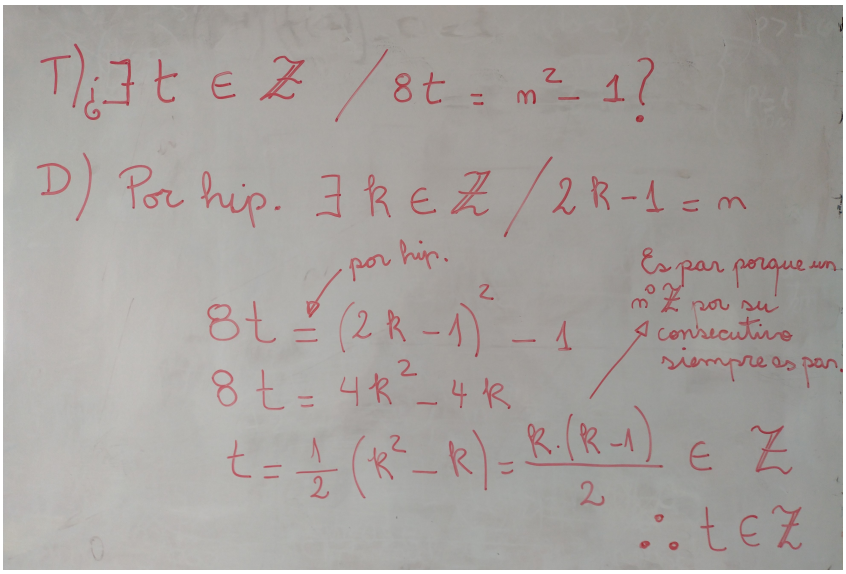



Figura 7. Demostración de la primera reformulación

*Segunda reformulación del enunciado*

Si $16|(n^2 - 1)$ entonces $8|(n^2 - 1)$.

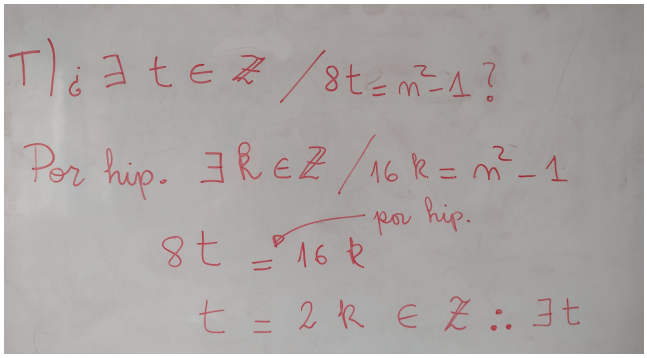


Figura 8. Demostración de la segunda reformulación

En las figuras 7 y 8, el estudiante expresa la tesis de cada reformulación (es decir, la afirmación $8|(n^2 - 1)$ mediante una afirmación equivalente, utilizando la definición de divisor.

**SITUACIÓN 6**. *Comentarios*

Esta situación tiene nuevamente la intención de que el estudiantado produzca definiciones. A continuación compartimos la fotografía (figura 9) de una carpeta que recoge las conclusiones que un grupo de estudiantes produjo de número primo.

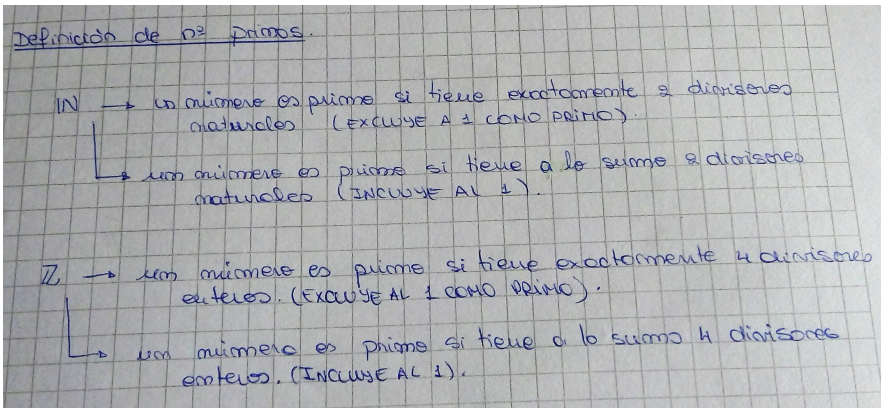


Figura 9. Distintas definiciones de número primo

La producción plantea cuatro definiciones diferentes, dos enunciadas en el conjunto de números naturales y dos en el conjunto de números enteros. En cada conjunto, el grupo de estudiantes enuncia una definición que incluye al número 1 como número primo y otra que no lo hace. La definición seleccionada en el Capítulo 3 (Definición 3.2) coincide con la primera definición planteada en la figura 9. Gentile (2012a) propone en su desarrollo matemático la tercera definición.

Este análisis realizado con el estudiantado permita reflexionar sobre ciertas características de las definiciones. Como sostiene de Villiers (2009) una definición es un acuerdo mutuo entre partes interesadas

acerca de lo que un objeto específico realmente es. Una idea errónea que suele sostenerse en relación con las definiciones es que existe solo una definición (correcta) para cada objeto definido en matemática. Por el contrario, pueden existir diferentes definiciones (correctas). Asimismo, no existen definiciones independientemente de la experiencia humana en algún mundo *ideal* platónico, de modo que nosotros podamos *descubrirlas*. Por el contrario, ellas no son descubrimientos, sino invenciones humanas con el principal propósito de una comunicación matemática precisa.
En la elaboración de la teoría (como realizamos en el Capítulo 3), una vez seleccionada una definición de número primo (en nuestro caso la que los estudiantes presentaron en primer lugar) es preciso sostener la definición elegida, tanto en la demostración de teoremas como en la producción de definiciones de nuevos conceptos, con el fin de mantener la coherencia.

**SITUACIÓN 7**. *Comentarios*
En el video se presentan imágenes potentes para caracterizar a los números primos y se aborda la cuestión de su utilización en el comercio electrónico mundial. Consideramos interesante que en la formación docente se apele al uso de videos educativos.

**SITUACIÓN 8**. *Comentarios*
La prueba de la existencia de infinitos números primos ya figura en los *Elementos* de Euclides. Consideramos pertinente que el estudiantado conozca la prueba que dio Euclides respecto a la infinitud de números primos.

**SITUACIÓN 9**. *Comentarios*
Esta situación se propone con la intención de abordar el algoritmo de la división, antes de trabajar el Teorema 3.9. El contexto en el que se sitúa tiene ciertas limitaciones. En primer lugar, se trata de un contexto no real, porque no existen edificios con un número infinito de cuartos. Los puntos suspensivos tal como se presentan en la tabla, en matemática se interpretan como que cada sucesión continúa indefinidamente.
En segundo lugar, promueve un tratamiento en el conjunto de los números naturales, en tanto que en nuestro desarrollo matemático (Teorema 3.9) el teorema prueba la existencia y unicidad de los números $q$ (entero) y $r$ (entero, $0 \leq r < b$) para cada $a$ entero y $b$ entero positivo que satisfacen la igualdad $a = bq + r$.

**SITUACIÓN 10**. *Comentarios*
Esta situación ha sido reformulada de Sadovsky (2005) y permite introducir el algoritmo de la división (previo al abordaje del Teorema 3.9) tomando como dominio para el valor de a el conjunto de los números enteros. En este caso, como sostiene Sadovsky (2005) la renuncia o el abandono del contexto permite promover una práctica más general respecto de lo que ocurre con la situación 9. Podría plantearse de modo

previo al teorema (tal como sugerimos en dicha situación).
La consigna incluye varios interrogantes con la intención de promover una generalización. Rodriguez (2017) sostiene que preguntas muy guiadas le restan potencial matemático a una consigna. Por esa razón, la utilización de esos interrogantes u otros quedarán a criterio del docente, que dependiendo de su propósito de enseñanza y de las características del estudiantado, propondrá una consigna más adecuada, que permita potenciar el trabajo matemático.

**SITUACIÓN 11**. *Comentarios*
Este enunciado constituye una situación típica para el abordaje de la noción de máximo común divisor. Se propone, por tanto, para trabajar antes de abordar la Definición 3.3. Una vez que el estudiantado alcanza el resultado numérico que da respuesta a la situación, se puede plantear un interrogante del tipo: ¿qué condiciones cumple este valor, en relación con los datos del enunciado del problema? La intención es que se reconozca que se trata de un divisor comunes, y que es el mayor posible de todos los divisores común. Estas u otras expresiones similares dan pie para institucionalizar la definición. Se puede discutir en la clase que la segunda expresión resulta equivalente a la segunda condición planteada en la Definición 3.3, lo cual permite retomar las características de las definiciones matemáticas.

**SITUACIÓN 12**. *Comentarios*
Con esta situación se propone abordar algunos resultados sencillos vinculados con el máximo común divisor. El que se presenta en el Teorema 3.11 constituye una estrategia de cálculo del máximo común divisor entre dos números dados.

**SITUACIÓN 13**. *Comentarios*
Esta situación se implementó inicialmente con estudiantes de educación secundaria (Fedonczuk *et al.*, 2011) con la finalidad de abordar las reglas del debate matemático (Arsac *et al.*, 1992). La situación permite enfatizar que en matemática, los ejemplos que verifican un enunciado no son suficientes para probar que el mismo es verdadero. Si bien en futuras/os profesoras/es esto estará bastante claro, es interesante discutir el hecho de que estas reglas no tienen por qué ser conocidas por estudiantes de educación secundaria, por lo que tienen que ser objeto de análisis y discusión.
En Scaglia y Kiener (2015) se estudian los intercambios producidos en una clase de futuras profesoras en las que se pone en juego esta situación. En particular, el análisis muestra la complejidad de la gestión de la clase cuando se espera promover la actividad autónoma de los estudiantes. En efecto, se identifican intervenciones en las que la profesora «valida las respuestas de los estudiantes en lugar de promover una actividad argumentativa autónoma» (Scaglia y Kiener, 2015:209).
En la formación de profesores resulta de interés reflexionar sobre el modo en que un docente interviene en los momentos en que se debe

decidir sobre la adecuación de una determinada respuesta. Margolinas (1992:128) describe dos modos de atravesar esta situación: en el primero (que denomina fase de evaluación), la responsabilidad del profesor se ejerce bajo la forma de un trabajo público para el alumno, en relación con el problema y el saber. A partir de la relación privilegiada que mantiene el docente con el saber, proporciona un juicio de validez sin recurrir a la respuesta del estudiante. En el segundo, que denomina fase de validación, el estudiante decide sobre la validez de su respuesta. En este caso, el trabajo del docente no está ausente (porque sigue manteniendo la responsabilidad), pero es privado, porque no lo explicita al estudiante. Por último,en vinculación con el desarrollo matemático del Capítulo 3, esta situación podría proponerse previamente al Teorema 3.13. Este teorema, así como el 3.16, constituyen posibles enunciados que podrían utilizarse para reemplazar la proposición falsa que se enuncia en la consigna.

**SITUACIÓN 14** .*Comentarios*

Esta situación (tomada de Alassia *et al.,* 2023) se propone para iniciar el estudio de las ecuaciones diofánticas. Tal como se ha propuesto en otras situaciones, en lugar de comenzar con la definición se plantea esta situación problemática que el estudiantado deberá explorar y resolver.

En primer lugar, se espera que se plantee la ecuación diofántica que modeliza la situación. Luego, se espera que el estudiantado reconozca que esta ecuación no tiene soluciones naturales, por lo cual la promoción es un fraude.

Resulta especialmente útil la situación para conjeturar cuándo una ecuación diofántica tiene solución (Teorema 3.15). No obstante, con esa intención específica se propone la siguiente situación.

**SITUACIÓN 15**. *Comentarios*

La resolución de la situación exige, en primer lugar, el análisis de los datos para plantear el modelo matemático (ecuación algebraica lineal en dos variables con coeficientes enteros) que los relaciona. Esto conduce a la elaboración de ecuaciones que difieren en sus términos independientes. El análisis de esas ecuaciones permite identificar que, en un caso, el término independiente no es divisible por el máximo común divisor de los coeficientes de las variables, en tanto que en el otro lo es.

En Racca y Scaglia (2018) se describen las producciones e intercambios generados en un grupo de futuras/os profesores. En primer lugar, la situación es abordada en forma individual. Posteriormente se realiza una puesta en común durante la cual se comparten las resoluciones de algunas/os estudiantes. El análisis de los intercambios se realiza especialmente en torno a las intervenciones de la docente, identificando algunas que resultan pertinentes para promover la discusión y el trabajo matemático. Las intervenciones que permiten mantener la incertidumbre y propician la validación por parte de los estudiantes son las siguientes: no responde directamente las preguntas, sino que las devuelve al grupo de alumnos; no convalida de entrada las respuestas correctas; y

finalmente, pide mayores explicaciones. Como aspecto negativo de los intercambios se menciona el hecho de que en las discusiones de la clase completa solo participa un tercio del total de estudiantes, por lo que se concluye la importancia de la intervención docente para distribuir la palabra incentivando la participación a todo el estudiantado.

**SITUACIONES 16 y 17**. *Comentarios*

Las situaciones 16 y 17 se proponen con la finalidad de explorar la factorización única de un número en factores primos. La sugerencia es el planteo de estas situaciones antes del abordaje del teorema fundamental de la aritmética (Teorema 3.17).

La primera ha sido tomada de Cambriglia y Sessa (2011). Las autoras describen las interacciones que se producen en una clase de primer año de educación secundaria, que da lugar al reconocimiento de la «necesidad de encontrar un procedimiento general para argumentar respecto de la divisibilidad» (Cambriglia y Sessa, 2011:46) que resulte independiente de la descomposición inicial que se presenta para el número 2640. Asimismo, se pone de manifiesto en la gestión de parte de la docente la consideración de planteos, imprecisos e incompletos del estudiantado «como punto de partida para la construcción de un medio propicio que permita elaborar colectivamente criterios generales sobre la divisibilidad» (Cambriglia y Sessa, 2011:47).

**SITUACIÓN 18** .*Comentarios*

Esta situación proporciona un contexto prototípico para el abordaje de la noción de mínimo común múltiplo, por lo que se sugiere su utilización en forma previa a la Definición 3.4. En la segunda parte se espera que el estudiantado logre enunciar las condiciones necesarias y suficientes que constituyen esta definición.

**SITUACIÓN 19**. *Comentarios*

Esta última situación se propone con la finalidad de que las/os futuras/os profesoras/es reconozcan en la secuencia de teoremas sugeridos por el autor, el modo en que la estructuración de una teoría matemática requiere de la concatenación pertinente de resultados. La lógica de un sistema axiomático deductivo requiere que cada afirmación esté basada en axiomas, definiciones o propiedades previas.

# Capítulo 3
# Divisibilidad en los enteros

## 3.1. Conceptos básicos de divisibilidad

**Principio del Buen Orden**
Cualquier conjunto no vacío de $N$ contiene un elemento mínimo.

**Observación**
Consideramos a $N = \{1, 2, 3, \dots\}$, el conjunto de números naturales.
Consideramos a $Z = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, el conjunto de números enteros.

**Definición 3.1.** *Definición de divisor*
*Sean $a$ y $b \in Z$ siendo $b \neq 0$. Decimos que $b \mid a$, si y solo si existe un entero $n$ tal que $a = b.n$.*

Ejemplos:

- (-5) | 35 pues existe el entero (-7) tal que 35=(-5).(-7)
- 6 no es divisor de (-20) pues no existe $n$ entero tal que (-20)= 6.$n$

Se establece de este modo una relación en el conjunto de los números enteros tal que dos de ellos están relacionados si satisfacen la Definición 3.1.

**Teorema 3.1.** *$1 \mid a$, para todo entero $a$*

Se deja la demostración a cargo del lector.

**Teorema 3.2.** *Sea $a$ entero no nulo, entonces $a \mid 0$*

**Demostración**:
Puesto que existe el entero $n = 0$ tal que $0 = a.n = a.0$ entonces por la definición de divisor $a \mid 0$. •

**Teorema 3.3.** *Si $a$ y $b$ son enteros no nulos tales que $a \mid b$ y $b \mid a$, entonces $a = \pm b$*

**Demostración**:
Si $a \mid b$, existe $n$ entero tal que $b = n.a$ (*).
Si $b \mid a$, existe $m$ entero tal que $a = m.b$.

Así, $b = n.a = n.m.b \Rightarrow b - n.m.b = 0 \Rightarrow b(1 - n.m) = 0 \Rightarrow b = 0$ ó $1 - n.m = 0$[1]
Como $b \neq 0$, debe ser $1 - n.m = 0$. Por lo tanto $1 = n.m$.
Esto último es verdadero si y solo si $m = n = 1$ ó $m = n = -1$.
Si $m = n = 1$ en (*) $b = a$, de lo contrario $b = -a$. •

**Teorema 3.4.** *Sean a y b enteros no nulos y c entero. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$*

Se deja la demostración a cargo del lector.

**Teorema 3.5.** *Sea a entero no nulo y b entero. Si $a \mid b$ y t es un entero cualquiera, entonces $a \mid b.t$*

Se deja la demostración a cargo del lector.

**Teorema 3.6.** *Sean p, q y t enteros tales que $p = q + t$. Si b entero no nulo es divisor de dos de ellos, entonces es divisor del tercero*

**Demostración**:
Supongamos que $b \mid p$ y $b \mid q$. Existen $n$ y $m$ enteros tales que $p = b.n$ y $q = b.m$.
Entonces $b.n = b.m + t$ y $t = b.(n - m)$. Como $n - m$ es un entero, entonces por la definición de divisor afirmamos que $b \mid t$. •
Se dejan al lector las pruebas de los otros casos.

**Teorema 3.7.** *Sean b entero no nulo y a y c enteros. Si $b \mid a$ y $b \mid c$, entonces $b \mid ax + cy$, para dos enteros cualesquiera x e y*

Se deja la demostración a cargo del lector.

Esta última propiedad puede generalizarse (usando el principio de inducción matemática). Sea $b$ no nulo divisor de los $n$ enteros $a_1, a_2, \ldots, a_n$.
Entonces $b \mid a_1.x_1 + a_2.x_2 + \ldots + a_n.x_n$
para $n$ enteros cualesquiera $x_1, x_2, \ldots, x_n$.

## 3.2. Números primos y números compuestos

**Definición 3.2.** *Definición de número primo y número compuesto.*
*Un entero positivo mayor que 1 es primo si posee exactamente dos divisores positivos: 1 y el mismo número. Ejemplos de números primos:* 13, 41, 91.
*Un entero positivo es compuesto si posee más de dos divisores positivos. Ejemplos de números compuestos: 9 (posee tres divisores positivos:* 1, 3, 9*); 20 (posee 6 divisores positivos:* 1, 2, 4, 5, 10, 20*).*

**Teorema 3.8.** *Para todo número compuesto a, existe p primo tal que $p \mid a$*

[1] El conjunto de números enteros con la suma y el producto usuales es un dominio de integridad.

**Demostración**:
Supongamos por reducción al absurdo que existen enteros compuestos que no tienen divisores primos.
Sea $C = \{x \text{ compuesto} : x \text{ no posee divisor primo}\}$.
Como $C$ es un subconjunto de $N$ que suponemos no vacío, posee primer elemento por el principio del buen orden. Sea $m$ este elemento mínimo.
Como $m$ es compuesto entonces por definición tiene más de dos divisores positivos. Sea $k \neq 1$ y $k \neq m$ divisor de $m$.
Si $k \mid m$ y $k$ y $m$ son positivos, $k < m$.
Así que $k$ no puede pertenecer a $C$, pues es menor que el elemento mínimo $m$ de $C$.
Si $k$ no pertenece a $C$, entonces es primo o es compuesto y tiene (al menos) un divisor primo.
Si $k$ es primo, entonces existe un número primo divisor de $m$ y en consecuencia $m \notin C$ (absurdo).
Si $k$ tiene un divisor primo $p$, entonces $p \mid k$, $k \mid m$ y por Teorema 3.7, $p \mid m$ (absurdo).
El absurdo proviene de suponer que $C$ no es vacío, por lo tanto, $C$ es vacío y se cumple que todo número compuesto es divisible por un número primo. •

## 3.3. Algoritmo de la división

**Teorema 3.9.** *Algoritmo de la división. Sean a y b números enteros siendo* $b > 0$. *Entonces existen dos enteros q (cociente) y r (resto) únicos tales que* $a = b.q + r$, *siendo* $0 \leq r < b$

Antes de demostrar este resultado, veamos algunos ejemplos.

- Para 85 y 8, existen $q = 10$ y $r = 5$, tales que 85= 8.10+5, con $0 \leq 5 < 8$.
- Para - 97 y 4, existen $q = -25$ y $r = 3$, tales que $-97 = 4.(-25) + 3$, siendo $0 \leq 3 < 4$.
- Para -72 y 9, existen $q = -8$ y $r = 0$, tales que $-72 = 9.(-8) + 0$, con $0 \leq 0 < 9$.

**Demostración**:
**Caso 1:** $a > 0$.
La secuencia $0, 1b, 2b, 3b, ..., mb, ...(m \in Z^+)$ está formada por múltiplos positivos de $b$.
Sea $T = \{m \in N / mb > a\}$. Como N está bien ordenado y T es un subconjunto no vacío de N ($a$+1 es un elemento de T, por ejemplo), T posee primer elemento, al que llamamos $q + 1$.
El entero anterior a este primer elemento, es decir $q$, verifica que $qb \leq a$.
Así tenemos que $qb \leq a < (q + 1)b$.
$(q + 1)b - qb = qb + b - qb = b$ Si la diferencia entre $(q + 1)b$ y $qb$ es $b$, entonces $a - qb < b$.

A este número $a - qb$ menor que $b$, lo denominamos $r$.
Así cuando $a > 0$, existen $q$ y $r$ que verifican $a = qb + r$, con $0 \leq r < b$.

**Caso 2: a = 0**.
Si $a = 0$, para $b$ entero positivo existe $q = 0$ y $r = 0$ que verifican $a = qb + r$, pues $0 = b.0 + 0$.

**Caso 3:** $a < 0$.
i) Si $a$ es múltiplo de $b$, por definición existe $n$ entero tal que $a = b.n$.
Así existen $q = n$ y $r = 0$ enteros que satisfacen las condiciones pedidas. (En particular, $n < 0$).
ii) Si $a$ no es múltiplo de $b$, $-a$ tampoco es múltiplo de $b$. Por el caso 1, para $-a > 0$ existen $q$ y $r$ tales que: $-a = qb + r$, con $0 < r < b$.
Multiplicando por -1 la igualdad anterior resulta: $a = -qb - r$.
Sumamos y restamos $b$ al segundo miembro:

$$a = -qb - r + b - b = (-q - 1)b + (b - r).$$

Como $0 < r < b$, se verifica que $0 < b - r < b$.
Así, para $a$ negativo y no divisible por $b$, existen $-b - 1$ y $b - r$ que satisfacen las condiciones pedidas.

Falta probar ahora que los números $q$ y $r$ hallados son únicos.
Supongamos que existen números $q_1$, $q_2$, $r_1$ y $r_2$ que satisfacen:
$a = q_1.b + r_1$, con $0 \leq r_1 < b$
$a = q_2.b + r_2$, con $0 \leq r_2 < b$
Restamos las igualdades anteriores y obtenemos:

$$0 = b.(q_1 - q_2) + r_1 - r_2$$

$$b.|q_1 - q_2| = |r_2 - r_1|$$

con $|r_2 - r_1| < b$.
Como $|q_1 - q_2| > 0$ y es un entero, entonces $b.|q_1 - q_2| < b$ resulta una contradicción cuando $q_1 \neq q_2$. Luego estos números son iguales y lo son también los restos $r_1$ y $r_2$. •

## 3.4. Máximo común divisor y algoritmo de Euclides

**Definición 3.3.** *Máximo Común Divisor*
*Sean a y b dos enteros no simultáneamente nulos. El máximo común divisor de a y b es el entero positivo c que verifica las siguientes condiciones:*
*a)* $c \mid a$ *y* $c \mid b$.
*b) para cualquier divisor d de a y b, se verifica que* $d \mid c$.
*El máximo común divisor de a y b se simboliza mcd(a,b).*

Ejemplos:

1. $mcd(72, 90) = 18$. Se verifica la condición a) pues $18 \mid 72$ y $18 \mid 90$. Otros divisores comunes de estos enteros son 1, 2, 3, 6 y 9. Todos ellos son divisores de 18 (condición b).

2. $mcd(96, 144) = 48$. Se verifica la condición a) pues $48 \mid 96$ y $48 \mid 144$. También se verifica la condición b) (se deja al lector verificarlo).

3. $mcd(8, 15) = 1$. En este último caso, cuando el máximo común divisor entre dos números es 1, los números se denominan *coprimos*.

**Teorema 3.10.** *Para dos enteros positivos a y b cualesquiera, existe un único entero positivo c que es el máximo común divisor de a y b*

**Demostración**:
Sean $a$ y $b$ enteros positivos. Definimos el conjunto

$$S = \{as + bt / \ s, \ t \text{ son enteros y } as + bt > 0\}.$$

Dado que los elementos de S, por definición son números naturales, por el principio del buen orden S tiene un primer elemento, al que denominamos $c$.
Vamos a probar que $c = mcd(a, b)$. Como $c \in S$, existen $x$ e $y$ tales que $c = ax + by$.

a) Probamos que $c \mid a$. (Demostración por reducción al absurdo).
Si $c$ no es divisor de $a$, por el algoritmo de la división existen $q$ (cociente) y $r$ (resto) que verifican: $a = c.q + r$ con $0 < r < c$.
Reemplazamos $c$ por su valor en la igualdad anterior:
$a = (ax + by).q + r = axq + byq + r$ entonces $a(1 - xq) - byq = r$
Así, $r = a(1 - xq) + b(-yq) = am + bn$. Como $r > 0$, resulta que $r \in S$.
Pero $r < c$, entonces $c$ no es el elemento mínimo de S, como habíamos supuesto. El absurdo proviene de suponer que $c$ no es divisor de $a$, por lo tanto, $c \mid a$.
De modo similar se prueba que $c \mid b$.

b) Probaremos ahora que si $d$ es un número entero positivo tal que $d \mid a$ y $d \mid b$, entonces $d \mid c$. Tenemos que $c = ax + by$ para algunos $x$ e $y$ enteros. Si $d \mid a$ y $d \mid b$, por Teorema 3.6, $d \mid c$.

Falta probar la unicidad del $mcd(a, b)$.
Supongamos que existen dos enteros positivos $c_1$ y $c_2$ que satisfacen la definición de $mcd(a, b)$. Como $c_1 = mcd(a, b)$ y $c_2 \mid a$ y $c_2 \mid b$, por la segunda condición de la definición de máximo común divisor, $c_2 \mid c_1$.
De modo similar: $c_2 = mcd(a, b)$ y $c_1 \mid a$ y $c_1 \mid b$, $c_1 \mid c_2$.
Por el Teorema 3.3 se tiene que $c_1 = \pm c_2$. Dado que son positivos, resulta la igualdad. •

La demostración anterior resulta especialmente interesante porque presenta al máximo común divisor entre dos números a y b como el menor entero positivo que puede escribirse como combinación lineal de a y b. Es decir, si c= $mcd(a, b)$, entonces existen x e y enteros tales que $c = ax+by$, y la anterior es la menor combinación lineal entera positiva de a y b. Como resultado de esta afirmación, resulta que a y b son coprimos si y solo si existen x e y enteros tales que $ax + by = 1$. (Este resultado es muy útil).

**Teorema 3.11.** *Para a , b enteros positivos, tales que $a > b$ se verifica que $mcd(a, b) = mcd(a - b, b)$*

**Demostración**:
Sea $p = mcd(a, b)$ y sea $q = mcd(a - b, b)$. Se probará que $p \mid q$ y $q \mid p$.
a) $p \mid q$.
Si $p = mcd(a, b)$, por definición $p \mid a$ y $p \mid b$. Entonces existen $m$ y $n$ enteros tales que $a = pm$ y $b = pn$.
Como $q = mcd(a - b, b)$ existen $r$ y $s$ enteros tales que $q = (a - b)r + bs = ar - br + bs = ar + b(s - r)$.
Reemplazando $a$ y $b$ por su valor, resulta:
$q = pmr + pn(s - r) = p(mr + n(s - r)) = p.t$, donde $t = mr + n(s - r)$ es un entero y por definición de divisor $p \mid q$.

b) $q \mid p$.
Como $q = mcd(a - b, b)$, por definición $q \mid a - b$ y $q \mid b$. Entonces existen $v$ y $w$ enteros tales que $a - b = qv$ y $b = qw$.
Así $a - b = a - qw = qv$ Entonces $a = qw + qv = q(w + v)$ donde $w + v$ es un entero y por definición de divisor $q \mid a$.
Así, $q \mid a$ y $q \mid b$, y $p = mcd(a, b)$. Por la segunda condición de la definición de máximo común divisor $q \mid p$.

De a) y b), por el Teorema 3.3 y dado que el mcd es por definición un número positivo, resulta que $mcd(a, b) = mcd(a - b, b)$. •

**Un método para calcular el** $mcd(a, b)$ **en caso que** $a, b \in Z^+$
Si queremos calcular el $mcd(320, 540)$ utilizamos de modo sucesivo la propiedad anterior: $mcd(320, 540) = mcd(320, 540 - 320) = mcd(320, 220) = mcd(100, 220) = mcd(100, 120) = mcd(100, 20) = mcd(80, 20) = mcd(60, 20) = mcd(40, 20) = mcd(20, 20) = 20$ (pues satisface las condiciones de la definición).

**Teorema 3.12.** *Sea $mcd(a, b) = c$, entonces $mcd\left(\frac{a}{c}, \frac{b}{c}\right)=1$*

**Demostración**:
Como $mcd(a, b) = c$, existen r y s enteros tales que $ar + bs = c$.
Además como $c \mid a$ y $c \mid b$ existen m y n enteros tales que $a = cm$ y $b = cn$.
Por lo tanto, $cmr + cns = c$. Dividiendo por c, que es un entero positivo, resulta que $mr + ns = 1$. De donde se prueba que $mcd(m, n)=mcd\left(\frac{a}{c}, \frac{b}{c}\right)=1$.•

**Teorema 3.13.** *Sean a, b y c enteros, $a \neq 0$ y $mcd(a, b) = 1$. Si $a \mid bc$, entonces $a \mid c$*

**Demostración**:
Como $a \mid bc$, existe m entero tal que $bc = ma$.
Si $mcd(a, b) = 1$, existen enteros r y s tales que $ar + bs = 1$.
Multiplicando por c la igualdad anterior resulta: $arc + bsc = c$.
Reemplazando bc por ma, resulta: $c = arc + sma = a(rc + sm)$ de donde $a|c$ pues $rc + sm$ es un entero. •

**Teorema 3.14.** *Algoritmo de Euclides. Sean a y b enteros positivos. Por el algoritmo de la división, existen dos enteros $q_1$ y $r_1$ tales que:*

$$a = bq_1 + r_1, \text{ siendo } 0 < r_1 < b \qquad (1)$$

*Aplicando de modo sucesivo el algoritmo de la división tenemos:*

$$b = r_1q_2 + r_2, \text{ siendo } 0 < r_2 < r_1 \qquad (2)$$
$$r_1 = r_2q_3 + r_3, \text{ siendo } 0 < r_3 < r_2 \qquad (3)$$
$$r_2 = r_3q_4 + r_4, \text{ siendo } 0 < r_4 < r_3 \qquad (4)$$
$$\vdots$$
$$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, \text{ siendo } 0 < r_{k-1} < r_{k-2} \qquad (k\text{-}1)$$
$$r_{k-2} = r_{k-1}q_k + r_k, \text{ siendo } 0 < r_k < r_{k-1} \qquad (k)$$
$$r_{k-1} = r_kq_{k+1} \qquad (k\text{+}1)$$

Los restos de estas divisiones forman una sucesión decreciente de enteros no negativos: $d > r_1 > r_2 > \ldots$ y este procedimiento lo podemos continuar mientras se obtengan restos no nulos, ya que la división entera por un número positivo es siempre posible. Al cabo de un cierto número de divisiones llegaremos a la relación $r_{k-1} = r_kq_{k-1}$.
**El algoritmo de Euclides afirma que el último resto no nulo, $r_k$, es el máximo común divisor de a y b.**

**Demostración**:
Condición a) Debemos probar que el $r_k \mid a$ y $r_k \mid b$.
Por (k+1), $r_k \mid r_{k+1} \rightarrow r_k \mid r_{k-1}q_{k-1}$ por el Teorema 3.5.
Además, $r_k \mid r_k$. Por el Teorema 3.6 en (k) tenemos que $r_k \mid r_{k-2}$. Aplicando sucesivamente los Teoremas 3.5 y 3.6, vamos subiendo por las igualdades (k-1), ..., (4), (3).
De resultados anteriores, $r_k \mid r_3$. En (4), tendremos que $r_k \mid r_2$. Aplicamos 3.5 para afirmar que $r_k \mid r_2q_3$. Luego aplicamos 3.6 en (3) para afirmar que $r_k \mid r_1$. Por 3.5, $r_k \mid r_1q_2$. Como $r_k \mid r_2$ afirmamos por (2) que $r_k \mid b$.
Si $r_k \mid b$, entonces $r_k \mid bq_1$. Además, $r_k \mid r_1$, por lo que afirmamos por (1) que $r_k \mid a$. Así se prueba la primera condición de la definición.

Condición b) Debemos probar que si $d \mid a$ y $d \mid b$, entonces $d \mid r_k$.
Aplicando en (1) los Teoremas 3.6 y 3.7, como $d \mid a$ y $d \mid b$, entonces $d \mid r_1$.
Si $d \mid b$ y $d \mid r_1$ se cumple en (2) que $d \mid r_2$.
Si $d \mid r_1$ y $d \mid r_2$ se cumple en (3) que $d \mid r_3$. Así sucesivamente, si llega a afirmar que $d \mid r_k$. •

**Observación**.
Cuando en la igualdad (1) $r_1 = 0$, entonces $b \mid a$ y $mcd(a, b) = b$.

Tenemos así un método para calcular el $mcd(a, b)$, que (se puede comprobar) es una aplicación resumida del método probado anteriormente. Veamos un ejemplo de su aplicación.
Hallar el $mcd(342, 540)$.
Usamos el algoritmo de Euclides como sigue:
$540 = 342 \cdot 1 + 198$
$342 = 198 \cdot 1 + 144$
$198 = 144 \cdot 1 + 54$
$144 = 54 \cdot 2 + 36$
$54 = 36 \cdot 1 + 18$
$36 = 18 \cdot 2$
El último resto no nulo es 18, por lo tanto $mcd(342, 540) = 18$.

## 3.5. Mínimo común múltiplo

**Definición 3.4.** *Mínimo Común Múltiplo*
*El mínimo común múltiplo de dos enteros positivos a y b es otro entero positivo d que verifica que es el más pequeño de los enteros positivos tales que $a \mid d$ y $b \mid d$.*
*Lo simbolizamos d=mcm(a,b).*

**Ejemplo**
Hallar el $mcm(45, 30)$.
Múltiplos positivos de 45: 45, 90, 135, 180, ...
Múltiplos positivos de 30: 30, 60, 90, 120, ...
El entero positivo más pequeño $d$ que satisface que $45|d$ y $30|d$ es 90. Por lo tanto, el $mcd(45, 30) = 90$.
Luego del estudio del *Teorema Fundamental de la Aritmética* (sección 3.7), presentaremos una estrategia sintética para calcularlo.

**Teorema 3.15.** *Sean a, b y c enteros positivos, con $c = mcm(a, b)$. Si d es un múltiplo común de a y b, entonces $c \mid d$*

**Demostración**:
Supongamos que $c$ no divide a $d$.
Por el algoritmo de la división, existen $q$ y $r$ enteros tales que $d = qc + r$, donde $0 < r < c$.
Como $c$ es el $mcm(a, b)$, existe $m$ entero positivo tal que $c = ma$.
Como $d$ es múltiplo de $a$, existe algún $n$ entero positivo tal que $d = na$.
Reemplazando $c$ y $d$ en $d = qc + r$ nos queda:

$$na = qma + r$$

Entonces $(n - qm)a = r$, de donde $r$ es múltiplo de $a$.
De igual modo se prueba que $r$ es múltiplo de $b$.
Tenemos por lo tanto un número entero positivo $r$ múltiplo de $a$ y de $b$, menor que $c$, lo que es absurdo porque $c$ es el mínimo común múltiplo.
El absurdo proviene de suponer que $c$ no divide a $d$. •

**Teorema 3.16.** *$a.b = mcd(a,b).mcm(a,b)$ para cualesquiera a y b enteros positivos*

**Demostración**:
Sea $c = mcd(a,b)$ y $d = mcm(a,b)$. La igualdad anterior resulta $ab = dc$ que es equivalente a $\frac{ab}{c} = d$.
Probaremos que $d \mid \frac{ab}{c}$ y que $\frac{ab}{c} \mid d$. Como se trata de números enteros positivos resultará la igualdad buscada. Observemos que $c \mid a$ y $c \mid b$. Entonces, existen $m$ y $n$ enteros positivos tales que $a = mc$ y $b = nc$ de donde resulta: $\frac{ab}{c} = mnc = na = mb$.
Por lo tanto $\frac{ab}{c}$ es múltiplo de $a$ y de $b$ y por tanto $d \mid \frac{ab}{c}$ por el Teorema 3.15.

Como $c = mcd(a,b)$, existen $r$ y $s$ enteros tales que $c = ar + bs$. Dividiendo por $c$ y multiplicando por $d$ de nos queda:

$$d = \frac{ar}{c}d + \frac{bs}{c}d(*)$$

Como $d = mcm(a,b)$ existen $p$ y $q$ enteros tales que $d = ap$ y $d = bq$. Reemplazando y agrupando convenientemente en la igualdad (*) resulta:

$$d = \frac{ab}{c}(rq + sp)$$

De donde resulta que $\frac{ab}{c} \mid d$. •

**Teorema 3.17.** *Si a y b son enteros positivos y $mcd(a,b) = 1$, entonces $mcm(a,b) = ab$*

La demostración es una consecuencia directa del teorema anterior.

## 3.6. Ecuaciones diofánticas

Una ecuación diofántica es una ecuación de la forma $ax + by = c$, donde $a$, $b$ y $c$ son enteros, de la que se esperan hallar soluciones enteras[2].
¿Cuándo es resoluble una ecuación diofántica?
La respuesta de esta pregunta la encontramos en el siguiente Teorema:

[2]La ecuación $ax + by = c$ en $R^2$ para $a$, $b$, $c$, $x$, $y$ reales, representa una recta. Hallar las soluciones de la ecuación diofántica consiste en determinar los puntos de la recta que poseen coordenadas enteras. Esto no siempre es posible. Por ejemplo, la ecuación 12 x + 8 y = 7 no tiene soluciones (x,y) tales que x e y sean ambos enteros.

**Teorema 3.18.** *Para a, b, c enteros, la ecuación diofántica $ax + by = c$ tiene solución si y solo si $mcd(a, b)|c$*

**Demostración**:
Supongamos, en primer lugar que la ecuación tiene la solución entera $(x_o, y_o)$. Se verifica entonces que $ax_o + by_o = c$.
Sea $mcd(a, b) = d$ y supongamos que $a = md$ y $b = nd$. Reemplazamos estos valores en la igualdad anterior y resulta:
$mdx_o + ndy_o = c \rightarrow d(mx_o + ny_o) = c \rightarrow d \mid c$.

Recíprocamente, supongamos que $d = mcd(a, b)$ es divisor de $c$.
Por el Teorema 3.12, $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Entonces, existen enteros r y s tales que: $\frac{a}{d}.r + \frac{b}{d}.s = 1$(*). Como $d \mid c$, existe $t$ entero tal que $c = dt$.
Multiplicamos por $c$ la igualdad (*) para obtener $\frac{a}{d}.r.c + \frac{b}{d}.s.c = c$.
Reemplazamos $c = dt$ para obtener: $\frac{a}{d}.r.d.t + \frac{b}{d}.s.d.t = c$
De modo que $a.(rt) + b.(st) = c$.
Así $(rt, st)$ es una solución de la ecuación con coordenadas enteras.•

**Teorema 3.19.** *Si la ecuación diofántica $ax + by = c$ tiene solución, esta no es única*[3]

**Demostración**:
Supongamos que hallamos la solución particular $(x_o, y_o)$ de la ecuación y que $mcd(a, b) = d$.
Demostraremos que cualquier par ordenado de la forma

$$\left(x_o - \frac{b}{d}k, y_o + \frac{a}{d}k\right), \text{ con } k \text{ variando en } Z$$

es solución de la ecuación.
En efecto:
Reemplazamos $x$ e $y$ por $x_o - \frac{b}{d}k$ e $y_o + \frac{a}{d}k$ respectivamente para obtener:
$ax+by = a\left(x_o - \frac{b}{d}k\right)+b\left(y_o + \frac{a}{d}k\right) = ax_o - a\left(\frac{b}{d}k\right)+by_o+b\left(\frac{a}{d}k\right) = ax_o+by_o = c$
(esto último resulta del hecho que $(x_o, y_o)$ es una solución de la ecuación).
En definitiva:

Sea $ax + by = c$ , con $a$, $b$, $c$ enteros y $d = mcd(a, b) \mid c$.
Entonces, una vez hallada una solución particular $(x_o, y_o)$,
$\left(x_o - \frac{b}{d}k, y_o + \frac{a}{d}k\right)$, con $k \in Z$ produce un número infinito de soluciones para la ecuación dada.•

[3]Si hemos determinado que la recta $ax+by = c$ pasa por un punto del plano de coordenadas enteras, entonces (se puede demostrar que) pasará por infinitos puntos de coordenadas enteras.

Una solución particular $(x_0, y_0)$ se obtiene aplicando de modo sucesivo el *Algoritmo de Euclides*, partiendo de los coeficientes $a$ y $b$, hasta llegar al $mcd(a, b)$.

Veamos unos ejemplos.
1. Dada la ecuación $100x + 35y = 420$,[4] ¿cuántas soluciones enteras positivas tiene?
Como $mcd(100, 35) = 5$ y $5 \mid 420$, la ecuación tiene soluciones enteras.
Dividimos la ecuación por 5 para obtener $20x + 7y = 84$.
Como $mdc(20, 7) = 1$, existen enteros $x'$ e $y'$ que permiten escribir 1 como combinación lineal (con coeficientes enteros) de 20 y 7.
Para hallar $x'$ e $y'$, aplicamos el algoritmo de la Euclides para 20 y 7:

$$20=7.2+6$$
$$7=6.1+1$$

Ahora empezamos desde la segunda igualdad para escribir:
1=7-6.1= 7-(20-7.2).1=20.(-1)+7.3
Así tenemos que 20.(-1)+7.3=1
Multiplicamos la igualdad anterior por 84:

$$20.(-84)+7.\ 252=84$$

Multiplicando por 5 para obtener una solución particular de la ecuación original:

$$100.(-84)+35.\ 252=420$$

Así (-84, 252) es una solución particular.
Las infinitas soluciones de la ecuación diofántica podemos expresarlas:

$$\left(-84 - \tfrac{35}{5}k, 252 + \tfrac{100}{5}k\right), \text{ es decir}$$
$$(-84-7k,\ 252+20k) \text{ con } k \in Z.$$

Aún no llegamos a la solución del problema, dado que pide determinar cuántas soluciones enteras positivas tiene la ecuación. Para ello debemos calcular para cuántos valores de k se obtienen soluciones positivas. Para ello planteamos:
$-84-7k > 0$ y $252+20k > 0$ De la primera resulta $k < -\frac{84}{7}$, de la segunda $k > -\frac{252}{20}$.

Por lo tanto, resulta $-12.6 < k < -12$ pero $k$ es un entero y no existe un entero comprendido entre esos valores.
Como consecuencia esta ecuación diofántica no posee solución entera positiva.

2. La municipalidad compró 454,60 metros de tejido de alambre para cercar el perímetro de los canteros en el Parque Municipal. Para cada

[4]Modificado de Fauring y Gutiérrez (1996).

cantero rectangular se necesitan 8,2 metros de tejido, en tanto que cada cantero triangular requiere de 7,8 metros. ¿Cuántos canteros de cada tipo tiene el Parque (suponga que se usa todo y no se desperdicia)?
La ecuación $8,2x + 7,8y = 454,60$ donde $x$ e $y$ son números enteros, modeliza el problema.
Multiplicando por 10 resulta la ecuación diofántica $82x + 78y = 4546$. La ecuación tiene solución pues el $mcd(82, 78) = 2$ y $2 \mid 4546$. Esto no garantiza que el problema tenga soluciones *enteras positivas*.

**Teorema 3.20.** *Sea $p$ primo y sea $p \mid ab$ para $a$ y $b$ enteros cualesquiera. Entonces $p \mid a$ o $p \mid b$*

**Demostración**:
Si $p$ divide a $a$ queda probado el teorema. Supongamos que $p$ no dividide a $a$.
Entonces $p$ y $a$ son coprimos[5] y existen $m$ y $n$ enteros tales que $pm + an = 1$
Multiplicando por $b$ resulta $pmb + anb = b$
Como $p \mid ab$ por hipótesis entonces $p \mid anb$ por el Teorema 3.5.
De igual modo, como $p \mid p$ entonces $p \mid pmb$.
Si $p \mid anb$ y $p \mid pmb$, por el Teorema 3.6, $p \mid b$.•

## 3.7. El teorema fundamental de la aritmética

**Teorema 3.21.** *Teorema Fundamental de la Aritmética (TFA). Todo número entero positivo mayor que uno puede escribirse de modo único, salvo el orden, como un producto de números primos*

**Demostración**:
Si $n$ es primo, entonces aceptamos que el teorema es cierto pensando que $n$ es un producto de un solo factor. Si $n$ no es primo, entonces es compuesto.
Supongamos que el teorema es falso. Es decir, no es verdad que todo entero positivo mayor que 1 puede escribirse como producto de primos. Por lo tanto, existen (al menos 1) enteros positivos que no satisfacen el Teorema. Denominamos $A$ al conjunto formado por estos enteros, es decir:
$A = \{x \in Z^+ / \ x > 1$ *y $x$ no puede escribirse como producto de primos*$\}$
Como $A$ es un conjunto de $Z^+$ no vacío (supusimos que existen enteros que no cumplen con el Teorema) está bien ordenado, es decir, tiene un elemento mínimo. Sea $m$ ese elemento. Este número no es primo. Por lo tanto, es compuesto. Sí es compuesto, es divisible por algún primo (Teorema 3.8). Sea $p$ el menor primo tal que $p \mid m$.
Existe $t$ entero positivo tal que $m = p.t$
Pero $t < m$, entonces $t \notin A$. Por lo tanto, existen primos $p_1, p_2, \ldots, p_n$ tales que

$$t = p_1^{r_1}.p_2^{r_2} \ldots p_n^{r_n}$$

[5] Dejamos al lector, probar que si $p$ es primo y $p$ no divide a $a$ entonces $mcd(a, p) = 1$.

Luego $m = p.t = p.\ p_1^{r_1}.p_2^{r_2}\ldots p_n^{r_n}$
Vemos que existen los números $p$ y $p_i$ primos, con $0 < i \leq n$, y tales que $m$ es el producto $p.\ p_1^{r_1}.p_2^{r_2}\ldots p_n^{r_n}$. En consecuencia el número $m$ no puede pertenecer a $A$. Este absurdo proviene de suponer que $A$ es no vacío.
Por lo tanto todo entero positivo mayor que 1 puede escribirse como producto de primos.
Para la unicidad, utilizamos el principio de inducción matemática fuerte.
Para $n = 2$ el teorema es verdadero. Si ahora suponemos que es verdadero para $n = 2, 3, 4, \ldots, n-2, n-1$ (es decir, todo entero positivo mayor igual que 2 y menor o igual que $n-1$ admite una única factorización de números primos), debemos probar que es verdadero para $n$.
Sean:
$n = p_1^{s_1}.p_2^{s_2}\ldots p_k^{s_k}$, donde $p_i$ primo y $s_i$ entero positivo, para $i = 1, \ldots, k-1, k$, y $n = q_1^{t_1}.q_2^{t_2}.\ldots.q_r^{t_r}$, donde $q_j$ primo y $t_j$ entero positivo, para $j = 1, \ldots, r-1, r$ dos factorizaciones de $n$ en números primos.
Supongamos, sin pérdida de generalidad, que $p_1 < p_2 < \ldots < p_k$ y que $q_1 < q_2 < \ldots < q_r$.
Como $p_1 \mid n \to p_1 \mid q_1^{t_1}.q_2^{t_2}.\ldots.q_r^{t_r}$ entonces por el Teorema 3.20, existe $j$, $1 \leq j \leq r$, tal que $p_1 \mid q_j$.
Como $p_1$ y $q_j$ son primos, debe ser $p_1 = q_j$. Aún más: afirmamos que $j = 1$.
Para probar esto último, como $q_1 \mid n \to q_1 \mid p_1^{s_1}.p_2^{s_2}.\ldots.p_k^{s_k} \to$ por el Teorema 3.20, existe $e$ con $1 \leq e \leq k$, tal que $q_1 \mid p_e$. Como $q_1$ y $p_e$ son primos, debe ser $q_1 = p_e$.
Tenemos entonces: $p_1 \leq p_e = q_1 \leq q_j = p_1$.
Por lo tanto $j = 1$ y $p_1 = q_1$.
Dividimos a $n$ por $p_1$ ($q_1$). Se obtiene $n_1$, donde:

$$n_1 = \frac{n}{p_1} = p_1^{s_1-1}.p_2^{s_2}.\ldots.p_k^{s_k} = q_1^{t_1-1}.q_2^{t_2}.\ldots.q_r^{t_r}$$

Como $n_1 < n$, vale la hipótesis inductiva, es decir, la factorización de $n_1$ en factores primos es única.
Por lo tanto, $k = r$, $p_i = q_i$ para $1 \leq i \leq k$, $s_1 = t_1$ y $s_i = t_i$ para $2 \leq i \leq k$.
Como consecuencia de estos resultados, la factorización de $n$ en factores primos es única. •

**Aplicación 1**

Hallar el número de divisiones positivos del número 234000.
Expresamos este número como producto de números primos: 234000 $=2^4.3^2.5^3.13$
Los divisores de 234000 deben tener la forma $2^{r_1}.3^{r_2}.5^{r_3}.13^{r_4}$, donde:
$0 \leq r_1 < 4$, es decir $r_1$ puede tomar 5 (5=4+1) valores: 0, 1, 2, 3 ó 4.
$0 \leq r_2 < 2$, $r_2$ puede tomar 3 = 2+1 valores.
$0 \leq r_3 < 3$, $r_3$ puede tomar 4 = 3+1 valores.
$0 \leq r_4 < 1$, $r_4$ puede tomar 2 = 1+1 valores.
Así, tenemos 5 posibilidades para el exponente de 2, por cada una de esas cinco, tenemos 3 posibilidades para el exponente de 3, por cada una de las anteriores tenemos 4 posibilidades para el exponente de 5 y

(del mismo modo) dos para el exponente de 13. Eso da un total de 5.3.4.2 = 120 divisores positivos de 234000 (incluimos $1 = 2^0.3^0.5^0.13^0$ y 234000).

**Aplicación 2**

El TFA conduce a un nuevo método para calcular al máximo común divisor de dos (o más) números. Hallar, por ejemplo, *mcd*(3600, 14040).

$3600 = 2^4 .3^2 .5^2$ y $14040 = 2^3. 3^3 .5. 13$

Buscamos los divisores primos comunes, que son 2, 3 y 5.

Como se trata de hallar el máximo divisor común, entonces buscamos el mayor exponente posible para estos números primos.

Resulta entonces $mcd(3600, 14040) = 2^3. 3^2. 5^1 = 360$.

De modo similar, utilizamos el TFA para calcular el *mcm*(3600, 14040)

En este caso, el mínimo común múltiplo se obtiene multiplicando entre sí los factores primos de 3600 y 14040, cada uno elevado al máximo exponente con el que se presenta: $mcm(3600, 14040) = 2^4.3^3.5^2.13^1 = 140400$.

# Capítulo 4
# Situaciones para profundizar conceptos de divisibilidad

**SITUACIÓN 1**
Analiza si cada enunciado sobre el conjunto de números enteros es verdadero o falso. Si es verdadero, demostrarlo. Si es falso, modificar el antecedente o el consecuente (pero no los dos al mismo tiempo) para que resulte un enunciado verdadero y luego demostrarlo.

a) Si $d$ es divisor de $a + b$ entonces $d$ divide a $a$ o bien $d$ divide a $b$.
b) $d$ divide a 0.
c) Si $a$ es divisor de $b$ y $b$ es divisor de $a$ entonces $a = b$.
d) Si $d$ es divisor de $a^2$ entonces $d$ es divisor de $a$.
e) El producto de dos números consecutivos es par.
f) El producto de dos números pares consecutivos es divisible por 8.
g) Si $d|a$ y $d|a + 1$ entonces $d = |1|$.
h) Si $b, c \geq 1$ y $a = b.c$ entonces $b \leq a$ y $c \leq a$.
i) Si $a > 1$ entonces $a$ tiene un número finito de divisores.

**SITUACIÓN 2**
Halla $a$ entero positivo, $a < 5000$ y con la siguiente propiedad: si se le resta 7, el resultado es divisible por 7; si se le resta 8, la diferencia es divisible por 8 y si se le resta 9, el resultado es divisible por 9. ¿Es único?

**SITUACIÓN 3**
La suma de tres números impares consecutivos, ¿es divisible por 3 y por 6? Justifica.

**SITUACIÓN 4**
Prueba que si $m$ es un cuadrado perfecto entonces $m$ es de la forma $4k$ ó $4k + 1$ para $k$ entero.

**SITUACIÓN 5**
a) Estudia en qué casos se incluye o excluye el 0 en las Definiciones 3.1, 3.2 y 3.3.
b) Para $a$ y $b$ enteros positivos y $a \neq 0$, demuestra que $mcd(a, 0) = a$; $mcd(-a, b) = mcd(a, -b) = mcd(-a, -b) = mcd(a, b)$.

**SITUACIÓN 6**
Halla todos los pares de números naturales cuya suma es 182 y el mcd 13.

**SITUACIÓN 7**
¿Qué números naturales $a$, menores que 300, satisfacen la condición que el $mcd(a, 156) = 26$? ¿Y que el $mcd(a, 360) = 20$?

**SITUACIÓN 8**
Determina para qué enteros positivos $n$ es $2n + 1$ divisible por 3. Justifica tu respuesta. Analiza la misma cuestión pero para la divisibilidad por 5.

**SITUACIÓN 9**
Prueba que la suma de cuatro enteros consecutivos no puede ser un cuadrado perfecto.

**SITUACIÓN 10**
Al sumar los números de tres cifras $6a3$ y $2b5$ se obtiene un número divisible por 3 pero no por 9. Halla los valores posibles de $a + b$.

**SITUACIÓN 11**
Atilio embala hormas de quesos en cajas de 10 ó de 24. Ayer embaló 198 quesos y llenó más de 10 cajas. ¿Cuántas cajas de cada clase llenó ayer?

**SITUACIÓN 12**
Si $a$, $b$ y $k$ son enteros positivos, demostrar que $mcd(a, b + k.a) = mcd(a, b)$.

**SITUACIÓN 13**
¿Para qué valores de $b$ es $15b^2 + 13b + 2$ divisible por 15?

**SITUACIÓN 14**
Un número natural es abundante si la suma de sus divisores positivos supera a su doble. Prueba que para cada primo impar $p$ mayor que 13, el número $n = p.15015$ es impar y abundante.

**SITUACIÓN 15**
a) Descompone en factores primos 23!.
b) Determina la mayor potencia de 50 que divide a 100!.
c) ¿Cuál es la mayor potencia de 7 que divide al producto 10!.20!.30!.40!.50!?

**SITUACIÓN 16**
Se consideran los números racionales entre 0 y 1 escritos en forma de fracción irreducible. Si se multiplica el numerador por el denominador, ¿en cuántos casos el resultado será 10!?

**SITUACIÓN 17**
José tiene fichas con los números 2, 5 y 10. Sumando todos los puntajes de sus fichas da 1937 puntos. Además se sabe que tiene igual número

de fichas de puntaje 5 que de puntaje 10 y que tiene menos fichas con puntaje 2 que con puntaje 5. ¿Cuántas fichas de cada clase puede tener José?

**SITUACIÓN 18**
Martín coloca en un frasco grande una cantidad de bolitas en marzo y en abril una cantidad mayor que la de marzo. A partir del tercer mes (mayo) coloca todos los meses una cantidad igual a la suma de las cantidades que colocó en los dos meses anteriores. Después del décimo mes el frasco contiene 407 bolitas. ¿Cuántas bolitas colocó en marzo y en abril?

**SITUACIÓN 19**
Sea $n$ primo. Demuestre que $n|x^2 - y^2$ si y solo si $n|(x - y)$ ó $n|(x + y)$. ¿Es válida la afirmación si $n$ no es primo? Justifica.

**SITUACIÓN 20**
Plantea y resuelve un problema que se modelice con las siguientes ecuaciones diofánticas:
a) $30x + 36y = 4$
b) $41x\text{-}19y = 8$

**SITUACIÓN 21**
Se tienen tres recipientes sin graduar de distintos tamaños: uno de 3 litros, otro de 19 litros y uno de 40 litros. Con ellos se quiere medir exactamente 14 litros de leche, de modo que el desperdicio del alimento sea mínimo. ¿Es posible hacerlo? Justificar la respuesta.

**SITUACIÓN 22**
Sea m un número entero positivo. Demuestra que m es compuesto si es divisible por algún número primo p tal que $p \leq \sqrt{m}$.
¿Cuál es la proposición recíproca de la anterior? ¿Es verdadera?
Halla todos los números primos menores que 200 utilizando los resultados anteriores.

# Capítulo 5

# Situaciones para introducir conceptos de congruencia

**SITUACIÓN 1**

***La carrera al 20***

Un jugador comienza diciendo uno de los siguientes números: 1 ó 2. Su contrincante debe sumar 1 o 2 unidades al número que dijo el primer jugador. Luego el primero debe sumar 1 ó 2 al resultado que acaba de decir su adversario y así sucesivamente. Gana el jugador que logre decir primero el número 20. Consigna: juega varias partidas. Identifica y escribe una estrategia ganadora.

**SITUACIÓN 2**

Observa los siguientes grupos de números:

25, 13, 31, 7, 55, 19, 37
20, 32, 44, 8, 26, 62, 92
47, 23, 65, 5, 11, 101, 17
10, 22, 40, 34, 52, 70, 76
3, 9, 33, 15, 21, 39
6, 12, 18, 24, 30, 36

i) Determina alguna propiedad o característica que compartan entre sí los grupos de números.

ii) Agrega a cada grupo un par de números que cumplan esa característica.

iii) Trata de formar dos grupos nuevos (cada uno con cinco números) usando números naturales que no pertenezcan a ninguno de los grupos anteriores.

**Nota histórica: Carl Friedrich Gauss «El príncipe de las matemáticas» (1777–1855)**

A muy temprana edad desarrolló un procedimiento muy eficaz para obtener la suma de los 100 primeros números naturales. ¿Lo conoces? Mira este video: https://www.youtube.com/watch?v=D_XKKJKu3IU.
En el video anterior se mencionan los números triangulares. Gauss demostró que todo número natural es la suma de tres números triangulares como máximo.


Una frase que se atribuye a Gauss es la siguiente: «La Matemática es la reina de las ciencias y la teoría de números es la reina de la Matemática» (Boyer, 1986:627). En su obra *Disquisitiones arithmetica* estableció las bases fundamentales de la moderna teoría de números. Este libro «reúne la obra de sus predecesores, pero la enriquece en tal magnitud que sin lugar a dudas marca el inicio de la moderna teoría de números» (Gentile, 1985:8). Define allí la noción de congruencia e introduce la notación utilizada en la actualidad. Desarrolló, además, una demostración rigurosa del Teorema Fundamental de la Aritmética (Teorema 3.21).

**SITUACIÓN 3**
Indica, en cada caso, si es V o F la afirmación. Justifica la respuesta.

$$-12 \equiv 4(5);\ 32 \equiv 25(7);\ 0 \equiv -34(3);\ -15 \equiv -18(2)$$

**SITUACIÓN 4**
¿Qué valores de $m$ hacen verdaderas las siguientes congruencias?

$$5 \equiv 4(m)$$
$$1197 \equiv 186(m)$$
$$1214567 \equiv 3124567(10m)$$
$$3 \equiv -3(m)$$

**SITUACIÓN 5**
Analiza si cada enunciado es V o F. Si es V, demostrarlo. Si es F, modifica

el antecedente o el consecuente (pero no los dos al mismo tiempo) para que resulte un enunciado V. Demuestra el enunciado resultante. En todos los casos $a, b, c, d \in Z$ y $m, n \in N$.

a) Si $a \equiv b(m) \rightarrow a + c \equiv b + c(m)$

b) Si $a \equiv b(m)$ y $c \equiv d(m) \rightarrow a + c \equiv b.d(m)$

c) Si $a \equiv b(m) \rightarrow a^n \equiv b^n(m)$

**SITUACIÓN 6**

¿Vale la ley cancelativa con respecto a la multiplicación en la relación de congruencia? Desarrolla una justificación que permita dar respuesta a esa pregunta. Enuncia conjeturas y contrástalas teniendo en cuenta las condiciones que consideres pertinentes.

**SITUACIÓN 7**

a) ¿Cuál es la última cifra de $17^{254}$?

b) ¿Cuáles son las dos últimas cifras de $38^{50}$?

**SITUACIÓN 8**

¿Existe algún múltiplo de 33 cuyo desarrollo decimal termine en 555?

**SITUACIÓN 9**

a) ¿Siempre es posible hallar una solución para la ecuación $a.x \equiv b(m)$ siendo $a, b \in Z$ y $m \in N$? Justifica.

b) En caso que la ecuación tenga solución, ¿es única?

**SITUACIÓN 10**

¿Cuántas ternas de números naturales consecutivos menores que 1000 tienen la propiedad de que el primero es múltiplo de 4, el segundo es múltiplo de 5 y el tercero es múltiplo de 6?

**SITUACIÓN 11**

Enuncia y prueba una conjetura que generalice la siguiente afirmación: si $x \equiv 4(5)$ , $x \equiv 4(6)$ y $mcd(5, 6) = 1 \rightarrow x \equiv 4(5.6)$.

**Nota histórica: Pierre de Fermat (1601–1665)**

Se considera el creador de la moderna teoría de números. Según Boyer (1986), Fermat desarrolla el método de descenso infinito. Veamos cómo funciona con un ejemplo:

*Probar que un número primo de la forma* $4n + 1$ *puede expresarse de una y solo una manera como suma de dos cuadrados.*

Ejemplos: $17=16+1$, $29=25+4$

Si existe un número primo que no posee esa propiedad, debe haber un número primo menor que él de la forma $4n + 1$ que tampoco la posea.


Como $n$ es arbitrario, debe haber otro más pequeño aún. Descendiendo a todos los valores enteros positivos de $n$, debemos llegar a $n = 1$. Para $n = 1$, resulta $4.1 + 1 = 5$ que es primo y que no debería gozar de la propiedad.

Pero $5 = 4 + 1$, es decir, se expresa de modo único como suma de dos cuadrados. Por tanto todo primo de la forma $4n + 1$ también la cumple.

**Nota histórica: Pierre de Fermat (1601–1665)(continuación)**

En un margen de la *Arithmetica de Diofanto*, Fermat afirma que es imposible convertir un cubo en la suma de dos cubos, una potencia cuarta en la suma de dos potencias cuartas, o en general cualquier potencia más alta que el cuadrado, en la suma de dos potencias de la misma clase. «He encontrado una demostración de esa proposición, realmente maravillosa, pero el margen del libro es demasiado estrecho para contenerlo» (Rey Pastor y Babini, 1997:56).

Este resultado se conoce como «el último teorema de Fermat».

Expresa en símbolos esta conjetura.

En 1993 Andrew Wiles (matemático inglés) anunció que había encontrado una demostración. Sin embargo, se encontró un error que la invalidaba. Wiles y su ayudante Richard Taylor tardaron casi 2 años en superar el obstáculo. En 1995 se publicó la definitiva.

Otras conjeturas enunciadas por Pierre de Fermat son:

- **Pequeño Teorema de Fermat**: si $p$ es primo y $a$ es coprimo con $p$, $a^{p-1} - 1$ es divisible por $p$.
  Esta conjetura está probada como Teorema 7.23.
- **Los números de la forma $2^{2^n} + 1$ son números primos**.
  Esta conjetura resultó ser falsa. Euler encontró (un siglo después) un contraejemplo: $2^{2^5} + 1$ es compuesto. En efecto: $2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$.

**SITUACIÓN 12**

Una banda de 13 piratas obtuvo un cierto número de monedas de oro que trataron de distribuir entre sí equitativamente, pero les sobraban 8 monedas. De imprevisto 2 de ellos murieron. Al volver a intentar el reparto, sobraban ahora 3 monedas. Posteriormente, 3 de ellos se ahogaron y al intentar distribuir las monedas quedaban 5. ¿Cuántas monedas había en juego?

**SITUACIÓN 13**

Calcula los restos al dividir por 6 a los elementos de cada conjunto:
$\{3, 4, 5, 6, 7\}$, $\{6, 25, 14, 51, 10\}$, $\{10, 12, 13, 33, 34\}$, $\{31, 36, 49, 61, 66\}$, $\{-11, 36, 49, 61, 66\}$
Analiza los restos en cada conjunto y describe en forma coloquial las conclusiones a las que llegues.

**SITUACIÓN 14**
Sea m un entero mayor que 1. De todos los restos posibles al dividir un número entero cualquiera por m, determinar cuántos son coprimos con m. Enuncia alguna regularidad obtenida durante la exploración realizada para dar respuesta a la pregunta.

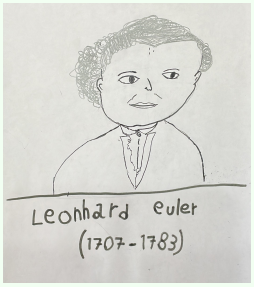
**SITUACIÓN 15**
Para conjeturar: ¿qué condiciones deben satisfacer los números enteros $b$ y $n$ para que se cumpla la siguiente relación: $b^{n-1} \equiv 1(n)$.

**SITUACIÓN 16**
Halla el resto de dividir al número $525^{377}$ por 13.

**SITUACIÓN 17**
Te invitamos a ver el siguiente video:
https://www.youtube.com/watch?v=Q8K311s7EiM, de Eduardo Sáenz de Cabezón para desentrañar el rol que cumplen los números primos para guardar secretos.
¿Qué es un test de primalidad? En el siguiente video conocerás el test de primalidad de Lucas, que hace uso del Pequeño Teorema de Fermat (Teorema 7.23): https://www.youtube.com/watch?v=L5UEoLzoskg.
Escribe dos ejemplos diferentes al presentado en el video del test de primalidad de Lucas en un caso que conduzca a afirmar que el número es primo y en el otro caso que conduzca a justificar que no lo es.

**Nota histórica: Leonhard Euler (1707–1783)**

Nació en Basilea (Suiza) y desarrolló una intensa actividad científica en las cortes de San Petersburgo y Berlín. Según Boyer (1986), ningún matemático ha superado su producción científica.




Publicó trabajos en matemática (teoría de números, álgebra, cálculo de probabilidades, cálculo infinitesimal y geometría) y en disciplinas afines (mecánica racional y aplicada, astronomía, física y geografía matemática) (Rey Pastor y Babini, 1997).
Entre sus contribuciones en teoría de números, mencionamos:

- Encontró un contraejemplo para la conjetura de Fermat respecto de que un número de la forma $2^{2^{n+1}}$ es primo. Para $n = 5$, resulta compuesto. En efecto: $2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 . 6700417$.
- Investigó la conjetura de Fermat y demostró que para $n = 3$ y $n = 4$ no existen tripletas de números $x$, $y$, $z$ enteros tales que $x^n + y^n = z^n$.
- Trabajó la ley de reciprocidad de los restos cuadráticos.
- Reconoció, sin demostrar, la conjetura de Goldbach anunciada en 1742: «todo número par es suma de dos números primos».

**SITUACIÓN 18**
Te proponemos la lectura del artículo de Canavelli *et al.* (2009) (ver en referencias bibliográficas)
Analiza la descripción del sistema RSA utilizado en criptografía para mantener la confidencialidad en la comunicación y para identificar al emisor de un mensaje. Desarrolla un ejemplo de uso diferente al propuesto en el artículo. Elabora una presentación para compartir el ejemplo con tus compañeros.

# Capítulo 6

# Aportes para la enseñanza de congruencia

**SITUACIÓN 1**. *Comentarios*

Este juego fue propuesto por Brousseau (2007) con los objetivos de repasar la división imprimiendo un nuevo sentido a la operación y favorecer el descubrimiento de la demostración de algunos teoremas. Ha desempeñado un rol importante en el desarrollo de su teoría. Sugerimos proponer el juego antes de trabajar la Definición 7.1. Proporciona un contexto ideal para introducir la noción de congruencia. Comentamos a continuación el modo en que se puede gestionar la clase durante su implementación con estudiantes de Profesorado en Matemática.

Al comienzo, los estudiantes disputan varias jugadas (de a pares o bien conformando dos grupos, en los que un representante de cada grupo juega contra un representante del otro y se suman los puntos de las sucesivas partidas). Luego de jugar varias partidas, se estimula a la clase para que formule alguna estrategia ganadora. Lo primero que identifican suele ser que la enunciación del número 17 conduce a ganar el juego. Así, se pueden seguir sucediendo partidas, de modo que se terminan identificando otros números *ganadores*. Este proceso normalmente se produce contando para atrás: para decir 20, se debe decir antes 17, antes, 14, antes 11, y así hasta llegar a 2. En este punto, el/la docente propone escribir en el pizarrón el listado de números ganadores e invita a las/os estudiantes a expresar qué tienen en común.

Inicialmente identifican que algunos son pares y otros impares, por lo que descartan enseguida el criterio de ser o no múltiplo de 2. Observan también que algunos son primos y otros son compuestos, por lo cual esa condición también es descartada. Con el fin de favorecer una discusión colectiva, resulta útil anotar en el pizarrón todas las condiciones enunciadas, de modo que puedan visualizarse por la clase completa, y de la misma surjan (si existen) contraejemplos que las contradigan. En la figura 10 compartimos una foto del pizarrón en la que se muestran las condiciones identificadas durante una clase.

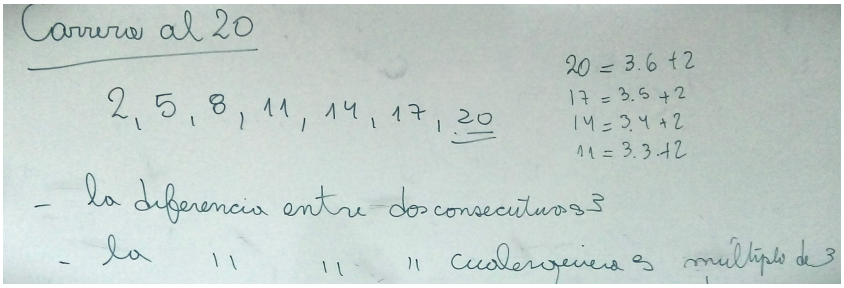



Figura 10. Dos regularidades reconocidas en el listado de números ganadores

En este momento, el/la docente puede solicitar que se expresen en símbolos las condiciones. La segunda conduce directamente a la Definición 7.1, por lo que da pie a la institucionalización de la noción de congruencia. Cabe señalar que, durante la implementación del juego en otro grupo de estudiantes, la regularidad identificada entre los números ganadores fue que tenían resto dos al dividirlos por 3. En el desarrollo matemático del Capítulo 7, se incluye el Teorema 7.1 que enuncia como condición necesaria y suficiente que para que dos números sean congruentes módulo m (natural) deben tener el mismo resto al dividirlos por m. Al tratarse de una bicondicional, es posible considerar esta condición (igual resto al dividir por m) como definición de la congruencia, de la cual se puede deducir la Definición 7.1. Nuevamente cabe aquí una reflexión respecto de la posibilidad de seleccionar una u otra de estas condiciones para proponer como definición en el desarrollo deductivo de la aritmética.

Finalmente, se puede invitar a los estudiantes para que propongan un juego similar cambiando las variables de su enunciado. En la figura 11 se muestra una fotografía del pizarrón en la que el grupo propuso la Carrera a 30. Se observa que los números iniciales pueden ser 1, 2 o 3, y que cada jugador debe sumar al número que dijo su contrincante un número natural menor que 4. En la fotografía se observa el listado de números ganadores y la condición que cumplen: 4 es divisor de la diferencia entre dos de ellos.

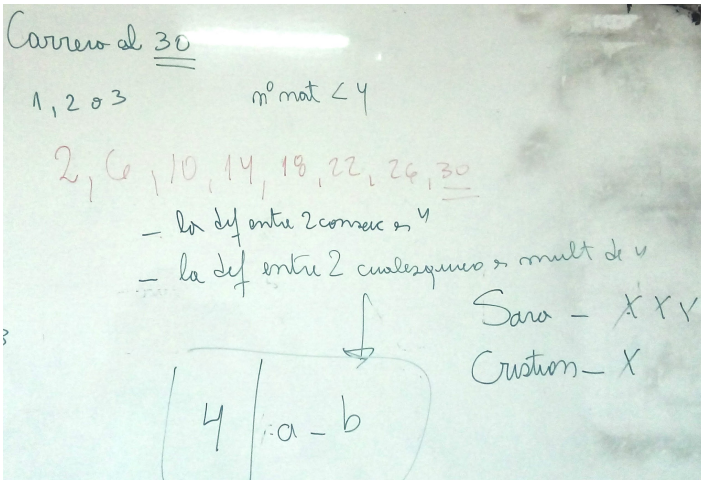



Figura 11. Carrera a 30. Variante del juego propuesta por los estudiantes

La formulación de esta variante permite reconocer que el estudiantado, en general, se ha apropiado de la noción de congruencia.

**SITUACIÓN 2**. *Comentarios*
Esta situación se plantea como otra opción para introducir el estudio de congruencias. También se puede proponer luego de trabajar la Situación 1. Se espera que los estudiantes reconozcan que en cada grupo de números la diferencia entre dos cualquiera de ellos es un múltiplo de 6.
En el último inciso se espera que reconozcan que los 6 grupos de números permiten completar el conjunto de los números enteros, por lo que constituye una situación adecuada para implementar antes de abordar la partición de Z en clases de equivalencia (es decir, antes de la sección 7.2). La definición de congruencia establece una clasificación del conjunto de números enteros según los posibles restos en la división por m (el módulo de la congruencia).

**SITUACIONES 3 y 4**. *Comentarios*
Las situaciones 3 y 4 se plantean con el fin de poner en juego la definición de congruencia módulo m o bien la condición necesaria y suficiente enunciada en el Teorema 7.1.
Si no se ha discutido aún sobre este hecho, resulta interesante destacar que demostrar la equivalencia entre las proposiciones $m|b-a$ y $r_m(a) = r_m(b)$ para $a$ y $b$ enteros y $m$ natural habilita a considerar cualquiera de ellas como definición de $a \equiv b$ (m), lo cual fortalece el reconocimiento de la arbitrariedad de las definiciones.

**SITUACIÓN 5**. *Comentarios*
Esta situación se diseña con la intención de que las/os estudiantes exploren la veracidad de enunciados que involucran la relación de congruencia antes de abordar los Teoremas 7.6, 7.7, 7.8, 7.9 y 7.10. La exploración desarrollada a partir del inciso a) puede conducir a los

Teoremas 7.6 y 7.7, que dan cuenta de la compatibilidad de la adición y la multiplicación de enteros con la relación de congruencia. Como sostiene Gentile (2012b), la posibilidad de *trasladar* estas operaciones al conjunto cuyos elementos son clases de congruencia (donde cada clase está formada por un conjunto infinito de enteros congruentes entre sí según el módulo de congruencia) origina el anillo de los enteros módulo m, es decir, lo que se conoce como «aritmética módulo m».
Se tiene la oportunidad de trabajar algunas reglas del debate matemático (Arsac *et al.*, 1992) como por ejemplo: un enunciado matemático es verdadero o falso, un contraejemplo es suficiente para invalidar un enunciado y en matemática, para debatir se puede apoyar en cierto número de propiedades o definiciones claramente enunciadas sobre las cuales se está de acuerdo.

**SITUACIÓN 6**. *Comentarios*
Esta situación se propone con la intención de explorar la ley cancelativa de la multiplicación en la relación de congruencia, dado que una serie de teoremas (7.11, 7.12, 7.13 y 7.14) explora distintas posibilidades respecto de la cancelación de un factor en un producto en el marco de esta relación. Las conjeturas pueden adoptar el formato de implicaciones: $p \rightarrow q$, donde $p$ y $q$ son proposiciones en las que se expresa una relación de congruencia entre dos números bajo cierto módulo. Entre las acciones permitidas en cuanto a la proposición $q$, a partir de efectuar la cancelación de algún factor que aparece en $p$, mencionamos las siguientes:

a) Cancelar el mismo factor $n$ en los números que expresan la congruencia y en el módulo (Teorema 7.11).

b) Cancelar un factor $a$ en los números que expresan la congruencia y dividir el módulo m de la congruencia por $mcd(a, m)$ (Teorema 7.12).

c) Cancelar un factor en el módulo de la congruencia (Teorema 7.13).

d) Cancelar un factor en los números que expresan la congruencia (Teorema 7.14).

Los casos c) y d) son verdaderos cuando se imponen ciertas condiciones entre los números intervinientes.
Con respecto a los resultados esperados en torno a la exploración realizada por el estudiantado, nos interesa mencionar que no es nuestro objetivo alcanzar la enunciación de los cuatro teoremas tal como figuran en el desarrollo matemático. En cambio, el objetivo es problematizar las relaciones matemáticas que están en juego, reconocer la posibilidad de cancelar o no algún factor y admitir que en algunos casos se requiere del cumplimiento de ciertas condiciones de hipótesis. Pensamos que esta exploración previa permitirá dotar de sentido el estudio de los teoremas.

**SITUACIÓN 7**. *Comentarios*
Esta situación se plantea con el fin de aplicar algunas de las propiedades demostradas para la relación de congruencia en la obtención de

resultados sencillos. En particular, permite vislumbrar la potencia de la congruencia para conocer las últimas cifras de números naturales cuya representación decimal no se puede manipular con el uso de calculadoras científicas ni programas informáticos por su elevado número de cifras.

**SITUACIÓN 8**. *Comentarios*
La modelización de esta situación problemática tomada de Becker *et al.* (2000) conduce al planteo de una ecuación lineal de congruencia, razón por la que resulta adecuada para trabajar antes de abordar el tema (es decir, antes de su definición).
Con respecto a la respuesta a la pregunta, las/os estudiantes pueden obtenerla haciendo uso de la definición de congruencia, de divisor y de los conocimientos sobre ecuaciones diofánticas.

**SITUACIÓN 9**. *Comentarios*
Estas situaciones problemáticas se formulan para explorar en torno a la resolución de ecuaciones lineales de congruencia. Promueven la inspección y contrastación de conjeturas acerca de las condiciones bajo las cuales la ecuación tiene solución y, en caso de que las tenga, el número de soluciones. Como en la situación anterior, es posible encontrar una justificación adecuada recurriendo a conocimientos previos.
No se pretende obtener respuestas completas y rigurosas matemáticamente a estas preguntas. Lo que interesa es que las preguntas le dan sentido al estudio que se realiza con mayor rigurosidad en el desarrollo matemático. Se sugiere su implementación antes de abordar los Teoremas 7.15 y 7.16.

**SITUACIÓN 10**. *Comentarios*
La interpretación de la situación en términos de los conocimientos aritméticos de los que dispone el estudiantado permite modelizarla mediante un sistema de ecuaciones lineales de congruencia. Por esa razón, el problema se puede presentar antes de trabajar el trabajo con tales sistemas.
En este momento se puede invitar al estudiantado a explorar el modo en que se puede abordar la resolución de un sistema y sobre la existencia de soluciones. Se sugiere la utilización de esta situación problemática antes del estudio del Teorema 7.19.

**SITUACIÓN 11**. *Comentarios*
Se espera que los estudiantes, a partir del análisis de las relaciones mostradas, enuncie una conjetura y la pruebe. Supondrá la obtención de un nuevo resultado (un teorema) en el marco de la teoría que está estudiando.

**SITUACIÓN 12**. *Comentarios*
Este problema tomado de Gentile (1985) se enuncia para que las/os estudiantes modelicen la situación mediante un sistema de relaciones de congruencia cuyos módulos son coprimos dos a dos.

En la situación 11 se necesita de la coprimalidad de los módulos para que el resultado sea verdadero. Se puede pedir a los estudiantes que comparen el sistema que modeliza esta situación con los sistemas producidos en las situaciones 10 y 11 en función de las características de los módulos.
En este problema, nuevamente, no interesa que las/os estudiantes alcancen resultados numéricos, sino que reconozcan en la situación algunas condiciones de partida, para promover la necesidad de estudiar un resultado matemático (el Teorema Chino del Resto). Por tanto, se sugiere plantear la situación antes de trabajar el Teorema 7.21.

**SITUACIÓN 13**. *Comentarios*
Esta situación problemática se plantea para llamar la atención sobre los restos de un conjunto de, en este caso, seis números enteros. Se espera que la exploración otorgue algún sentido a la definición de sistema de restos módulo m (Definición 7.2). Se sugiere, por lo tanto, presentar la situación antes de dicha definición.

**SITUACIÓN 14**. *Comentarios*
Mediante esta situación los estudiantes explorarán inductivamente algunos valores de la función $\phi$ de Euler. Es posible que reconozcan que el número de enteros coprimos con $n$ es $n - 1$ cuando $n$ es primo. Se sugiere su abordaje antes de la definición de dicha función.

**SITUACIÓN 15**. *Comentarios*
Se espera que el estudiantado explore relaciones matemáticas que permitan dar alguna respuesta a la pregunta. Pensamos que para ello recurrirán a ejemplos.
La pregunta apunta a identificar una condición que se plantea en la hipótesis del Pequeño Teorema de Fermat, razón por la cual se sugiere que la situación se presente antes del estudio del Teorema 7.23.

**SITUACIÓN 16**. *Comentarios*
Se trata de una situación típica para la aplicación del Pequeño Teorema de Fermat, una vez constatado que se dan las condiciones de hipótesis que se necesitan. En la misma se pone de manifiesto nuevamente la utilidad de la congruencia para obtener información sobre una característica particular de un número que tiene una cantidad de dígitos en su escritura decimal imposible de observar en el visor de una pantalla (de la calculadora o de la computadora).
Como en todos los problemas abordados en este capítulo, el tipo de información del número está vinculada con el resto que se obtiene al dividirlo por algún natural m, aspecto en el cual focaliza la relación de congruencia módulo m.

**SITUACIÓN 17**. *Comentarios*
Con esta situación se espera que las/os estudiantes continúen explorando la utilización de los números primos para mantener la confidencialidad

de la información que circula por Internet. Esta cuestión da sentido al interés por conocer si un número es o no primo, y por lo tanto a la necesidad de desarrollar estrategias para conocer esa condición, es decir, al desarrollo de tests de primalidad. Además, se espera se familiaricen con un test de primalidad sencillo, que hace uso de un teorema conocido (Teorema 7.23).

**SITUACIÓN 18**. *Comentarios*
Se trata de una situación típica para la aplicación del Teorema de Euler–Fermat una vez constatado que se dan las condiciones de hipótesis necesarias. Nuevamente la congruencia permite obtener información de un número cuya cantidad de cifras decimales imposibilita su manipulación a partir de operaciones sobre su representación o escritura decimal. Se propone se abordaje una vez conocido el Teorema 7.25.

**SITUACIÓN 19**. *Comentarios*
Esta situación se proporciona para que el futuro profesor acceda a información específica relacionada con el uso de la congruencia en criptografía. Se espera también que la lectura y la elaboración de un ejemplo para compartir con la clase promueva una oportunidad para desarrollar autonomía en la lectura de textos matemáticos.

# Capítulo 7
# Congruencias en los enteros

## 7.1. Conceptos básicos de congruencia

**Definición 7.1.** *Definición de congruencia*
*Sean $m \in N$ y $a, b \in Z$, se dice que $a$ es congruente con $b$, módulo $m$, si y solo si $m$ divide a $(b - a)$. En símbolos:*

$$a \equiv b(m) \Leftrightarrow m|(b - a)$$

*También se puede escribir:*

$$a \equiv b(md\ m) \Leftrightarrow m|(b - a)$$

Ejemplos:

$$1 \equiv -3(2) \text{ pues } 2|(-3 - 1)$$
$$3 \equiv 13(10) \text{ pues } 10|(13 - 3)$$
$$317 \equiv 4317(1000) \text{ pues } 1000|(4317 - 317)$$
$$b \equiv a(1) \text{ para todos } a \text{ y } b \text{ enteros, pues } 1|(b - a)$$

Para las propiedades enunciadas en este capítulo consideramos que $a$, $b$, $c$ y $d$ son números enteros y que $m$ y $n$ son números naturales.

**Teorema 7.1.** *Dos enteros son congruentes módulo $m$ si y solo si tienen el mismo resto en la división por $m$*

Observación:
La condición de que dos números tengan el mismo resto al dividirlos por otro puede tomarse como definición de congruencia. Así la definición dada en este capítulo se puede tomar como una propiedad que se deduce de la nueva definición.

Ejemplos:

- $13 \equiv 28(5)$ pues $5|(28 - 13)$ donde 13 y 28 tienen el mismo resto (3) si se los divide por 5.
- 7 y 10 tienen el mismo resto si se los divide por 3 y podemos verificar que $7 \equiv 10(3)$.

**Demostración:**
Denotamos el resto de la división de $a$ por $m$ por $r_m(a)$.
Sean

$$a = m.h + r_m(a) \text{ con } h \in Z \text{ y } 0 \leq r_m(a) < m \text{ y}$$
$$b = m.k + r_m(b) \text{ con } k \in Z \text{ y } 0 \leq r_m(b) < m$$

Supondremos además, sin pérdida de generalidad, que $r_m(b) \geq r_m(a)$.
Restando miembro a miembro las ecuaciones y agrupando convenientemente nos queda:

$$b\text{-}a = m.(k\text{-}h) + (r_m(b) - r_m(a)) \text{ con } 0 \leq r_m(b)\text{-}r_m(a) < m$$

de donde se sigue que $(r_m(b) - r_m(a))$ es el resto de la división de $b$-$a$ por $m$ por lo tanto

$$a \equiv b(m) \Leftrightarrow m|(b\text{-}a) \Leftrightarrow r_m(a) = r_m(b) \bullet$$

Se propone probar los siguientes teoremas utilizando la definición de congruencia.

**Teorema 7.2.** *Propiedad reflexiva.* $a \equiv a(m)$

**Teorema 7.3.** *Propiedad simétrica.* $a \equiv b(m) \Rightarrow b \equiv a(m)$

**Teorema 7.4.** *Propiedad transitiva.* $a \equiv b(m)$ *y* $b \equiv c(m) \Rightarrow a \equiv c(m)$

**Teorema 7.5.** $m|a \Leftrightarrow a \equiv 0(m)$

*Observación*: este teorema expresa que un entero $a$ es múltiplo de $m$ si y solo si $a \equiv 0(m)$

**Teorema 7.6.** *Si* $a \equiv b(m) \Rightarrow a + c \equiv b + c(m)$

**Teorema 7.7.** *Si* $a \equiv b(m) \Rightarrow a.c \equiv b.c(m)$

**Teorema 7.8.** *Si* $a \equiv b(m)$ *y* $c \equiv d(m) \Rightarrow a \pm c \equiv b \pm d(m)$

**Demostración:**
Si $a \equiv b(m)$ entonces $b = a + k.m$ y si $c \equiv d(m)$ implica que $d = c + h.m$ para algunos $k$ y $h$ enteros. Sumando miembro a miembro y agrupando convenientemente las igualdades que nos quedaron, obtenemos:

$$b + d = (a + c) + (k + h).m \Rightarrow a + c \equiv b + d(m)$$

Si en lugar de sumar, restamos miembro a miembro las igualdades, obtenemos la otra parte del teorema.•

**Teorema 7.9.** *Si* $a \equiv b(m)$ *y* $c \equiv d(m) \Rightarrow a.c \equiv b.d(m)$

**Teorema 7.10.** *Si* $a \equiv b(m)$ *y* $n \in N \Rightarrow a^n \equiv b^n(m)$

**Teorema 7.11.** *Si* $a.n \equiv b.n(m.n) \Rightarrow a \equiv b(m)$

**Demostración:**
Si $a.n \equiv b.n(m.n)$ entonces $bn = an + k.n.m$ para algún $k$ entero. Puesto que $n$ es un número natural, podemos dividir miembro a miembro la igualdad anterior y simplificando nos queda: $b = a + k.m$ de lo cual $a \equiv b(m)$. •

**Teorema 7.12.** *Si* $a.b \equiv a.c(m) \Rightarrow b \equiv c\left(\frac{m}{mcd(a,m)}\right)$

**Demostración:**
Si $a.b \equiv a.c(m)$ entonces $(c\text{-}b).a = k.m$ para algún $k$ entero. Dividimos ambos miembros de la ecuación por el $mcd(a,m)$ (por definición es un número natural) y queda

$$(c-b)\frac{a}{mcd(a,m)} = k.\frac{m}{mcd(a,m)}$$

donde $a' = \frac{a}{mcd(a,m)}$ y $m' = \frac{m}{mcd(a,m)}$ son números enteros. Reescribiendo la ecuación obtenemos: $(c-b).a' = k.m'$.
De aquí podemos asegurar que $m'|(c-b).a'$.
Además sabemos por el Teorema 3.12 que $mcd(a', m') = 1$ y por el Teorema 3.13, $m'|(c-b)$ con lo cual $b \equiv c(m')$. •

**Teorema 7.13.** *Si* $a \equiv b(m)$ *y* $n|m \Rightarrow a \equiv b(n)$

**Teorema 7.14.** *Corolario del Teorema 7.12.*
*Si* $a.c \equiv b.c(m)$ *y* $mcd(c,m) = 1 \Rightarrow a \equiv b(m)$

## 7.2. Congruencia como relación de equivalencia

Antes de continuar, observemos que las propiedades expresadas en los Teoremas 7.2; 7.3 y 7.4 expresan que la congruencia es una relación de equivalencia en los enteros y como tal determina una partición de Z en clases. Una clase está formada por todos los enteros congruentes entre sí, módulo m. Los enteros quedan partidos en m conjuntos no vacíos, ya que la propiedad reflexiva asegura que todo entero a pertenece a su propia clase, y disjuntos, ya que por las propiedades simétrica y transitiva dos clases son iguales o no tienen elemento en común.
La propiedad presentada en el Teorema 7.1 es la que caracteriza a la congruencia, y dice que la congruencia módulo m clasifica a los enteros por su resto en la división por m. Es por eso que lo más natural para representar a las clases de equivalencias módulo m sea elegir a dichos restos, es decir, $0, 1, 2, \ldots\ldots, m-1$.

Ejemplo: observemos la partición que produce la congruencia módulo 3 en el conjunto de los enteros. Los restos de dividir cualquier entero por 3 son: 0, 1 ó 2. Luego los enteros quedan partidos en tres clases de equivalencia que denotaremos $\overline{0}$, $\overline{1}$ ó $\overline{2}$ por lo que dijimos anteriormente.

$\overline{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$ los enteros que tienen resto 0 al dividirlos por 3.

$\overline{1} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ los enteros que tienen resto 1 al dividirlos por 3.

$\overline{2} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$ los enteros que tienen resto 2 al dividirlos por 3.
Observamos además que: $Z = \overline{0} \cup \overline{1} \cup \overline{2}$ y que $\overline{0} \cap \overline{1} = \emptyset$; $\overline{0} \cap \overline{2} = \emptyset$ y $\overline{1} \cap \overline{2} = \emptyset$

## 7.3. Criterios de divisibilidad

La noción de congruencia proporciona una regla práctica para obtener los criterios de divisibilidad en N. Se trata de determinar, para cada n natural, una condición suficiente que debe satisfacer un número natural expresado en el sistema de notación decimal posicional para determinar si es o no divisible por n. Presentamos un ejemplo de un criterio de divisibilidad.

**Criterio de divisibilidad por 3**
Si $a$ es un número natural, se puede escribir en su forma polinómica como:

$$a = a_r 10^r + \ldots + a_2 10^2 + a_1 10 + a_0$$

donde los $a_i$ para i = 0, 1, ..., r son los dígitos del número.
Se tiene usando la definición de congruencia y el Teorema 7.7:

$$a_0 \equiv a_0(3)$$

$$10 \equiv 1(3) \Rightarrow a_1 10 \equiv a_1(3)$$

$$10^2 \equiv 1(3) \Rightarrow a_2 10^2 \equiv a_2(3)$$

Y, en general, para $n$ natural:

$$10^n \equiv 1(3) \Rightarrow a_n 10^n \equiv a_n(3)$$

Y aplicando el Teorema 7.8, se obtiene:

$$a \equiv a_0 + a_1 + a_2 + \ldots + a_r(3)$$

lo cual dice (por Teorema 7.1) que $a$ y la suma de los dígitos $a_0 + a_1 + \ldots + a_r$ del desarrollo decimal de $a$ tienen el mismo resto en la división por 3. De aquí resulta la regla de divisibilidad por 3: un número es divisible por 3 si y solo si, la suma de sus dígitos es divisible por 3.

## 7.4. Ecuación lineal de congruencia

Estudiaremos la resolución de la ecuación en la variable $x$ que sigue, donde $a$ y $b$ son números enteros y $m$ es un número natural:

$$a \cdot x \equiv b(m)$$

Lo primero que investigaremos es la cuestión de la resolubilidad, ya que no siempre tendremos soluciones.
Por ejemplo: $2x \equiv 5(2)$ no posee solución en $Z$, pues cualquiera sea $x$ entero, $2x$ tiene resto 0 en la división por 2 y 5 tiene resto 1 en dicha división. Por lo visto anteriormente nunca $2x$ será congruente con 5 módulo 2.

**Teorema 7.15.** *Si $mcd(a, m) = 1$ entonces la ecuación $a.x \equiv b(m)$ tiene solución*

**Demostración:**
Si $mcd(a, m) = 1$, entonces existen $k$ y $h$ enteros tales que $a.k + h.m = 1$.
Multiplicando por $b$ ambos miembros de la igualdad anterior y conmutando y asociando convenientemente tenemos $a.(b.k) + (h.b).m = b$ ó $b - a.(b.k) = (h.b).m$ entonces $m|b - a.(b.k)$ lo que implica que $a(b.k) \equiv b(m)$ y $x = b.k$ es la solución buscada. •

Esta condición es suficiente pero no necesaria, pues, por ejemplo, la ecuación $2.x \equiv 2(4)$ es resoluble (cualquier entero impar la satisface) y sin embargo, el $mcd(2, 4) = 2 \neq 1$.

Enunciaremos ahora una propiedad que nos dará las condiciones suficiente y necesaria para que una ecuación lineal de congruencias tenga solución.

**Teorema 7.16.** *La ecuación $a.x \equiv b(m)$ tiene solución, si y solo si $mcd(a, m)|b$*

**Demostración:** Sea $x_0$ una solución de $a.x \equiv b(m)$ entonces $a.x_0 \equiv b(m)$. Así $b - a.x_0 = k.m$ para algún $k \in Z$. Luego $b = a.x_0 + k.m$ y como $mcd(a, m)$ es divisor de $a$ y de $m$ entonces, $mcd(a, m)|b$ por Teorema 3.7.
Con esto se prueba que si $a.x \equiv b(m)$ tiene solución, entonces $mcd(a, m)|b$.

Por Teorema 7.11, si $mcd(a, m)|b$ y $a.x \equiv b(m)$ entonces

$$\frac{a}{mcd(a, m)}.x \equiv \frac{b}{mcd(a, m)} \left(\frac{m}{mcd(a, m)}\right)$$

y como

$$mcd\left(\frac{a}{mcd(a, m)}, \frac{m}{mcd(a, m)}\right) = 1$$

(Teorema 3.12) la ecuación anterior admite solución $x_0$ por el Teorema 7.15. Probaremos que si $x_0$ es solución de

$$\frac{a}{mcd(a,m)}.x \equiv \frac{b}{mcd(a,m)}\left(\frac{m}{mcd(a,m)}\right)$$

entonces también lo es de $a.x \equiv b(m)$.

$$\frac{b}{mcd(a,m)} - \frac{a}{mcd(a,m)}.x_0 = k.\frac{m}{mcd(a,m)}$$

entonces $b - a.x_0 = k.m$ ya que el $mcd(a,m)$ es distinto de cero, entonces $m|b - a.x_0$ de lo cual $a.x_0 \equiv b(m)$.
Con esto se prueba que si $mcd(a,m)|b \Rightarrow a.x \equiv b(m)$ tiene solución. •

Si una ecuación lineal de congruencias tiene solución, estas son infinitas. Este resultado es el que presenta el siguiente teorema:

**Teorema 7.17.** *Si $x_0$ es solución de $a.x \equiv b(m)$ entonces también son soluciones los números $x_0 + k.m$, con $k \in Z$*

**Demostración:**
Si $x_0$ es solución de $a.x \equiv b(m)$ entonces $b - a.x_0 = m.h$ para algún $h$ entero. Restando a ambos miembros de la ecuación el número entero $a.k.m$, donde $k$ es un número entero tenemos:

$$b - a.x_0 - a.k.m = m.h - a.k.m$$

que se puede reescribir como:

$$b - a(x_0 + k.m) = m(h - a.k)$$

lo cual indica que $m|b - a(x_0 + k.m)$ o que $a(x_0 + k.m) \equiv b(m)$ que nos muestra que $x_0 + k.m$ es solución de la ecuación.•

A las soluciones tales que $0 \leq x < m$ las llamaremos *«soluciones principales»* de la ecuación.

Los números $x_0 + k.m$ ($k \in Z$) son congruentes con $x_0$ módulo $m$. Esto significa que entre las soluciones de $a.x \equiv b(m)$ están los infinitos números enteros pertenecientes a una misma clase de equivalencia módulo $m$: la clase a la que pertenece $x_0$.

Nos preguntamos: ¿cuántas clases de equivalencia modulo $m$ proporcionan soluciones a la ecuación? El siguiente teorema proporciona respuesta a esta pregunta.

**Teorema 7.18.** *El número de clases de equivalencia cuyos elementos son soluciones de $a.x \equiv b(m)$ es igual a $mcd(a,m)$*

**Demostración:**
Sea $x_0$ solución de la ecuación

$$\frac{a}{mcd(a,m)}.x \equiv \frac{b}{mcd(a,m)} \left(\frac{m}{mcd(a,m)}\right)$$

Las siguientes clases módulo $m$ proporcionan soluciones a la ecuación $a.x \equiv b(m)$:

$$x_0, x_0 + \frac{m}{mcd(a,m)}, x_0 + 2.\frac{m}{mcd(a,m)}, \ldots, x_0 + (mcd(a,m) - 1)\frac{m}{mcd(a,m)}$$

como se demuestra a continuación:

Sea $x_0 + i.\frac{m}{mcd(a,m)}$, con $0 \leq i \leq (mcd(a,m) - 1)$ una cualquiera de estas clases. Sustituyendo en la ecuación $a.x \equiv b(m)$ resulta:

$$a.\left(x_0 + i.\frac{m}{mcd(a,m)}\right) \equiv b(m)$$

$$a.x_0 + a.i.\frac{m}{mcd(a,m)} \equiv b(m)$$

donde $a.x_0 \equiv b(m)$ y dado que $mcd(a,m)|a$ podemos escribir $a.i.\frac{m}{mcd(a,m)} = k.m$ para algún $k$ entero. Así:

$$b + k.m \equiv b(m)$$

lo que prueba que $x_0 + i.\frac{m}{mcd(a,m)}$ es solución de la ecuación. •

Describimos a continuación los pasos a seguir para resolver la ecuación lineal de congruencia $a.x \equiv b(m)$:

1) Comprobar que el $mcd(a,m)|b$. (En caso negativo, la ecuación no tiene solución).

2) Resolver la ecuación $\frac{a}{mcd(a,m)}.x \equiv \frac{b}{mcd(a,m)} \left(\frac{m}{mcd(a,m)}\right)$

3) Si $x_0$ es una solución de la ecuación anterior, con

$$x_0 < \frac{m}{mcd(a,m)}$$

las soluciones de la ecuación original no congruentes entre sí módulo m, son:

$$x_0, x_0 + \frac{m}{mcd(a,m)}, x_0 + 2.\frac{m}{mcd(a,m)}, \ldots, x_0 + (mcd(a,m) - 1)\frac{m}{mcd(a,m)},$$

es decir, hay $mcd(a, m)$ soluciones no congruentes entre sí módulo m.

**Ejemplo:** Sea la ecuación $85.x \equiv 70(30)$.
Puesto que $mcd(85, 30) = 5$ y como 5 divide a 70, la ecuación tiene solución.
Debemos resolver la ecuación $17.x \equiv 14(6)$.
Para ello necesitamos hallar $x$ y $k$ enteros tales que $6.k + 17.x = 14$. Aplicando el algoritmo de Euclides para hallar el mcd(6, 17), y escribiendo este mcd como combinación lineal de 6 y 17, obtenemos:

$$1 = 6.(3) + 17.(-1)$$

multiplicando miembro a miembro por 14 queda

$$14 = 6.(42) + 17.(-14)$$

Reordenando la igualdad anterior:

$$14 - 17.(-14) = 6.(42) \Rightarrow 6|14 - 17.(-14) \Rightarrow 17.(-14) \equiv 14(6)$$

lo cual expresa que $x = -14$ es una solución de la ecuación. Además $x = -14 + 6.h$ con $h$ entero son todas las soluciones de la ecuación.

Para hallar las $5(= mcd(85, 30))$ soluciones no congruentes entre sí módulo 30, debemos observar que $-14 \equiv 4(6)$. Las 5 soluciones son: 4; 10; 16; 22 y 28.

## 7.5. Sistemas de ecuaciones lineales de congruencias

Estamos interesados en hallar un entero que satisfaga a la vez las ecuaciones: $x \equiv a\ (m)$ y $x \equiv b\ (n)$

**Ejemplo:** Analizar el sistema $\begin{cases} x \equiv 3\ (5) \\ x \equiv 4\ (7) \end{cases}$

Las soluciones de $x \equiv 3\ (5)$ son: $3, 8, 13, 18, \ldots$ y de $x \equiv 4\ (7)$ son: $4, 11, 18, 25, \ldots$ Por lo tanto, la solución común es 18, que es la solución del sistema. Podemos preguntarnos sobre la existencia y unicidad de las

soluciones. Para responder a estas cuestiones se presenta el siguiente teorema.

**Teorema 7.19.** *El sistema de congruencias* $\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}$ *admite solución si y solo si* $a - b$ *es múltiplo del* $mcd(m, n)$*. En este caso hay una única solución en el intervalo* $0 \leq x < mcm(m, n)$*.*

**Demostración:**
Si $x_0$ es solución del sistema entonces $a - x_0 = k.m$ para $k \in Z$ y $b - x_0 = h.n$ para $h \in Z$.
Restando miembro a miembro estas ecuaciones obtenemos

$$a - b = k.m - h.n$$

y como $mcd(m, n)|k.m$ y $mcd(m, n)|h.n \Rightarrow mcd(m, n)|a - b$.
(Se ha probado que si el sistema tiene solución entonces $mcd(m, n)|(a-b)$)

Para que exista solución se deben hallar $k$ y $h$ enteros tales que

$$x = a + k.m = b + h.n$$

Si $a - b$ es múltiplo del $mcd(m, n) \Rightarrow$ existe $k' \in Z$ tal que:

$$a - b = k'.mcd(m, n).$$

Si escribimos el mcd(m,n) como combinación lineal de m y n se tiene:
$a - b = k'(t.m + h'.n)$ con $t$ y $h'$ enteros de donde $a - k'.t.m = b + h'.k'n$ y llamando $k = -k'.t$ y $h = h'.k'$ se tiene la solución buscada, a saber,

$$x = a + k.m = b + h.m$$

(Se ha probado que si $mcm(m, n)|(a - b)$ entonces el sistema admite solución).

Consideremos la unicidad. Para ello se suponen dos soluciones $x$ e $y$ tales que $0 \leq x < y < mcm(m, n)$.
Como $x$ e $y$ son soluciones, entonces $x \equiv y(m)$ y $x \equiv y(n)$ lo cual nos dice que $y - x$ es divisible por $m$ y por $n$, y por Teorema 3.15, $y - x$ es divisible por $mcm(m, n)$. Esto último es imposible dado que $0 < y - x < mcm(m, n)$. El absurdo proviene de suponer que existen dos soluciones distintas en el intervalo $[0, mcm(m, n))$. •

**Ejemplo:** Resolver el sistema $\begin{cases} 5.x \equiv 9\ (11) \\ 3.x \equiv 5\ \ (4) \end{cases}$
Puesto que $mcd(11, 4) = 1$, entonces el sistema tiene solución.
Multiplicando por 9 la primer ecuación y por 3 la segunda y observando

que $5.9=45 \equiv 1(11)$; $9.9=81 \equiv 4(11)$; $3.3=9 \equiv 1(4)$ y que $3.5=15 \equiv 3(4)$ obtenemos el sistema equivalente $\begin{cases} x \equiv 4\ (11) \\ x \equiv 3\ \ (4) \end{cases}$

Observemos que en el sistema equivalente obtenido, el coeficiente de $x$ (en las dos ecuaciones) es 1. Antes de proseguir, veamos cómo se han obtenido los números 9 y 3 (respectivamente) que han permitido la obtención de este sistema.

En el primer caso, a partir de la ecuación $5x \equiv 9(11)$, se trata de hallar un entero $y$, tal que $5y \equiv 1(11)$. Aplicando la definición de congruencia, esta ecuación conduce a afirmar que $11|1 - 5y$, es decir, que existe $k$ entero tal que $1 = 11.k + 5.y$. Esta ecuación diofántica tiene solución, dado que $mcd(11, 5) = 1$.
La resolución de esta ecuación diofántica conduce a hallar los enteros $k = 1$ e $y = -2$. Este último número (-2) o cualquier otro congruente con él módulo 11, es útil para transformar la ecuación original en una ecuación donde el coeficiente de $x$ sea 1. Dado que $-2 \equiv 9(11)$ se ha escogido 9.
En el segundo caso, y resolviendo de modo análogo, se ha obtenido 3 como solución de la ecuación $3y \equiv 1(4)$, que tiene solución dado que $mcd(3, 4) = 1$.
Continuando ahora con la resolución del sistema equivalente obtenido, tenemos que $x = 4 + 11k$ y que $x = 3 + 4h$ con $k$ y $h$ enteros.
Restando miembro a miembro ambas ecuaciones obtenemos $0 = 1 + 11k - 4h$ ó $1 = 4h - 11k$ ó $4h \equiv 1(11)$
que tiene como solución $h = 3$. Luego $x = 3 + 4.3 = 15$ es la solución del sistema (comprobarlo).

Además $x = 15$ es la única en el intervalo $[0, 44)$ y todas las soluciones del sistema son de la forma $x = 15 + 44.k$ para $k$ entero.

**Teorema 7.20.** *Corolario del Teorema 7.19*
*Si el* $mcd(m, n) = 1$, *el sistema de congruencias* $\begin{cases} x \equiv a\ (m) \\ x \equiv b\ (n) \end{cases}$ *siempre tiene solución*

Veremos ahora un teorema que soluciona gran parte de los sistemas de ecuaciones lineales de congruencia, a saber: aquellos en los que los módulos son coprimos dos a dos. La demostración de este teorema nos da el método para resolver dicho sistema, de allí su importancia.

## 7.6. TEOREMA CHINO DEL RESTO

**Teorema 7.21.** *Teorema Chino del Resto. Un sistema lineal de congruencias*

$$\begin{cases} x \equiv a_1 \ (m_1) \\ x \equiv a_2 \ (m_2) \\ \quad \ldots \\ x \equiv a_k \ (m_k) \end{cases}$$

*tal que* $mcd(m_i, m_j) = 1$ *si* $i \neq j$ *(o sea que los módulos son dos a dos coprimos) admite solución única en el intervalo* $[0, \prod_{i=1}^{k} m_i)$

**Demostración**:
Sea $t_i = \dfrac{\prod_{j=1}^{k} m_j}{m_i}$ (producto de todos los módulos omitiendo el $m_i$) para cada $i = 1, \ldots, k$.
Es claro que $mcd(t_i, m_i) = 1$ para todo i. Por lo tanto, existen $x_i$, $1 \leq i \leq k$ tales que $t_i.x_i \equiv 1(m_i)$.
El número entero $t = a_1.x_1.t_1 + \ldots + a_k.x_k.t_k$ es evidentemente solución del sistema de congruencia.
Veamos que $t$ satisface la primera ecuación.
Como $m_1 | \ 1 - t_1.x_1 \ \Rightarrow \ m_1 | \ a_1(1 - t_1.x_1)$ y $m_1 | \ t_i$ para $2 \leq i \leq k \ \Rightarrow$ $m_1 | \ a_1 - a_1.t_1.x_1 - a_2.t_2.x_2 - \ldots - a_k.t_k.x_k$, es decir que $m_1 | \ a_1 - t \Rightarrow t \equiv a_1(m_1)$ que es lo que queríamos demostrar.
En forma análoga se puede probar que $t$ satisface todas las ecuaciones del sistema. (Hemos probado la existencia de solución).

Sean $0 \leq t_1 < t_2 < \prod m_i$ dos soluciones del sistema. Entonces, dado que, $t_2 - t_1 \equiv 0 \ (m_i) \ \ \forall i = 1, \ldots, k$ entonces $m_i | t_2 - t_1$ y por Teoremas 3.15 y 3.17 se tiene que $\prod m_i | t_2 - t_1$ lo cual es imposible, dado que $0 < t_2 - t_1 < \prod m_i$. El absurdo provino de suponer que existen dos soluciones distintas en el $[0, \prod m_i)$. (Hemos probado la unicidad). •

**Ejemplo:** Resolvemos el sistema $\begin{cases} x \equiv 8 \ (13) \\ x \equiv 3 \ (11) \\ x \equiv 5 \ (8) \end{cases}$ con este método.

Como mcd(13,11)=1; mcd(13,8)=1 y mcd(11,8)=1 estamos en condiciones de aplicar el Teorema Chino del Resto.
Como $t_1 = 88$; $t_2 = 104$ y $t_3 = 143$ se tiene las congruencias:
$88x_1 \equiv 1 \ (13)$, o también $10x_1 \equiv 1 \ (13)$
$104x_2 \equiv 1 \ (11)$ o también $5x_2 \equiv 1 \ (11)$
$143x_3 \equiv 1 \ (8)$ o también $7x_3 \equiv 1 \ (8)$
Resolviendo las ecuaciones obtenemos que $x_1 = 4$; $x_2 = 9$ y $x_3 = 7$ (comprobarlo).
Por tanto t=8.4.88+3.9.104+5.7.143=10629 $\equiv$ 333 (1144). Así 333 es la única solución principal.

## 7.7. Sistema de restos

*Supondremos de aquí en más que m es un entero mayor que 1.*

**Definición 7.2.** *Se denominará sistema completo de restos módulo m a todo conjunto $\{x_1, ..., x_m\}$ de números enteros tales que todo entero es congruente módulo m a uno, y solo uno de los $x_i$, para $1 \leq i \leq m$.*

**Ejemplos:** $\{0, 1, 2, 3, 4\}$; $\{1, 2, 3, 4, 5\}$; $\{10, 11, 12, 13, 14\}$ son algunos de los sistemas completos de restos módulo 5.

$\{0, 1, 2, \ldots, (m-1)\}$ es un sistema completo de restos módulo m.

**Definición 7.3.** *Se denominará sistema reducido de restos módulo m a todo conjunto $\{x_1, ..., x_s\}$ de números enteros tales que todo entero coprimo con m es congruente módulo m a uno, y solo uno de los $x_i$ , para $1 \leq i \leq s$.*

**Ejemplos:** $\{1, 2, 3, 4\}$; $\{6, 7, 8, 9\}$; $\{11, 12, 13, 14\}$ son algunos de los sistemas reducidos de restos módulo 5.

Dado $m$, la totalidad de restos $k$, $1 \leq k \leq m$, coprimos con $m$, forma un sistema reducido de restos módulo $m$. Cualquier otro sistema reducido de restos módulo $m$ tiene el mismo número de elementos. Este número se denotará por $\phi(m)$ y da lugar a la conocida función de Euler $\phi$.

**Ejemplos:** $\phi(1) = 1$; $\phi(2) = 1$; $\phi(3) = 2$; $\phi(4) = 2$; $\phi(5) = 4$; $\phi(6) = 2$ y $\phi(7) = 6$.
Utilizando el Principio de Inclusión y Exclusión notamos que
$\phi(m) = m.(1-\frac{1}{p_1})...(1-\frac{1}{p_r})$ donde $p_1, p_2, ..., p_r$ son los divisores primos de m.

**Teorema 7.22.** *Sea $mcd(a, m) = 1$. Si $\{r_1, ..., r_m\}$ es un sistema completo de restos módulo m, también lo es $\{a.r_1, ..., a.r_m\}$. Si $\{r_1, ..., r_{\phi(m)}\}$ es un sistema reducido de restos módulo m, también lo es $\{a.r_1, ..., a.r_{\phi(m)}\}$*

**Demostración:** (Por el método de reducción al absurdo)
Supongamos que $\{a.r_1, ..., a.r_m\}$ no es un sistema completo de restos módulo m. Entonces, existen (al menos) i y j tales que $a.r_i$ y $a.r_j$ dan el mismo resto en la división por m. Eso es verdadero si y solo si $a.r_i \equiv a.r_j(m)$. Puesto que $mcd(a, m) = 1$ por Teorema 7.14, esta congruencia equivale a afirmar que $r_i \equiv r_j(m)$. Esta afirmación contradice la hipótesis. Por lo tanto, $\{a.r_1, ..., a.r_m\}$ es un sistema completo de restos módulo m. Se deja la prueba al lector para el caso de sistema reducido de restos módulo m. •

## 7.8. Pequeño teorema de Fermat

**Teorema 7.23.** *Pequeño Teorema de Fermat. Sea p un número primo y a un entero tal que $mcd(a, p) = 1$, entonces $a^{p-1} \equiv 1(p)$*

**Demostración:**
Los números $\{1, 2, 3, ..., (p-1)\}$ forman un sistema reducido de restos módulo p. Por el Teorema 7.22 los números $\{a, 2.a, 3.a, ..., (p-1).a\}$ también forman un sistema reducido de restos módulo m, por lo tanto:

$$\begin{gathered} 1.a \equiv x_1(p) \\ 2.a \equiv x_2(p) \\ \dots \\ (p-1).a \equiv x_{p-1}(p) \end{gathered}$$

donde los $x_1, x_2, \dots, x_{p-1}$ son un reordenamiento de 1, 2, ..., (p-1). Aplicando el Teorema 7.9 obtenemos

$$a^{p-1}.1.2.3...(p-1) \equiv 1.2.3...(p-1)\ (p)$$

y como $1.2.3...(p-1)$ es coprimo con $p$, por Teorema 7.14 nos queda $a^{p-1} \equiv 1(p)$. •

**Ejemplo:** Hallar el resto de la división de $a$ por $b$, donde $a = 8^{931}$ y $b = 3$.
Puesto que 3 es primo y como mcd(8,3)= 1, por el P. T. de Fermat tenemos que: $8^2 \equiv 1(3)$ y utilizando el Teorema 7.10 obtenemos $(8^2)^{465} \equiv 1^{465}(3)$ o que $8^{930} \equiv 1(3)$ y como $8 \equiv 2(3)$ aplicando el Teorema 7.9 tenemos:
$8^{930}.8 \equiv 1.2(3)$ ó $8^{931} \equiv 2(3)$.
Por lo tanto el resto de la división de $a$ por $b$ es 2, lo cual no resultaria tan sencillo hallar de otro modo ya que el número $8^{931}$ tiene 840 cifras.

**Teorema 7.24.** *Corolario del Teorema 7.23. Si p es primo y a entero, entonces* $a^p \equiv a(p)$

**Demostración:**
Si $p$ divide a $a$ entonces $p \mid a - a^p$, de donde $a^p \equiv a(p)$.
Si $p$ no divide a $a$, como $p$ es primo, el $mcd(a, p) = 1$. Por el Pequeño Teorema de Fermat, $a^{p-1} \equiv 1(p)$. Multiplicando por $a$ por Teorema 7.7 resulta $a^p = a(p)$. •

## 7.9. Teorema de Euler-Fermat

Una generalización del Pequeño Teorema de Fermat a partir de la utilización de la función de Euler $\phi$ es el siguiente resultado.

**Teorema 7.25.** *Teorema de Euler–Fermat. Sea m natural. Para todo a entero, coprimo con m, se verifica que:*

$$a^{\phi(m)} \equiv 1(m)$$

**Demostración:**
Si $mcd(a, m) = 1$, y si $\{r_1, ..., r_{\phi(m)}\}$ es un sistema reducido de restos módulo

$m$, entonces $\{a.r_1, ..., a.r_{\phi(m)}\}$ es también un sistema reducido de restos módulo m (Teorema 7.22).
Por lo tanto:

$$a.r_1 \equiv x_1(m)$$

$$a.r_2 \equiv x_2(m)$$

...

$$a.r_{\phi(m)} \equiv x_{\phi(m)}(m)$$

donde los $x_1, x_2, \ldots, x_{\phi(m)}$ son un reordenamiento de $r_1, r_2, ..., r_{\phi(m)}$. Aplicando el Teorema 7.9 obtenemos:

$$a^{\phi(m)}.r_1.r_2...r_{\phi(m)} \equiv r_1.r_2...r_{\phi(m)}(m)$$

y como $r_1.r_2...r_{\phi(m)}$ es coprimo con $m$, podemos aplicar el Teorema 7.14 y obtenemos $a^{\phi(m)} \equiv 1(m)$. •

**Aplicación** Calcular las dos últimas cifras de $9^{763}$
Resolver este problema equivale a hallar x comprendido entre 0 y 99 (incluidos) tal que $9^{763} \equiv x(100)$
Como $100 = 2^2.5^2$, hallamos $\phi(100) = 100.\frac{1}{2}.\frac{4}{5} = 40$.
Por el Teorema de Euler–Fermat (puesto que $mcd(9, 100) = 1$):
$9^{40} \equiv 1(100)$.
Como 763=19. 40+3, tenemos que $9^{763} = (9^{40})^{19}.9^3 \equiv 9^3 \equiv 29(100)$
Así, el número $9^{763}$ termina en 29.

# Capítulo 8
# Situaciones para profundizar conceptos de congruencia

**SITUACIÓN 1**
Halla el resto de dividir al número 525377 por 13.

**SITUACIÓN 2**
a) ¿Cuál es el último dígito de $3^{55}$?
b) Halla las últimas dos cifras de $531^{377}$.

**SITUACIÓN 3**
Si el $mcd(m, n) = 1$; $a \equiv b(m)$ y $a \equiv b(n)$ entonces $a \equiv b(m.n)$. Justifica.

**SITUACIÓN 4**
Demuestra que $a \equiv b(m)$ implica $mcd(a, m) = mcd(b, m)$.

**SITUACIÓN 5**
¿Cuántos pares de enteros $(a, b)$ se requieren como mínimo para tener la certeza que existen dos pares $(a_1, b_1)$ y $(a_2, b_2)$ tal que $a_1 \equiv a_2(5)$ y $b_1 \equiv b_2(5)$?

**SITUACIÓN 6**
Formula una conjetura del tipo: «Todo número natural de la forma ... es congruente con 1 módulo 2, con 1 módulo 3, con 3 módulo 4 y con 3 módulo 5». Justifica esa conjetura.

**SITUACIÓN 7**
Determina, si es posible, todos los enteros $n$ para los que la ecuación $10x \equiv 15\ (n)$ no tiene solución. Justifica.

**SITUACIÓN 8**
Resuelve las siguientes ecuaciones en congruencias y escribe las soluciones principales:
a) $3x \equiv -14\ (9)$.
b) $17x \equiv 12\ (87)$.
c) $-5x \equiv 13\ (71)$.
d) $138x \equiv 4\ (140)$.

e) $14x \equiv 21\ (49)$.

**SITUACIÓN 9**
a) Demuestra que $\forall n \in \mathbf{N}$, $10^n \equiv (-1)^n\ (11)$.
b) Enuncia y demuestra el criterio de divisibilidad por 11.

**SITUACIÓN 10**
Halla cuatro enteros consecutivos divisibles por 7, 9, 11 y 13 respectivamente.

**SITUACIÓN 11**
Halla los $a \in \mathbf{Z}$ para los que la ecuación $ax \equiv 11^{256}\ (17)$ tiene por solución principal a 8.

**SITUACIÓN 12**
Para x natural, ¿es $x^7 - x$ múltiplo de 42? Justifica.

**SITUACIÓN 13**
Si $n \equiv a\ (16)$; $n \equiv b(5)$; $n \equiv c(11)$, entonces $n \equiv 1265a - 704b + 320c\ (880)$. Justifica.

**SITUACIÓN 14**
Halla todos los $a$ enteros que verifiquen simultáneamente las siguientes congruencias: $a \equiv 2\ (6)$; $a \equiv 2\ (15)$; $a \equiv 0\ (7)$.

**SITUACIÓN 15**
¿Es 4 el resto de dividir a $2.3^{47} - 5.421^{23}$ por 13? justifica.

**SITUACIÓN 16**
Calcula:
a) $x$ si $x \equiv 5^{1231}\ (16)$, siendo el menor entero positivo con esa propiedad.
b) $n$ si $n \equiv 2^{76}\ (77)$, y $0 \leq n < 77$.

**SITUACIÓN 17**
Propone un sistema de tres ecuaciones lineales de congruencia que:
a) tenga solución pero que no pueda aplicarse el Teorema Chino del Resto para resolverlo. Justifica.
b) no tenga solución. Justifica.

**SITUACIÓN 18**
En torno al Pequeño Teorema de Fermat (Teorema 7.23):
a) Escribe su recíproco. Analiza si es verdadero.
b) Estudia si puede ser útil para determinar la no coprimalidad de dos enteros.

**SITUACIÓN 19**
Prueba que si $mcd(a, 91) = mcd(b, 91) = 1$, entonces $a^{12} \equiv b^{12}\ (91)$.

**SITUACIÓN 20**

Calcula todos los números enteros que son múltiplo de 11, son impares y tales que al dividirlos por 5 nos dan resto 3. ¿Cuál entre todos es el número natural más pequeño?

**SITUACIÓN 21**

Demuestra, de dos formas distintas, que para cualquier $n$ entero positivo $7^n - 4^n$ es divisible por 3.

# Referencias bibliográficas


**Alassia, Gianella; Hoffman, Valentina; Kuchen, Celina; Götte, Marcela y Scaglia, Sara** (2023, noviembre). Las matemáticas en la cotidianidad. *XVII Encuentro Internacional de Profesorados de Enseñanza Superior, Media y Primaria en Ciencias Naturales, Matemática y Tecnología.* Organizado por la Facultad de Ciencias Exactas y Naturales (UBA).

**Arsac, Gilbert; Chapiron, Gisele; Colonna, Alain; Germain, Gilles; Guichard, Yves y Mante, Michel** (1992). *Initiation au raisonnement déductif au collège*. Press Universitaire de Lyon, IREM.

**Becker, María Elena; Pietrocola, Norma y Sánchez, Carlos** (2001). *Aritmética*. Red Olímpica.

**Boyer, Carl** (1986). *Historia de la matemática*. Alianza Editorial. Traducción de M. Martínez Pérez.

**Bouvier, Alan y George, Michel** (1995). *Diccionario de Matemáticas*. Akal.

**Brousseau, Guy** (2007). *Iniciación al estudio de la teoría de las situaciones didácticas*. Libros del Zorzal.

**Cambriglia, Verónica y Sessa, Carmen** (2011). Construcciones colectivas en torno a lo general. El caso de la divisibilidad y las descomposiciones multiplicativas. *Yupana*, 6, 39-48.

**Canavelli, Juan Carlos; Gaitán, María Mercedes y Carrera Elena F. de** (2009). TICs. Teoría de Números y Formación Docente. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología*, 3, 24-32. https://www.researchgate.net/publication/228964271_TIC's_Teoria_de_Numeros_y_Formacion_Docente.

**Canavelli, Juan Carlos** (2011). *Aritmética en la era digital. De los números primos a los cajeros automáticos*. Rediciones.

**Chevallard, Yves** (1989). Le passage de l'arithmetique a l'algebre dans l'enseignement des mathematiques au college. Deuxieme partie. Perspectives curriculaires: la notion de modelisation. *petit x*, 19, 43-72.

**Coriat, Moisés** (1997). Cultura, educación matemática y currículo. En L. Rico (Ed.) *Bases teóricas del currículo de matemáticas en educación secundaria* (pp. 151-209). Síntesis.

**Davis, Philip y Hersh, Reuben** (1988). *Experiencia matemática.* Labor, S.A.

**De Lorenzo, Javier** (1998). *La matemática: De sus fundamentos y crisis*. Tecnos S.A.

**De Villiers, Michael** (2009). *Some Adventures in Euclidean Geometry. Dyna-mic Mathematics Learning*.

**Euclides** (1996). *Elementos, Libros V-IX.* Gredos. Traducción de M. Puertas.

**Fauring, Patricia y Gutiérrez, Flora** (1996). *Problemas 4.* Red Olímpica.

**Fedonczuk, Miguel; Torres, María Cecilia; Nassiff, Keila y Scaglia, Sara** (2011). La discusión en el aula de reglas del debate matemático. *IV Jornadas de Educación Matemática, I Jornadas de Investigación*. Santa Fe.

**Gentile, Enzo** (1985). *Aritmética Elemental*. Secretaría General de la Organización de los Estados Americanos.
**Gentile, Enzo** (2012a). *Aritmética elemental para la formación matemática. Volumen 1.* Red olímpica.
**Gentile, Enzo** (2012b). *Aritmética elemental para la formación matemática. Volumen 2.* Red olímpica.
**Grimaldi, Ralph** (1998). *Matemáticas Discreta y Combinatoria.* Addison Wesley Longman.
**Itzcovich, Horacio** (2007) (Coord.). *La Matemática escolar. Las prácticas de enseñanza en el aula.* Aique Educación.
**Kline, Morris** (1999). *El pensamiento matemático desde la antigüedad a nuestros días*. Alianza Editorial.
**Margolinas, Claire** (1992). Eléments pour l'analyse du rôle du maître: les phases de conclusion. *Recherches en Didactique des Mathématiques*, 12(1), 113-158.
**Ministerio de Educación** (2013). *Núcleos de Aprendizajes Prioritarios. Matemática. Ciclo Básico Educación Secundaria.* 1 y 2 / 2 y 3 Años. Ministerio de Educación y Consejo Federal de Educación.
**Racca, Bruno y Scaglia, Sara** (2018). El papel de las interacciones en la construcción del sentido del trabajo aritmético. En N. Di Franco (Comp.) *Memorias VII Reunión Pampeana de Educación Matemática* (pp. 140-150). EdUNLPam.
https://repem.exactas.unlpam.edu.ar/cdrepem18/MemoriasRepem 2018completas.pdf.
**Rey Pastor, Julio y Babini, José** (1997). *Historia de la Matemática. Volumen II. Del Renacimiento a la actualidad*. Gedisa editorial.
**Rodríguez, Mabel** (Coord.) (2017). *Perspectivas metodológicas en la enseñanza y en la investigación en educación matemática* (2da. ed.). Universidad Nacional de General Sarmiento.
**Rougier, Cinthia y Scaglia, Sara** (2012). Una experiencia con futuros profesores basada en la formulación y contrastación de conjeturas. *Revista de Educación Matemática*. https://doi.org/10.33044/revem.10177.
**Sadovsky, Patricia** (2005). *Enseñar Matemática hoy. Miradas, sentidos y desafíos.* Libros del Zorzal.
**Scaglia, Sara y Kiener, Fabiana** (2015). La gestión de una clase de aritmética en torno a la formulación y verificación de conjeturas: el papel de las interacciones en el aula. *Práxis Educacional*, 11(19), 191-212. https://www.redalyc.org/pdf/6954/695476960011.pdf.

# Sobre las autoras

**Sara Scaglia**
Doctora en Ciencias Matemáticas en la especialidad Didáctica de la Matemática (Universidad de Granada, España). Profesora en Matemática (Universidad Nacional del Litoral). Profesora Asociada ordinaria del Seminario de Investigaciones en Didáctica de la Matemática del Profesorado en Matemática (Facultad de Humanidades y Ciencias, UNL). Investigadora categoría 1 (Programa de Incentivos, SPU–MEN–UNL). Ha dirigido proyectos de investigación en torno a la problemática de la construcción del sentido en la clase de matemática. Ha dictado seminarios de posgrado, tiene antecedentes en la formación de recursos humanos de grado y posgrado y cuenta con diversas publicaciones.

**Marcela Götte**
Profesora en Matemática y Magíster en Didácticas Específicas (Universidad Nacional del Litoral). Profesora Adjunta ordinaria de Geometría Euclídea Espacial y Matemática Discreta I y Matemática Discreta II del Profesorado en Matemática (Facultad de Humanidades y Ciencias, UNL). Docente investigador en temas referidos a la enseñanza de la matemática en distintos niveles educativos. Autora de publicaciones sobre esta temática en revistas especializadas nacionales e internacionales y, junto a Ana María Mántica, de *Geometría en 3D* (Ediciones UNL, 2022).

# Teoría de números en la formación docente

Sara Scaglia
Marcela Götte

CÁTEDRA

El libro tiene la finalidad de compartir experiencias en torno a la enseñanza de la teoría de números en la formación de profesores/as de matemática. Este dominio de la matemática constituye un campo propicio para estudiar los modos de producir y organizar el conocimiento matemático porque permite plantear problemas de todo tipo de complejidad a partir de enunciados sencillos.

La obra se organiza en torno al estudio de dos campos conceptuales de la teoría de números: divisibilidad y congruencias. Se plantean situaciones que permiten problematizar los conceptos, acompañadas con comentarios que apuntan a reflexionar sobre el trabajo matemático que es posible desplegar en torno a cada una y notas históricas. Se incluye un desarrollo deductivo de definiciones y teoremas elementales vinculados con estos campos y una selección de situaciones problemáticas que permiten profundizar su estudio.

UNIVERSIDAD NACIONAL DEL LITORAL