Dosier módulo V

Módulo V

o v·u Œ} v šµŒ o • o }v ‰š} u š u Ÿ } }Œ]P]v o ‰}Œ Æ o v] Ç•µ Œ}oU
• ŒŒ}oo} o D š u Ÿ X> • •‰ µo]}v ••} Œ •µ v šµŒ o Ì Ç ‰Œ}‰] • }v
o ‰ v• u] vš} u š u Ÿ }X
> d }Œ_ E·u Œ}•Z } µ‰ }•] u‰Œ µv ‰}•]]•v ‰ µo] Œ Œ •‰ š} o •]•
‰}Œ•µ Œ ‰µš]•v • Œ]0]o Ç ‰}Œ •š Œ Œ À •Ÿ µv µŒ] Œš} u]•š Œ]}
v]À o µ ŸÀ} v •‰] o Ç ·v v o • µ o ‰Œ]u Œ] •µ‰}š v] o] v}Z •] } Œ o
• Z y}•U o v• y vÌ o D š u Ÿ v š} }• o}• v]À o • •š v À Œ Œ Œ
o }Œ Œ ‰ ŸŸÀ }v ‰} Œ i Œ]š]•v Ç‹µ o u Ç}Œ_ o • À •(oo v •µ•]š
• Œ µv u Œ}Œ ‰š}Œ }v}]u] vš}•‹µ]0]ou vš ‰µ]P Œ]Œ Ç o}oo À v
o • v•]•v (Œ •}X ^µ ‰ ŒŸ]‰]•v • ‰Œ Ÿ u vš vµo X
> Œ]šu Ÿ Œ ‰Œ • vš µv Æ o vš }‰]•v ‰ Œ u i}Œ Œ o v• y vÌ o
}Ÿ] v U ‰ Ì šŒ Œ µ o‹µ] Œ ‰ Œ•}v ‹µ ‰}• ••o}µv‰} } µŒ]}•] X ^µ
‰o vš Œ ‰Œ} o u • š} } Ÿ‰} }u‰o i] X o Œ •}oÀ Œo}• • o i Œ]]} •‰
•u} o • Œ À]•š • vš Œ š v]u] vš}•vµu Œ] }• oo u v o š v]•v uµ Z P vš U
NW}Œ‹µ v} Æ‰o}Œ Œ • µŒ]}•] ‹µ ‰}• o P vš i}À v Ç o}•v]y}• v •‰] oM
o}‹µ • v• y U Z Ç‹µ À]š Œ oo v Œ o Ì o}• •šµ] vš • }v(•Œ uµo • Ç š }Œ
‰ v• Œ Ç Œ G Æ]}v Œ o] Œ u vš U]vÀ]š v }o}•]u P]v ŒX

Œ o u• µo}

•š }••] Œ o u• µo}• Z Œ š } š v] v } v µ vš o}u i}Œ o}•o] Œ}•‹µ • ‰
z• Z •šŒµ šµŒ } ‰}Œ µv] • Ç š u •

hv] /W /s/^/ />/

hv] //W EhD Z /ME

hv] ///W h /KE ^ /K& Ed/ ^

hv] /sW KE'Zh E / ^W h /KE ^z^/^d D ^

>}• }vš v] }• v •š •µv] •• • ŒŒ}oo Œ v u] vš o •šµ]} o š }Œ_ ‰ Œ
} i u‰o}• }v Œ š}•U ‰ Œ Æ‰}v Œ o}]všµ]ŸÀ}Ç v šµŒ o‹µ Æ]P v o}•Œ Ì}v u

}u} • ŒŒ}oo Œ o u• µo}

o u} µo}• • ŒŒ}oo Œ u] vš ŸÀ] •‰Œ • v] o •U À]Œšµ o • Ç ‰Œ
W Œ o • ŸÀ] •‰Œ • v] o •• Œ }u] v Œ š}u Œ o}• ‰Œ}]u] vš}• Ç o}•]v
o • µv] •V •š o] }• v o • Œ]‰š}Œ o u• µo}U Z_ •]v] u v Œ • µ
šŒ i Œ o • š •Œ] Ç o Œ •}oµ]•v ‰Œ} o u •X W Œ o • ŒŒ}oo}
•µP Œ v] •u š} }o•P] • •š o] • v µv o • µv] • o • Œ]‰š}Œ ou• µ
}v µv Œš] Ÿ • u v o v }v • •š o Œ u v Œ •‰ _. o}• }vš v] }•U
• ŒŒ}oo ŒU o Ÿ u‰}Œ ‹µ Œ] }U o À oµ]•v Ç o}• Œ µŒ•}• v • Œ]}•X
W Œ o ŸÀ] ‰Œ Ÿ } vš • •Ÿv Œ Ÿ u‰} všŒ} i}Œv Œ• P
‰ Œš }• o Pµ_ o ‰Œ Ÿ Ç š v Œ }v•µoš ••} Œ oo X
W Œ o ŸÀ À]Œšµ o • Œ Œ µv µŒ•} v o ‰o š (}Œu }ŒŒ •‰}v] vš o
Z]o]š Œ v](Œ vš • ŸÀ] •W o šµŒ • }u‰o u vš Œ] •U Œ¡ µo}• ‰ Œ (}Œ
µ •Ÿ}v Œ]}•‹µ Œ v }u‰o š Œ o}• ‰ Œ Ÿ]‰ vš •X
hv }u vš Œ]} ‹µ ‰} Œ_ Z Œ• o}• ‰Œ}(•}Œ • •‰] o]•š • •‹µ o } µu
]u‰ ŒŸŒ µŒ•}•]všŒ} µ š}Œ]}• Ç }v•}o]]•v •} Œ Œ]šu Ÿ U ‰š v } o
i Œ]]}•X
‹µ_ • ŒŒ}oo Œ u}• µv µŒ•} ‰} } •}.•Ÿ }U ‰ v• v } v‹µ Z Ç oP} À Œ
•]u‰}Œš vš U v •]u‰}Œš vš _X

Divisibilidad

1 Lógica

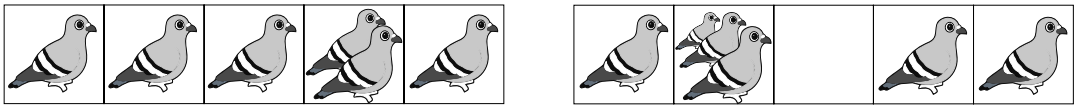
1.1. Conjuntos numéricos

En lo que sigue utilizaremos la siguiente notación para los conjuntos numéricos:

- Conjunto de los números naturales $\mathbb{N} = \{1, 2, \ldots\}$
- Conjunto de los números enteros $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- Conjunto de los números enteros positivos $\mathbb{Z}^+ = \{1, 2, \ldots\}$
- Conjunto de los números enteros no negativos $\mathbb{Z}_0^+ = \{0, 1, 2, \ldots\}$

1.2. Principios

Principio 1.1 (Principio del palomar)**.** *Si asignamos* m *palomas en* n *palomares, si* $m > n$ *entonces hay al menos dos palomas ocupando el mismo palomar.*



Principio 1.2 (Principio del buen orden)**.** *Todo conjunto no vacío de números naturales contiene un elemento mínimo.*

En particular, si $S \subset \mathbb{Z}$ y si S tiene al menos un elemento positivo, entonces S tiene un entero positivo mínimo.

Este principio aplica en la demostración de la siguiente propiedad.

Propiedad 1.3 (Propiedad arquimediana de $\mathbb{R}$)**.** *Si* $x, y \in \mathbb{R}$ *y* $x > 0$ *entonces existe al menos un número natural* $n \in \mathbb{N}$ *tal que* $nx > y$*.*

La propiedad arquimediana de $\mathbb{R}$ tiene una "variante" en la que interviene el producto en lugar de la suma:

Propiedad 1.4. *Si* $x > 1$ *y* y *son números reales, entonces existe* $n \in \mathbb{N}$ *tal que* $x^n > y$*.*

Más adelante cuando digamos "por la propiedad arquimediana de $\mathbb{R}$" nos referiremos a la propiedad 1.3 o a su variante 1.4.

Principio 1.5 (Principio de inclusión - exclusión)**.** *Si* A *y* B *son conjuntos finitos, entonces*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Principio 1.6 (Principio de la suma)**.** *Si un suceso* E_1 *puede ocurrir de* m *maneras y un segundo suceso* E_2 *puede ocurrir de* n *maneras, si ambos sucesos no pueden ocurrir simultáneamente, entonces el suceso* E_1 *o el suceso* E_2 *ocurre de* $m + n$ *maneras.*

Principio 1.7 (Principio de la multiplicación)**.** *Si un suceso* E_1 *puede ocurrir de* m *maneras y un segundo suceso* E_2 *puede ocurrir de* n *maneras y si ambos sucesos son independientes, entonces las combinaciones de* E_1 *y de* E_2 *pueden ocurrir de* $m \cdot n$ *maneras.*

Ejemplos 1.8. **[A]** *Supongamos que para almorzar tenemos cinco opciones de establecimientos que ofrecen comida saludable y dos opciones de establecimientos que ofrecen comida rápida ¿A cuántos diferentes lugares podemos ir a almorzar? Respuesta* $5 + 2 = 7$ *establecimientos.*

[B] *Si un joven tiene tres camisas (de colores blanco, negro y rojo) y dos pantalones (de color café y azul), ¿de cuántas maneras puede vestirse? Respuesta: de* $3 \cdot 2 = 6$ *maneras.*

Usando el Principio de Inclusión-Exclusión, en el caso que A y B son conjuntos finitos podemos interpretar los principios de la suma y conjuntos de la siguiente manera:

[A] $|A \times B| = |A| \cdot |B|$ (principio de la multiplicación)

[B] $|A \cup B| = |A| + |B|$ siempre que A y B sean disjuntos (principio de la suma).

Nótese que estos últimos tres principios se pueden extender a una cantidad finita de sucesos.

Principio 1.9 (Principio de inducción matemática)**.** *Para probar que una proposición* $P(n)$ *es verdadera para todo entero positivo* n*, se deben realizar las siguientes etapas en orden:*

[A] *(Caso base) Verificar que* $P(n)$ *es verdadera para* $n = 1$*,*

[B] *(Hipótesis inductiva) Suponer que* $P(k)$ *es verdadera para un entero positivo* $k > 1$*.*

[C] *(Paso inductivo) Demostrar que si* $P(k)$ *es verdadera, entonces* $P(k + 1)$ *es verdadera.*

Se puede probar que el principio de inducción matemática es un método válido de demostración si asumimos el principio del buen orden como un axioma.

Principio 1.10 (Principio de inducción matemática completa)**.** *Para probar que una proposición* $P(n)$ *es verdadera para todo entero positivo* n*, se deben realizar las siguientes etapas en orden:*

[A] *(Caso base) Verificar que* $P(n)$ *es verdadera para* $n = 1$*,*

[B] *(Hipótesis inductiva) Suponer que* $P(2)$*,* $P(3)$*, . . .,* $P(k)$ *son verdaderas para un entero positivo* $k > 1$*.*

[C] *(Paso inductivo) Demostrar que si* $P(1)$*,* $P(2)$*,* $P(3)$*, . . .,* $P(k)$ *son verdaderas, entonces* $P(k + 1)$ *es verdadera.*

Se puede probar que el principio de inducción completa es equivalente al principio de inducción. Es decir, cada principio puede ser demostrado asumiendo el otro. La ganancia es que el principio de inducción completa es más flexible. Al principio de inducción también se le suele llamar inducción matemática o primer principio de inducción y al principio de inducción completa también se le conoce como principio de inducción fuerte o segundo principio de inducción.

1.3. Lógica Proposicional, Teoremas y Demostraciones

Aquí hacemos una introducción a la lógica matemática y se explican algunos de los conceptos necesarios, para en la medida de lo posible comprender los argumentos que daremos en el estudio del aritmética.

1.3.1. Proposiciones

Una **proposición** es una oración declarativa o una expresión matemática que es verdadera o es falsa, pero *no* ambas. De esta manera, una proposición tiene un **valor de verdad**, que puede ser V, si es verdadera o puede ser F, si es falsa. Consideraremos exclusivamente proposiciones matemáticas.

Algunos ejemplos de proposiciones verdaderas son:

- "4 es un número entero par".
- "$15 \leq 15$".
- "La solución de $2x - 3 = 1$ es 2".
- "18 es múltiplo de 3".

Algunos ejemplos de proposiciones falsas son:

- "144 es un número entero impar".
- "$2 = 17$".
- "La solución de $2x - 3 = 1$ es 0".
- "16 es múltiplo de 5".

Algunos ejemplos de expresiones que no son proposiciones son:

- "73"
- "$2x - 1 = 3$"
- "¿Cuál es la solución de $2x - 3 = 1$?".
- "x es múltiplo de 3".

Generalmente, para referirnos a proposiciones específicas se usan letras mayúsculas. Por ejemplo,

$P:$ 25 es un número entero par. $Q:$ $3 + 4 = 7$. $R:$ $2x + 3$ es una ecuación.

Las proposiciones pueden contener variables. Por ejemplo, sea x un número entero y consideremos

$P:$ $2x + 1$ es un entero impar.

Esta es una proposición que es verdadera no importa que número entero sea la variable x, entonces podemos denotarla por

$P(x):$ $2x + 1$ es un entero impar.

Hay oraciones o expresiones matemáticas que contienen variables y no son proposiciones. Por ejemplo,

$Q(x):$ El número entero x *es múltiplo de* 3.

Sólo será una proposición cuando le otorguemos un valor a x (y así podremos determinar si es verdadera o falsa). Por ejemplo, $Q(13)$ es falsa y $Q(21)$ es verdadera.

1.3.2. Operadores lógicos básicos

Comenzamos introduciendo los operadores lógicos más básicos, veremos más adelante que estos estarán completamente definidos por sus tablas de verdad, pero intuimos sus acciones en palabras:

"$\sim$" intercambia el valor de verdad de *V* (*V*erdadero) a *F* (*F*also), y de *F* a *V* para una sentencia,

"$\wedge$" asigna *V* si dos sentencias son verdaderas, si hay alguna (una o ambas) falsa asigna *F*,

"$\vee$" asigna *F* si dos sentencias son falsas, si hay alguna (una o ambas) verdadera asigna *V*,

"$\Rightarrow$" asigna *V* excepto cuando la primera sentencia (antecedente o hipótesis) es verdadera y la segunda (consecuente o conclusión) es falsa. En el caso particular cuando la hipótesis es falsa, entonces asigna *V* y se dice que es verdadero por *vacuidad*.

"$\Leftrightarrow$" asigna *V* si los valores de verdad de las dos sentencias coinciden y *F* si difieren.

El cuadro siguiente muestra la simbología, escritura, lectura, notación y uso de los operadores lógicos más básicos, con el fin de facilitar la comprensión de la estructura lógica de las proposiciones.

Símbolo	**Nombre**	**Notación**	**Uso**
$\sim$	negación	$\sim P$	P no es verdadero
$\wedge$	y	$P \wedge Q$	P y Q son verdaderos
$\vee$	o	$P \vee Q$	P o Q P es verdadero o Q es verdadero (o ambos son verdaderos)
$\Rightarrow$	condicional	$P \Rightarrow Q$	Si P entonces Q P implica Q P sólo si Q Si P, Q Q si P P es suficiente para Q Q es necesario para P Q con la condición de que P Q cuando P Q siempre que P
$\Leftrightarrow$	bicondicional	$P \Leftrightarrow Q$	P es equivalente a Q P si y sólo si Q

1.3.3. Construyendo tablas de verdad

Las tablas de verdad son tablas que muestran el valor de verdad de una sentencia compuesta para cada una de las distintas configuraciones de los valores de verdad de cada sentencia componente. Por ejemplo, para construir la tabla de verdad de una sentencia compuesta C en la que intervienen dos sentencias componentes P y Q se deben disponer en las filas todas las combinaciones posibles de valores de verdad de P y Q, y luego agregar tantas columnas como se desee para conseguir paso a paso los valores de verdad de la sentencia C, se puede usar el orden *V*, *F*.

Comenzamos construyendo las tablas de verdad de los operadores básicos ya introducidos para tener su definición formal

P	$\sim P$
V	F
F	V

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
V	*V*	*V*	*V*	*V*	*V*
V	*F*	*F*	*V*	*F*	*F*
F	*V*	*F*	*V*	*V*	*F*
F	*F*	*F*	*F*	*V*	*V*

Cuadro 1.1: Tablas de verdad y definición de operadores lógicos básicos

Si dice que el operador lógico $\sim$ es **unario** porque se aplica a un argumento, mientras que los operadores $\wedge, \vee, \Rightarrow, \Leftrightarrow$ son **binarios** porque se aplican a dos argumentos.

Veamos un ejemplo más

P	Q	R	$Q \vee R$	$P \wedge (Q \vee R)$	$P \wedge Q$	$P \wedge R$	$(P \wedge Q) \vee (P \wedge R)$
V	*V*	*V*	*V*	*V*	*V*	*V*	*V*
V	*V*	*F*	*V*	*V*	*V*	*F*	*V*
V	*F*	*V*	*V*	*V*	*F*	*V*	*V*
V	*F*	*F*	*F*	*F*	*F*	*F*	*F*
F	*V*	*V*	*V*	*F*	*F*	*F*	*F*
F	*V*	*F*	*V*	*F*	*F*	*F*	*F*
F	*F*	*V*	*V*	*F*	*F*	*F*	*F*
F	*F*	*F*	*F*	*F*	*F*	*F*	*F*

Las columnas son iguales

En virtud del principio de la multiplicación, es claro que para construir la tabla de una sentencia compuesta C donde intervienen $P_1, P_2, \ldots, P_n$ sentencias componentes se necesitan 2^n filas.

1.3.4. Tautologías, contradicciones y equivalencias lógicas

Definición 1.11. *Una sentencia compuesta formada por las sentencias componentes $P_1, P_2, \ldots, P_n$ es llamada* **tautología** *(respectivamente* **contradicción***) si y sólo si en la tabla de verdad, todas las entradas en su correspondiente columna tienen el valor V (resp. F) i.e.*[1] *para cada una de las 2^n posibilidades de sus sentencias componentes el valor de verdad es verdadero (resp. falso).*

Ejemplo 1.12. *Mostrar que $[\sim (P \vee Q)] \Leftrightarrow [(\sim P) \wedge (\sim Q)]$ es una tautología.*

Resolución.

P	Q	$P \vee Q$	$\sim (P \vee Q)$	$\sim P$	$\sim Q$	$(\sim P) \wedge (\sim Q)$	$[\sim (P \vee Q)] \Leftrightarrow [(\sim P) \wedge (\sim Q)]$
V	*V*	*V*	*F*	*F*	*F*	*F*	*V*
V	*F*	*V*	*F*	*F*	*V*	*F*	*V*
F	*V*	*V*	*F*	*V*	*F*	*F*	*V*
F	*F*	*F*	*V*	*V*	*V*	*V*	*V*

Las columnas son iguales — *Tautología*

Notar que en lógica matemática, el operador"$\Leftrightarrow$" desempeña un papel similar al que desempeña el operador "$=$" en álgebra. Ahora definimos formalmente la equivalencia lógica de dos sentencias compuestas.

Definición 1.13. *Dadas n sentencias independientes $P_1, \ldots, P_n$, y dos sentencias R, S compuestas, cuyas sentencias componentes son $P_1, \ldots, P_n$, diremos que R y S son* **lógicamente equivalentes***, y lo denotaremos $R \Leftrightarrow S$, si y sólo si sus respectivas columnas en la tabla de verdad tienen los mismos valores de verdad para cada una de las 2^n combinaciones de los valores de verdad de $P_1, \ldots, P_n$.*

A continuación se listan algunas equivalencias lógicas entre los operadores básicos que hemos definido, se deja como ejercicio la comprobación de cada una de ellas se puede hacer construyendo tablas de verdad.

[1] "i.e." es la abreviatura de las palabras en latín *id est*, que en español significan "es decir"

$$P \wedge P \iff P \iff P \vee P \tag{1.1}$$
$$\sim(\sim P) \iff P \tag{1.2}$$
$$\sim(P \vee Q) \iff (\sim P) \wedge (\sim Q) \tag{1.3}$$
$$\sim(P \wedge Q) \iff (\sim P) \vee (\sim Q) \tag{1.4}$$
$$P \vee (\sim P) \iff \mathsf{T} \tag{1.5}$$
$$P \wedge (\sim P) \iff \mathsf{F} \tag{1.6}$$
$$P \Rightarrow Q \iff Q \wedge (\sim P) \tag{1.7}$$
$$\sim(P \Rightarrow Q) \iff P \wedge (\sim Q) \tag{1.8}$$
$$\sim(P \Leftrightarrow Q) \iff [P \wedge (\sim Q)] \vee [Q \wedge (\sim P)] \tag{1.9}$$
$$P \vee Q \iff Q \vee P \tag{1.10}$$
$$P \wedge Q \iff Q \wedge P \tag{1.11}$$
$$P \Leftrightarrow Q \iff Q \Leftrightarrow P \tag{1.12}$$
$$P \vee (Q \vee R) \iff (P \vee Q) \vee R \tag{1.13}$$
$$P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R \tag{1.14}$$
$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R) \tag{1.15}$$
$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R) \tag{1.16}$$
$$P \Rightarrow Q \iff (\sim P) \vee Q \tag{1.17}$$
$$P \Rightarrow Q \iff (\sim Q) \Rightarrow (\sim P) \tag{1.18}$$
$$P \Leftrightarrow Q \iff (\sim P) \Leftrightarrow (\sim Q) \tag{1.19}$$
$$P \Rightarrow (Q \wedge R) \iff (P \Rightarrow Q) \wedge (P \Rightarrow R) \tag{1.20}$$
$$P \Rightarrow (Q \vee R) \iff (P \Rightarrow Q) \vee (P \Rightarrow R) \tag{1.21}$$
$$(P \Rightarrow Q) \wedge (Q \Rightarrow P) \iff P \Leftrightarrow Q \tag{1.22}$$
$$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \wedge (R \Rightarrow P) \iff (P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R) \wedge (P \Leftrightarrow R) \tag{1.23}$$

Cuadro 1.2: Tabla de algunas equivalencias lógicas.

Comprobaremos que $P \Rightarrow Q$, $(\sim Q) \Rightarrow (\sim P)$ y $(\sim P) \vee Q$ son lógicamente equivalentes.

P	Q	$P \Rightarrow Q$	$\sim Q$	$\sim P$	$(\sim Q) \Rightarrow (\sim P)$	$\sim P$	Q	$(\sim P) \vee Q$
V	*V*	*V*	*F*	*F*	*V*	*F*	*V*	*V*
V	*F*	*F*	*V*	*F*	*F*	*F*	*F*	*F*
F	*V*	*V*	*F*	*V*	*V*	*V*	*V*	*V*
F	*F*	*V*	*V*	*V*	*V*	*V*	*F*	*V*

Las columnas son iguales

Las equivalencia **[1.18]** aparece con mucha frecuencia, razón por la cual tiene nombre especial.

Definición 1.14. *Para cualquier implicación* $P \Rightarrow Q$*, llamaremos* **contrarecíproca** *o* **contrapositiva** *a la implicación (lógicamente equivalente)* $(\sim Q) \Rightarrow (\sim P)$.

Es decir, $[P \Rightarrow Q] \iff [(\sim Q) \Rightarrow (\sim P)]$. En efecto, lo probaremos sin usar tablas de verdad y usando las equivalencias lógicas del cuadro 1.2.

$$P \Rightarrow Q \underset{\text{por 1.17}}{\iff} (\sim P) \vee Q \underset{\text{por 1.10}}{\iff} Q \vee (\sim P) \underset{\text{por 1.2}}{\iff} [\sim(\sim Q)] \vee (\sim P) \underset{\text{por 1.17}}{\iff} (\sim Q) \Rightarrow (\sim P).$$

Las equivalencias lógicas del cuadro 1.2 tienen interesantes interpretaciones, por ejemplo la equivalencia 1.1 dice que los operadores $\wedge, \vee$ son idempotentes, es decir,

$$P \wedge P \iff P \iff P \vee P.$$

Las equivalencias 1.10, 1.11 y 1.12 respectivamente dicen que los operadores lógicos $\vee, \wedge$ y $\Leftrightarrow$ son "conmutativos":

$$P \vee Q \iff Q \vee P, \qquad P \wedge Q \iff Q \wedge P, \qquad P \Leftrightarrow Q \iff Q \Leftrightarrow P,$$

y las equivalencias 1.13 y 1.14 dicen que los operadores $\wedge$ y $\vee$ son asociativos:

$$P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R, \qquad P \vee (Q \vee R) \iff (P \vee Q) \vee R.$$

Las equivalencias 1.15 y 1.16 dicen respectivamente que "$\wedge$ se distribuye sobre $\vee$" y "$\vee$ se distribuye sobre $\wedge$":

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R), \qquad P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R).$$

1.3.5. Cuantificadores

Aquí introduciremos los cuantificadores que son otros símbolos lógicos que servirán. El uso de los cuantificadores requiere la referencia a algún conjunto universo, tal y como veremos en los ejemplos que se proponen.

Cuantificador universal: $\forall$ *se lee, "para todo" o "para cualquier";*
Cuantificador existencial: $\exists$ *se lee, "existe";*
Cuantificador de unicidad: $!$ *se lee, "único"*

Los dos primeros son los más relevantes y el tercero aparece en pocas situaciones, a continuación ilustramos la manera en que suelen aparecer, emplearse y/o utilizarse.

$(\forall x \in S)P(x)$, i.e., para todo elemento x que pertenece al conjunto S, $P(x)$ es verdadero;

$(\exists x \in S)P(x)$, i.e., existe algún elemento x que pertenece al conjunto S tal que $P(x)$ es verdadero;

$(\exists! x \in S)P(x)$, i.e., existe un único (exactamente un) elemento x que pertenece al conjunto S tal que $P(x)$ es verdadero.

Donde S es un conjunto y $P(x)$ es alguna sentencia sobre x.

Ahora mostramos el uso de los cuantificadores en algunos ejemplos concretos.

$$(\forall x \in \mathbb{R})(x + x = 2x): \text{ para todo } x \in \mathbb{R},\ x + x = 2x;$$
$$(\exists x \in \mathbb{R})(x^2 = 1): \text{ existe } x \in \mathbb{R} \text{ tal que } x^2 = 1;$$
$$(\exists! x \in \mathbb{R})(x + 2 = 2): \text{ existe un único } x \in \mathbb{R} \text{ tal que } x + 2 = 2.$$

Las tres sentencias anteriores son verdaderas. Las sentencias que involucran cuantificadores también tienen un valor de verdad, y deben ser analizadas en su contexto y basadas en los principios matemáticos adecuados; la dificultad es que para este tipo de proposiciones no se conoce algún procedimiento mecánico para analizar sus tablas de verdad como lo hemos hecho anteriormente, ¡es aquí justamente donde se vuelve interesante el razonamiento matemático!

A continuación estudiamos formas equivalentes de como se deben interpretar las negaciones de sentencias que involucran cuantificadores.

Negación del cuantificador universal y existencial

Solo mencionamos el caso en que la sentencia involucre un sólo cuantificador, ya sea universal o existencial. Se tienen las siguientes equivalencias.

$$\sim [(\forall x \in S)P(x)] \iff (\exists x \in S)[\sim P(x)], \tag{1.24}$$

$$\sim [(\exists x \in S)P(x)] \iff (\forall x \in S)[\sim P(x)], \tag{1.25}$$

El lado izquierdo de (1.24) establece que no es el caso que $P(x)$ es verdadera para todo $x \in S$; el lado derecho establece que existe un $x \in S$ para el cual $P(x)$ es falsa. ¿Cuándo *no* es cierto que para todo x, $P(x)$ es verdadera? Exactamente cuando encontramos algún x para el cual $P(x)$ es falsa, i.e., $\sim P(x)$ es verdadera.

Lo anterior dice que para *demostrar* que una proposición $P(x)$ es falsa, basta con exhibir un **contraejemplo** i.e. encontrar un $x \in S$ para el cual $P(x)$ es falsa.

El lado izquierdo de (1.25) establece que no es el caso que exista un $x \in S$ para el cual $P(x)$ es verdadera; el lado derecho dice que $P(x)$ es falsa para todo $x \in S$. ¿Cuándo *no* es cierto que existe un x tal que $P(x)$ es verdadera? Cuando $P(x)$ es falsa para toda x.

Para negar $(\forall x)P(x)$ o $(\exists x)P(x)$ se debe intercambiar $\forall$ por $\exists$ o vice-versa, y negar las sentencias después del cuantificador.

Ejemplo 1.15. *Escribir la negación de* $(\forall x \in S)[P(x) \Rightarrow Q(x)]$.

Resolución. *Necesitamos (1.8), pág. 9, así* $\sim (P \Rightarrow Q) \iff P \wedge (\sim Q)$.

$$\sim [(\forall x \in S)(P(x) \Rightarrow Q(x))] \iff (\exists x \in S)[\sim (P(x) \Rightarrow Q(x))] \iff (\exists x \in S)[P(x) \wedge (\sim (Q(x)))].$$

1.4. Métodos de demostración

"Entiendo todo el material pero no puedo hacer las demostraciones". Este hecho no sorprende, pues los matemáticos dedican su vida a descubrir y demostrar nuevos resultados, algo que lleva experiencia (incluso genialidad), esfuerzo y ocasionalmente suerte. Realizar una demostración es similar a armar un rompecabezas. Al inicio se tienen cientos de piezas que no parecen encajar y es muy probable que la figura que intentamos formar no se parezca en nada a otras figuras que hayamos formado anteriormente. Sin embargo, nuestra experiencia construyendo otros rompecabezas nos dice que existen ciertas técnicas que pueden ayudarnos y, entre ellas, hay unas que funcionan mucho mejor que otras.

Las demostraciones no pueden reducirse a un proceso mecánico, pero existen ciertos caminos (métodos de demostración) que son muy útiles para escribirlas.

1.4.1. Conceptos básicos

El primer paso para demostrar "si P, entonces Q" es verdadero consiste en identificar cual es el enunciado P y cual es Q. En general, todo lo que esta después de la palabra "si" y antes de la palabra "entonces" es P (hipótesis). Todo lo que esta después de la palabra "entonces" es Q (conclusión). Recuérdese las formas equivalentes para sacar las hipótesis y conclusiones de una proposición.

1.4.2. Método directo (retroceder-avanzar)

PROCESO RETROCEDER: Comenzamos haciendo una pregunta abstracta (o pregunta clave) ¿Cómo o cuando puedo concluir que Q es verdadero?. Este proceso consiste en determinar un enunciado Q_1 de manera que Q sea verdadero como resultado de que Q_1 sea verdadero:

$$Q_m \Rightarrow \cdots \Rightarrow Q_2 \Rightarrow Q_1 \Rightarrow Q.$$

PROCESO AVANZAR: Este proceso consiste en derivar, a partir del enunciado P, que suponemos verdadero, otro enunciado P_1 que sea verdadero como resultado que P es verdadero.

$$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow P_n.$$

Los enunciados derivados a partir de P pueden ser muchos y variados, pero estaremos interesados en aquellos que parezcan acercarnos al último enunciado Q_m que obtuvimos en el proceso retroceder.

Terminamos la demostración si $P_n \Rightarrow Q_m$.

Se ilustra este proceso de retroceder-avanzar en la figura 1.1, queremos llegar a Q desde P, para esto es útil ver los posibles caminos comenzando de Q que me pueden servir, luego se observa desde P como podemos llegar a los caminos ya analizados que me llevan a mi objetivo Q.

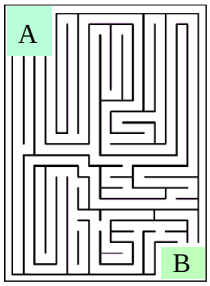


Figura 1.1: Laberinto.

Considérese el siguiente ejemplo.

Proposición 1.16. *Sea ABC un triángulo rectángulo cuyos catetos tienen longitudes a y b e hipotenusa c. Si el área es $\frac{c^2}{4}$, entonces el triángulo ABC es isósceles.*

Analisis de la demostración.

- **P:**(Hipótesis) el triángulo rectángulo ABC tiene área $\frac{c^2}{4}$.
- **Q:**(Conclusión) el triángulo ABC es isósceles.

Afirmación	Justificación
P : El área de ABC es $\frac{c^2}{4}$	Hipótesis
$P_1 : \frac{1}{2}ab = \frac{1}{4}c^2$	Área=$\frac{1}{2}$(base)(altura)
$P_2 : a^2 + b^2 = c^2$	Teorema de Pitágoras
$P_3 : \frac{1}{2}ab = \frac{1}{4}(a^2 + b^2)$	Se sustituye P_2 en P_1
$P_4 : a^2 - 2ab + b^2 = 0$	A partir de P_3 por álgebra
$P_5 : (a - b)^2 = 0$	Se factoriza P_4
$Q_2 : a - b = 0$	A partir de P_5 por álgebra
$Q_1 : a = b$	Sumando b a ambos lados de Q_2
Q : ABC es isósceles	Por que Q_1 es verdadera

Lectura de Demostraciones. Por tiempo y espacio no es práctico escribir las demostraciones con tanto detalle, aquí muchas veces escribimos una versión condensada de la demostración con el cuidado de dar suficientes explicaciones para comprender la lectura. El comprender una demostración depende en buena parte de saber el razonamiento lógico que se sigue, es decir, el método de demostración que se esta utilizando y el resto manejar conceptos y resultados.

Una demostración condensada de la proposición anterior es:

Demostración. Por el teorema de Pitágoras tenemos $a^2 + b^2 = c^2$ y sabemos que $\frac{1}{2}ab = \frac{1}{4}c^2$, así tenemos $\frac{1}{2}ab = \frac{1}{4}(a^2+b^2)$ y de aquí obtenemos $(a-b)^2 = 0$, es decir, $a = b$. Por lo tanto, los catetos son iguales. □

1.4.3. Método de reducción al absurdo

La efectividad del método directo con sus procesos retroceder-avanzar, no siempre conducen a una demostración exitosa, por lo que es imperioso ver otra formas de demostrar $P \Rightarrow Q$.

¿Cómo y cuando se hace uso el método de reducción al absurdo? Se inicia siempre suponiendo que P es verdadero, pero para llegar a la conclusión que Q es verdadero, se procede formulando la pregunta: "¿Por qué Q no puede ser falso?", la idea de una demostración por este método es suponer que P es verdadero y que Q es falso, y ver porque esto no puede ocurrir, es decir, llegar a una contradicción en un enunciado cuya falsedad esté absolutamente fuera de duda (ejemplos: 2=4, $\sin(x) = 5$, etc). La gran pregunta ¿Cual contradicción es la que busca? no hay criterios específicos, cada problema da lugar a su propia contradicción, se requiere creatividad e ingenio para encontrarla.

En general, utilizaremos este método cuando la negación de Q nos proporcione información útil, es decir, cuando $\sim Q$ sea un enunciado del cual tengamos mas información que de Q. Este método lo explicaremos con un ejemplo concreto más adelante (ejemplo 2.31).

Con el método de reducción al absurdo queremos demostrar: **si** P **y** $\sim Q$ **entonces** C **(contradicción)**, que es una implicación como en el método directo con hipótesis P y $\sim Q$ y conclusión C, pero al no saber cual es la contradicción buscada no podemos utilizar el proceso retroceder sino solo el de avanzar.

1.4.4. Método del Contrapositivo (contrarrecíproco).

Ya hemos visto que $P \Rightarrow Q$ es equivalente a $\sim Q \Rightarrow \sim P$, es decir, el método consiste en probar la segunda implicación para demostrar la primera. También, podemos analizar este método como un caso particular del reducción al absurdo, tomamos como verdaderos a P y $\sim Q$ y buscamos a partir de $\sim Q$ llegar a $\sim P$, con esto, hemos encontrado una contradicción totalmente evidente $P \wedge (\sim P)$.

Ejemplo 1.17. *Demostrar que si* $2x - 6 \neq 0$*, entonces* $x \neq 3$*.*

Observar la siguiente equivalencia lógica

$$\textit{si } \underbrace{2x - 6 \neq 0}_{P}\textit{, entonces } \underbrace{x \neq 3}_{Q} \iff \textit{si } \underbrace{x = 3}_{\sim Q}\textit{, entonces } \underbrace{2x - 6 = 0}_{\sim P}.$$

Para demostrar $P \Rightarrow Q$*, probaremos* $\sim Q \Rightarrow \sim P$*. Lo cual solo requiere una simple sustitución: en efecto, por hipótesis* $x = 3$*, entonces* $2x - 6 = 2 \cdot 3 - 6 = 6 - 6 = 0$*, como queríamos probar.*

Muchas veces este método se usa cuando una proposición está enunciada en forma negativa (como el ejemplo anterior), y en otros casos no es fácil darse cuenta que este método es el correcto, como veremos más adelante en los ejercicios.

1.4.5. Demostración por Casos

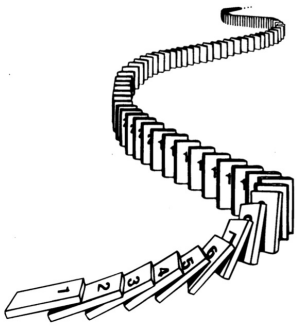
Es común que durante la demostración de una proposición lleguemos a un punto donde sea natural que el argumento sea dividido en un número finito de casos, o posiblemente desde el inicio de la misma nos veamos obligados a separar en casos. Cuando queremos probar una propiedad sobre un número real x puede que convenga utilizar la propiedad de tricotomía y separar en tres casos: $x < 0$, $x = 0$ y $x > 0$. Veremos más adelante que para demostrar una propiedad sobre un entero n es ventajoso considerar los residuos en la división por otro.

La separación por casos tiene dos propiedades muy importantes. La primera es que los casos son *exhaustivos*: todas las instancias del problema cumplen con al menos uno de los casos, es decir, todas las posibilidades son cubiertas por los casos listados. *Esta es una propiedad que debe cumplir toda división en casos de un argumento para que la demostración sea válida*. La segunda es que los casos son *mutuamente excluyentes*: todas las instancias del problema son cubiertas por a lo sumo uno de los casos. Aunque esta última no es indispensable que la cumpla, es preferible siempre que se pueda hacerlo de esa manera.

1.4.6. Inducción Matemática

Este método de demostración consiste esencialmente en aplicar cualquiera de los dos principios 1.9 o 1.10 de inducción matemática que hemos dado, ilustraremos este método de demostración con un ejemplo más adelante (ejemplo 2.15).

La idea intuitiva del método consiste en que si tuviéramos un arreglo infinito de piezas de dominó (ver la siguiente figura) si la primera pieza de dominó cae, y si cualquiera al caer hace caer a la siguiente, entonces todas caen.



EJERCICIOS

Ejercicio 1.1. *Diga cuales de las siguientes, son proposiciones:*

[A] $6x^2 - 3x + 9 = 0$

[B] *Para todo ángulo* θ, $\sin^2(\theta) + \cos^2(\theta) = 1$

Ejercicio 1.2. *Determinar el valor de verdad de cada proposición:*

[A] *La raíz cúbica de todo número entero es un número real.*

[B] $(\forall x, y \in \mathbb{R})(x^2 + y^2 > 1)$

[C] $(\exists x, y \in \mathbb{R})(x^2 + y^2 > 1)$

[D] $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x^2 + y^2 < 1)$

Ejercicio 1.3. *Demuestre mediante tablas de verdad que:*

[A] $P \Leftrightarrow Q \iff (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

[B] $P \Rightarrow (Q \Rightarrow R)$

Ejercicio 1.4. *En cada caso identificar la hipótesis y la conclusión:*

[A] *Si* $r \in \mathbb{R}$ *y* $r^2 = 2$*, entonces* r *es un número irracional.*

[B] *Dos triángulos son semejantes cuando tienen proporcionales sus tres lados.*

[C] f *es una función continua cuando* f *es derivable.*

Ejercicio 1.5. *Si se quiere demostrar que* $P \Rightarrow Q$ *es verdadero y se sabe que* Q *es falso, ¿querría probarse que* P *es verdadero o falso? Explique la respuesta.*

Ejercicio 1.6. *Demostrar la falsedad de las siguientes proposiciones:*

[A] *Toda ecuación de la forma* $ax^2 + bx + c = 0$ *donde* a*,* b *y* c *son números reales tiene al menos una solución real.*

[B] *Sean* w *y* z *dos números reales con* $w \neq 2$*. Si* $z^3w^4 = 16z^3$*, entonces* $z = 0$*. Sugerencia: encontrar el error en la siguiente demostración.*

Demostración. Supongamos que $z^3w^4 = 16z^3$, de donde $z^3(w^4 - 16) = 0$. Ya que $w \neq 2$, entonces $w^4 \neq 16$, por lo que $w^4 - 16 \neq 0$. Entonces podemos dividir a ambos lados de la ecuación por $w^4 - 16$, lo que nos lleva a la conclusión que $z^3 = 0$ y, por lo tanto, a que $z = 0$. □

Ejercicio 1.7. *Demostrar que:*

[A] *Si* x*,* y *y* z *son tres enteros consecutivos, entonces 9 divide a la suma de sus cubos.*

[B] *Si* a*,* b *y* c *son números reales para los que* $a > 0$*,* $b < 0$ *y* $b^2 - 4ac = 0$*, entonces la solución de la ecuación* $ax^2 + bx + c = 0$ *es positiva.*

[C] *Si* x *es un número racional y* y *es un número irracional, entonces* $x + y$ *es un número irracional.*

[D] *Si* p *y* q *son números reales positivos y* $\sqrt{pq} \neq (p + q)/2$*, entonces* $p \neq q$.

[E] *Si* a *y* b *son números reales positivos y* $a \neq b$*, entonces* $(a + b)/2 > \sqrt{ab}$.

[F] *Si* x *y* y *son números reales, entonces* $\min(x, y) = \frac{1}{2}(x + y - |x - y|)$ *y* $\max(x, y) = \frac{1}{2}(x + y + |x - y|)$.

[G] *Para todo número entero* $n \geq 1$ *se verifica que,* $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

[H] *Para todo número entero* $n \geq 5$ *se verifica que* $2^n > n^2$.

Lectura complementaria:
Estrategias de Resolución de Problemas Matemáticos [7, Capitulo 0].

2 | Divisibilidad

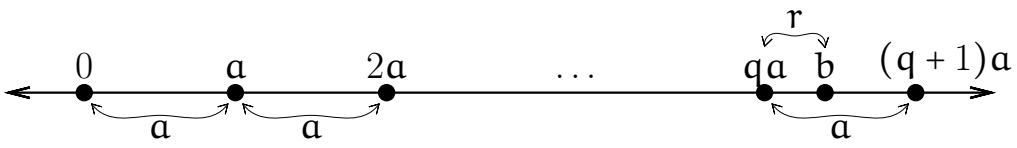
2.1. Lema de la división

Todos hemos aprendido junto con las operaciones aritméticas básicas a efectuar la división entera de dos números naturales, así que podemos determinar el cociente y el residuo de la división de un número natural b por otro número natural a. Ahora enunciamos y demostramos el Lema de la división el cual formaliza matemáticamente la división de números enteros.

Lema 2.1 (Lema de la división)**.** *Para cada par de enteros* $a \neq 0$ *y* b*, existe un único par de enteros* q *y* r *satisfaciendo:* $b = aq + r$ *y* $0 \leq r < |a|$*. A los enteros* b*,* a*,* q *y* r *los llamaremos respectivamente* **dividendo***,* **divisor***,* **cociente** *y* **residuo** *de la división entera de* b *por* a*.*

Demostración. Primero demostraremos la *existencia* de los enteros q y r, por simplicidad consideraremos sólo el caso $a > 0$ y $b \geq 0$. Los demás casos pueden deducirse de éste fácilmente (ver el ejercicio 2.1). Consideremos todos los múltiplos no negativos de a: $0, a, 2a, 3a, \ldots$

Sea $q \cdot a$ el mayor múltiplo de a tal que $qa \leq b$, es decir b se encuentra entre qa y $(q+1)a$ en la recta numérica (permitiéndose el caso en que $b = qa$). Definimos $r := b - qa$.



Entonces $b = qa + r$, como la distancia entre dos múltiplos consecutivos de a es $|a|$ (en este caso $|a| = a$), tenemos que $0 \leq r < |a|$, como queríamos.

Segundo demostraremos la *unicidad* de los enteros q y r. Supongamos que existen dos pares de enteros q_1, r_1 y q_2, r_2 los cuales respectivamente satisfacen $b = q_1a + r_1$, $b = q_2a + r_2$ y $0 \leq r_1, r_2 < |a|$.

Comprobaremos que $q_1 = q_2$ y $r_1 = r_2$, supongamos que $q_2 > q_1$, entonces

$$0 = b - b = (q_2a + r_2) - (q_1a + r_1) = (q_2 - q_1)a - (r_1 - r_2),$$

de donde $r_1 - r_2 = (q_2 - q_1)a \geq a$, lo cual claramente es una contradicción, pues $r_1 - r_2 < a$, (el caso $q_1 > q_2$ es análogo). Por lo tanto $q_1 = q_2$ y de esto sigue que $r_1 = r_2$. □

Observar que en el lema de la división el dividendo y divisor pueden ser positivos o negativos, para cada uno de estos casos ilustramos en el siguiente ejemplo como proceder para determinar el cociente y residuo de la división.

Ejemplo 2.2. *Encontrar el cociente* q *y residuo* r *cuando se realizan las siguientes divisiones:*

[A] $b = 7$ *entre* $a = 3$ **[B]** $b = 7$ *entre* $a = -3$ **[C]** $b = -7$ *entre* $a = 3$ **[D]** $b = -7$ *entre* $a = -3$

Resolución. **[A]** *Para encontrar el cociente y residuo cuando el dividendo y divisor son positivos, se divide como es habitual. Al efectuar la división en este caso se obtiene como cociente* $q = 2$ *y residuo* $r = 1$*, así* $7 = 3 \cdot 2 + 1$*.*

Veamos ahora los otros casos (cuando dividendo o divisor son negativos), los mas práctico es hacer la división con los valores positivos $|a|$ *y* $|b|$ *y luego adaptar el resultado.*

Sabemos que $7 = 3 \cdot 2 + 1$.

[B] *Observemos que también se cumple que* $7 = -3 \cdot (-2) + 1$, *y así el cociente es* $q = -2$ *y residuo* $r = 1$.

[C] *Del literal anterior tenemos que* $7 = -3 \cdot (-2) + 1$, *multiplicando por* -1 *esta igualdad, tenemos que* $-7 = 3(-2) - 1$, *pero* -1 *no puede ser el residuo, pues no cumple la condición* $0 \leq r < |a|$, *entonces sumamos y restamos* 3 *en el lado derecho de la igualdad para obtener que* $-7 = 3(-2) - 1 + 3 - 3$, *y asociando adecuadamente* $-7 = 3 \cdot (-3) + 2$, *por tanto* $q = -3$ *y* $r = 2$.

[D] *Cambiando un signo de lugar en la división anterior se obtiene que* $-7 = -3 \cdot 3 + 2$, *así* $q = 3$ *y* $r = 2$.

Comparamos los cuatro casos

[A] $b = 7$ *entre* $a = 3$

$$\begin{array}{r|l} 7 & 3 \\ \hline 1 & 2 \end{array}$$

$\Rightarrow 7 = 3 \cdot 2 + 1$

[B] $b = 7$ *entre* $a = -3$

$$\begin{array}{r|l} 7 & -3 \\ \hline 1 & -2 \end{array}$$

$\Rightarrow 7 = -3 \cdot (-2) + 1$

[C] $b = -7$ *entre* $a = 3$

$$\begin{array}{r|l} -7 & 3 \\ \hline 2 & -3 \end{array}$$

$\Rightarrow -7 = 3 \cdot (-3) + 2$

[D] $b = -7$ *entre* $a = -3$

$$\begin{array}{r|l} -7 & -3 \\ \hline 2 & 3 \end{array}$$

$\Rightarrow -7 = -3 \cdot 3 + 2$

Observar que en los casos A, B y C, D los residuos son iguales, los cocientes son números opuestos (respecto a la suma) y además difieren en una unidad. Esto puede demostrarse en general ver ejercicio **[2.7]**.

EJERCICIOS

Ejercicio 2.1. *En cada uno de los siguientes casos encontrar el cociente* q *y residuo* r *de la división* b *por* a.

[A] $b = 20$; $a = 6$ **[B]** $b = 20$; $a = -6$ **[C]** $b = -20$; $a = 6$ **[D]** $b = -20$; $a = -6$.

Ejercicio 2.2. *Sabiendo que el resto de la división de un entero* b *por* 7 *es* 5, *calcular el resto de la división por* 7 *de los números siguientes:*

[A] $-b$ **[C]** $3b + 7$ **[E]** $-b + 1$ **[G]** $b^2 + b + 1$

[B] $2b$ **[D]** $10b + 1$ **[F]** $7b + 1$ **[H]** b^3

Ejercicio 2.3. *¿Cuáles de los siguientes conjuntos son iguales?*

$A := \{17 + 157t : t \in \mathbb{Z}\}$ $C := \{-768 + 157t : t \in \mathbb{Z}\}$ $E := \{51 - 157t : t \in \mathbb{Z}\}$

$B := \{1744 + 157t : t \in \mathbb{Z}\}$ $D := \{100 - 157t : t \in \mathbb{Z}\}$ $F := \{-57 + 157t : t \in \mathbb{Z}\}$

Dos conjuntos X *y* Y *son iguales (*$X = Y$*) si y sólo si* $X \subseteq Y$ *(i.e.* $\forall x \in X \Rightarrow x \in Y$*) y* $Y \subseteq X$ *(i.e.* $\forall y \in Y \Rightarrow y \in X$*).*

Ejercicio 2.4. ☺ *Encontrar el mayor número natural con la propiedad de tener el mismo cociente al ser dividido por* 144 *que al ser dividido por* 120.

Ejercicio 2.5. *La suma de dos números enteros es* 240. *Si se divide el mayor por el menor el cociente es* 3 *y el residuo es* 8. *Encontrar los dos números enteros.*

Ejercicio 2.6. *Al realizar la división entre dos números enteros se obtiene como cociente* 8 *y residuo* 3. *Encontrar dichos números si el producto de ambos es* 121401.

Ejercicio 2.7. *Sean a y b enteros positivos. Demostrar que cuando dividimos b por a y b por $-a$ se obtiene el mismo residuo y cocientes opuestos. Al igual que cuando dividimos $-b$ por a y $-b$ por $-a$. Además esos cocientes difieren en una unidad.*

Lectura complementaria:
Revisar la solución al problema de aritmética [7, Problema 1.31].

2.2. Operadores aritméticos $\%$ y $\backslash$

Ya conocemos algunos operadores binarios aritméticos: $+$ (suma), $-$ (resta), $\cdot$ (multiplicación) y $/$ (división), ahora definimos otros dos operadores binarios $\%$ y $\backslash$, estos son utilizados en computación para encontrar residuos y cocientes. Se definen de la siguiente manera:

$$b\backslash a =: q \qquad \text{(cociente cuando } b \text{ se divide por } a\text{)}$$
$$b\,\%a =: r \qquad \text{(residuo cuando } b \text{ se divide por } a\text{)}$$

El Lema de la división dice que $b = aq + r$ y de acuerdo a lo anterior

$$b/a = q + r/a, \text{ donde } 0 \le r/a < 1.$$

Por lo tanto $q = b\backslash a = \lfloor b/a \rfloor$[1] y $r = b\,\%a = b - aq = b - a \cdot \lfloor b/a \rfloor$. También es habitual denotar por $r_a(b)$ el residuo de b en la división por a.

Por ejemplo: $23\backslash 5 = 4$ y $23\,\%5 = 3$, $-23\backslash 5 = -5$ y $-23\,\%5 = 2$. En lo que sigue veremos algunas aplicaciones de estos operadores junto con el Lema de la división.

Ejemplo 2.3. *Un número entero se llama **par** si al dividirlo por 2 el residuo es 0 e **impar** si al dividirlo por 2 el residuo es 1, construir las tablas para las operaciones suma y producto de números pares e impares.*

Resolución. *Sea n_1 y n_2 dos números pares y m_1 y m_2 dos números impares, de acuerdo a la definición y al Lema de la división existen enteros q_1, q_2, q_3 y q_4 tales que $n_1 = 2q_1$, $n_2 = 2q_2$, $m_1 = 2q_3 + 1$ y $m_2 = 2q_4 + 1$ resumimos todos los resultados posibles de sumar y multiplicar números pares e impares en las siguientes tablas*

$+$	*par*	*impar*
par	*par*	*impar*
impar	*impar*	*par*

Adición / Suma

$\cdot$	*par*	*impar*
par	*par*	*par*
impar	*par*	*impar*

Multiplicación / Producto

Observación 2.4. *En aritmética es habitual decir que los números son de alguna "**forma**" en particular. Por ejemplo, "los números pares son de la forma $2k$ y los impares son de la forma $2k + 1$".*

[1] La función **parte entera** o **mayor entero** de un número real x se denota por $\lfloor x \rfloor$ y se define como:

$$\lfloor x \rfloor := \text{ el } \textit{mayor entero} \text{ que es menor o igual a } x$$
$$= \begin{cases} x & x \in \mathbb{Z} \\ x - \dfrac{1}{2} - \dfrac{1}{\pi}\arctan(\tan(\pi x)) & x \notin \mathbb{Z} \end{cases}$$

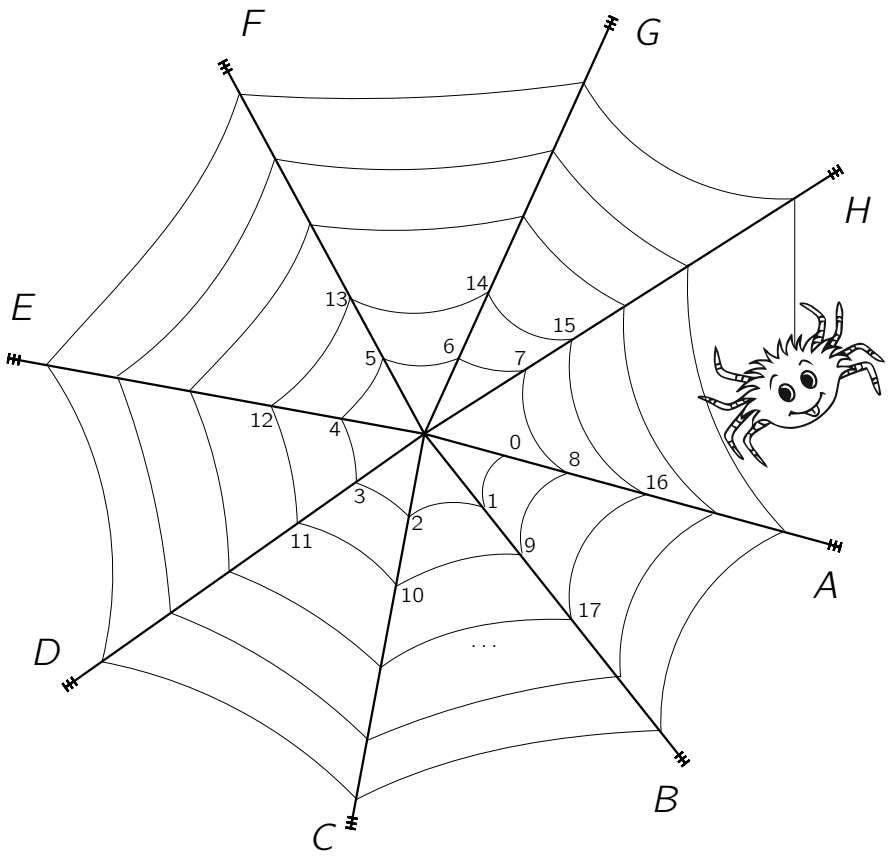
Actividad 2.5. *Sea* $\mathfrak{n}$ *un número entero positivo, utilizar el Principio del palomar y el Lema de la división para demostrar que*

[A] *el producto de* $\mathfrak{n}$ *(o más) números enteros consecutivos es divisible por* $\mathfrak{n}$*.*

[B] *al escribir una lista con más de* $\mathfrak{n}$ *números enteros cualesquiera, al menos dos de ellos dejan el mismo residuo en la división por* $\mathfrak{n}$*.*

[C] *al escribir una lista con* $\mathfrak{n}+1$ *números enteros cualesquiera, la diferencia de dos de ellos es divisible por* $\mathfrak{n}$*.*

Actividad 2.6 (Variante del Problema 1, Séptimo grado. XV ONM)**.** *La señora Materácnida es una araña matemática. Ella ha comenzado a tejer una telaraña en una base de ocho hilos* A*,* B*, . . .,* H *como lo indica la figura, utilizando la notación de los operadores* $\%$ *y* $\setminus$ *definidos anteriormente, responder las siguientes cuestiones.*



[A] *Se observa que comienza por el hilo* A *y que después de tejer* 6 *lados se encuentra en el hilo* G*, después de tejer* 11 *lados más se encuentra en el hilo* B*, siguiendo con el patrón ¿en cuál hilo estará la señora Materácnida después de tejer* 2015 *lados?*

[B] *¿En cuál hilo estará después de tejer* 2015^2 *y* 2015^3 *lados?*

[C] *¿Cuántas vueltas habrá dado después de tejer* 2015*,* 2015^2 *y* 2015^3 *lados? (entiéndase por "vueltas" la cantidad entera de veces que ha pasado por el hilo donde comenzó a tejer)*

[D] *La señora Materácnida ha decidido construir una nueva telaraña con una base de ocho hilos, pero esta vez comenzando por el hilo* F. *¿En cuál hilo estará después de tejer* 2015, 2015^2 *y* 2015^3 *lados?*

[E] *Para cualquier número natural* n *explicar procedimientos y dar expresiones que determinen cuántas vueltas ha dado y en qué hilo estará Materácnida después de tejer* n *lados.*

[F] *¿Puede mencionar al menos dos propiedades que caracterizan a los números naturales que están en cada hilo?*

EJERCICIOS

Ejercicio 2.8. *Sean* M *y* n *números naturales. Determinar cuántos múltiplos de* n *hay entre* 1 *y* M.

Ejercicio 2.9. *Muestre que si* $\mathrm{n} \in \mathbb{N}$ *es un número impar, entonces el residuo de dividir* n^2 *por 8 es 1.*

Ejercicio 2.10. *Demostrar que:*

[A] *Un número entero* n^2 *es impar siempre que* n *es impar.*

[B] *Un número entero* n *es par si y sólo si* n^2 *es par.*

Ejercicio 2.11. *Demostrar que si* a *y* b *son enteros, y* b *es impar, entonces* $+1$ *y* -1 *no son raíces de* $\mathrm{a}\mathrm{x}^2+\mathrm{b}\mathrm{x}+\mathrm{a}$.

2.3. Divisibilidad

Sabemos que el resultado de la suma, diferencia y producto de dos números enteros es de nuevo otro número entero, es decir, las operaciones adición, sustracción y multiplicación son cerradas en $\mathbb{Z}$, la división de dos números enteros puede ser o no un número entero, lo que permite hablar de números divisibles y no divisibles.

El Lema de la división afirma que para cada par de enteros $\mathrm{a} \neq 0$ y b existe un único par de enteros q y r tales que $\mathrm{b} = \mathrm{a}\mathrm{q} + \mathrm{r}$. En el caso particular que $\mathrm{r} = 0$ decimos que la división de b por a es exacta, pues existe un (único) número entero q tal que $\mathrm{b} = \mathrm{a}\mathrm{q}$. Convendremos en decir que a **divide a** b si existe un único número entero q tal que $\mathrm{b} = \mathrm{a}\mathrm{q}$, y escribiremos $\mathrm{a} \mid \mathrm{b}$ para indicar que "a divide a b" y $\mathrm{a} \nmid \mathrm{b}$ para indicar "a no divide a b" (cuando el residuo de la división de b por a es distinto de cero). Para decir que "a divide a b" también se utilizan indistintamente otros conceptos equivalentes, tales como "b **es divisible por** a", "b **es múltiplo de** a", "a **es un divisor de** b" ó "a **es factor de** b".

Nota 2.7. *Cuidado al escribir los símbolos* /, | *y* \, *cada uno se interpreta de forma diferente, por ejemplo* $2/5 = 0.4$, $2 \mid 5$ *es falso y* $2\backslash 5 = 0$, *de hecho los símbolos* / *y* \ *devuelven valores numéricos, mientras que* | *valores lógicos (Verdadero o Falso).*

Dado un entero positivo n, diremos que d es un **divisor positivo propio** si $\mathrm{d} \mid \mathrm{n}$ y $1 < \mathrm{d} < \mathrm{n}$, nos referiremos como **divisores triviales** de n a los casos $\mathrm{d} = \pm 1, \pm \mathrm{n}$.

El Lema de la división es un procedimiento que permite decidir si a divide a b, hemos resumido las propiedades siguientes para estudiar las consecuencias prácticas y teóricas que tienen.

Propiedades 2.8 (Propiedades de divisibilidad)**.** *Sean* $\mathrm{a} \neq 0$, b, c, d, m, x *y* y *números enteros*

[A] $1 \mid \mathrm{a}$, $\mathrm{a} \mid 0$

[B] *Si* $\mathrm{a} \mid \mathrm{b}$, *entonces* $\mathrm{a} \mid \mathrm{b}\mathrm{c}$

[C] *Si* $c \neq 0$*, entonces* $ac \mid bc$ *si y sólo si* $a \mid b$ *(Propiedad de simplificación)*

[D] $a \mid a$ *(Propiedad reflexiva)*

[E] *Si* $b \neq 0$*,* $a \mid b$ *y* $b \mid c$*, entonces* $a \mid c$ *(Propiedad transitiva)*

[F] *Si* $a \mid b$ *entonces* $|a| \leq |b|$ *(Propiedad de comparación)*

[G] *Si* $a \mid b$ *y* $a \mid c$*, entonces* $a \mid bx \pm cy$*, para cualesquiera números enteros* x *y* y *(Propiedad de linealidad)*

[H] *Si* $a \mid b$ *y* $c \mid d$*, entonces* $ac \mid bd$ *(Propiedad de multiplicación)*

[I] *Si* $m \neq 0$*,* $m \mid (a - b)$ *y* $m \mid (c - d)$*, entonces* $m \mid (ac - bd)$

[J] *Si* $b \neq 0$*,* $a \mid b$ *y* $b \mid a$*, entonces* $a = \pm b$.

Demostración. Demostraremos únicamente las propiedades **[C]**, **[G]** y **[I]** dejando las demostraciones de las otras propiedades como ejercicio.

[C] "*Solo si.*" En efecto, supongamos que $ac \mid bc$. Entonces, existirá un entero q tal que

$$bc = acq \Rightarrow (b - aq)c = 0$$

pero $c \neq 0$ y $\mathbb{Z}$ no tiene divisores de cero, luego

$$b - aq = 0 \Leftrightarrow b = aq, \text{ con } q \in \mathbb{Z}$$

es decir,

$$a \mid b$$

"*Si.*" En efecto, si $a \mid b$, se sigue que $ac \mid bc$.

[G] Como $a \mid b$ y $a \mid c$, por definición existen respectivamente números enteros m y n tales que $b = am$ y $c = an$, como x y y son cualesquiera números enteros multiplicamos respectivamente las ecuaciones anteriores por x y y y las sumamos miembro a miembro, obteniendo $bx + cy = amx + any = a(mx + ny)$, como $mx + ny \in \mathbb{Z}$, concluimos que $a \mid bx + cy$.

[I]

$$\left.\begin{array}{c} m \mid a - b \Rightarrow m \mid ac - bc \\ \text{y} \\ m \mid c - d \Rightarrow m \mid bc - bd \end{array}\right\} \quad \Rightarrow \quad m \mid (ac - bc) + (bc - bd) \quad \Rightarrow \quad m \mid ac - bd.$$

□

Definición 2.9. *Cuando* x *y* y *son números enteros, llamaremos a la expresión* $bx \pm cy$ ***combinación lineal*** *de* b *y* c*.*

La definición anterior justifica el nombre de la propiedad **[G]**.

Ejemplo 2.10. *Sean* a *y* b *dos números enteros positivos. Probar que si* $b \mid a$ *y* $b \mid (a + 2)$*, entonces* $b = \pm 1$ *ó* $b = \pm 2$*.*

Resolución. *Por la propiedad* **[G]**

$$\left.\begin{array}{l} b \mid a \\ \wedge \\ b \mid a + 2 \end{array}\right\} \Rightarrow b \mid a + 2 - a \Rightarrow b \mid 2 \Rightarrow b = \pm 1 \text{ ó } b = \pm 2$$

Ejemplo 2.11. *Sea* n *un entero. Encontrar todos los enteros positivos* d *tales que* $d \mid n^2+1$ *y* $d \mid (n+1)^2+1$.

Resolución. *Si* $d \mid n^2+1$ *y* $d \mid (n+1)^2+1$, *entonces* $d \mid n^2+2n+2$. *Entonces* $d \mid n^2+2n+2-(n^2+1)$, *es decir,* $d \mid 2n+1 \Rightarrow d \mid 4n^2+4n+1$, *entonces* $d \mid 4(n^2+2n+2)-(4n^2+4n+1)$, *así* $d \mid 4n+7$. *Entonces* $d \mid (4n+7)-2(2n+1)$, *es decir* $d \mid 5$, *entonces* d *puede ser solamente* 1 *o* 5. *Tomando* $n=2$ *vemos que ambos valores cumplen las condiciones requeridas.*

Ejemplo 2.12. *Sean* x *y* y *enteros. Demostrar que* $2x+3y$ *es divisible por* 17 *si y sólo si* $9x+5y$ *es divisible por* 17.

Resolución. $17 \mid 2x+3y \Rightarrow 17 \mid 13(2x+3y)$ *o* $17 \mid 26x+39y \Rightarrow 17 \mid 9x+5y$. *Recíprocamente,* $17 \mid 9x+5y \Rightarrow 17 \mid 4(9x+5y)$ *o* $17 \mid 36x+20y \Rightarrow 17 \mid 2x+3y$.

EJERCICIOS

Ejercicio 2.12. *Responder Verdadero o Falso a las siguientes cuestiones:*

[A] $-1 \mid a$

[B] *Si* $a \mid b$ *entonces* $a \mid -b$

[C] $a \mid 0$

[D] *Si* $a \mid b$ *y* $b \mid a$ *entonces* $a = b$

[E] *Si* $a \mid b$ *entonces* $a < b$

[F] *Si* $a < b$ *entonces* $a \mid b$

[G] *Si* $c \mid a$ *y* $b \mid c$ *entonces* $b \mid a$

[H] *Si* $a \nmid b$ *entonces* $b \nmid a$.

[I] *Si* $a^2 = b^2$ *entonces* $a = b$

[J] *Si* $a \mid b+c$ *entonces* $a \mid b$ *y* $a \mid c$

[K] *Si* $a \mid b+c$ *entonces* $a \mid b$ *o* $a \mid c$

[L] *Si* $a \mid b \cdot c$ *entonces* $a \mid b$ *y* $a \mid c$

[M] $a \mid b \cdot c$ *entonces* $a \mid b$ *ó* $a \mid c$.

[N] $a \mid b$ *y* $b \mid a$ *entonces* $a = b$

[Ñ] $a \mid b^2$ *entonces* $a \mid b$

[O] $a \mid b$ *y* $c \mid b$ *entonces* $a \cdot c \mid b$

[P] $a \mid a+b$ *entonces* $a \mid b$

[Q] $a \mid a^2$

[R] $a^2 \mid b^2$ *entonces* $a \mid b$

[S] $a \mid b^2$ *entonces* $a^2 \mid b^2$

[T] $a^2 \mid b^3$ *entonces* $a \mid b$.

Ejercicio 2.13. *Para cada una de las proposiciones siguientes, indicar su valor de verdad: Verdadero (V) o Falso (F), en el caso V dar una demostración y para el caso F dar un contrajemplo:*

[A] *Si un número entero es divisible por* 6 *entonces es divisible por* 3

[B] *Si un número entero es divisible por* 6 *entonces no es divisible por* 3

[C] *Si un número entero no es divisible por* 6 *entonces no es divisible por* 9

[D] *Si un número entero es divisible por* 3 *entonces es divisible por* 6

[E] *Si un número entero no es divisible por* 6 *entonces no es divisible ni por* 3 *ni por* 2

[F] *Si un número entero es par su cuadrado es par*

[G] *Si el cuadrado de un número entero es par el número entero es par*

[H] *Un número entero es par si y sólo si es divisible por* 4

[I] *Un número entero es par si y sólo sí es divisible por* 2 *ó por* 3

[J] *Un número entero es divisible por* 6 *si y sólo si es divisible por* 2 *o por* 3

[K] *Si el producto de dos números enteros es par entonces a lo sumo uno de los números enteros es par*

[L] *Si el producto de dos números enteros es un cuadrado entonces uno de los números enteros es un cuadrado.*

Ejercicio 2.14. *Probar que si* $k \mid a$ *y* $k \mid b$ *entonces* $k \mid (2a + b)$ *y* $k \mid (a - 3b)$.

Ejercicio 2.15. *Encontrar los números enteros* x *tales que:*

[A] $x - 1 \mid x^3 - 1$

[B] $x + 7 \mid 4x + 33$

[C] $x + 1 \mid x^2 + 5x + 11$

Ejercicio 2.16. *Sea* $a \in \mathbb{N}$. *Calcular los posibles residuos al dividir* a^m *por* 7, *para* $m = 1, 2, 3$ *y* 7, *y comprobar los resultados siguientes:*

[A] $7 \mid a^7 - a$.

[B] $7 \mid a^2 + b^2 \Rightarrow 7 \mid a$ *y* $7 \mid b$.

[C] $7 \mid a^3 + b^3 + c^3 \Rightarrow 7 \mid abc$.

Ejercicio 2.17. *Usando el lema de la división demostrar que si* $3 \mid a^2 + b^2 \Rightarrow 3 \mid a$ *y* $3 \mid b$, *donde* $a, b \in \mathbb{Z}$.

Ejercicio 2.18. *Si* p, q *y* r *son tres enteros consecutivos, entonces 24 no divide a* $p^2 + q^2 + r^2 + 1$.

Ejercicio 2.19. *Demostrar las propiedades* **[2.8]**

Ejemplo 2.13. *Pruébese que si* a *y* b *son números enteros positivos e impares, entonces* 2 *divide a* $a^2 + b^2$ *pero* 4 *no divide a* $a^2 + b^2$.

Resolución.

$$\left.\begin{array}{l} a \in \mathbb{Z}^+ \\ a \text{ impar} \end{array}\right\} \Rightarrow a = 2p - 1, \text{ con } p \in \mathbb{Z}^+$$

$$\left.\begin{array}{l} b \in \mathbb{Z}^+ \\ b \text{ impar} \end{array}\right\} \Rightarrow b = 2q - 1, \text{ con } q \in \mathbb{Z}^+$$

Entonces,

$$a^2 + b^2 = (2p - 1)^2 + (2q - 1)^2 = 4p^2 - 4p + 1 + 4q^2 - 4q + 1 = 2(2p^2 + 2q^2 - 2p - 2q + 1)$$

siendo $2p^2 + 2q^2 - 2p - 2q + 1$ *entero, luego* $2 \mid a^2 + b^2$.

Veamos ahora que $4 \nmid a^2 + b^2$. *En efecto, razonamos por contradicción suponiendo que* $4 \mid a^2 + b^2$. *Como* $4 \mid 4(p^2 - p + q^2 - q)$, *entonces* $4 \mid a^2 + b^2 - 2$. *De donde*

$$\left.\begin{array}{l} 4 \mid a^2 + b^2 \\ y \\ 4 \mid (a^2 + b^2) - 2 \end{array}\right\} \Rightarrow 4 \mid (a^2 + b^2) - [(a^2 + b^2) - 2] \Rightarrow 4 \mid 2$$

lo cual obviamente es una contradicción, y por tanto la suposición hecha no es cierta. Por lo tanto $4 \nmid a^2 + b^2$.

Ejemplo 2.14. *Demostrar que la diferencia de los cubos de dos números consecutivos no puede ser múltiplo de* 3.

Resolución. *Sea* p *un número entero arbitrario. Entonces,*

$$(p+1)^3 - p^3 = p^3 + 3p^2 + 3p + 1 - p^3 = 3(p^2+p) + 1,\ p^2 + p \in \mathbb{Z}.$$

Luego por el lema de la división se sigue que el residuo de dividir $(p+1)^3 - p^3$ *entre* 3 *es* 1, *luego* $(p+1)^3 - p^3 \neq 3k$, $\forall k \in \mathbb{Z}$, *es decir* $3 \nmid (p+1)^3 - p^3$, *así la diferencia de los cubos de dos números consecutivos no es múltiplo de* 3.

Ejemplo 2.15. *Probar que para cada* $n \geq 0$, *el número* $4^{2n+1} + 3^{n+2}$ *es múltiplo de* 13.

Resolución. *Utilizamos para la demostración el primer principio de inducción matemática. Sean* $P(1)$, $P(2)$, *. . ., proposiciones sobre el conjunto universo del discurso (los números enteros no negativos).*

"Si $P(1)$ *es verdad y de la veracidad de* $P(k)$ *se deduce la veracidad de* $P(k+1)$, *entonces la proposición* $P(n)$ *es cierta para cualquier número natural* n."

Sea $P(n) :=$ "$13 \mid 4^{2n+1} + 3^{n+2}$".

- *(Caso base) Para* $n = 0$, $4^{2\cdot 0+1} + 3^{0+2} = 4 + 9 = 13$, *es verdadero.*
- *(Hipótesis de inducción) Supongamos que* $P(n)$ *es verdadero para* $n = k$, *es decir* $4^{2k+1} + 3^{k+2}$ *es múltiplo de* 13.
- *(Paso inductivo) Ahora probaremos que* $P(n)$ *es cierto para* $n = k+1$. *En efecto,*

$$\begin{aligned} 4^{2(k+1)+1} + 3^{(k+1)+2} &= 4^{(2k+1)+2} + 3^{(k+2)+1} \\ &= 4^{2k+1}\cdot 4^2 + 3^{k+2}\cdot 3 \\ &= 4^{2k+1}\cdot 16 + 3^{k+2}\cdot 3 \\ &= 4^{2k+1}\cdot (13+3) + 3^{k+2}\cdot 3 \\ &= 4^{2k+1}\cdot 13 + 4^{2k+1}\cdot 3 + 3^{k+2}\cdot 3 \\ &= 4^{2k+1}\cdot 13 + 3\cdot (4^{2k+1} + 3^{k+2}) \end{aligned}$$

Utilizando la hipótesis de inducción (paso inductivo), tendremos

$$\left.\begin{array}{rcl} 13 \mid 4^{2k+1} + 3^{k+2} & \Rightarrow & 13 \mid 3\cdot (4^{2k+1} + 3^{k+2}) \\ 13 \mid 13 & \Rightarrow & 13 \mid 4^{2k+1}\cdot 13 \end{array}\right\} \Rightarrow 13 \mid 4^{2k+1}\cdot 13 + 3\cdot (4^{2k+1} + 3^{k+2})$$

$$\therefore\ 13 \mid 4^{2(k+1)+1} + 3^{(k+1)+2}$$

Así la proposición $P(n)$ *es cierta para* $n = k+1$ *y por el primer principio de inducción matemática* $4^{2n+1} + 3^{n+2}$ *es múltiplo de* 13 *para todo número entero no negativo* n.

EJERCICIOS

Ejercicio 2.20. *Utilizar la definición de divisibilidad para comprobar que* $31 \mid 20^{15} - 1$ *y* $13 \mid 2^{10} + 3^{10}$.

Ejercicio 2.21. *Probar que cualquiera que sea* $n \in \mathbb{N}$, *el número* $7^{2n+1} - 48n - 7$ *es divisible por* 288.

Ejercicio 2.22. *Probar que cualquiera que sea* $n \in \mathbb{N}$, *el número* $3\cdot 5^{2n+1} + 2^{3n+1}$ *es divisible por* 17

Ejercicio 2.23. *Probar que un número entero no puede ser simultáneamente múltiplo de* 12 *aumentado en* 5 *y múltiplo de* 15 *aumentado en* 4.

Ejercicio 2.24. *Demostrar que para todo número entero* n *el número* $n^3 - n$ *es divisible por* 6.

Ejercicio 2.25. *Sea* a *un entero impar, Probar que:*

[A] $a^2 - 1$ *es divisible por* 8*;*

[B] $a^4 - 1$ *es divisible por* 16*;*

[C] $\forall n \in \mathbb{N}$, $a^{2^n} - 1$ *es divisible por* 2^{n+2}

Ejercicio 2.26. *Demostrar que si* $m \mid a - b$ *entonces* $m \mid a^k - b^k$ *para todo entero* k.

Ejercicio 2.27. *Demostrar que* $(n-1)^2 \mid n^k - 1$ *si y sólo si* $n - 1 \mid k$.

2.4. MCD y MCM

Seguimos desarrollando la teoría de divisibilidad estudiando los factores comunes de dos o más números enteros positivos. Terminaremos dando un método efectivo y eficiente para calcular el Máximo Común Divisor (MCD) de dos números enteros.

En el afán de encontrar el mayor de los divisores comunes de dos o más números enteros, ilustramos algunos procedimientos que pueden seguirse.

Supongamos que debemos calcular el MCD de los números enteros $a = 8316$ y $b = 2808$, una forma de proceder es calcular el conjunto de los divisores de cada número y luego dar como respuesta el más grande de los divisores comunes, observando que basta calcular solo los divisores positivos: calculamos los divisores de a y b, obteniendo respectivamente:

$$\mathcal{D}_a = \mathcal{D}_{8316} = \{\ldots, \boxed{1}, \boxed{2}, \boxed{3}, \boxed{4}, \boxed{6}, 7, \boxed{9}, 11, \boxed{12}, 14, \boxed{18}, 21, 22, \boxed{27}, 28, 33, \boxed{36}, 42, 44, \boxed{54}, 63, 66, 77, 84, 99, \boxed{108}, 126, 132, 154, 189, 198, 231, 252, 297, 308, 378, 396, 462, 594, 693, 756, 924, 1188, 1386, 2079, 2772, 4158, 8316\}$$

$$\mathcal{D}_b = \mathcal{D}_{2808} = \{\ldots, \boxed{1}, \boxed{2}, \boxed{3}, \boxed{4}, \boxed{6}, 8, \boxed{9}, \boxed{12}, 13, \boxed{18}, 24, 26, \boxed{27}, \boxed{36}, 39, 52, \boxed{54}, 72, 78, 104, \boxed{108}, 117, 156, 216, 234, 312, 351, 468, 702, 936, 1404, 2808\}$$

En los conjuntos anteriores se ha marcado los divisores comunes:

$$\mathcal{D}_{8316} \cap \mathcal{D}_{2808} = \{\ldots, 1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$$

Claramente el más grande de todos ellos es 108. Así el MCD de a y b es 108.

Nótese que se invierte mucho trabajo para hacer el procedimiento anterior y para números grandes este procedimiento es poco eficiente, por eso nos interesamos en un procedimiento (o algoritmo) que permita calcular *eficientemente* el máximo de los divisores comunes de una lista finita de números enteros.

La discusión anterior surge de manera muy intuitiva y natural y puede interpretarse como un primer acercamiento a la definición intuitiva de MCD, sin embargo se hace necesario dar una definición simbólica de MCD que formalice (matemáticamente) lo que entenderemos por MCD de números enteros. Primero comenzamos dando una definición en el caso particular de dos números enteros, para luego dar la definición de MCD para más de dos números enteros, y veremos más adelante que el cálculo de MCD de más de dos números enteros se resume a calcularlo de manera *recursiva* calculando el MCD de parejas números enteros.

2.4.1. Definición de MCD y MCM para dos números enteros

Definición 2.16 (Definición de MCD para dos números enteros)**.** *Sean* a *y* b *dos números enteros no ambos iguales a cero. Diremos que el número entero positivo* d *es el Máximo Común Divisor (***MCD***) de* a *y* b *si y sólo si satisface las siguientes dos condiciones:*

[MCD1] $d \mid a$ *y* $d \mid b$*,*

[MCD2] *Si* n *es cualquier otro número entero tal que* $n \mid a$ *y* $n \mid b$*, entonces* $n \mid d$*.*

Escribiremos $d = (a : b)$ *para denotar el MCD de* a *y* b*.*

La condición **[MCD1]** dice que d es un divisor común de a y b, la condición **[MCD2]** dice que d es el mayor de todos esos divisores comunes de a y b. Observemos que sin importar el signo de a y b, el MCD de ellos $d = (a : b)$ siempre es positivo.

Definición 2.17 (Definición de MCM para dos números enteros)**.** *Sean* a *y* b *dos números enteros no ambos iguales a cero. Diremos que el número entero positivo* m *es el Mínimo Común Múltiplo (***MCM***) de* a *y* b *si y sólo si satisface las siguientes dos condiciones:*

[MCM1] $a \mid m$ *y* $b \mid m$*,*

[MCM2] *Si* n *es cualquier otro número entero positivo tal que* $a \mid n$ *y* $b \mid n$*, entonces* $m \mid n$*.*

Escribiremos $m = [a : b]$ *para denotar el MCM de* a *y* b*.*

En la definición anterior, la condición **[MCM1]** dice que m es un múltiplo común de a y b, la condición **[MCM2]** dice que m es el menor de todos los múltiplos positivos comunes de a y b.

2.4.2. Propiedades y ejemplos

Hemos dicho que para números enteros grandes se vuelve poco alentador calcular su MCD con el procedimiento descrito, por este motivo enseguida enunciamos una serie de propiedades que permiten calcular el MCD de dos números de manera más práctica, y al mismo tiempo estas propiedades permitirán establecer un método *eficiente* de calcular el MCD el cual se conoce como Algoritmo de Euclides.

Teorema 2.18 (Propiedades del MCD y MCM)**.** *Sean* $a \neq 0$*,* b*,* c*,* d*,* m*,* q *y* r *números enteros.*

[A] $(a : 1) = 1$*,* $(a : 0) = |a|$*,* $(a : a) = |a|$

[B] $(a : b) = (b : a)$ *(Simetría del MCD)*

[C] $(a : b) = (a : a - b)$

[D] *Si* $a \neq 0$*, entonces* $a \mid b$ *si y sólo si* $(a : b) = |a|$

[E] $(a : b) = (|a| : |b|)$

[F] *Si* $a \mid c$ *y* $b \mid c$*, entonces* $[a : b] \mid c$.[2]

[G] *Sean* a *y* b *dos números enteros, entonces* $(a : b) \cdot [a : b] = |ab|$*.*

[H] *Si* m *es un divisor común de* a *y* b *(i.e.* $m \mid a$ *y* $m \mid b$*), entonces* $\left(\frac{a}{m} : \frac{b}{m}\right) = \frac{(a : b)}{|m|}$

[2] Es decir, cualquier múltiplo de a y b es de la forma $t \cdot [a : b]$ para algún $t \in \mathbb{Z}$.

[I] *Si* $m \neq 0$*, entonces* $(am : bm) = |m|(a : b)$

[J] *Sea* $d := (a : b)$*, entonces* $\left(\frac{a}{d} : \frac{b}{d}\right) = 1$

[K] *Si* $b \neq 0$ *y* $a = bq + r$*, entonces* $(a : b) = (b : r)$

[L] *Si* m *es cualquier número entero, entonces* $(a : b) = (a + bm : b)$

[M] $(a : b) = 1$ *si y sólo si existen números enteros* x*,* y *tales que* $ax + by = 1$

[N] *Si* $(a : b) = 1$ *y* $(a : c) = 1$*, entonces* $(a : bc) = 1$

[Ñ] *Si* $(a : b) = 1$*, entonces* $(ac : b) = (c : b)$

Demostración. Demostraremos algunos apartados y los demás quedan como ejercicio.

[F] Sea $m := [a : b]$, por el algoritmo de la división $c = qm + r$, donde $0 \leq r < m$. Como $a \mid c$ y $a \mid m$, tenemos que $a \mid r$, análogamente, $b \mid r$. Así r es un múltiplo común de a y b que es menor que m. Como m es el *mínimo* común múltiplo, se sigue que $r = 0$, y por lo tanto m divide a c.

[G] El número entero positivo $\frac{|ab|}{(a : b)}$ es divisible por a y b. Así $\frac{|ab|}{(a : b)} \geq [a : b]$.

Por otro lado el número entero positivo $\frac{|ab|}{[a : b]}$ divide a a y b. Así $\frac{|ab|}{[a : b]} \leq (a : b)$.

Por lo tanto $(a : b) \cdot [a : b] = |ab|$.

[H] Sea $d = (a : b)$ y demostraremos $\left(\frac{a}{m} : \frac{b}{m}\right) = \frac{d}{|m|}$. Notemos en primer lugar que $\frac{d}{|m|}$ es un número entero. Por otra parte, como $d \mid a$, se tiene que $\frac{d}{|m|} \mid \frac{a}{|m|}$ y $\frac{d}{|m|} \mid \frac{b}{|m|}$. Si n es otro entero que divide a $\frac{a}{|m|}$ y $\frac{b}{|m|}$, se tendrá $\frac{a}{|m|} = nj$ y $\frac{b}{|m|} = nk$ para algunos enteros j y k.

Finalmente multiplicando ambas igualdades por $|m|$ obtenemos $a = |m|nj$ y $b = |m|nk$, de donde $(|m|n) \mid a$ y $(|m|n) \mid b$, entonces $(|m|n) \mid d$, por lo tanto $n \mid \frac{d}{|m|}$. Lo que termina la demostración.

[K] Se tiene que $(a : b) \mid a$ y $(a : b) \mid b$, de donde $(a : b) \mid r$ y entonces $(a : b) \mid (b : r)$. Por otro lado, $(b : r) \mid b$ y $(b : r) \mid r$, de donde $(b : r) \mid a$, entonces $(b : r) \mid (a : b)$, por lo tanto $(a : b) = (b : r)$.

□

Para evidenciar que estas propiedades simplifican el trabajo al calcular el MCD de dos números enteros, regresemos a nuestro ejemplo $a = 8316$ y $b = 2808$.

$$
\begin{aligned}
(8316 : 2808) &= (8316 - 2808 \times 2 : 2808) && \text{Propiedad } \textbf{[K]} \text{ con } m = 2 \\
&= (2700 : 2808) = (2700 : 2808 - 2700) && \text{Propiedad } \textbf{[C]} \\
&= (2700 : 108) = (2700 - 108 \times 25 : 180) && \text{Propiedad } \textbf{[K]} \text{ con } m = 25 \\
&= (0 : 180) = 180 && \text{Propiedad } \textbf{[A]}
\end{aligned}
$$

EJERCICIOS

Ejercicio 2.28. *Demostrar que si* $(a : b) = d$*, entonces* $(a : d) = d$ *y* $(b : d) = d$*.*

Ejercicio 2.29. *Demostrar que si* $(a : b) = 1$*, entonces:* $(a - b : a + b) = 1$ *o* 2*.*

Ejercicio 2.30. *Si* $(a : b) = 1$*. Encontrar el valor de* $(a + b : a^2 - ab + b^2)$

Ejercicio 2.31. *Probar que si* a *y* b *son números enteros positivos que satisfacen* $(a : b) = [a : b]$ *entonces* $a = b$*.*

Ejercicio 2.32. *Demostrar que si* a*,* b*,* c*,* d*,* m *y* n *son números enteros tales que* $ad - bc = 1$ *y* $mn \neq 0$*, entonces* $(am + bn : cm + dn) = (m : n)$*.*

Ejercicio 2.33. *Demostrar que el MCD y MCM de dos números enteros no ambos iguales a cero existe y es único.*

Ejercicio 2.34. *Probar que* $(a : b) = (a + b : [a : b])$

Ejercicio 2.35. *Demostrar las propiedades* **[2.18]**.

2.4.3. Definición de MCD y MCM para más de dos números enteros

Las definiciones 2.16 y 2.17 son particulares, ahora definimos el MCD y MCM para más de dos números enteros:

Definición 2.19 (Definición de MCD y MCM de números enteros)**.** *Dados* ℓ *números enteros* $a_1, a_2, \ldots, a_\ell$ *no todos iguales a cero.*

Diremos que el número entero positivo d *es el Máximo Común Divisor (***MCD***) de* $a_1, a_2, \ldots, a_\ell$ *si y sólo si satisface las siguientes dos propiedades*

[MCD1*] $d \mid a_1$ *y* $d \mid a_2$ *y* $\ldots$ *y* $d \mid a_\ell$

[MCD2*] *Si* n *es cualquier otro número entero tal que* $n \mid a_1$ *y* $n \mid a_2$ *y* $\ldots$ *y* $n \mid a_\ell$ *entonces* $n \mid d$*.*

Escribiremos $d = (a_1 : a_2 : \ldots : a_\ell)$ *para denotar el MCD de* $a_1, a_2, \ldots, a_\ell$*.*

Diremos que el número entero positivo m *es el Mínimo Común Múltiplo (***MCM***) de* $a_1, a_2, \ldots, a_\ell$ *si y sólo si satisface las siguientes dos condiciones:*

[MCM1*] $a_1 \mid m$ *y* $a_2 \mid m$ *y* $\ldots$ *y* $a_\ell \mid m$

[MCM2*] *Si* n *es cualquier otro número entero tal que* $a_1 \mid n$ *y* $a_2 \mid n$ *y* $\ldots$ *y* $a_\ell \mid n$*, entonces* $m \mid n$*.*

Escribiremos $m = [a_1 : a_2 : \ldots : a_\ell]$ *para denotar el MCM de* $a_1, a_2, \ldots, a_\ell$*.*

Es claro que estas definiciones no son operativas y mucho menos prácticas a la hora de cálculos concretos de MCD y MCM, el lector puede convencerse y demostrar (ver ejercicio 2.36) concretamente que:

$$(a_1 : a_2 : \ldots : a_\ell) = ((a_1 : a_2 : \ldots : a_{\ell-1}) : a_\ell) \qquad \text{y} \qquad [a_1 : a_2 : \ldots : a_\ell] = [[a_1 : a_2 : \ldots : a_{\ell-1}] : a_\ell].$$

Ejemplo 2.20.

$$\begin{aligned}(24:14:42:33) &= ((24:18:42):33) = (((24:18):42):33)\\ &= ((6:42):33) = (6:33) = 3,\\ [24:14:42:33] &= [[24:18:42]:33] = [[[24:18]:42]:33]\\ &= [[72:42]:33] = [504:33] = 5544.\end{aligned}$$

Observe que $24 \cdot 14 \cdot 42 \cdot 33 = 465696 \neq 16632 = 3 \cdot 5544$.

EJERCICIOS

Ejercicio 2.36. *Demostrar que si* $a_1, a_2, \ldots, a_\ell \in \mathbb{Z}$ *no todos iguales a cero, entonces el MCD y MCM se calcula de forma recursiva:*

$$(a_1 : a_2 : \ldots : a_\ell) = ((a_1 : a_2 : \ldots : a_{\ell-1}) : a_\ell) \qquad y \qquad [a_1 : a_2 : \ldots : a_\ell] = [[a_1 : a_2 : \ldots : a_{\ell-1}] : a_\ell].$$

2.5. Algoritmo de Euclides

Existen diversos métodos que permiten calcular el MCD de dos números enteros, estos métodos están fundamentados esencialmente en el lema de la división. Un método es el **Algoritmo de Euclides** consiste en una serie de divisiones sucesivas y el MCD se obtiene como uno de los residuos en el proceso de división. Este procedimiento además de calcular el MCD, permite dar otra demostración alternativa de la existencia.

Algoritmo 2.21 (Algoritmo de Euclides)**.** *Dados* a *y* b *números enteros positivos, hagamos*

$$\begin{aligned} b &= aq_1 + r_1, & 0 \le r_1 < a\\ a &= r_1q_2 + r_2, & 0 \le r_2 < r_1\\ r_1 &= r_2q_3 + r_3 & 0 \le r_3 < r_2\\ &\ldots\\ r_n &= r_{n+1}q_{n+2} & 0 = r_{n+2} < r_{n+1}\end{aligned}$$

Entonces $(a : b) = r_{n+1}$.

Demostración. Basta observar que $\{r_i\}$ es una secuencia estrictamente decreciente de números enteros positivos, y por tanto existe un n tal que $r_{n+2} = 0$. Además por la propiedad **[K]** anterior:

$$(a : b) = (b : a) = (a : r_1) = (r_1 : r_2) = \ldots = (r_n : r_{n+1}) = (r_{n+1} : r_{n+2}) = r_{n+1}$$

pues $r_{n+1} \mid r_n$ o bien $(r_{n+1} : r_{n+2}) = (r_{n+1} : 0) = r_{n+1}$, lo que demuestra el algoritmo. □

En la práctica los cálculos suelen disponerse en un arreglo de la siguiente manera:

	q_1	q_2	q_3	$\cdots\cdots$	q_{n+1}	q_{n+2}
b	a	r_1	r_2	$\cdots\cdots$	r_n	$r_{n+1} = (a : b)$
r_1	r_2	r_3	$\cdots\cdots$	r_{n+1}	$r_{n+2} = 0$	

Ejemplo 2.22. *Ahora damos una interpretación geométrica del algoritmo de Euclides para el caso donde los dos números enteros son positivos: al calcular* $(23 : 13)$ *por el algoritmo de Euclides tenemos*

$$23 = 1 \cdot 13 + 10$$
$$13 = 1 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + \mathbf{1}$$
$$3 = 3 \cdot 1$$

	1	1	3	3
23	13	10	3	$1 = (23 : 13)$
10	3	1	0	

Por lo que $(23 : 13) = 1$.

Ahora considere un rectángulo de dimensiones 23×13*, como el de la izquierda en la Figura 2.1. El mayor cuadrado que puede estar dentro del rectángulo es de lado* 13 *y solamente hay uno. Ahora también podemos usar un cuadrado de lado* 10*, tres cuadrados de lado* 3 *y tres cuadrados de lado* 1 *para terminar de llenar el rectángulo, tal como se muestra al lado derecho en la Figura 2.1.*

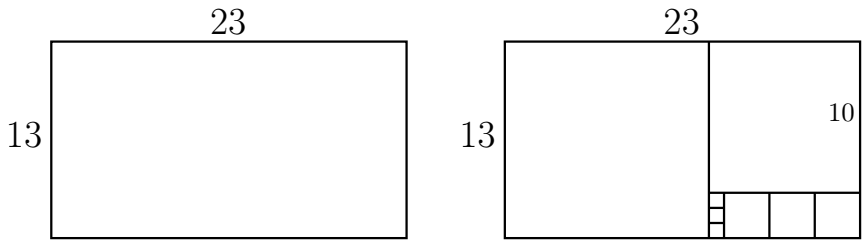


Figura 2.1: Interpretación geométrica del Algoritmo de Euclides

En cada paso del algoritmo de Euclides, el cociente q *y divisor* d *son respectivamente la cantidad y dimensión del cuadrado que pueden utilizarse para teselar el cuadrado. La dimensión más grande del cuadrado posible a usar está dada por el MCD.*

Ejemplo 2.23. *Podemos calcular el MCD de* 672 *y* 38*, usando el método anterior, para lo cual haremos las divisiones sucesivas correspondientes:*

$$\mathbf{672} = 17 \cdot \mathbf{38} + 26$$
$$38 = 1 \cdot 26 + 12$$
$$26 = 2 \cdot 12 + 2$$
$$12 = 6 \cdot 2$$

$$26 = \mathbf{672} - 17 \cdot \mathbf{38}$$
$$12 = 38 - 1 \cdot 26$$
$$2 = 26 - 2 \cdot 12$$
$$2 = 26 - 2 \cdot (38 - 26) = 3 \cdot 26 - 2 \cdot 38$$
$$2 = 3 \cdot (\mathbf{672} - 17 \cdot \mathbf{38}) - 2 \cdot \mathbf{38}$$
$$2 = 3 \cdot \mathbf{672} - 53 \cdot \mathbf{38}$$

Como el último residuo diferente de cero es 2*, el Algoritmo de Euclides afirma que* $(672 : 38) = 2$*, hemos encontrado aún más:* $(672 : 38) = 2 = 3 \cdot \mathbf{672} + (-53) \cdot \mathbf{38}$.

El siguiente lema asegura que en general haciendo las sustituciones sucesivas en orden inverso siempre se pueden encontrar números enteros x y y tales que $(a : b) = ax + by$.

Teorema 2.24. *El MCD de dos números enteros* a *y* b *siempre se puede expresar como combinación lineal de* a *y* b*. Es decir, existen números enteros* x *y* y *tales que* $(a : b) = ax + by$*. A los números enteros* x *y* y *se les conoce como* ***coeficientes de Bezout****.*

Demostración. El conjunto $\mathcal{C}$ de todas las combinaciones lineales de a y b contiene números enteros positivos (así como enteros negativos y 0). Al menor elemento positivo de $\mathcal{C}$ lo denotaremos por $m := \min_{ax+by>0} \mathcal{C}$, es decir, $m = sa + tb$. Usamos el lema de la división para escribir $a = qm + r$, donde $0 \leq r < m$. Entonces $r = a - qm = a - q(sa + tb) = (1 - qs)a + (-qt)b$, por lo que r también es combinación lineal de a y b. Pero $r < m$, por la definición de m se sigue que $r = 0$. Así $a = qm$, es decir, $m \mid a$; análogamente, $m \mid b$. Por lo que m es un divisor común de a y b.

Sea $d := (a : b)$, entonces $d \mid a$ y $d \mid b$, entonces d divide a cualquier combinación lineal de a y b, es decir $d \mid m$ y por la propiedad de comparación $d \leq m$. Pero d es el *máximo* común divisor, por lo tanto $d = m$. □

Sabías que…. *El Algoritmo de Euclides también funciona para polinomios.*

$$18x^4 - 9x^3 + 3x^2 + 4x - 1 = \left(18x^3 - 9x^2 - 3x + 3\right) \cdot x + \left(6x^2 + x - 1\right)$$
$$18x^3 - 9x^2 - 3x + 3 = \left(6x^2 + x - 1\right) \cdot \left(3x - 2\right) + \left(2x + 1\right)$$
$$6x^2 + x - 1 = \left(2x + 1\right) \cdot \left(3x - 1\right) + 0$$

Hemos usado la división larga de polinomios y el Algoritmo de Euclides para encontrar que $(18x^4 - 9x^3 + 3x^2 + 4x - 1 : 18x^3 - 9x^2 - 3x + 3) = 2x + 1$

EJERCICIOS

Ejercicio 2.37. *El MCD de dos números es* 51 *y los cocientes parciales obtenidos al calcularlo por el algoritmo de Euclides son* 2*,* 3 *y* 5*. Encontrar los números.*

Ejercicio 2.38. *En cada uno de los siguientes casos, calcular* $(a : b)$ *y* $[a : b]$ *y encontrar los coeficientes de Bezout, i.e. números enteros* x *y* y *tales que* $(a : b) = ax + by$*.*

[A] $a = 150$*;* $b = 240$

[B] $a = 60$*;* $b = 84$

[C] $a = 150$*;* $b = 77$

[D] $a = 12345$*;* $b = 67890$

[E] $a = 54321$*;* $b = 9876$*.*

Ejercicio 2.39. *Si se divide* 4294 *y* 3521 *por un mismo número entero positivo, y se obtiene respectivamente* 10 *y* 11 *como residuo. ¿Cuál es este número entero? Sugerencia: Todo divisor común de dos números enteros es un divisor de su MCD.*

Ejercicio 2.40. *Encuentre el MCD de los siguientes números cuando* $n \in \mathbb{N}$*.*

[A] $(2n + 1 : 9n + 4)$

[B] $(2n - 1 : 9n + 4)$

[C] $(36n + 3 : 90n + 6)$

[D] $(2n + 3 : n + 7)$*.*

Ejercicio 2.41. *Encuentre el mayor valor que puede tomar el MCD de dos términos consecutivos de la siguiente secuencia:* $101, 104, 109, 116, 125, 136, \ldots$.

2.6. Números primos

Comenzamos definiendo los siguientes tipos de números: número primo, número compuesto y números primos relativos.

Definición 2.25. *Un número entero positivo* p *se dice que es* ***número primo*** *(o simplemente primo) si sus únicos divisores positivos son* 1 *y* p*.*

A todo número entero positivos que no es primo se le llama ***número compuesto*** *(o simplemente compuesto), a excepción del número* 1 *el cual no es primo ni compuesto.*

Dos números enteros positivos a *y* b*, se dicen* **coprimos** *(o* ***primos relativos****) si y sólo si* $(a : b) = 1$*.*

Observación 2.26. *El único primo par es el* 2 *y todos los primos mayores que* 2 *son impares.*

Todo número compuesto es de la forma $m = m_1 m_2$*, donde* $1 < m_1 < m$ *y* $1 < m_2 < m$*, por ejemplo* $6 = 2 \cdot 3$*. Los números* $2, 3, 5, 7$ *son todos números primos.*

Si dos números son coprimos no tiene porque alguno (o ambos) ser número primo, por ejemplo los números enteros consecutivos 20 *y* 21 *son coprimos, pues* $(20 : 21) = 1$*, sin embargo ninguno de ellos es primo.*

En general, si n *es un número entero entonces* $(n : n + 1) = (n : 1) = 1$*, esto asegura que dos números enteros consecutivos son coprimos.*

Ejemplo 2.27. *Demostrar que para todo número entero la fracción* $\dfrac{21n + 4}{14n + 3}$ *es irreducible.*

Resolución. *Una fracción es irreducible si está en su mínima expresión, i.e. el numerador y el denominador no tienen factores en común.* $(21n + 4 : 14n + 3) = (14n + 3 : 7n + 1) = (7n + 1 : 1) = 1$*, como el numerador y denominador son coprimos, la fracción es irreducible para todo número entero* n*.*

EJERCICIOS

Ejercicio 2.42. *Demostrar que* $2^{524} - 1$ *no es un número primo.*

Ejercicio 2.43. *Demostrar que si* p *y* q *son números primos y* $p \mid q$*, entonces* $p = q$*.*

Ejercicio 2.44. *Demostrar que si* a *y* b *son números naturales y* p *un número primo tales que* $a^2 - b^2 = p$*, entonces* a *y* b *son consecutivos. Mostrar además que la implicación recíproca es falsa.*

Ejercicio 2.45. *Demostrar que si la suma de dos números naturales es un número primo, entonces los dos números son primos entre sí.*

Ejercicio 2.46. *Demostrar que todo número primo mayor o igual que* 5 *es de la forma* $6k + 1$ *o* $6k + 5$ *para algún* $k \in \mathbb{N}$*.*

Ejercicio 2.47. *Demostrar que las siguientes proposiciones son falsas:*

[A] *Si* p *es un número primo entonces* p *es impar.*

[B] *Para todo número natural no primo* n *con* $n > 2$*, el número* $2n + 13$ *tampoco es primo.*

Ejercicio 2.48. *Demostrar que cada una de las fórmulas siguientes no sólo generan números primos:*

[A] $n^2 + n + 17$ **[B]** $2n^2 + 29$ **[C]** $n^2 - n + 41$

¿Existirá algún polinomio $p(n)$ *que siempre genere números primos al evaluarlo en cada* $n \in \mathbb{N}$*?*

Ejercicio 2.49. *Demostrar que la fracción* $\dfrac{n^4 + n^2 + 1}{n^2 + 1}$ *es irreducible para cada* $n \in \mathbb{Z}$*.*

Ejercicio 2.50. *Demostrar que si* $p \neq 5$ *es un número primo impar, entonces* $p^2 - 1$ *ó* $p^2 + 1$ *es divisible por* 10*.*

Ejercicio 2.51. *Supongamos que* $(a : b) = p$*, donde* p *es un número primo. Calcular:*

[A] $(a^2 : b^2)$ **[B]** $(a^2 : b)$ **[C]** $(a^3 : b)$ **[D]** $(a^2 : b^3)$

En cada caso, dar un ejemplo numérico que ilustre su respuesta.

Ejercicio 2.52. *Suponer que* $(a : p^2) = p$ *y* $(b : p^4) = p^2$*, donde* p *es número primo. Calcular:*

[A] $(ab : p^5)$ **[B]** $(a + b : p^4)$ **[C]** $(a - b : p^5)$ **[D]** $(pa - b : p^5)$

Ejercicio 2.53. *Sea* p *un número primo, para cada una de las proposiciones siguientes indicar si es Verdadera (V) o Falsa (F), en el caso V dar una demostración y para el caso F dar un contrajemplo.*

[A] $p \mid (a^2 + b^2), p \mid (b^2 + c^2) \Rightarrow p \mid (a^2 - c^2)$.

[B] $p \mid a^7 \Rightarrow p \mid a$.

[C] $p \mid a, p \mid (a^2 + b^2) \Rightarrow p \mid b$.

[D] $p \mid (a^2 + b^2), p \mid (b^2 + c^2) \Rightarrow p \mid (a^2 + c^2)$.

Ejercicio 2.54. *Demostrar que si* $(b : c) = 1$*, entonces para todo número entero positivo* a*, se tiene* $(a : bc) = (a : b)(a : c)$.

Ejercicio 2.55. *Sean* p*,* q *números primos gemelos*[3] *mayores que cinco. Probar que* $12 \mid p + q$.

Ejercicio 2.56. *Sean* a*,* b*,* c*, y* d *números enteros positivos tales que* $ab = cd$*. Demuestra que* $a + b + c + d$ *no es primo.*

2.6.1. Teoremas y resultados sobre números primos

El siguiente teorema establece algunos resultados clásicos y propiedades que nos interesarán por sus diversas aplicaciones en la resolución de problemas.

Teorema 2.28 (Resultados y propiedades sobre números primos y primos relativos)**.**

[A] *El menor divisor no trivial de cualquier número entero mayor que uno es primo.*

[B] *(Teorema de Euclides) Existe una cantidad infinita de números primos.*

[C] *(Teorema Fundamental de la Aritmética) Todo número entero* $N > 1$ *se puede representar de forma única como producto de números primos. Es decir,*

$$N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

donde $e_i \geq 1$ *y* p_i *son primos,* $i = 1, \ldots, r$*, a esta forma de representar* n *se le conoce también como* ***descomposición en factores primos*** *o* ***factorización canónica****.*

[D] *Si un número entero* $n > 1$ *no tiene divisores menores o iguales que* $\sqrt{n}$ *entonces es primo.*

[E] *(Teorema de Bezout) Dos números enteros positivos* a *y* b *son primos relativos, si y sólo si existen números enteros* x *y* y *tales que* $ax + by = 1$*.*

[F] *Sean* a*,* b*, y* c *tres números enteros, tales que* $(a : b) = 1$ *y* $a \mid bc$*, entonces* $a \mid c$*.*

[G] *(Lema de Euclides/Divisibilidad por un número primo) Si* a *y* b *son números enteros,* p *un primo tal que* $p \mid ab$ *entonces* $p \mid a$ *o* $p \mid b$*.*

[3] Dos números primos son **primos gemelos** si están separados por una distancia de 2, por ejemplo 5 y 7 son primos gemelos.

[H] $(a : b) = 1$ *si y sólo si* $(a^m : b^m) = 1$*, donde* $m \in \mathbb{N}$.

[I] *Si* $m \in \mathbb{N}$*, entonces* $a^m \mid b^m$ *si y sólo si* $a \mid b$

[J] *(Teorema de Gauss) Si* $a \mid c$*,* $b \mid c$ *y* $(a : b) = 1$*, entonces* $ab \mid c$

Demostración. Demostraremos algunos apartados.

[A] Sea $p > 1$ el menor divisor de n. Si p no fuera primo, tendría un divisor $1 < d < p$. Pero entonces d es un divisor de n y ésto contradice la minimalidad con que fue elegido p.

[B] Supongamos que existe una cantidad finita de primos $p_1, p_2, \ldots, p_k$. Sea $n = p_1 p_2 \cdots p_k + 1$. Puesto que $n > p_i$, $i = 1, 2, \ldots, k$, n no puede ser primo. Sea p el menor divisor de n, por la propiedad **[A]** sabemos que es primo y claramente $p \neq p_i$ para todo i (pues $p_i \nmid n$). Así se ha obtenido un primo distinto a los anteriores. Esta contradicción demuestra que el conjunto de números primos es infinito.

[D] Supongamos que $n > 1$ y compuesto. Entonces, $n = ab$ donde $1 < a < n$ y $1 < b < n$. Concluimos que al menos uno de a o b es menor o igual a $\sqrt{n}$. Pues en caso contrario, $a > \sqrt{n}$ y $b > \sqrt{n}$, Y por lo tanto $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, lo cual es imposible. Supongamos, sin pérdida de generalidad, que $a \leq \sqrt{n}$. Como $a > 1$, por la propiedad **[A]** existe un primo p tal que $p \mid a$, además $a \mid n$ por transitividad $p \mid n$ y por la Propiedad de Comparación en **[2.8]** se concluye que $p \leq a \leq \sqrt{n}$.

Podemos utilizar este resultado para averiguar si un número entero es primo. Teniendo en cuenta $n > 1$, sólo tenemos que tratar de dividirlo por todos los primos $p \leq \sqrt{n}$. Si ninguna de estas divisiones de n por p es exacta, entonces n debe ser primo. Por ejemplo, para averiguar si 97 es primo, observamos que $\sqrt{97} < \sqrt{100} = 10$. Los primos menores 10 son 2, 3, 5 y 7. Ninguno de estos primos divide a 97, así que 97 es primo.

□

Las siguientes proposiciones formalizan resultados clásicos muy conocidos e intuitivos.

Proposición 2.29 (Caracterización de los divisores de un número)**.** *Si* $(m : n) = 1$*, entonces el conjunto de divisores de* mn *son todas las multiplicaciones* $d \cdot d'$*, donde* $d \mid m$*,* $d' \mid n$ *y* $(d : d') = 1$ *y los resultados de todas esas multiplicaciones son números diferentes.*

Proposición 2.30 (Fórmula del MCD y MCM de dos números en términos de su factorización canónica)**.** *Sean* $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ *y* $m = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$*, donde* $e_i, f_i \geq 0$ *y* p_i *números primos diferentes para* $i = 1, 2, \ldots, r$.

[A] *Los divisores de* n *son todos los números de la forma* $p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r}$*, donde* $0 \leq u_i \leq e_i$*, para* $i = 1, 2, \ldots, r$.

[B] $(n : m) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_r^{\min\{e_r, f_r\}}$

[C] $[n : m] = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_r^{\max\{e_r, f_r\}}$

La proposición anterior puede generalizarse para calcular el MCD y MCM de más de dos enteros no todos iguales a cero a partir de su descomposición en factores primos, siempre tomando respectivamente las mínimas y máximas de las potencias comunes.

EJERCICIOS

Ejercicio 2.57. *Determinar si los siguientes números son primos:*

[A] $123782846123897461283 72$ **[B]** 541 **[C]** 7919

Ejercicio 2.58. *En cada caso hacer lo indicado.*

[A] *Encontrar* $(a : b)$ *y* $[a : b]$*, donde* $a = 3^2 \cdot 5^2 \cdot 11$*;* $b = 2^3 \cdot 3^3 \cdot 5^7$.

[B] *Encontrar* $(a : b : c)$ *y* $[a : b : c]$*, donde* $a = 2^2 \cdot 5^2 \cdot 13 \cdot 35^8$*;* $b = 2^3 \cdot 3^2 \cdot 5^2 \cdot 14^6$*;* $c = 2^2 \cdot 5 \cdot 7^3$.

Ejercicio 2.59. *Mostrar que los números* $n! + 1$ *y* $(n + 1)! + 1$ *son primos relativos.*

Ejercicio 2.60. *Si* $(r : s) = 1$*, entonces* $(r \pm s : rs) = 1$.

Ejercicio 2.61. *Demostrar la propiedad* **[H]** *del teorema 2.28.*

Ejercicio 2.62. *Demostrar que si* $(b : c) = 1$*, entonces para todo entero positivo* a*, se tiene* $(a : bc) = (a : b)(a : c)$.

Ejercicio 2.63. *Sea* p *un número primo, probar que si* $p \mid a^n$ *entonces* $p \mid a$.

Ejercicio 2.64. *Sea* p *un número primo y* $(a : b) = 1$ *demostrar que* $p \nmid (a^n : b^n)$.

Ejercicio 2.65. *Demostrar que si el número primo* p *no divide a los números enteros* $n_1, n_2, \ldots, n_k$ *entonces tampoco divide a su producto.*

Ejercicio 2.66 (Lema de Wilson)**.** *Demostrar que existen vacíos arbitrariamente largos entre los números primos. Es decir, para cualquier número entero positivo* n *hay una sucesión de* n *números enteros consecutivos compuestos. Sugerencia:* $(k + 1)! + 2, (k + 1)! + 3, \ldots, (k + 1)! + (k + 1)$.

Ejercicio 2.67. *DeBouvelles (1509) afirmaba que para cada* $n \geq 1$ *uno o ambos de los números* $6n + 1$ *y* $6n - 1$ *eran números primos. Demostrar que estaba equivocado y además que existen infinitos números* n *tales que* $6n - 1$ *y* $6n + 1$ *son compuestos. (Comparar con el ejercicio 2.46)*

2.6.2. Ejemplos y problemas resueltos

Veamos los siguientes ejemplos que muestran las diversas aplicaciones de las propiedades.

Ejemplo 2.31. *Demostrar que* $\sqrt{2}$ *es irracional.*

Resolución. *Utilizaremos el método de demostración por contradicción. Para obtener una contradicción, asumimos que* $\sqrt{2}$ *es racional. Entonces podemos escribir* $\sqrt{2} = \frac{a}{b}$*, donde* a *y* b *son números enteros,* b *es diferente de cero, y la fracción se encuentra en su mínima expresión (ya no puede simplificada). Al elevar ambos lados al cuadrado obtenemos* $2 = \frac{a^2}{b^2}$*, de donde* $2b^2 = a^2$*. Pero esto implica que* a^2 *es par, y por el lema de Euclides* a *es par. Pero si* a *es par,* a^2 *es múltiplo de* 4*. Debido a la igualdad* $2b^2 = a^2$*,* $2b^2$ *es también un múltiplo de* 4*. Esto implica que* b^2 *es par, y por lo tanto,* b *es también par. Pero ya que* a *y* b *son ambos pares, la fracción* $\frac{a}{b}$ *no se encuentra en su mínima expresión. Esto es una contracción, por lo que la suposición que* $\sqrt{2}$ *es racional debe ser falsa.*

Ejemplo 2.32. *Encontrar todos los naturales tales que* $a + b = 112$ *y* $(a : b) = 14$.

Resolución. *El MCD de* a *y* b *es* 14*, entonces* $a = 14u$ *y* $b = 14v$ *con* u *y* v *números enteros primos relativos. Reemplazando en la igualdad* $a + b = 112$*, obtenemos* $14(u + v) = 112$*, simplificando* $u + v = 8$*. Como* u *y* v *son primos relativos, la soluciones son* $u = 1$*,* $v = 7$*;* $u = 3$*,* $v = 5$*;* $u = 5$*,* $v = 3$ *ó* $u = 7$*,* $v = 1$*. Multiplicando por* 14 *encontramos que los pares* $(14; 98)$*,* $(42; 70)$*,* $(70; 42)$*,* $(98; 14)$*. Compruebe que en efecto son soluciones del sistema.*

EJERCICIOS

Ejercicio 2.68. *Probar que* $\log_{10} 2$*,* $\log_2 6$ *y* $\sqrt[3]{5}$ *son irracionales.*

Ejercicio 2.69. *Resuelva para* x *y* y *los siguientes sistemas en el conjunto* $\mathbb{N}$

[A] $\begin{aligned} x + y &= 150 \\ (x : y) &= 30 \end{aligned}$ **[B]** $\begin{aligned} x + y &= 85 \\ [x : y] &= 546 \end{aligned}$ **[C]** $\begin{aligned} (x : y) &= 45 \\ 7x &= 11y \end{aligned}$ **[D]** $\begin{aligned} xy &= 20 \\ [x : y] &= 10 \end{aligned}$

2.6.3. Mayor potencia de un número primo que divide a $n!$

El factorial de un número entero no negativo se define como $n! = \begin{cases} n \cdot (n-1)! & n \geq 1 \\ 1 & n = 0 \end{cases}$

Ejemplo 2.33. *Descomponer canónicamente a* $12!$*.*

$12! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2^3 \cdot 3^2 \cdot 2 \cdot 5 \cdot 11 \cdot 2^2 \cdot 3 \quad \Rightarrow \quad 12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7^1 \cdot 11^1$

Legendre fue el primero en hacer un análisis del mayor exponente e de un número primo p que divide a $n!$, donde $n \in \mathbb{N}$ y en 1808 estableció la siguiente fórmula.

Teorema 2.34 (Fórmula de Legendre)**.** *El exponente* e *con que aparece el primo* p *en la factorización canónica de* $n!$ *es*

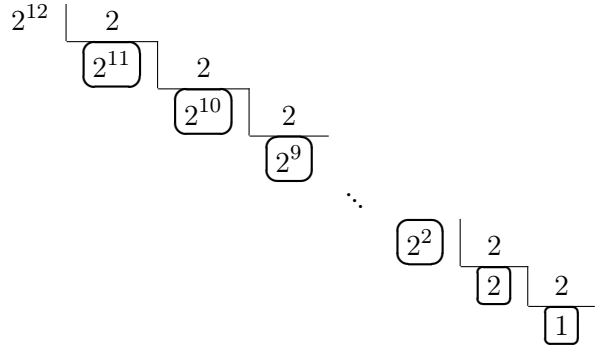
$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Notar que la suma $\displaystyle\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ en realidad es finita. En efecto, por la propiedad arquimediana de $\mathbb{R}$ para p y n existe un número natural m tal que $p^m > n$, entonces para todo $k \geq m$ se tiene que $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$.

Ejemplo 2.35. *¿Cuál es el exponente* e *de* 2 *en la descomposición canónica de* $2^{12}!$*?*

[a] 511 [b] 1023 [c] 2047 [d] 4095 [e] 8191

Resolución. *Para encontrar el exponente de* 2 *bastará dividir sucesivamente* 2^{12} *entre* 2 *y sumar los cocientes:*



Luego: $e = 1 + 2 + 2^2 + 2^3 + \ldots + 2^{10} + 2^{11} = \dfrac{2^{12} - 1}{2 - 1} \quad \therefore \quad e = 2095.$ *Respuesta* d

Ejemplo 2.36. *¿En cuántos ceros termina* $300!$*?*

Resolución. *La cantidad de ceros queda determinado por la mayor potencia de* 10 *que divida a* $300!$*. Ya que abundan más los múltiplos de* 2 *en* $300!$ *que los múltiplos de* 5*, el número de ceros queda determinado por la potencia mayor de* 5 *que divida a* $300!$ *En virtud de la fórmula de Legendre (teorema 2.34), la potencia buscada es*

$$\sum_{k=1}^{\infty} \left\lfloor \frac{300}{5^k} \right\rfloor = 60 + 12 + 2 = 74.$$

EJERCICIOS

Ejercicio 2.70. *Mostrar que los números* $n! + 1$ *y* $(n + 1)! + 1$ *son primos relativos.*

Ejercicio 2.71. *Para* $p = 2, 3, 5, 7$*, encontrar la máxima potencia de* p *que divide a* $100!$*. Encontrar también la mayor potencia de* 25 *y* 125 *que divide a* $100!$*.*

Ejercicio 2.72. *Encontrar la descomposición en factores primos de* $100!$*.*

Ejercicio 2.73. *Calcular el menor* $n \in \mathbb{N}$ *tal que* $\sqrt{100! \cdot a}$ *es un número entero.*

Lectura complementaria:
Revisar las soluciones a los problemas de aritmética [7, Problemas 1.32, 1.34, 1.35, 1.44 y 1.50].

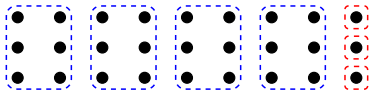
Numeración

3 Sistemas de numeración

Un *sistema de numeración* se refiere a los conjuntos de reglas y normas que permiten formar, expresar y representar todos los números.

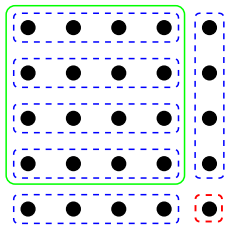
Aquí solamente estudiaremos los sistemas de numeración posicionales y motivaremos su estudio con algunos ejemplos. El punto de partida para formar un sistema de numeración es la *base del sistema de numeración*, ésta base es un número que indica la cantidad de unidades de un orden cualquiera que se requiere para formar una unidad de un orden inmediato superior. El sistema DECIMAL obtiene su nombre porque con 10 UNIDADES de un orden cualquiera, se logra formar una unidad de un orden inmediato superior.

Ejemplo 3.1. *Si se tuviera* 27 *bolitas; para representar esta cantidad en el sistema base* 6*, se tendría que agrupar de* 6 *en* 6*, es decir:*



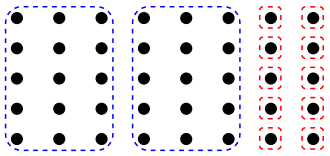
De donde se tiene 4 *grupos de* 6 *y sobran* 3*, lo que se expresa así:* $4\,3_{(6)}$

Ejemplo 3.2. *Si se desea expresar* 25 *en el sistema base* 4*, debe agruparse de* 4 *en* 4 *en forma sucesiva, es decir:*



Tendremos entonces un grupo de $16 = 4^2$*,* 2 *grupos de* 4 *y sobra* 1*, lo que se escribe:* $1\,2\,1_{(4)}$

Ejemplo 3.3. *Para expresar* 40 *en el sistema base* 15 *se agrupa de* 15 *en* 15*, así tenemos:*



Donde notamos que hay 2 *grupos de* 15 *y sobran* 10 *que se representa por "*A*" y se escribe:* $2\,A_{(15)}$

3.1. Consideraciones importantes

[A] Cuando la base es superior a 10, y los números 10; 11; 12; 13; ... sean cifras, se emplea la siguiente equivalencia:

$$A = 10 \quad ; \quad B = 11 \quad ; \quad C = 12 \quad ; \quad D = 13 \quad ; \quad \ldots$$

[B] La base de un sistema de numeración debe ser un número entero y mayor que 1; en consecuencia, existen *infinitos* sistemas de numeración, siendo los principales:

Base	Sistema de Numeración	Cifras que utiliza
2	Binario	$0, 1$
3	Ternario	$0, 1, 2$
4	Cuaternario	$0, 1, 2, 3$
5	Quinario	$0, 1, 2, 3, 4$
6	Senario	$0, 1, 2, 3, 4, 5$
7	Heptal	$0, 1, 2, 3, 4, 5, 6$
8	Octal	$0, 1, 2, 3, 4, 5, 6, 7$
9	Nonario	$0, 1, 2, 3, 4, 5, 6, 7, 8$
10	Decimal	$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$
11	Undecimal	$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}$
12	Duodecimal	$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}$
16	Hexadecimal	$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}$

Otros sistemas frecuentemente utilizados son el hexadecimal (base 16) y el vigesimal (base 20).

[C] La base de un sistema de numeración siempre es mayor que cualquiera de las cifras que se usan en dicho sistema; esto permite determinar si un número está bien o mal escrito, por ejemplo:

$37194_{(12)}$ Número bien escrito
$615\mathrm{B}3_{(11)}$ Número mal escrito

[D] En el sistema de numeración de base "N" se dispone de "N" cifras para representar a todos los números, como puede observarse en el cuadro anterior, la mínima cifra es cero y la máxima es *menor en* 1 que la base del sistema de numeración.

3.2. Formación de un sistema de numeración

Principio básico

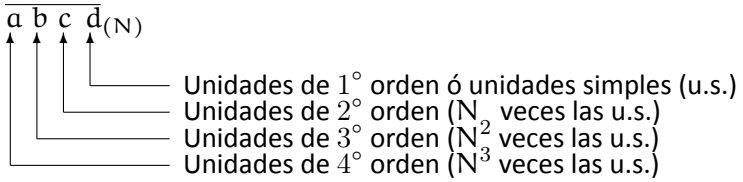
En un sistema de base N, toda cifra escrita un lugar a la izquierda de otra, representa unidades de orden N veces mayor al orden que representa la otra, escrita a la derecha.

Ejemplo 3.4. *Sea el número* $468_{(10)}$*, el* 4 *es de orden* 10 *veces mayor que cada unidad de* 60 *y cada unidad de* 6 *es de orden* 10 *veces mayor que cada unidad de* 8*.*
De aquí en adelante cuando nos refiramos a números de base 10 *evitaremos especificar la base, es decir, el número* $468_{(10)}$ *simplemente lo escribiremos* 468 *siempre y cuando no haya peligro de confusión.*

Descomposición polinómica de un número

Es el procedimiento de cálculo que permite determinar la cantidad de unidades simples que posee un número y con ello su valor real.

Sea el número $\overline{\mathrm{a\,b\,c\,d}}$ de base N:



Método práctico para descomponer un número en su forma polinómica

"Se toma la primera cifra de la izquierda y se multiplica por la base del sistema elevado a un exponente igual a la cantidad de cifras que le siguen a la cifra tomada, a este resultado se le suma el producto de la segunda cifra multiplicada por la base del sistema elevada a un exponente igual a la cantidad de cifras que le siguen y así sucesivamente".

- Número de 3 cifras de base "N":
  $\overline{a\,b\,c}_{(N)} = a \cdot N^2 + b \cdot N + c$
- Número de 4 cifras del sistema decimal (m millares, c centenas, d decenas y u unidades):
  $\overline{m\,c\,d\,u}_{(10)} = m \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + u$
- Número capicúa: Es aquel cuya escritura y lectura de izquierda a derecha es igual que de derecha a izquierda. Por ejemplo:
  Capicúa de 6 cifras: $\overline{abccba}$
- Número de M cifras de base "N":
  $\underbrace{\overline{a\,b\,\ldots\,x\,y\,z}}_{\text{"M" cifras}}{}_{(N)} = a \cdot N^{M-1} + b \cdot N^{M-2} + \ldots + x \cdot N^2 + y \cdot N + z$

3.3. Operaciones aritméticas

Aquí estudiaremos como realizar operaciones aritméticas en sistemas de numeración diferentes al decimal. Explicamos cómo sumar y restar, pues la multiplicación y división son abreviaciones de la suma y resta.

Suma

Tal como en el sistema decimal, si la suma parcial supera el valor de la base, se escribe el valor numérico de lo que excede a la base y se lleva como unidades tantas veces como excede al valor de la base.

Ejemplo 3.5. *Operar* $423_{(7)} + 566_{(7)} + 2521_{(7)}$

Resolución. *Colocamos los números como se nos es habitual:*

$$\begin{array}{r} 423+ \\ 566 \\ 2521 \\ \hline 4143_{(7)} \end{array}$$

lo cual se desarrolló de la siguiente manera:

$$3 + 6 + 1 = 10$$

como $10 = 7 + 3$*; se pone* 3 *y se lleva* $\boxed{1}$.

$$\boxed{1} + 2 + 6 + 2 = 11$$

como $11 = 7 + 4$*; se pone* 4*, se lleva* $\boxed{1}$.

$$\boxed{1} + 4 + 5 + 5 = 15$$

como $15 = 14 + 1$ *;* $15 = 2 \cdot 7 + 1$*; se pone* 1*, y se lleva* $\boxed{2}$.

$$\boxed{2} + 2 = 4$$

Resta

El método es similar a la resta en la base 10. Cuando la base es otra, se añade como unidad el valor de la base.

Ejemplo 3.6. *Operar* $4735_{(8)} - 2367_{(8)}$

Resolución.

$$\begin{array}{r} 4735- \\ 2367 \\ \hline 2346_{(8)} \end{array}$$

Desarrollo:
$5-7$ *no se puede restar, entonces, en la segunda columna tomamos prestada* 1 *unidad a* 3*, lo que nos permite añadir a* 5 *el valor de la base:*

$$(5+8)-7=6$$

Como a 3 *se quitó* 1 *unidad, ahora es* 2*, pero* $2-6$ *no se puede restar, entonces:*

$$(2+8)-6=4$$

Como a 7 *se le había quitado* 1 *unidad, ahora es* 6*:*

$$6-3=3$$

Ahora no se ha quitado nada.
Finalmente:

$$4-2=2$$

3.4. Cambio de base

Caso I: Un número de cualquier base pasar a base 10

Regla:
Se descompone polinómicamente el número dado. El número que resulta de sumar las unidades simples (u.s.) de este número es el número en base 10.

Ejemplo 3.7. *Convertir* $2674_{(8)}$ *al sistema de numeración decimal.*

Resolución. *Se descompone polinómicamente y se suma:*

$$\begin{aligned} 2674_{(8)} &= 2\cdot 8^3 + 6\cdot 8^2 + 7\cdot 8 + 4 \\ &= 2(512) + 6(64) + 7(8) + 4 \\ &= 1024 + 384 + 56 + 4 \\ &= 1468 \end{aligned}$$

$$\therefore \quad 2674_{(8)} = 1468$$

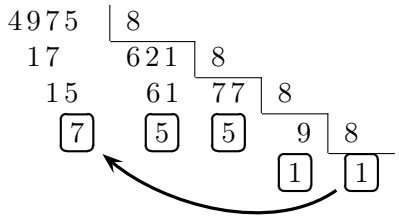
Caso II: Un número de base 10 pasar a otro sistema de base "$\mathbb{N}$"

Regla:

Se divide el número dado entre el valor "$\mathbb{N}$" de la base deseada, lo cual arroja un cociente. Este cociente se divide nuevamente entre el valor "$\mathbb{N}$", sucesivamente hasta obtener un último cociente cuyo valor sea menor a la base. Luego, tomando la cifra del último cociente y las cifras de los residuos en el orden del último al primero, queda formado el número de base "$\mathbb{N}$".

Ejemplo 3.8. *Pasar 4975 a base 8.*

Resolución.



$$\therefore \quad 4975 = 11557_{(8)}$$

Caso III: De un número no decimal a otro no decimal

Regla:

Primero se pasa a base 10 y luego, el nuevo número, a la base pedida.

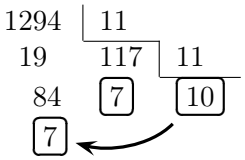
Ejemplo 3.9. *Convertir $3526_{(7)}$ al sistema de numeración undecimal.*

Resolución.

Paso I: Convertir $3526_{(7)}$ al sistema decimal (Caso I).

$$\begin{aligned} 3526_{(7)} &= 3\cdot 7^3 + 5\cdot 7^2 + 2\cdot 7 + 6 \\ &= 3(343) + 5(49) + 2(7) + 6 \\ &= 1029 + 245 + 14 + 6 \\ &= 1294 \end{aligned}$$

Paso II: Convertir 1294 al sistema de numeración undecimal (Caso II).



$$\therefore \quad 3526_{(7)} = A77_{(11)} \qquad (A: \textit{Diez})$$

Casos abreviados de conversión

Caso I: De base "$\mathbb{N}$" a base "$\mathbb{N}^k$" $(k \in \mathbb{N})$.

Se divide al número de base "$\mathbb{N}$" en grupos de "k" cifras (comenzando por la derecha) y luego a cada grupo se le convierte directamente (mediante descomposición polinómica) al sistema de base "$\mathbb{N}^k$".

Ejemplo 3.10. *Convertir $10100110101111100011_{(2)}$ al sistema octal.*

Resolución. *De base* 2 *a base* $8 = 2^3$ *(*$N = 2$ *y* $k = 3$*)*

$$\overbrace{10}^{\downarrow 2}\ \overbrace{100}^{\downarrow 4}\ \overbrace{110}^{\downarrow 6}\ \overbrace{101}^{\downarrow 5}\ \overbrace{111}^{\downarrow 7}\ \overbrace{100}^{\downarrow 4}\ \overbrace{011}^{\downarrow 3}{}_{(2)}$$

$$\therefore \quad 10100110101111100011_{(2)} = 2465743_{(8)}$$

Caso II: De base "N^k" a base "N" $(k \in \mathbb{N})$**.**
A cada una de las cifras del número de base "N^k" se les convierte directamente (mediante divisiones sucesivas) al sistema de base "N" teniendo cuidado de obtener grupos de "k" cifras por cada cifra convertida (los grupos incompletos se llenan con ceros a la izquierda).

Ejemplo 3.11. *Convertir* $642673_{(8)}$ *al sistema de numeración binario.*

Resolución. *De base* $8 = 2^3$ *a base* 2 *(*$N = 2$ *y* $k = 3$*)*

$$\overbrace{110}^{\downarrow 6}\ \overbrace{100}^{\downarrow 4}\ \overbrace{010}^{\downarrow 2}\ \overbrace{110}^{\downarrow 6}\ \overbrace{111}^{\downarrow 7}\ \overbrace{011}^{\downarrow 3}{}_{(2)}$$

$$\therefore \quad 642673_{(8)} = 110100010110111011_{(2)}$$

3.5. Propiedades de la numeración

[A] Toda base es mayor que cualquiera de sus cifras.

$$\text{BASE} > \text{CIFRA}$$

CIFRA MAYOR = BASE -1

[B] Si un número se expresa en dos sistemas de numeración, se cumple que:

"A mayor representación aparente le corresponde menor base y viceversa"

Por ejemplo, en la igualdad $(a \neq 0)$: $\overline{a\,b\,c\,d}_{(x)} = \overline{m\,n\,p}_{(y)}$ por tener una cantidad mayor de cifras se tiene que: $\overline{a\,b\,c\,d} > \overline{m\,n\,p} \Rightarrow \quad x < y$

Observaciones importantes

[A] Las operaciones aritméticas básicas en sistemas de numeración no decimales también tienen las mismas propiedades de asociatividad, conmutatividad y distributividad que ya conocemos para el sistema decimal.

[B] La representación de un número en determinada base es única. Por ejemplo, si

$$\overline{a\,b\,c}_{(N)} = \overline{w\,x\,y\,z}_{(N)}$$

entonces: $c = z$, $b = y$, $a = x$, y $w = 0$. Esto lo demostraremos más adelante (teorema 4.4).

Consideraciones finales

[A] Para convertir al mayor número de "k" cifras de base N al sistema decimal se puede utilizar la siguiente relación:

$$\underbrace{\overline{(N-1)(N-1)(N-1)\ldots(N-1)}_{(N)}}_{\text{"k" cifras}} = N^k - 1$$

Ejemplos 3.12.

$$666_{(7)} = 7^3 - 1 = 343 - 1 = 342$$
$$5555_{(6)} = 6^4 - 1 = 1296 - 1 = 1295$$
$$33333_{(4)} = 4^5 - 1 = 1024 - 1 = 1023$$

[B] Para bases sucesivas, o base de bases, puede usarse:

$$\overline{1a}_{\overline{1b}_{\overline{1c}\ddots_{\overline{1x}_{(N)}}}} = N + (a + b + c + \ldots + x)$$

Ejemplos 3.13.

$$16_{19_{15_{14_{17_{(N)}}}}} = N + (6 + 9 + 5 + 4 + 7) = N + 31$$

$$\overset{24 \text{ veces}}{15_{15_{15_{\ddots_{15}}}}}{}_{(X)} = X + (\underbrace{5 + 5 + 5 + \ldots + 5}_{24 \text{ sumandos}}) = X + 120$$

3.6. Problemas resueltos

En esta sección de ejercicios resueltos, las letras minúsculas representaran incógnitas que toman valores en el conjunto de las cifras válidas en el sistema de numeración en cuestión, así pues a es diferente a A ya que a es una incógnita mientras que A es una constante cuyo valor es 10.

Problema Resuelto 3.14. *Si los siguientes números están correctamente escritos:*

$$1211_{(p)} \quad ; \quad \overline{p21}_{(n)} \quad ; \quad \overline{n32q}_{(m)} \quad ; \quad \overline{n3m}_{(6)}$$

Calcular el máximo valor de $(m + n + p + q)$.

[a] 13 [b] 14 [c] 15 [d] 16 [e] 17

Resolución. *Observando convenientemente las desigualdades en cada número, se tiene:*

$$\begin{array}{cccc} 1211_{(p)} & \overline{p21}_{(n)} & \overline{n32q}_{(m)} & \overline{n3m}_{(6)} \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ 2 < p & p < n & n < m & m < 6 \end{array}$$

De donde:

$$2 < \underset{\downarrow}{p} < \underset{\downarrow}{n} < \underset{\downarrow}{m} < 6$$
$$\boxed{3} \quad \boxed{4} \quad \boxed{5}$$

Además $q < m \quad \Rightarrow \quad q < 5 \quad \Rightarrow$ *El mayor valor de* q *es* 4

$$\therefore \quad \textit{máx}\,(m + n + p + q) = 5 + 4 + 3 + 4 = 16$$

Respuesta $\boxed{d}$

Problema Resuelto 3.15. *Determine el valor de* $(a + b + c)$ *si se cumple que:*

$$\overline{a\,b\,c\,5}_{(n)} = \overline{5\,n\,0}_{(7)}$$

$\boxed{a}$ 7 $\boxed{b}$ 8 $\boxed{c}$ 9 $\boxed{d}$ 6 $\boxed{e}$ 5

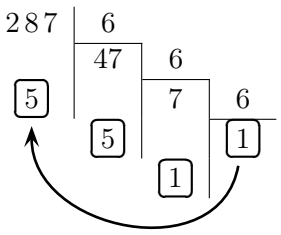
Resolución.

$$\overset{\Downarrow}{\overline{a\,b\,c\,5}_{(n)}} = \overset{\Downarrow}{\overline{5\,n\,0}_{(7)}}$$
$$5 < n \qquad n < 7$$

Vinculando las desigualdades: $5 < n < 7 \quad \Rightarrow \quad n = 6$
Entonces el dato quedará:

$$5\,6\,0_{(7)} = \overline{a\,b\,c\,5}_{(6)} \qquad (3.1)$$

Para calcular a, b *y* c *convertimos el número* $5\,6\,0_{(7)}$ *a base* 6*:*

- $5\,6\,0_{(7)} = 5 \cdot 7^2 + 6 \cdot 7 + 0 = 245 + 42 + 0 = 287 \qquad \longleftarrow \qquad$ *Base* 10
- 

$$\Rightarrow \quad 5\,6\,0_{(7)} = 1\,1\,5\,5_{(6)}$$

De **[3.1]** *y* **[3.15]***:* $a = 1$, $b = 1$, $c = 5$

$$\therefore \quad a + b + c = 7$$

Respuesta $\boxed{a}$

Problema Resuelto 3.16. *Calcular "*n*" si se cumple que:* $24_{19_{19_{19\ldots_{19}}}}{}_{(n)} = 558_{(9)}$

24 veces

$\boxed{a}$ 10 $\boxed{b}$ 11 $\boxed{c}$ 12 $\boxed{d}$ 13 $\boxed{e}$ 14

Resolución. *Aplicando bases de bases:* $19_{19_{19_{\cdot^{\cdot^{\cdot}}19_{(n)}}}} = n + 24 \cdot 9 = n + 216$

El dato queda: (24 *veces*)

$$24_{(n+216)} = 558_{(9)}$$

Por descomposición polinómica:

$$2(n+216)+4 = 5 \cdot 9^2 + 5 \cdot 9 + 8$$
$$2n + 432 + 4 = 405 + 45 + 8 \quad \Rightarrow \quad \therefore \quad n = 11$$

Respuesta [b]

EJERCICIOS

Ejercicio 3.1. *Si se cumple que:* $\overline{a89}_{(m)} = \overline{81m}_{(n)} = \overline{6mp}_{(12)}$
¿Cuál es el valor de $(a+m+n+p)$*?*

[a] 31 [b] 33 [c] 35 [d] 27 [e] 24

Ejercicio 3.2. *Calcular el valor de* $(a+b+n)$*, si:*

$$\overline{aa07}_{(n)} = \overline{bab}_{(9)}$$

[a] 13 [b] 14 [c] 15 [d] 16 [e] 17

Ejercicio 3.3. *Calcular* $(a+b+n)$ *en:* $1105_{(n)} = \overline{aba}_{(7)}$

[a] 11 [b] 12 [c] 13 [d] 14 [e] 15

Ejercicio 3.4. *Sabiendo que:* $\overline{23a}_{(9)} = \overline{27b}_{(n)} = \overline{36a}_{(p)}$
Determinar el valor de: $(b-a+n+p)$

[a] 17 [b] 18 [c] 19 [d] 20 [e] 21

Ejercicio 3.5. *Calcular "n" si se cumple que:* $\overline{1n}_{\overline{1n}_{\overline{1n}_{\cdot^{\cdot^{\cdot}}\overline{1n}_{(8)}}}} = 112_{(n)}$

"n" veces

[a] 3 [b] 4 [c] 5 [d] 6 [e] 7

Lectura complementaria:
Revisar las soluciones a los problemas de aritmética [7, Problemas 1.23, 1.23, 1.24, 1.25, 1.26 y 1.28].

4 | Representación decimal de enteros

Otra aplicación del lema de la división, es la demostración que cualquier número puede escribirse en base k de forma única, comenzamos con el sistema decimal ($k = 10$).

Teorema 4.1. *Si b es un entero positivo, entonces existen enteros únicos $r_0, r_1, \ldots, r_n$ tales que*

$$b = r_n 10^n + r_{n-1} 10^{n-1} + \ldots + r_1 10 + r_0$$

con $0 \leq r_i < 10$ para todo i.

Demostración. Usaremos inducción sobre b. Si $b = 1$ es cierto. Supongamos el resultado cierto para todo entero menor que b, y probaremos la afirmación para b. Podemos dividir b por 10 para obtener enteros únicos q y r_0 tales que $b = q \cdot 10 + r_0, \quad 0 \leq r_0 < 10$. Como q es menor que b, aplicamos la hipótesis de inducción a q. Luego existen enteros únicos $r_1, r_2, \ldots, r_n$, con $0 \leq r_i < 10$, tales que $q = r_n 10^{n-1} + \ldots + r_2 10 + r_1$. Por lo tanto

$$b = (r_1 + r_2 10 + \ldots + r_n 10^{n-1})10 + r_0 = r_n 10^n + \ldots + r_1 10 + r_0.$$

Es claro que todos los r_i son únicos, esto termina la demostración. □

Podemos aprovechar esto momento en la discusión para enunciar un teorema más general, al cual llamaremos Teorema de existencia y unicidad de representación en sistemas de numeración posicionales. El cual nos dice que teniendo una base k de un sistema de numeración, cualquier número N admite una única representación en base k. Para la demostración utilizaremos dos lemas:

Lema 4.2. *Si x es cualquier número real distinto de uno, entonces* $\sum_{i=0}^{n-1} x_i = \dfrac{x^n - 1}{x - 1}$.

Lema 4.3. *Sean m y n dos enteros positivos, tal que $m > 1$, entonces $m^n > n$.*

Teorema 4.4 (Teorema de existencia y unicidad de representación en sistemas de numeración)**.** *Sea k cualquier entero mayor que uno. Entonces, para cada entero positivo N, existe una representación $N = a_n k^n + a_{n-1} k^{n-1} + \ldots + a_1 k^1 + a_0 k^0$, donde $a_n \neq 0$ y cada a_i es no negativo y menor que k. Además, esta representación es única; llamada la representación de N en la base k.*

Demostración. Sea $P_k(N)$ la cantidad de representaciones de N en base k. Se debe probar que $P_k(N)$ siempre es igual a 1. Algunos a_i en la representación particular pueden ser cero. Luego, la representación no se afecta si excluimos dichos términos. Así supóngase:

$$N = a_n k^n + a_{n-1} k^{n-1} + \ldots + a_t k^t$$

donde $a_n \neq 0$ y $a_t \neq 0$. Entonces

$$\begin{aligned} N - 1 &= a_n k^n + a_{n-1} k^{n-1} + \ldots + a_t k^t - 1 \\ &= a_n k^n + a_{n-1} k^{n-1} + \ldots + a_t k^t - k^t + k^t - 1 \\ &= a_n k^n + a_{n-1} k^{n-1} + \ldots + k^t(a_t - 1) + k^t - 1 \\ &= a_n k^n + a_{n-1} k^{n-1} + \ldots + k^t(a_t - 1) + \Sigma_{i=0}^{t-1} k^i (k - 1) \end{aligned}$$

De aquí deducimos que para cada representación de N en base k, se puede hallar una representación para $N-1$, así: $P_k(N) \leq P_k(N-1)$, y en general si $N \geq 3$, entonces $P_k(N) \leq P_k(N-1) \leq P_k(N-2)$ y

$$P_k(N) \leq P_k(N-1) \leq P_k(N-2) \leq \ldots \leq P_k(1) = 1.$$

Además $k^{n+1} > N$ y como k^{n+1} tiene al menos una representación ($P_k(k^{n+1}) \geq 1$), se tiene que

$$1 \leq P_k(k^{n+1}) \leq P_k(N) \leq P_k(1) = 1 \Rightarrow 1 \leq P_k(k^{n+1}) \leq 1 \Rightarrow P_k(N) = 1$$

□

Definición 4.5. *La **representación decimal de enteros** es un sistema de numeración que tiene 10 como base. Bajo este sistema de representación, un número con $(n+1)$ dígitos (donde n es un entero no negativo)* $N = \overline{a_n a_{n-1} \ldots a_1 a_0}$ *es:*

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0. \tag{4.1}$$

La ventaja de la representación **[4.1]** es un número entero que se expande como $n+1$ partes independientes, por lo que a pesar de que puede haber cifras desconocidas, las operaciones de suma, resta y multiplicación de enteros puede llevarse a cabo fácilmente.

4.1. Expansión decimal

En este apartado exponemos la expansión decimal de números enteros cuando están formados por el mismos dígitos o bloques periódicos de dígitos

$$\underbrace{\overline{aaa\ldots a}}_{n} = a(10^{n-1} + 10^{n-2} + \ldots + 10 + 1) = \frac{a}{9}(10^n - 1),$$

$$\underbrace{\overline{abcabc\ldots abc}}_{n \text{ de } \overline{abc}} = \overline{abc}(10^{3(n-1)} + 10^{3(n-2)} + \ldots + 10^3 + 1) = \frac{\overline{abc}}{999}(10^{3n} - 1)$$

4.2. Problemas resueltos

Problema Resuelto 4.6. *Encontrar el menor número entero tal que su primer dígito es 4, y el valor del número obtenido al mover este 4 al último lugar es $\frac{1}{4}$ del valor del número original.*

Resolución. *Supongamos que el número entero buscado es N y que tiene $n+1$ dígitos, entonces $N = 4 \cdot 10^n + x$, donde x es un número de n dígitos. De las hipótesis se desprende que*

$$4(10x + 4) = 4 \cdot 10^n + x, \text{ i.e. } 39x = 4(10^n - 4) = 4 \cdot \underbrace{\overline{99\ldots96}}_{n-1},$$

$$13x = 4 \cdot \underbrace{\overline{33\ldots32}}_{n-1} \text{ y } 13 \mid \underbrace{\overline{33\ldots32}}_{n-1}$$

Al revisar cada caso: $n = 1, 2, \ldots$, es fácil ver que el valor mínimo de n es 5:

$$33332 \div 13 = 2564 \quad \therefore \quad x = 4 \cdot 2564 = 10256 \text{ y } N = 410256.$$

Problema Resuelto 4.7. *Sea $\overline{abcdef}$ un número entero de 6 dígitos tal que $\overline{defabc}$ es seis veces el valor de $\overline{abcdef}$. Encuentre el valor de $a + b + c + d + e + f$.*

Resolución. *De las condiciones se deducen las siguientes igualdades:*

$$(1000)(\overline{def}) + \overline{abc} = 6[(1000)(\overline{abc}) + \overline{def}],$$
$$(994)(\overline{def}) = (5999)(\overline{abc}),$$
$$(142)(\overline{def}) = (857)(\overline{abc}).$$

Por lo que $857 \mid (142)(\overline{def})$. *Como* 857 *y* 142 *no tienen factores comunes más que 1, entonces* $857 \mid \overline{def}$. *Además* $2 \cdot 857 > 1000$ *no es un número de tres dígitos, se tiene que* $\overline{def} = 857$. *Por lo que,* $\overline{abc} = 142$, *y*

$$a + b + c + d + e + f = 1 + 4 + 2 + 8 + 5 + 7 = 27.$$

Problema Resuelto 4.8. *Probar que cada número en la sucesión* $12, 1122, 111222, \ldots$ *es producto de dos números consecutivos.*

Resolución. *Por la representación decimal de números con cifras repetidas, tenemos:*

$$\underbrace{11\ldots11}_{n}\underbrace{22\ldots22}_{n} = \overline{\left[\frac{1}{9}(10^n - 1)\right]\left[\frac{2}{9}(10^n - 1)\right]}$$
$$= \frac{1}{9}(10^n - 1) \cdot 10^n + \frac{2}{9}(10^n - 1)$$
$$= \frac{1}{9}(10^n - 1)(10^n + 2) = \left(\frac{10^n - 1}{3}\right) \cdot \left(\frac{10^n + 2}{3}\right)$$
$$= \left(\frac{10^n - 1}{3}\right) \cdot \left(\frac{10^n - 1}{3} + 1\right) = A \cdot (A + 1),$$

donde $A = \frac{1}{3}(10^n - 1) = \underbrace{\overline{33\ldots33}}_{n}$ *es un número entero. La conclusión está probada.*

Problema Resuelto 4.9. *Encuentre el menor número natural* n *que tiene las siguientes propiedades:*

[A] *Su representación decimal tiene* 6 *como dígito de las unidades.*

[B] *Si el dígito de las unidades* 6 *se borra y se coloca delante de los dígitos restantes, el número resultante es cuatro veces más grande que el original número* n.

Resolución. *Es claro que* n *no es un número de un dígito. Sea* $n = 10x + 6$, *donde* x *is un número natural de* m *dígitos. Entonces*

$$6 \cdot 10^m + x = 4(10x + 6) \Rightarrow 39x = 6 \cdot 10^m - 24 \Rightarrow 13x = 2 \cdot 10^m - 8,$$

entonces $13 \mid (2 \cdot 10^m - 8)$ *para algún* m, *i.e. el residuo de* $2 \cdot 10^m$ *es 8 cuando se divide por* 13. *Por la división larga, podemos averiguar que el mínimo valor de* m *es* 5. *Entonces,*

$$x = \frac{2 \cdot 10^m - 8}{13} = \frac{199992}{13} = 15384, \qquad n = 153846.$$

EJERCICIOS

Ejercicio 4.1. *Demostrar que cuando* $\overline{abc}$ *es múltiplo de* 37, *entonces también* $\overline{bca}$ *lo es.*

Ejercicio 4.2. *Encontrar todos los números enteros positivos con dígito inicial 6 de tal manera que el número entero formado por la eliminación de este 6 es* $\frac{1}{25}$ *del entero inicial.*

Ejercicio 4.3. *Sea x un número de tres dígitos tal que la suma de sus dígitos es 21. Si los dígitos de x se invierten, el número así formado excede a x por 495. ¿Quién es x?*

Ejercicio 4.4. *Demostrar que cada uno de los siguientes números es un número cuadrado perfecto:*

$$729, 71289, 7112889, 711128889, \ldots$$

Ejercicio 4.5. *Encontrar el menor número natural $\mathfrak{n}$, de tal manera que su valor se convertirá en $5\mathfrak{n}$ cuando el último dígito se desplaza hasta el primer lugar.*

Ejercicio 4.6. *Sabiendo que la suma de un número $\mathfrak{n}$ de cuatro dígitos con la de todos sus dígitos es 2001. Encontrar $\mathfrak{n}$.*

Ejercicio 4.7. *Si un número de cuatro dígitos satisface las siguientes condiciones:*

- **[A]** *cuando su cifra de las unidades y centenas se intercambian, y también se intercambian la cifra de las decenas y millares, entonces el valor del número aumenta 5940.*
- **[B]** *el residuo es 8 cuando se divide por 9.*

Encontrar el menor número de cuatro dígitos que cumpla estas condiciones.

Ejercicio 4.8. *Encontrar el valor máximo del cociente de un número de tres dígitos con la suma de sus dígitos.*

Ejercicio 4.9. *Cuando un número de dos dígitos se divide por el número formado al intercambiar dos dígitos, el cociente es igual a su residuo. Encuentre el número de dos dígitos.*

Ejercicio 4.10. *Encontrar un número cuadrado perfecto de cuatro dígitos, de tal manera que los dos primeros dígitos son iguales y los últimos dos dígitos también lo son.*

Lectura complementaria:
Revisar las soluciones a los problemas de aritmética [7, Problemas 1.11, 1.12, 1.13, y 1.19].

Ecuaciones diofánticas

5 | Ecuación diofántica lineal

Se llama **ecuación diofántica** a cualquier ecuación (generalmente de varias variables), planteada sobre el conjunto de los números enteros $\mathbb{Z}$, es decir, se buscan las soluciones enteras (soluciones con coordenadas enteras) que satisfacen la ecuación.

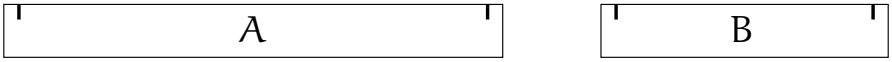
Aquí estudiaremos las ecuaciones diofánticas lineales.

Introducción

Actividad 5.1. ***¿Reglas sin graduación?***

Esta actividad sirve como motivación para el estudio de las ecuaciones diofánticas lineales. Los objetivos son descubrir cuando una ecuación diofántica lineal tiene solución, encontrar soluciones particulares e indagar cuántas soluciones tiene.

Proponemos el siguiente situación: Supongamos que tenemos dos reglas y que podemos marcarlas, la regla A tiene dos marcas cuya distancia es $31\,\mathrm{cm}$ y la regla B tiene dos marcas cuya distancia es $17\,\mathrm{cm}$ como lo indica la siguiente figura (a escala):



Responder las siguientes cuestiones:

[A] *¿Es posible graduar las reglas con marcas a $1\,\mathrm{cm}$ de distancia? Si su respuesta es "Si" dar dos demostraciones formales con distintos argumentos (una demostración puede ser el procedimiento para graduarlas) y si su respuesta es "No" basta solo una demostración.*

[B] *Si la situación se repite con otras reglas cuyas marcas están a $9\,\mathrm{cm}$ y $15\,\mathrm{cm}$ ¿que respondería a la cuestión anterior?*

[C] *Si la situación se vuelve a repetir con otras reglas cuyas marcas están a $337\,\mathrm{cm}$ y $243\,\mathrm{cm}$ ¿Es posible graduar las reglas con marcas a $1\,\mathrm{cm}$ de distancia? Basta decir "Si" o "No"*

[D] *Haga un planteamiento matemático de la cuestión anterior, observando que el problema se resuelve si con las reglas dadas se logra de alguna forma medir $1\,\mathrm{cm}$.*

Ahora consideramos el problema siguiente:

> Sean a, b y c enteros. Encontrar todas las soluciones *enteras* de la ecuación $ax + by = c$, es decir, pares ordenados $(x; y)$ tales que x y y son números enteros.

La igualdad $ax + by = c$ es una ecuación lineal y en el plano cartesiano su gráfica es una línea recta, por ende sabemos encontrar todas sus soluciones reales. Por ejemplo, si $b \neq 0$, es el conjunto de los puntos de la forma $(x, \frac{c - ax}{b})$ para $x \in \mathbb{R}$ son todas las soluciones. Decimos que $(x, \frac{c - ax}{b})$ es la *solución general* de la ecuación, es decir una fórmula que involucra parámetros (aquí un único parámetro x) que describe todas las soluciones.

El problema que consideramos aquí es diferente y más complicado, porque buscamos solamente las soluciones con x y $y = \dfrac{c - ax}{b}$ enteros. Nuestro problema por lo tanto, es escribir la solución general de la ecuación diofántica lineal $ax + by = c$ con x y y como incógnitas y a, b y c como constantes conocidas. Veremos más adelante que para escribir esta solución general solamente necesitaremos un parámetro t

Como la situación se trata de resolver ecuaciones, siempre hay tres preguntas naturales que hacer:

- ¿Cómo averiguar si tiene soluciones?
- ¿Cuántas soluciones tiene?
- ¿Cuáles son las soluciones? o ¿Cuál es la fórmula general para las soluciones (pude que involucre parámetros)?

En la resolución de las ecuaciones diofánticas $ax + by = c$, el MCD de a y b tiene un papel fundamental, y puede comenzarse estudiando el caso homogéneo ($c = 0$). Nosotros nos aventuraremos directamente a estudiar el caso general.

Resolución de la ecuación lineal diofántica $ax + by = c$

El método práctico para encontrar todas las soluciones a la ecuación diofántica lineal está fundamentado en los siguientes dos teoremas

Teorema 5.2. *La ecuación*

$$ax + by = c \tag{5.1}$$

tiene solución si y sólo si $d \mid c$*, donde* $d = (a : b)$.

Demostración. Notemos en primer lugar que $d \mid a$ y $d \mid b$, si además la ecuación **[5.1]** tiene solución $(x; y)$ se tiene que $d \mid ax + by$, por lo tanto $d \mid c$.

Recíprocamente, supongamos que $d \mid c$. Dividiendo por d la ecuación original, nos da

$$a'x + b'y = c' \tag{5.2}$$

donde $a' = a/d$, $b' = b/d$ y $c' = c/d$. Es claro que si **[5.2]** tiene solución, entonces **[5.1]** también posee solución y viceversa. Luego ambas ecuaciones son equivalentes.

Notemos que $(a' : b') = 1$, y por lo tanto existen enteros x'_0 e y'_0 tales que

$$a'x'_0 + b'y'_0 = 1.$$

No es difícil verificar que $x_0 = c'x'_0$ e $y_0 = c'y'_0$ son solución de **[5.2]** y por lo tanto solución de **[5.1]**. □

Teorema 5.3. *Si la ecuación lineal diofántica* **[5.1]** *posee solución y* $(x_0; y_0)$ *es una solución particular, entonces toda otra solución* $(x; y)$ *es de la forma*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

donde t *es cualquier número entero y* $d = (a : b)$.

Demostración. En primer lugar, probaremos que x y y son solución. En efecto

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 = c$$

Por otro lado si $(x;y)$ es cualquier solución de **[5.1]**, también lo será de **[5.2]** y en consecuencia

$$a'(x-x_0)+b'(y-y_0)=c'-c'=0$$

de donde

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

De acá se deduce $a' \mid b'(y-y_0)$ y por lo tanto $a' \mid (y-y_0)$. Luego $y=y_0+a't$, donde t es un entero. Igualmente, se verifica $x=x_0+b's$, con s entero.

Probaremos que $s=-t$, para lo cual sustituimos la solución $(x;y)$ en **[5.2]**

$$\begin{aligned} a'(x_0+b's)+b'(y_0+a't)&=c'\\ a'x_0+b'y_0+a'b'(s+t)&=c' \end{aligned}$$

como $(x_0;y_0)$ es solución de **[5.2]** se tiene $a'x_0+b'y_0=c'$, y por lo tanto

$$\begin{aligned} c'+a'b'(s+t)&=c'\\ a'b'(s+t)&=0 \end{aligned}$$

de donde $s=-t$. Con esto termina la demostración. □

Detallamos a continuación la estrategia para resolver la ecuación diofántica lineal $ax+by=c$.

[A] Determinar si la ecuación tiene o no tiene soluciones. La ecuación tiene solución si y solo si el MCD de a y b divide c. Si $(a:b) \nmid c$ parar. Podemos calcular $(a:b)$ utilizando el algoritmo de Euclides y luego hacer sustituciones sucesivas desde la última a la primera igualdad.

[B] Encontrar una solución particular de $ax+by=c$. Una solución particular es proporcionada por la identidad de Bezout. En efecto, esta identidad es de la forma $ua+vb=(a:b)$. En el etapa anterior hemos determinado que $(a:b)$ divide c. Encontramos el entero m tal que $c=m(a:b)$. Multiplicamos la igualdad por m, obtenemos: $(mu)a+(mv)b=m(a:b)=c$. Por lo tanto, $x_0=mu$, $y_0=mv$ es una solución particular de la ecuación.

[C] Escribir la solución general de la ecuación.

Veamos ahora algunos ejemplos de cómo se aplica la estrategia de solución.

Ejemplo 5.4. *Resolvamos la ecuación diofántica* $143x+231y=321$.

Al calcular el MCD de 143 *y* 231 *obtenemos (comprobarlo) que* $(143:231)=11$ *y* $11 \nmid 321$*. Por lo tanto la ecuación no tiene soluciones enteras.*

Ejemplo 5.5. *A continuación, resolvemos el problema siguiente:*

> *Se ha gastado $\$85.39$ en bolígrafos y cuadernos. Cada bolígrafo costaba $\$1.27$ y cada cuaderno costaba $\$3.23$. ¿Cuál es la menor cantidad de bolígrafos y cuadernos que fueron comprados?*

Sea x la cantidad de bolígrafos y y la cantidad de cuadernos. Expresamos los precios en centavos. Tenemos la relación $127x+323y=8539$.

Comprobamos que la ecuación admite soluciones enteras calculando el MCD de 127 *y* 323 *con el algoritmo de Euclides.*

$$\begin{aligned} 323&=2\times 127+69\\ 127&=1\times 69+58\\ 69&=1\times 58+11\\ 58&=5\times 11+3\\ 11&=3\times 3+2\\ 3&=1\times 2+1\\ 2&=2\times 1+0 \end{aligned}$$

El MCD de 127 *y* 323 *es* 1*. Por lo tanto la ecuación admite soluciones.*

Buscamos ahora una solución particular de la ecuación haciendo sustituciones sucesivas. Comenzamos con $a = 127$ *y* $b = 323$

$$\begin{array}{rcll} b = 2\times a + 69 & \longrightarrow & 69 = b - 2a & \\ a = 1\times 69 + 58 & \longrightarrow & 58 = a - 69 & = a - (b-2a) \qquad = 3a - b \\ 69 = 1\times 58 + 11 & \longrightarrow & 11 = 69 - 58 & = (b-2a) - (3a-b) \qquad = -5a + 2b \\ 58 = 5\times 11 + 3 & \longrightarrow & 3 = 58 - 5\times 11 & = (3a-b) - 5(-5a+2b) \qquad = 28a - 11b \\ 11 = 3\times 3 + 2 & \longrightarrow & 2 = 11 - 3\times 3 & = (-5a+2b) - 3(28a-11b) \qquad = -89a + 35b \\ 3 = 1\times 2 + 1 & \longrightarrow & 1 = 3 - 2 & = (28a-11b) - (-89a+35b) \qquad = 117a - 46b \end{array}$$

Por lo tanto, $117a - 46b = 1$*. Multiplicando por* 8539 *obtenemos* $999063a - 392794b = 8539$*. Vemos que una solución particular de la ecuación es* $(x;y) = (999063;-392794)$*.*

Resolvemos ahora la ecuación homogénea asociada $127x + 323y = 0$*. Como* 127 *y* 323 *son coprimos, su solución general es* $(-323t;127t)$*. Finalmente, la solución general de la ecuación diofántica* $127x + 323y = 8539$ *es* $(x;y) = (999063 - 323t;-392794 + 127t)$*.*

Ahora imponemos las condiciones $x \geq 0$ *y* $y \geq 0$*, ya que las cantidades de bolígrafos y de cuadernos no pueden ser negativas. Para* $(x;y) = (999063 - 323t;-392794 + 127t)$*, son equivalentes a*

$$\begin{array}{lcll} 999063 - 323t \geq 0 \quad \wedge \quad -392794 + 127t \geq 0 & \Leftrightarrow & 392794/127 \leq t \leq 999063/323 \\ & \Leftrightarrow & 3092 + 110/127 \leq t \leq 3093 + 24/323 \\ & \Leftrightarrow & 3093 \leq t \leq 3093 \end{array}$$

Por lo tanto hay una única solución, corresponde a $t = 3093$*. Encontramos que la solución es* $x = 24$ *y* $y = 17$*, es decir, hemos comprado 24 bolígrafos y 17 cuadernos.*

Existe otro método debido a Euler para resolver la ecuación diofántica, consiste en despejar la incógnita con menor coeficiente en función de la otra, esto nos conduce a establecer una ecuación diofántica con coeficientes menores. Ilustramos este método con el siguiente ejemplo.

Ejemplo 5.6. *Resolver* $7x + 15y = 12$*.*

Despejamos de la ecuación original

$$x = \frac{12 - 15\cdot y}{7} = 1 - 2\cdot y + \frac{5-y}{7}$$

Si se requiere que x *y* y *sean enteros, debe suceder que* $t = \dfrac{5-y}{7}$ *sea entero, de donde* $y = 5 - 7t$*. Dándole valores enteros arbitrarios a* t*, podemos obtener valores enteros de* x *y* y*, que cumplen la ecuación original. Expresando* x *y* y *en función de* t *se deduce*

$$\begin{aligned} x &= -9 + 15t \\ y &= 5 - 7t. \qquad t \in \mathbb{Z} \end{aligned}$$

Haciendo $t = 0$ *obtenemos la solución particular* $x = -9$*,* $y = 5$*.*

EJERCICIOS

Ejercicio 5.1. *Encontrar todas las soluciones a las siguientes ecuaciones diofánticas lineales:*

[A] $30x + 36y = 24$,

[B] $30x + 36y = 4$,

[C] $54x + 21y = 906$,

[D] $158x - 57y = 7$

[E] $4147x + 10672y = 58$.

Ejercicio 5.2. *¿De cuántas maneras puede descomponerse a* 834 *como suma de dos números pares positivos, uno múltiplo de* 15 *y otro múltiplo de* 21*?*

Ejercicio 5.3. *Un cliente compró una docena de piezas de frutas, manzanas y naranjas por $1.32. El costo de una manzana es 3 centavos más que el de una naranja. Además compró más manzanas que naranjas. ¿Cuántas naranjas y manzanas compró?*

Ejercicio 5.4. *Resolver el siguiente sistema de ecuaciones:*

$$\begin{aligned} 16x + 15y &= 1 \\ 6x + 10y + 15z &= 11 \end{aligned}$$

Ejercicio 5.5. *Encontrar todas las soluciones positivas (soluciones que cumplan* $x > 0$ *y* $y > 0$*) de las siguientes ecuaciones:*

[A] $18x + 7y = 302$,

[B] $18x - 7y = 302$,

[C] $54x - 38y = 82$,

[D] $11x + 13y = 47$,

[E] $10x + 28y = 1240$

Ejercicio 5.6. *Mostrar que no existen enteros* a *y* b *tales que* $(a : b) = 7$ *y* $a + b = 100$*. Además comprobar que existen infinitos pares de números* $(a; b)$ *tales que* $(a : b) = 5$ *y* $a + b = 100$

Ejercicio 5.7. *Encontrar dos fracciones con* 5 *y* 7 *como denominadores, cuya suma sea igual a* $\dfrac{26}{35}$.

Ejercicio 5.8. *Encontrar un número que deje residuo* 16 *cuando se divide por* 39 *y residuo* 27 *cuando se divide por* 56.

Ejercicio 5.9. *Mostrar que* $a = 14t + 3$ *y* $b = 21t + 1$ *son primos relativos para cada* $t \in \mathbb{Z}$

Ejercicio 5.10. *¿Cuántos triángulos rectángulos cumplen con la siguiente condición: "Sus catetos son números enteros y si al mayor se le resta* 14 *y al menor se le agrega* 8*, la hipotenusa no varía"?*

6 | Ecuación pitagórica

Definición 6.1. *Se llama **ecuación pitagórica** a la ecuación diofántica* $x^2 + y^2 = z^2$ *y* **terna pitagórica** *a toda terna de números* $(x; y; z)$ *que satisface la igualdad* $x^2 + y^2 = z^2$*; si, además,* $(x : y : z) = 1$ *dicha terna pitagórica se llama* **primitiva**.

Teorema 6.2. *Las soluciones de la ecuación* $x^2 + y^2 = z^2$*, con* $x, y, z > 0$*,* $2 \mid x$*,* $(x : y : z) = 1$ *son*

$$\begin{aligned} x &= 2pq \\ y &= p^2 - q^2 \\ z &= p^2 + q^2 \end{aligned}$$

donde $p > q$*,* p *y* q *tienen distinta paridad y* $(p : q) = 1$.

Ejemplo 6.3. *Lo primero que vamos a hacer es ilustrar la demostración mediante un ejemplo:*

[A] *Tomamos dos números racionales positivos cuyo producto sea* 2*. Por ejemplo:*

$$\frac{3}{7} \quad y \quad \frac{14}{3} \qquad \left(\frac{3}{7} \cdot \frac{14}{3} = 2\right)$$

[B] *Sumamos* 2 *a cada racional:*

$$\frac{3}{7} + 2 = \frac{17}{7} \qquad \frac{14}{3} + 2 = \frac{20}{3}$$

[C] *Operamos para que las fracciones tengan el mismo denominador:*

$$\frac{17}{7} \cdot \frac{3}{3} = \frac{51}{21} \qquad \frac{20}{3} \cdot \frac{7}{7} = \frac{140}{21}$$

[D] *Tomamos los numeradores, elevamos cada uno de ellos al cuadrado y sumamos:*

$$51^2 + 140^2 = 22201$$

Como se tiene que $\sqrt{22201} = 149$*, hemos encontrado una terna pitagórica*

$$(51; 140; 149)$$

Demostración. **[A]** Tomamos dos números racionales positivos cuyo producto sea 2. Por ejemplo:

$$\frac{m}{n} \quad y \quad \frac{2n}{m} \qquad \left(\frac{m}{n} \cdot \frac{2n}{m} = \frac{2mn}{mn} = 2\right)$$

[B] Sumamos 2 a cada racional:

$$\frac{m}{n} + 2 = \frac{m + 2n}{n} \qquad \frac{2n}{m} + 2 = \frac{2n + 2m}{m}$$

[C] Operamos para que las fracciones tengan el mismo denominador:

$$\frac{m+2n}{n}\cdot\frac{m}{m}=\frac{m^2+2mn}{mn} \qquad \frac{2n+2m}{m}\cdot\frac{n}{n}=\frac{2n^2+2mn}{mn}$$

[D] Tomamos los numeradores, elevamos cada uno de ellos al cuadrado y sumamos:

$$(m^2+2mn)^2+(2n^2+2mn)^2=m^4+4m^3n+8m^2n^2+8mn^3+4m^4$$

Nos aparece un polinomio dependiente de m y de n que, para que el método funcione, debería ser un cuadrado perfecto. Y, en efecto, lo es:

$$(m^2+2mn+2n^2)^2=m^4+4m^3n+8m^2n^2+8mn^3+4n^4$$

Por tanto obtenemos la siguiente terna pitagórica

$$(m^2+2mn;2n^2+2mn;m^2+2mn+2n^2)$$

□

Relación entre las dos ternas pitagóricas: Hemos visto una forma de encontrar ternas pitagóricas. Una pregunta casi directa a partir de ello es: ¿Hay alguna relación entre ellas? La respuesta es sí. Vamos a verla:

Tomemos la terna pitagórica que encontramos con el método descrito y cambiemos los dos primeros elementos, obteniendo:

$$(2n^2+2mn;m^2+2mn;m^2+2mn+2n^2)$$

Expresemos cada uno de sus elementos de la siguiente forma:

$$(2(m+n)n;(m+n)^2-n^2;(m+n)^2+n^2)$$

Tomando $p=m+n$ y $q=n$ obtenemos la terna pitagórica que aparece en el enunciado del teorema.

EJERCICIOS

Ejercicio 6.1. *Si* $x^2+y^2=z^2$*, entonces* $60 \mid xyz$*.*

Ejercicio 6.2. *Si* $x^2+y^2=3z^2$*, entonces* $x=y=z=0$*.*

Ejercicio 6.3. *Si* c *es un entero impar, entonces la ecuación* $x^2+x-c=0$ *no tiene una soluciones enteras para* x*.*

Congruencias

7 Funciones especiales

7.1. Funciones Multiplicativas

Diremos que una función f es **completamente multiplicativa** si cumple que $f(ab) = f(a)f(b)$ para cualesquiera números enteros a y b y si se cumple $f(ab) = f(a)f(b)$ siempre que a y b sean coprimos, diremos que f es una función **multiplicativa**.

Aquí estudiaremos algunas funciones multiplicativas que permitirán responder curiosidades acerca de los números naturales, por ejemplo: ¿Cuántos divisores tiene?, ¿Cuántos de estos divisores son primos o compuestos?, ¿Cuál es la suma de todos los divisores?, etc.

7.2. Funciones σ y τ

Definición 7.1. *Sea n un entero positivo dado, denotaremos por:*

- $\tau(n)$ *a la cantidad de divisores positivos de n;*
- $\sigma(n)$ *a la suma de los divisores positivos de n.*

Ejemplo 7.2. **[A]** *Si p es un número primo, entonces $\tau(p) = 2$ y $\sigma(p) = p + 1$.*

Pues los únicos divisores positivos de p son 1 y p.

[B] *Si p un número primo y $e \geq 0$, entonces $\tau(p^e) = e + 1$ y $\sigma(p^e) = \dfrac{p^{e+1} - 1}{p - 1}$.*

En efecto, escribimos los divisores de p^e:

$$1, p, p^2, p^3, \ldots, p^{e-1}, p^e$$

observando la lista anterior es claro que p^e tiene $e+1$ divisores. Notar que la lista de divisores están en progresión geométrica, por lo que la suma de los divisores de p^e es una serie geométrica cuya suma es

$$\sigma(p^e) = 1 + p + p^2 + \ldots + p^e = \frac{p^{e+1} - 1}{p - 1}.$$

[C] *Sean p_1 y p_2 números primos diferentes, entonces $\tau(p_1^{e_1}p_2^{e_2}) = (e_1 + 1)(e_2 + 1)$ y $\sigma(p_1^{e_1}p_2^{e_2}) = \dfrac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{e_2+1} - 1}{p_2 - 1}$.*

Para contar los divisores de $p_1^{e_1}p_2^{e_2}$ los ordenamos de la siguiente manera

$$\begin{array}{cccccc}
1 & p_1 & p_1^2 & p_1^3 & \cdots & p_1^{e_1} \\
p_2 & p_1p_2 & p_1^2p_2 & p_1^3p_2 & \cdots & p_1^{e_1}p_2 \\
p_2^2 & p_1p_2^2 & p_1^2p_2^2 & p_1^3p_2^2 & \cdots & p_1^{e_1}p_2^2 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
p_2^{e_2} & p_1p_2^{e_2} & p_1^2p_2^{e_2} & p_1^3p_2^{e_2} & \cdots & p_1^{e_1}p_2^{e_2}
\end{array}$$

Como $(p_1 : p_2) = 1$ en el arreglo no hay repeticiones y tiene $(e_2 + 1)$ filas y $(e_1 + 1)$ columnas, por lo tanto hay $\tau(p_1^{e_1}p_2^{e_2}) = (e_1 + 1)(e_2 + 1)$ divisores.

Ahora al sumar verticalmente cada columna del arreglo anterior obtenemos respectivamente:

$$\sigma(p_2^{e_2}) \quad p_1\sigma(p_2^{e_2}) \quad p_1^2\sigma(p_2^{e_2}) \quad p_1^3\sigma(p_2^{e_2}) \quad \cdots \quad p_1^{e^1}\sigma(p_2^{e_2})$$

de donde

$$\begin{aligned}\sigma(p_2^{e_1}p_2^{e_2}) &= \sigma(p_2^{e_2}) + p_1\sigma(p_2^{e_2}) + p_1^2\sigma(p_2^{e_2}) + p_1^3\sigma(p_2^{e_2}) + \ldots + p_1^{e^1}\sigma(p_2^{e_2}) \\ &= (1 + p_1 + p_1^2 + p_1^3 + \ldots + p_1^{e_1})\sigma(p_2^{e_2}) \\ &= \sigma(p_1^{e_1})\sigma(p_2^{e_2}).\end{aligned}$$

[D] *Encuentre todos los divisores pares de* 1960.

En primer lugar $1960 = 2^3 \cdot 5 \cdot 7^2$ *notamos lo siguiente, si de* $2^3 \cdot 5 \cdot 7^2$ *sacamos un factor* 2 *tenemos que* $1960 = 2(2^2 \cdot 5 \cdot 7^2)$*, entonces basta con que encontremos la cantidad de divisores de* $(2^2 \cdot 5 \cdot 7^2)$ *ya que estos también serán divisores de 1960 y multiplicados por el 2 que sacamos de factor, tendremos la seguridad de que serán todos pares.*

Por tanto la cantidad de divisores pares de 1960 es $\tau(2^2 \cdot 5 \cdot 7^2) = (2+1)(1+1)(2+1) = 18$.

Proposición 7.3. *Las funciones* τ *y* σ *son multiplicativas, es decir, si* $(a : b) = 1$ *entonces:*

[A] $\tau(n) = \tau(a)\tau(b)$,

[B] $\sigma(n) = \sigma(a)\sigma(b)$.

Teorema 7.4. *Dado un número entero positivo* $n > 2$*, sea* $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ *la factorización canónica, entonces:*

[A] $\tau(n) = (e_1 + 1)(e_2 + 1)\cdots(e_r + 1)$

[B] $\sigma(n) = \dfrac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \dfrac{p_r^{e_r+1} - 1}{p_r - 1}$

Ejemplo 7.5. *Sea* n *es un entero positivo, encontrar la cantidad de pares ordenados* $(x; y)$ *de enteros positivos que son soluciones a la ecuación* $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{n}$.

Resolución.

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n} \Leftrightarrow xy = nx + ny \Leftrightarrow (x - n)(y - n) = n^2.$$

Si $n = 1$*, entonces inmediatamente deducimos que la única solución es el par ordenado* $(2; 2)$*. Para* $n \geq 2$*, sea* $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ *la factorización canónica de* n*. Como* $x, y > n$*, hay una correspondencia* 1 *a* 1 *entre las soluciones en* (x, y) *y los factores de* n^2*, entonces la cantidad de soluciones es* $\tau(n^2) = (2e_1 + 1)(2e_2 + 1)\cdots(2e_r + 1)$.

EJERCICIOS

Ejercicio 7.1. *Construir ejemplos para los cuales* $\tau(ab) \neq \tau(a)\tau(b)$ *y* $\sigma(ab) \neq \sigma(a)\sigma(b)$.

Ejercicio 7.2. *Sea* $n = 1152$

[A] *Encontrar* $\tau(n)$.

[B] *Resolver en los números naturales la ecuación* $x^2 - y^2 = n$.

[C] *Resolver en los números enteros la ecuación* $x^2 - y^2 = n$.

[D] *Si* p *es un número primo ¿Cuántas soluciones en* $\mathbb{Z}$ *tiene la ecuación* $x^2 - y^2 = p$.

7.3. Problemas resueltos

Problema Resuelto 7.6. *Determinar la cantidad de divisores compuestos de:* $N = 24^3 \cdot 21^2$

[a] 180 [b] 177 [c] 176 [d] 194 [e] 175

Resolución. *Todo número entero positivo tiene divisores primos, compuestos y la unidad, descomponiendo canónicamente:*

$$N = (2^3 \cdot 3)^3 \cdot (3 \cdot 7)^2 = 2^9 \cdot 3^3 \cdot 3^2 \cdot 7^2 = 2^9 \cdot 3^5 \cdot 7^3$$

Por lo tanto $\tau(N) = (9+1)(5+1)(2+1) = 180$*, así la cantidad de divisores compuestos son* $180 - 1 - 3 = 176$.

Respuesta [c]

Problema Resuelto 7.7. *Para el número* 2160*, determinar:*

[A] *¿Cuántos de sus divisores son múltiplos de* 2*?*

[B] *¿Cuántos de sus divisores son múltiplos de* 3*?*

[C] *¿Cuántos divisores son múltiplos de* 12*?*

[D] *¿Cuántos divisores son múltiplos de* 15*?*

[a] 72 [b] 90 [c] 124 [d] 95 [e] 200

Resolución. *La descomposición canónica de* 2160 *es:* $2160 = 2^4 \cdot 3^3 \cdot 5^1$
Su cantidad de divisores es: $\tau(2160) = 5 \cdot 4 \cdot 2 = 60$

[A] *Para calcular la cantidad de divisores múltiplos de* 2*, se separa en la descomposición canónica un factor* 2*:* $2160 = 2(2^3 \cdot 3^3 \cdot 5^1)$*. De este modo la cantidad de divisores múltiplos de* 2 *serán:* $4 \cdot 4 \cdot 2 = 32$

[B] *Si se desea calcular la cantidad de divisores múltiplos de* 3*, se separa en la descomposición canónica un factor* 3*:* $2160 = 3(2^4 \cdot 3^2 \cdot 5^1)$*, así la cantidad de divisores de* 2160 *que son múltiplos de* 3 *son:* $5 \cdot 3 \cdot 2 = 30$.

[C] *La cantidad de divisores múltiplos de* $12 = 2^2 \cdot 3$ *se calcula de la siguiente manera:* $2160 = 2^2 \cdot 3(2^2 \cdot 3^2 \cdot 5^1)$*, así la cantidad divisores de* 2160 *que son múltiplos de* 12 *es* $3 \cdot 3 \cdot 2 = 18$

[D] *Análogamente, la cantidad de divisores múltiplos de* 15 *(*$= 3 \cdot 5$*) será:*

$$2160 = 3 \cdot 5(\underbrace{2^4 \cdot 3^2}_{})$$

Los divisores de 2160 *que son múltiplos de* 15 *son:* $5 \cdot 3 = 15$

La suma de todos los resultados es: $32 + 30 + 18 + 15 = 95$ *Respuesta* [d]

Problema Resuelto 7.8. *¿Cuántos ceros hay que agregar a la derecha de* 275 *para que el número resultante tenga* 70 *divisores?*

[a] 2 [b] 3 [c] 4 [d] 5 [e] 6

Resolución.

Sea "n*" la cantidad de ceros agregados:*

$$N = 275\underbrace{000\ldots0}_{\text{“}n\text{”}} = 275 \cdot 10^n$$

Descomposición canónica

$$N = 5^2 \cdot 11 \cdot (2 \cdot 5)^n = 2^n \cdot 5^{n+2} \cdot 11^1$$

Por la información del problema tenemos que:

$$\tau(N) = 70 \Rightarrow (n+1)(n+3)(2) = 70$$

$$(n+1)(n+3) = 35 = 5 \cdot 7 \Rightarrow n = 4$$

Respuesta [c]

EJERCICIOS

Ejercicio 7.3. *Si* $N = 15 \cdot 21^n$*, tiene* 60 *divisores, encontrar "*n*".*

[a] 2 [b] 3 [c] 4
[d] 5 [e] 6

Ejercicio 7.4. *Si* $8^k + 8^k + 2$ *tiene* 84 *divisores compuestos, encontrar "*k*".*

[a] 4 [b] 5 [c] 6
[d] 7 [e] 8

Ejercicio 7.5. *Si los números* $24 \cdot 30^n$*,* $24^{n+3} \cdot 3^{2n+3}$ *tienen la misma cantidad de divisores, encontrar "*n*".*

[a] 3 [b] 4 [c] 5
[d] 6 [e] 7

Ejercicio 7.6. *Si "*m*" y "*n*" son dos números naturales cuya diferencia es* 3*, encontrar el valor de* $(m + n)$ *si* $3^m + 3^n$ *tiene* 36 *divisores*

[a] 9 [b] 11 [c] 13
[d] 15 [e] 16

Ejercicio 7.7. *Encontrar el valor de "*n*" para que la cantidad de divisores de* 30^n *sea el doble que la cantidad de divisores de* $15 \cdot 18^n$*.*

[a] 5 [b] 6 [c] 7
[d] 8 [e] 9

Ejercicio 7.8. *¿Cuántos divisores tiene el número* $N = 2^2 \cdot 3^a$ *sabiendo que al multiplicarse por* 18 *la cantidad de divisores aumenta en* 12*?*

[a] 16 [b] 15 [c] 12
[d] 18 [e] 24

Ejercicio 7.9. *Calcular el valor de "*n*" sabiendo que la expresión* 481^n *tiene* $\overline{n1}$ *divisores.*

[a] 4 [b] 5 [c] 6
[d] 8 [e] 9

Ejercicio 7.10. *Encontrar el residuo de dividir el producto de los* 2000 *primeros números primos por* 60*.*

[a] 10 [b] 20 [c] 30
[d] 40 [e] 15

Ejercicio 7.11. *¿Cuántos triángulos existen cuyos catetos sean número enteros y además tengan área* $600\,m^2$*?*

[a] 11 [b] 12 [c] 13
[d] 14 [e] 15

Ejercicio 7.12. ☺ *Si:* $63!$ *tiene "*n *divisores. ¿Cuántos tendrá* $64!$ *?*

[a] $\frac{64n}{29}$ [b] $\frac{32n}{29}$ [c] $\frac{16n}{29}$
[d] $\frac{16n}{58}$ [e] $\frac{12n}{58}$

Ejercicio 7.13. ☺ *Dar la suma de las cifras del número que descompuesto en sus factores primos es:* $3^a \cdot b^b \cdot a^3$*, sabiendo que tiene* 74 *divisores y no es múltiplo de* 27*.*

[a] 9 [b] 18 [c] 24
[d] 27 [e] 30

Ejercicio 7.14. *Sabiendo que el número* $24^n \cdot 36^n$ *tiene* 589 *divisores. Encontrar cuántos divisores tendrá* $18^n \cdot 30^n$

[a] 1729 [b] 1056 [c] 2640
[d] 585 [e] N.A.

Lectura complementaria:
Revisar la solución del problema de aritmética [7, pág. 1.33].

7.4. Función φ de Euler

La función φ de Euler (también llamada función indicatriz de Euler) es una función importante en teoría de números. Si n es un número entero positivo, entonces $\varphi(n)$ se define como la cantidad de enteros positivos menores o iguales a n y coprimos con n, es decir, formalmente se puede definir como:

Definición 7.9. *La función φ de Euler, aplicada al entero positivo m se define por*

$$\varphi(m) = |\{n \in \mathbb{N} : n \leq m \text{ y } (m : n) = 1\}|$$

En otras palabras, $\varphi(m)$ es la cantidad de enteros positivos mayores o iguales a uno, y menores que m, los cuales son primos relativos con m. Veamos a continuación una tabla con algunos valores de la función φ de Euler.

m	$\varphi(m)$	m	$\varphi(m)$	m	$\varphi(m)$	m	$\varphi(m)$
2	1	7	6	12	4	17	16
3	2	8	4	13	12	18	6
4	2	9	6	14	6	19	18
5	4	10	4	15	8	20	8
6	2	11	10	16	8	21	12

Observando las tablas, notamos que $\varphi(m)$ es par, para todo $m \geq 3$. Esto puede probarse de manera general. También es evidente que si p es primo, entonces $\varphi(p)$ es igual a $p - 1$. Nuestra próxima meta, será obtener una fórmula para calcular la función de Euler de un número compuesto apartir de su factorización canónica, este y otros resultados sobre esta función se resumen en el siguiente teorema:

Teorema 7.10 (Propiedades de la función φ)**.** *Sean a, b y e números enteros positivos.*

[A] *Si p es primo, entonces $\varphi(p) = p - 1$.*

[B] *Si p es primo y $e \geq 1$, entonces $\varphi(p^e) = p^e - p^{e-1}$.*

[C] *Si $(a : b) = d$, entonces $\varphi(ab) = \varphi(a)\varphi(b)\dfrac{d}{\varphi(d)}$.*

[D] *Si $(a : b) = 1$, entonces $\varphi(ab) = \varphi(a)\varphi(b)$.*

[E] *Sea n un número entero positivo, si $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ es la factorización canónica de n, entonces:*

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1})\cdots(p_r^{e_r} - p_r^{e_r-1}),$$
$$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2)\cdots(1 - 1/p_r).$$

Para ilustrar la forma operativa de como calcular valores particulares de la función $\varphi(n)$, consideremos los siguientes ejemplos:

Ejemplos 7.11. **[A]** *Calcular $\varphi(600)$.*

Resolución. *Calculamos $\varphi(600)$ de acuerdo a las fórmulas del teorema 7.10-E:*

$$\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^3) = \varphi(2^3)\varphi(3)\varphi(5^3) = (2^3 - 2^2)(3 - 1)(5^3 - 5^2) = 4 \cdot 2 \cdot 20 = 160,$$
$$\varphi(600) = 600(1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) = 160,$$

obteniendo en ambos casos el mismo resultado.

[B] *Mostrar que para cualquier $n \in \mathbb{N}$ se tiene que $\varphi(4n + 2) = \varphi(2n + 1)$*

Resolución. *Debido que $2n + 1$ es impar, los números 2 y $2n + 1$ son primos relativos, entonces $\varphi(2 \cdot (2n + 1)) = \varphi(2) \cdot \varphi(2n + 1)$, además $\varphi(2) = 1$, y así mostramos que: $\varphi(4n + 2) = \varphi(2n + 1)$*

[C] *Encuentre todos los* $m \in \mathbb{N}$ *para los cuales* $\varphi(m)$ *es impar.*

Resolución. *Tenemos que* $\varphi(1) = \varphi(2) = 1$. *Si* $m \geq 3$, *entonces* m *es divisible por un primo impar* p, *o* $m = 2^n$, $n \geq 2$ *(por la factorización canónica de* m*). En el primer caso,* $\varphi(m)$ *es divisible por el número par* $p - 1$, *y en el segundo caso tenemos que* $\varphi(m) = 2^{m-1}$, *así* $\varphi(m)$ *es un número impar solamente cuando* $m = 1$ *o* $m = 2$.

[D] *Resolver la ecuación* $\varphi(5^x) = 100$ *para* $x \in \mathbb{N}$.

Resolución. $\varphi(5^x) = 5^x - 5^{x-1} = 5^{x-1}(5-1) = 4 \cdot 5^{x-1} = 100$, *esto es* $4 \cdot 5^{x-1} = 100$, *simplificando* $5^{x-1} = 25$, *de donde* $x - 1 = 2$, *y así* $x = 3$.

EJERCICIOS

Ejercicio 7.15. *Evaluar* $\varphi(1000)$, $\varphi(635)$, $\varphi(180)$, $\varphi(360)$, $\varphi(1001)$

Ejercicio 7.16. *Demostrar que* $\varphi(5186) = \varphi(5187) = \varphi(5188)$ *(¡Estos son los únicos tres enteros consecutivos que cumplen esta propiedad!)*

Ejercicio 7.17. *Sea* p *es un número primo, resolver las ecuaciones para* x

[A] $\varphi(p^x) = p^{x-1}$ **[C]** $\varphi(px) = \varphi(x)$ **[E]** $\varphi(3^x 5^y) = 600$

[B] $\varphi(p^x) = 6p^{x-2}$ **[D]** $\varphi(x) = 16$ **[F]** $\varphi(p^x) = p^{x-1}$

Ejercicio 7.18. *Encontrar una fórmula para* $\varphi(pq)$, *donde* p *y* q *son primos gemelos.*

Ejercicio 7.19. *Demostrar que si* p *es un número primo, entonces* $\varphi(p!) = (p-1)\varphi((p-1)!)$.

Ejercicio 7.20. *Encontrar los primos gemelos* p *y* q *si* $\varphi(pq) = 120$.

Ejercicio 7.21. *Demostrar que si* p *y* q *son primos gemelos* $p < q$ *entonces* $\varphi(q) = \varphi(p) + 2$.

Ejercicio 7.22. *Demostrar que si* $n = 2^k$, *entonces* $\varphi(n) = n/2$.

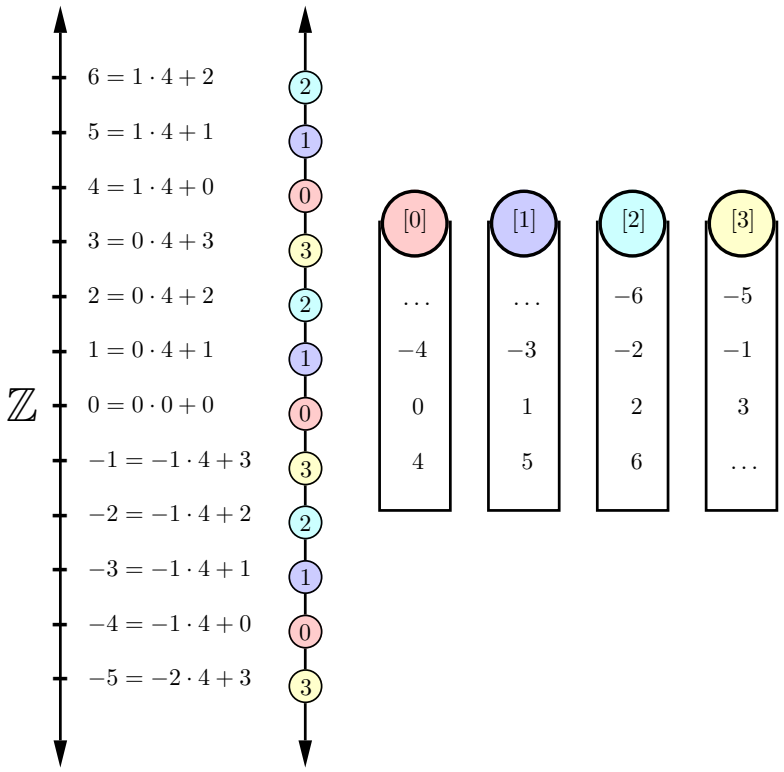
Ejercicio 7.23. *Demostrar que* $\varphi(4n) = 2\varphi(n)$ *cuando* n *es impar .*

Ejercicio 7.24. *Demostrar que* $\varphi(2n) = \begin{cases} \varphi(n) & \text{Si } n \text{ es impar} \\ 2\varphi(n) & \text{Si } n \text{ es par} \end{cases}$

8 | Congruencias

8.1. Introducción

Observemos la siguiente ilustración:



Comenzando por la izquierda, observamos que hemos colocado los números enteros $\mathbb{Z}$ en forma vertical y de acuerdo con el lema de la división se han escrito en la división por 4, si sólo nos fijamos en los residuos (¿Qué observas con los cocientes?) observamos que estos tienen un patrón: $\ldots, 2, 1, 0, 3, 2, 1, 0, 3, 2, 1, 0, 3, \ldots$, este ciclo se repite indefinidamente, es decir, a todos los números enteros los hemos *agrupado* en cuatro clases:

- Los que dejan residuo 0 en la división por 4 están en la clase $[0]$
  $[0] = \{\ldots, -4, 0, 4, 8, \ldots\} = \{x \in \mathbb{Z} : x = 4q, q \in \mathbb{Z}\}$,
- Los que dejan residuo 1 en la división por 4 están en la clase $[1]$
  $[1] = \{\ldots, -3, 1, 5, 9, \ldots\} = \{x \in \mathbb{Z} : x = 4q + 1, q \in \mathbb{Z}\}$,
- Los que dejan residuo 2 en la división por 4 están en la clase $[2]$
  $[2] = \{\ldots, -6, -2, 2, 6, \ldots\} = \{x \in \mathbb{Z} : x = 4q + 2, q \in \mathbb{Z}\}$,
- Los que dejan residuo 3 en la división por 4 están en la clase $[3]$
  $[3] = \{\ldots, -5, -1, 3, 7, \ldots\} = \{x \in \mathbb{Z} : x = 4q + 3, q \in \mathbb{Z}\}$.

Razonar la siguiente cuestión: ¿Cuál residuo se obtiene al restar dos números enteros de la misma clase?, ¡siempre se obtiene cero!, con esta construcción hecha hemos logrado establecer una relación en $\mathbb{Z}$, es

decir, dos números enteros están relacionados o son *congruentes* si y sólo si tienen el mismo residuo en la división por 4.

Esta noción de congruencias fue introducida explícitamente por Gauss en su obra *Disquisitions Arithmeticae* (1801), aunque sin duda la idea no había sido ajena al pensamiento de grandes matemáticos anteriores, como Fermat, Euler y otros. Hasta podría creerse que solo introdujo un nuevo lenguaje, una manera diferente de referirse a hechos conocidos. Sin embargo fue mucho más que eso, ya que posibilitó una forma más nítida de pensar y simplificó considerablemente los cálculos con residuos.

Definición 8.1. *Sea* $m \in \mathbb{Z} \setminus \{0, \pm 1\}$ *diremos que dos números enteros* a *y* b *son* ***congruentes módulo*** m *(por comodidad* $m > 1$*) si y sólo si* $m \mid b - a$ *y lo escribiremos utilizando la notación* $a \equiv b \mod m$.

Propiedades 8.2 (Propiedades de congruencias)**.** *Sean* a, b *y* c *números enteros cualesquiera, entonces*

[A] $a \equiv a \mod m$ *(Propiedad reflexiva)*

[B] *Si* $a \equiv b \mod m$, *entonces* $b \equiv a \mod m$ *(Propiedad simétrica)*

[C] *Si* $a \equiv b \mod m$, *y* $b \equiv c \mod m$, *entonces* $a \equiv c \mod m$ *(Propiedad transitiva)*

[D] $a \equiv r_m(a) \mod m$, *donde* $r_m(a)$ *denota el residuo de* a *en la división por* m

[E] $a \equiv b \mod m$ *si y sólo si* $r_m(a) \equiv r_m(b) \mod m$

[F] n *es múltiplo de* m *si y sólo si* $n \equiv 0 \mod m$

[G] *Si* $d \mid m$, $d \neq \pm 1, 0$ *y* $a \equiv b \mod m$, *entonces* $a \equiv b \mod d$

[H] *Si* $a \equiv b \mod m$, *entonces* $a + x \equiv b + x \mod m$ *y* $ax \equiv bx \mod m$

[I] *Si* $a \equiv b \mod m$ *y* $c \equiv d \mod m$, *entonces* $a + c \equiv b + d \mod m$ *y* $ac \equiv bd \mod m$

[J] *Si* $a + b \equiv c \mod m$, *entonces* $a \equiv c - b \mod m$

[K] *Si* n *es un número natural y* $a \equiv b \mod m$, *entonces* $a^n \equiv b^n \mod m$

[L] *Si* $a \equiv b \mod m$, *entonces* $(a : m) = (b : m)$

[M] *Si* $(a : m) = 1$ *y* $a \equiv b \mod m$, *entonces* $(b : m) = 1$.

[N] *Si* $ac \equiv bc \mod m$ *y* $d = (c : m)$, *entonces* $a \equiv b \mod \frac{m}{d}$.

En particular, si $(c : m) = 1$ *el factor* c *se puede simplificar de la congruencia sin afectar el módulo.*

[Ñ] *Si* $(m : n) = 1$, $a \equiv b \mod m$ *y* $a \equiv b \mod n$, *entonces* $a \equiv b \mod mn$.

Ejemplo 8.3. *Demostrar que el resto de dividir* 20^{4572} *entre* 7 *es* 1

Resolución. *En efecto,*

$$\left.\begin{array}{l} 21 \equiv 0 \mod 7 \\ -1 \equiv -1 \mod 7 \end{array}\right\} \Rightarrow \quad 20 \equiv -1 \mod 7$$

$$\Rightarrow \quad 20^{4572} \equiv (-1)^{4572} \mod 7$$

$$\Rightarrow \quad 20^{4572} \equiv 1 \mod 7$$

es decir el resto es 1

Ejemplo 8.4. *Calcular el resto de dividir* $9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10$ *por* 730

Resolución. *Observemos lo siguiente:*

$$\begin{aligned} 9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 &= \left(9^3\right)^{2n} \cdot 9 + (3 \cdot 487)^{2n} \cdot 3 - 10 \\ &= (729)^{2n} \cdot 9 + (1461)^{2n} \cdot 3 - 10 \end{aligned}$$

Pues bien,

$$\begin{aligned} 729 \equiv -1 \mod 730 &\Rightarrow 729^{2n} \equiv (-1)^{2n} \mod 730 \\ &\Rightarrow 729^{2n} \equiv 1 \mod 730 \\ &\Rightarrow 729^{2n} \cdot 9 \equiv 9 \mod 730 \\ &\Rightarrow 9^{6n+1} \equiv 9 \mod 730 \end{aligned}$$

por otra parte,

$$\begin{aligned} 1461 \equiv 1 \mod 730 &\Rightarrow 1461^{2n} \equiv 1^{2n} \mod 730 \\ &\Rightarrow 1461^{2n} \equiv 1 \mod 730 \\ &\Rightarrow 1461^{2n} \cdot 3 \equiv 3 \mod 730 \\ &\Rightarrow 3^{2n+1} \cdot 487^{2n} \equiv 3 \mod 730 \end{aligned}$$

de aquí que

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} \equiv 12 \mod 730$$

es decir,

$$9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10 \equiv 2 \mod 730$$

y consecuentemente, el resto de dividir el número dado entre 730 *es* 2*.*

EJERCICIOS

Ejercicio 8.1. *Reescribir cada una de la siguientes cuestiones utilizando la notación de congruencias*

[A] n *es un entero impar*

[B] n *es un entero par*

[C] n *es divisible por 5*

[D] *El producto de tres enteros consecutivos es divisible por* 6

Ejercicio 8.2. *Utilizar las propiedades de congruencias para encontrar el residuo de dividir* a *por* b

[A] $11111 + 22222$*;* $b = 10$

[B] $a = 25 \cdot 46 + 23$*;* $b = 4$

[C] $a = 45 \cdot 2^8$*;* $b = 7$

[D] $a = 4^4 + 5^5$*;* $b = 3$

Ejercicio 8.3. *Dar un contraejemplo para mostrar que las siguientes proposiciones no son verdaderas*

[A] *Si* $a^2 \equiv b^2 \mod m$*, entonces* $a \equiv b \mod m$

[B] *Si* $a \not\equiv 0 \mod m$ *y* $b \not\equiv 0 \mod m$ *entonces* $ab \not\equiv 0 \mod m$

Ejercicio 8.4. *Encuentre todos los enteros positivos* $n > 1$*, tales que* $1848 \equiv 1914 \mod n$.

Ejercicio 8.5. *Probar que si* $a \equiv b \mod m$*, entonces* $a \equiv b \mod k$*, para todo* k *divisor no trivial de* m*. ¿Será cierto el recíproco de este resultado?*

Ejercicio 8.6. *Demostrar la siguiente propiedad. Si* $d \mid m$ *y* $a \equiv b \mod m$ *entonces* $a \equiv b \mod d$*, y demostrar las propiedades* **[8.2]**.

Ejercicio 8.7. *Cualquier número entero es congruente* $\mod m$ *con solamente uno de los enteros* $0, 1, \ldots, m-1$.

Ejercicio 8.8. *Dos números enteros son congruentes entre sí* $\mod m$ *si y sólo si ambos dan el mismo resto al dividirlos entre* m.

Ejercicio 8.9. *Probar que el consecutivo a cualquier potencia de* 5 *es múltiplo de* 2 *pero no de* 4.

Ejercicio 8.10. *Probar mediante congruencias, que* $3^{2n+5} + 2^{4n+1}$ *es divisible por* 7 *cualquiera que sea el entero* $n \geq 1$.

Ejercicio 8.11. *Para todo* $n \in \mathbb{N}$*, sea* $A_n = 2^n + 4^n + 8^n$*. Probar que si* $n \equiv m \mod 3$ *entonces* $A_n \equiv A_m \mod 7$.

Ejercicio 8.12. *En cada caso calcule el residuo de* a *en la división por* b.

[A] $a = 5^{2012}$ *y* $b = 11$

[B] $a = 8^{931}$ *y* $b = 3$

[C] $a = 57^{294}$ *y* $b = 5$

[D] $a = 3 \cdot 9^{94} - 2 \cdot 41^{23}$ *y* $b = 11$.

Ejercicio 8.13. *Si* p *es primo y* $n^2 \equiv 1 \mod p$*, probar que* $n \equiv \pm 1 \mod p$.

8.2. Criterios de divisibilidad

Existen criterios prácticos para decidir cuándo un número es divisible por $2, 3, 9, 11, \ldots$ etc, todos estos criterios se pueden enunciar y demostrar utilizando congruencias. En esta sección explicamos algunos criterios de divisibilidad.

Criterio 8.5 (Criterio de divisibilidad por nueve)**.** *Un número entero es divisible por nueve si y sólo si la suma de sus dígitos es divisible por nueve.*

Demostración. Sea $N = \overline{c_n \ldots c_1 c_0}$ la representación decimal de N, entonces $0 \leq c_i < 10$ para todo i, notemos en primer lugar que $10 \equiv 1 \mod 9$, entonces para todo $i = 0, 1, \ldots, n$: $10^i \equiv 1 \mod 9$, de donde:

$$N = c_n 10^n + \ldots + c_1 10 + c_0 \equiv c_n + \ldots + c_1 + c_0 \mod 9,$$

así concluimos que N es congruente con la suma de sus dígitos módulo 9, demostrado el criterio de divisibilidad por 9. □

Por ejemplo el número 1575 es divisible por 9, pues $1 + 5 + 7 + 5 = 18 = 2 \cdot 9$.

Criterio 8.6 (Criterio de divisibilidad por once)**.** *Un número entero es divisible por once si y sólo si la suma de sus dígitos en posición impar menos la suma de los dígitos en posición par es divisible por once.*

Demostración. Si $N = \overline{c_n \dots c_1 c_0}$ es la representación decimal de N, en este caso notemos que $10 \equiv -1 \mod 11$, entonces para todo $i = 0, 1, \dots, n$: $10^i \equiv (-1)^i \mod 11$, entonces:

$$N = c_n 10^n + c_{n-1} 10^{n-1} + \dots + c_1 10 + c_0 \equiv c_n (-1)^n + c_{n-1} (-1)^{n-1} + \dots - c_1 + c_0 \mod 11,$$

así concluimos que N es congruente con la diferencia de las sumas de sus dígitos en posición par e impar, demostrado el criterio de divisibilidad por 11. □

Observemos que la técnica general para crear un criterio de divisibilidad de este tipo para un número N, consiste en encontrar la mínima potencia de 10 (10^k para algún número natural k) tal que $10^k + 1$ o $10^k - 1$ sea divisible por N. En el primer caso, el criterio consiste en agrupar el número en bloques de k dígitos y sumar y restar alternadamente, mientras que en el segundo caso basta con sumar. De esta forma podemos crear criterios de divisibilidad por 27 y 37, que dividen a $10^3 - 1$.

Un criterio de divisibilidad por 7 se obtiene al observar que $7 \mid 21$ por lo tanto si $7 \mid N$, entonces $7 \mid N - 21a_0$, por lo tanto 7, debe dividir a $\overline{a_n a_{n-1} \dots a_1} - 2a_0$.

EJERCICIOS

Ejercicio 8.14. *Si $a = \overline{a_n \dots a_1 a_0}$ es la representación decimal de a. Demostrar que*

[A] $a \equiv a_0 \mod 10$

[B] $a \equiv \overline{a_1 a_0} \mod 100$

[C] $a \equiv \overline{a_2 a_1 a_0} \mod 1000$

[D] *Encontrar la última cifra de* $2 \cdot 325 + 3 \cdot 8^7 \cdot 5104 + 123^5$.

Ejercicio 8.15. *Enunciar y demostrar un criterio de divisibilidad por*

[A] 21 **[B]** 27 **[C]** 37 **[D]** 101

Ejercicio 8.16. *Criterio de divisibilidad por 21. Si tomamos un número de dos cifras, por ejemplo $\overline{ab}$, entonces:*

$$\begin{aligned} \overline{ab} &= a \times 10 + b \\ &= a \times 10 + 20b - 20b + b \\ &= (a - 2b) \times 10 + 21b \end{aligned}$$

Podemos decir que un número de dos cifras $\overline{ab}$ es divisible por 21 si $a - 2b$ es múltiplo de 21. Generalice este método para un número de más de dos cifras.

8.3. Los últimos dígitos de las potencias de algunos números enteros positivos

Sea P el dígito de las unidades de un número entero positivo a y para $n = 1, 2, \dots$ denotaremos por $U(P^n)$ el dígito de las unidades de P^n. Entonces el dígito de las unidades de a^n es el mismo que el dígito de las unidades de P^n, además la sucesión $\{U(P^n) : n = 1, 2, \dots\}$ tiene las siguientes propiedades:

Propiedades 8.7. **[A]** *La sucesión toma valores constantes para $P = 0, 1, 5, 6$, es decir, $U(P^n)$ no cambia, cuando n cambia.*

[B] *La sucesión es periódica con periodo 2 para $P = 4$ o 9.*

[C] *La sucesión es periódica con periodo 4 para $P = 2, 3, 7, 8$.*

[D] *Los dos últimos dígitos de* 5^n *para* $n \geq 2$ *son* 25.

[E] *Los dos últimos dígitos de* 6^n *para* $n \geq 2$ *aparecen en el orden "*$36, 16, 76, 56$*" cuando* n *cambia.*

[F] *Los dos últimos dígitos de* 7^n *para* $n \geq 2$ *aparecen en el orden "*$49, 43, 01, 07$*".*

[G] *Los dos últimos dígitos de* 76^n *siempre son 76.*

EJERCICIOS

Ejercicio 8.17. *¿En que cifra termina* 3^{300}*?*

Ejercicio 8.18. *Encontrar el periodo que repite la cifra de las unidades para los siguientes números*

[A] *14* **[C]** *122* **[E]** *347*

[B] *28* **[D]** *129* **[F]** *192*

Ejercicio 8.19. *Calcular el último dígito de las potencias* $6^{100}, 7^{123}$ *y* 23^{111}*.*

Ejercicio 8.20. *Calcular los últimos dos dígitos de* 6^{125}*,* 7^{1524} 15^{555} *y* 26^{136}*.*

Ejercicio 8.21. *Calcular las tres últimas cifras en el sistema heptal (base 7) de* 5^{300}*.*

Ejercicio 8.22. *Usando congruencias demostrar las propiedades* **[8.7]**.

Lectura complementaria:
Revisar las soluciones a los problemas de aritmética [7, Problemas 1.20 y 1.27].

8.4. Números cuadrados perfectos

Definición 8.8. *Un número entero* n *se llama número* ***cuadrado perfecto****, si existe un número entero* m *tal que* $n = m^2$*.*

A continuación se enuncian algunas propiedades sobre de los cuadrados perfectos y se dan algunas explicaciones que orientan al lector para completar las demostraciones.

Propiedades 8.9. **[A]** *El dígito de las unidades de un cuadrado perfecto puede ser solamente* $0, 1, 4, 5, 6$ *o* 9*. Es suficiente verificar esta propiedad para* $0^2, 1^2, 2^2, \ldots, 9^2$*.*

[B] *Si la descomposición en factores primos de un número natural* n *es* $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$*, entonces:*

$$n \text{ es cuadrado perfecto } \Leftrightarrow \text{ cada } \alpha_i \text{ es par } \Leftrightarrow \tau(n) \text{ es impar},$$

donde $\tau(n)$ *denota la cantidad de divisores positivos de* n*.*

[C] *Si un cuadrado perfecto* n *termina en muchos dígitos cero, esta cantidad de ceros debe ser par, ya que en la descomposición en factores primos de* n *los factores* 2 *y* 5 *deben aparecer una cantidad par de veces.*

[D] $n^2 \equiv 1$ *o* 0 *módulo* $2, 3, 4$*. Basta comprobar los números de las formas* $(2m)^2$ *y* $(2m+1)^2$ *al tomar módulo* 2 *y módulo* 4 *respectivamente; los números de las formas* $(3m)^2$ *y* $(3m \pm 1)^2$ *tomando módulo* 3*.*

[E] $n^2 \equiv 0, 1$ *o* $4 \mod 8$.

Basta con revisar la conclusión para $(4m \pm 1)^2$, $(4m)^2$, $(4m + 2)^2$, *donde* m *es cualquier entero.*

[F] *En un número cuadrado perfecto impar el dígito de las decenas debe ser par (para el caso de cuadrados perfectos de un dígito* 1^2 *y* 3^2 *pueden considerarse como* 01 *y* 09 *respectivamente).*

Es fácil ver la razón: Para $n > 3$, $n^2 = (10a + b)^2 = 100a^2 + 20ab + b^2$. *El número* $100a^2 + 20ab$ *tiene como dígito de las unidades* 0 *y dígito par de las decenas. Si* b *es un dígito impar, entonces el dígito de las decenas* b^2 *debe ser par, así el dígito de las decenas de* n^2 *debe ser par.*

[G] *Si el dígito de las decenas de* n^2 *es impar, entonces el dígito de las unidades de* n^2 *debe ser* 6.

Continuando el análisis de ***[F]****, si el dígito de las decenas* b^2 *es impar, entonces* $b = 4$ *o* 6 *solamente, y* $b^2 = 16$ *o* 36, *i.e. el dígito de las unidades de* n^2 *debe ser* 6.

[H] *No hay ningún número cuadrado perfecto entre los dos números cuadrados perfectos* k^2 *y* $(k + 1)^2$, *donde* k *es cualquier número entero no negativo.*

De lo contrario, existiría un tercer número entero entre los dos números enteros consecutivos k *y* $k+1$, *sin embargo, esto es imposible.*

Los problemas básicos involucrando cuadrados perfectos son (i) identificar si un número es un cuadrado perfecto; (ii) encontrar cuadrados perfectos sujetos a algunas condiciones; (iii) determinar la existencia de soluciones enteras a ecuaciones usando propiedades de los números cuadrados perfectos.

Problema Resuelto 8.10. *Sabiendo que el número de cinco dígitos* $\overline{2x9y1}$ *es un cuadrado perfecto. Encontrar el valor de* $3x + 7y$.

Resolución. *Utilizamos el método de estimación para determinar* x *y* y. *Sea* $A^2 = \overline{2x9y1}$.

Como $141^2 = 19881 < A^2$ *y* $175^2 = 30625 > A^2$, *entonces* $141^2 < A^2 < 175^2$. *El dígito de las unidades de* A^2 *es 1 implica que el dígito de las unidades de* A *puede ser* 1 *o* 9. *Por lo tanto, es suficiente comprobar solamente para* 151^2, 161^2, 171^2, 159^2, 169^2, *y encontramos que:*

$$161^2 = 25921$$

cumple todos los requisitos, además, los otros números no satisfacen todas las condiciones. Por lo tanto,

$$x = 5, y = 2, \text{ y que } 3x + 7y = 15 + 14 = 29.$$

EJERCICIOS

Ejercicio 8.23. *Usando congruencias demostrar las propiedades* **[8.9]**.

Ejercicio 8.24. *Demostrar que no existe número de tres dígitos* $\overline{abc}$, *tal que* $\overline{abc} + \overline{bca} + \overline{cab}$ *es un cuadrado perfecto.*

Ejercicio 8.25. *Demostrar que la ecuación* $a^2 + b^2 - 8c = 6$ *no tiene soluciones enteras.*

Ejercicio 8.26. *Probar que el número* $3^n + 2 \cdot 17^n$, *donde* n *es un entero no negativo, nunca es un cuadrado perfecto.*

Lectura complementaria:
Revisar las soluciones a los problemas de aritmética [7, Problemas 1.2 y 1.5].

8.5. Sistemas completos y reducidos de residuos

Si elegimos m enteros, cada uno de ellos perteneciente a una clase residual módulo m obtenemos un **sistema completo de residuos módulo** m. Por ejemplo, $\{0, 1, \ldots, m-1\}$ es un sistema completo de residuos módulo m, conocido también como **sistema canónico de residuos no negativos módulo** m.

Teorema 8.11. $k \in \mathbb{Z}$, $(k : m) = 1$. *Si* $\{a_1, \ldots, a_m\}$ *es un sistema completo de residuos módulo* m*, también lo es* $\{ka_1, \ldots, ka_m\}$.

Demostración. Basta ver que los números $ka_1, \ldots, ka_m$ son incongruentes entre sí. En efecto, si $ka_i \equiv ka_j \mod m$, puesto que $(k : m) = 1$, se tendrá que $a_i \equiv a_j \mod m$, de donde $i = j$. □

Se llama **sistema reducido de residuos módulo** m a un conjunto de $\varphi(m)$ enteros, incongruentes entre sí, de manera que todos son coprimos con m. Por ejemplo, si p es primo, $\{1, 2, 3, \ldots, p-1\}$ es un sistema reducido de residuos módulo p.

Teorema 8.12. *Sea* $k \in \mathbb{Z}, (k : m) = 1$. *Si* $\{a_1, \ldots, a_{\varphi(m)}\}$ *es un sistema reducido de residuos módulo* m *también lo es* $\{ka_1, \ldots, ka_{\varphi(m)}\}$.

Demostración. Igual que en la demostración del Teorema **[8.11]** los números $ka_1, \ldots, ka_{\varphi(m)}$ son incongruentes entre sí. Además, puesto que $(k : m) = 1$ entonces$(ka_i : m) = (a_i : m) = 1$. □

8.6. Teoremas de Euler, Fermat y Wilson

En esta sección enunciamos y demostramos tres teoremas fundamentales de la teoría de números: el Teorema de Euler-Fermat, el Pequeño Teorema de Fermat y el Teorema de Wilson, estos teoremas son de interés por sus aplicaciones en la resolución de problemas.

Comenzamos recordando la función φ de Euler, la cual juega un papel destacado en la teoría de números. Una de las razones es el siguiente teorema:

Teorema 8.13 (Teorema de Euler - Fermat)**.** *Sean* $a, m \in \mathbb{Z}, (a : m) = 1$. *Entonces:* $a^{\varphi(m)} \equiv 1 \mod m$.

Demostración. Sea $a_1, \ldots, a_{\varphi(m)}$ un sistema reducido de residuos módulo m. Entonces $aa_1, \ldots, aa_{\varphi(m)}$ también lo es por el Teorema **[8.12]**. Por tanto,

$$a_1 \cdots a_{\varphi(m)} \equiv aa_1 \cdots aa_{\varphi(m)} \equiv a^{\varphi(m)} a_1 \cdots a_{\varphi(m)} \mod m.$$

Como $(a_i : m) = 1$ para todo i, podemos cancelar cada a_i en la congruencia anterior, para obtener el resultado deseado. □

Teorema 8.14 (Pequeño teorema de Fermat)**.** *Si* p *es un número primo y* $a \in \mathbb{Z}$*, entonces* $a^p \equiv a \mod p$.

Demostración. Si $p \nmid a$, se tiene $(a : p) = 1$, además $\varphi(p) = p-1$, por el teorema de Euler-Fermat tenemos que $a^{p-1} \equiv 1 \mod p$. Multiplicando esta congruencia por a obtenemos $a^p \equiv a \mod p$, la cual también es válida si $p \mid a$. □

Si $x^2 \equiv 1 \mod p$, entonces $p \mid (x-1)(x+1)$, así $x \equiv \pm 1 \mod p$. Esto dice que $\{i, 2i, \ldots, (p-1)i\}$ es un conjunto reducido de residuos módulo p, luego para todo $i \in \{2, 3, \ldots, p-2\}$ existe $j \neq i$ en el mismo conjunto tal que $ij \equiv 1 \mod p$. Multiplicando todas estas parejas, obtenemos que $(p-2)! \equiv 1 \mod p$.

Multiplicando la última congruencia por $p - 1 \equiv -1 \mod p$, se deduce el siguiente teorema.

Teorema 8.15 (Teorema de Wilson)**.** *Si* p *es un número primo, entonces* $(p-1)! \equiv -1 \mod p$.

Teorema 8.16. *Sean* a *y* m *enteros positivos coprimos, si la factorización canónica de* m *es* $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$. *Entonces* $a^M \equiv 1 \mod m$, *donde* $M = [\varphi(p_1^{e_1}) : \varphi(p_2^{e_2}) : \ldots : \varphi(p_r^{e_r})]$.

Demostración. Para $i = 1, 2, \ldots, r$ aplicando el teorema de Euler-Fermat tenemos que $a^{\varphi(p_i^{e_i})} \equiv 1 \mod p_i^{e_i}$. Además como $M = [\varphi(p_1^{e_1}) : \varphi(p_2^{e_2}) : \ldots : \varphi(p_r^{e_r})]$ sabemos que $\varphi(p_i^{e_i}) \mid M$, así $a^M \equiv 1 \mod p_i^{e_i}$, de donde $a^M \equiv 1 \mod m$. □

Veamos aplicaciones de estos últimos teoremas en los siguientes ejemplos.

Ejemplo 8.17. *Mostrar que si* a *y* b *son enteros positivos primos relativos, entonces existen enteros* m *y* n *tales que* $a^m + b^n \equiv 1 \mod ab$

Resolución. *Consideremos* $S = a^{\varphi(b)} + b^{\varphi(a)}$, *entonces por el teorema de Euler-Fermat,* $S \equiv b^{\varphi(a)} \equiv 1 \mod a$ *o* $S - 1 \equiv 0 \mod a$ *y* $S \equiv a^{\varphi(b)} \equiv 1 \mod b$ *o* $S - 1 \equiv 0 \mod b$. *Entonces* $S - 1 \equiv 0 \mod ab$, *así* $S \equiv 1 \mod ab$.

Teorema 8.18. *Sean* a *y* m *enteros positivos coprimos. Sea* ℓ *el menor entero positivo tal que* $a^\ell \equiv 1 \mod m$, *entonces para todo entero* k *tal que* $a^k \equiv 1 \mod m$ *se tiene que* $\ell \mid k$. *En particular* $\ell \mid \varphi(m)$.

Demostración. Por el lema de la división, existen enteros no negativos q y r con $0 \le r < \ell$ tales que $k = \ell q + r$. Así

$$a^k = a^{\ell q + r} = a^{\ell q} a^r \equiv a^r \mod m,$$

es decir, $a^r \equiv 1 \mod m$, con $0 \le r < \ell$, por la minimalidad de ℓ tenemos que $r = 0$. Esto es, $\ell \mid k$, en particular por el teorema de Euler-Fermat $\ell \mid \varphi(m)$. □

Al menor entero ℓ en la demostración anterior se llama el **orden de** a **módulo** m.

Problema Resuelto 8.19. *Demostrar que* $n \mid \varphi(a^n - 1)$ *para todo entero* $a > 1$ *y todo entero positivo* n.

Resolución. *Como* $(a : a^n - 1) = 1$, *por el teorema de Euler tenemos que* $a^{\varphi(a^n-1)} \equiv 1 \mod (a^n - 1)$. *Por otra parte,* n *es el orden de* a *módulo* $a^n - 1$ *ya que* $a^n \equiv 1 \mod (a^n - 1)$ *y* $a^t < a^n - 1$ *para* $t < n$. *Por lo tanto, tenemos que* $n \mid \varphi(a^n - 1)$.

EJERCICIOS

Ejercicio 8.27. *Calcular el último dígito de las potencias* $6^{20}, 7^{93}$ *y* 23^{189}.

Ejercicio 8.28. *Calcular el residuo en la división por* 7 *de* $17^{17^{17}}$ *y* $(17^{17})^{17}$.

Ejercicio 8.29. *Probar que* $3^{105} + 4^{105} \equiv 0 \mod 13$.

Ejercicio 8.30. *Calcular el residuo de dividir* a *por* b

[A] $a = 7^{512}$; $b = 11$

[B] $a = 3^{47}$; $b = 23$

[C] $a = 3^{15}$; $b = 17$

[D] $a = 125^{4577}$; $b = 13$

[E] $a = 11^{954}$; $b = 20$

[F] $a = 140^{1221} + 28^{753}$; $b = 13$

Ejercicio 8.31. *Comprobar que* $2^{340} \equiv 1 \mod 11$ *y* $2^{340} \equiv 1 \mod 31$, *y concluir que* $2^{340} \equiv 1 \mod 241$.

Ejercicio 8.32. *Probar que para todo entero* n:

[A] *El número* n^{12} *es de la forma* $13k$ *o de la forma* $13k + 1$, *para algún entero* k.

[B] *Probar que para todo entero* n, *el número* n^8 *es de la forma* $17k$ *o* $17k \pm 1$, *para algún entero* k.

Ejercicio 8.33. *Probar que si* p *es un primo impar, entonces*

[A] $(x+y)^p \equiv x^p + y^p \mod p$, *para todo* $x, y \in \mathbb{Z}$.

[B] $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \mod p$.

[C] $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \mod p$.

Ejercicio 8.34. *Probar que para cualquier entero* n*, el número* $n^{37} - n$ *es divisible por* 383838.

Ejercicio 8.35. *Probar que* $a^{4n+1} - a$ *es divisible por 30 para todo entero* a *y todo entero positivo* n.

Ejercicio 8.36. *Encontrar todos los números enteros* n *tales que* $3^n - n$ *es divisible por* 17.

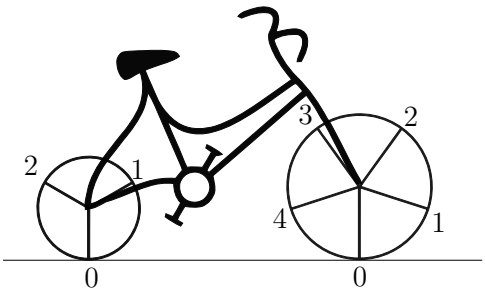
Ejercicio 8.37. *Si* p *y* q *son primos diferentes, probar que* $p^q + q^p \equiv p + q \mod pq$.

---

9 Congruencias lineales y sistemas lineales

9.1. Introducción

Consideremos una bicicleta cuyas ruedas tienen perímetros de longitudes 3 y 5 unidades. En el neumático de cada rueda están grabados respectivamente los números enteros del 0 al 2 y del 0 al 4 como se muestra en la figura.



Cuando la bicicleta avanza sobre una línea recta una unidad podemos marcar los números que están en el piso, generando una lista de parejas de números enteros $(a;b)$ donde a es la marca que deja la rueda pequeña y b es la marca que deja la rueda grande.

$(0;0)$	$(1;1)$	$(2;2)$	$(0;3)$	$(1;4)$	$(2;0)$
$(0;1)$	$(1;2)$	$(2;3)$	$(0;4)$	$(1;0)$	$(2;1)$
$(0;2)$	$(1;3)$	$(2;4)$	$(0;0)$	$(1;1)$	$(2;2)$
$(0;3)$	$(1;4)$	...	...	...	...

Es claro que dichos pares ordenados son todos diferentes y se repiten en ciclos de 15, nos preguntamos si es posible establecer una correspondencia entre los pares ordenados $(a;b)$ y los residuos x módulo 15.

x	0	1	2	3	4	5	6	7
$(a;b)$	$(0;0)$	$(1;1)$	$(2;2)$	$(0;3)$	$(1;4)$	$(2;0)$	$(0;1)$	$(1;2)$

x	8	9	10	11	12	13	14	$\cdots$
$(a;b)$	$(2;3)$	$(0;4)$	$(1;0)$	$(2;1)$	$(0;2)$	$(1;3)$	$(2;4)$	$\cdots$

¿Cuál es explícitamente la relación de x en términos de a y b? Observemos que para un residuo x en módulo 15, $a = r_3(x)$ y $b = r_5(x)$, de donde se obtiene el sistema de congruencias

$$\begin{cases} x \equiv a \mod 3 \\ x \equiv b \mod 5 \end{cases} \tag{9.1}$$

donde $x = 0, 1, 2 \ldots, 14$.

9.2. Congruencias lineales

Si a, b y m son números enteros dados, una congruencia

$$a \cdot x \equiv b \mod m \tag{9.2}$$

donde x es un número entero a determinar se llama **ecuación lineal de congruencia** en la incógnita x.

Se dice que x_0 es **solución** de la congruencia **[9.2]** si es un número entero que satisfacen la congruencia, es decir $ax_0 \equiv b \mod m$. Si x_1 es otro número entero tal que $x_1 \equiv x_0 \mod m$, entonces x_1 también es solución de la ecuación. Lo anterior dice que si la congruencia **[9.2]** tiene solución entonces existen infinitos números enteros que la satisfacen, en ese sentido diremos que dos soluciones x_0 y x_1 son **diferentes** ($\mod m$) si y sólo si $x_1 \not\equiv x_0 \mod m$. Así *Resolver* una congruencia lineal será encontrar *todas* las soluciones diferentes.

Tenemos un resultado de existencia y unicidad de soluciones para un caso particular:

Teorema 9.1. *Supongamos que* $(a : m) = 1$. *Entonces la congruencia* $ax \equiv b \mod m$ *tiene una única solución.*

Demostración. Por definición la congruencia $ax \equiv b \mod m$ es equivalente a la ecuación diofántica $ax - my = b$, la cual tiene solución, pues $(a : m) = 1 \mid b$. La solución general para x es $x = x_0 - mt$ para $t \in \mathbb{Z}$, módulo m tenemos que $x \equiv x_0 \mod m$. Es evidente que es única. □

Falta escribir explícitamente quien es la solución x_0, para lo cual es de ayuda el siguiente corolario cuya demostración es una sencilla aplicación del teorema de Euler-Fermat

Corolario 9.2. *Sea* $(a : m) = 1$. *Entonces la única solución de la congruencia* $ax \equiv b \mod m$ *viene dada por*

$$x \equiv ba^{\varphi(m)-1} \mod m.$$

Ejemplo 9.3. **[A]** *Consideremos la congruencia* $3x \equiv 1 \mod 7$. *Puesto que* $(3 : 7) = 1$, *tiene una solución por el corolario* **[9.2]** *viene dada por* $x \equiv 3^{\varphi(7)-1} = 3^5 \mod 7$.

Puesto que $3^2 = 9 \equiv 2 \mod 7$ *se tiene que* $3^4 \equiv 4 \mod 7$ *y por tanto* $3^5 \equiv 12 \equiv 5 \mod 7$. *Así, la solución de la congruencia es* $x \equiv 5 \mod 7$.

[B] *Sea* $2x \equiv 4 \mod 8$. *Puesto que* $(2 : 8) = 2$, *hay dos soluciones. Al dividir por 2 esta congruencia original, obtenemos* $x \equiv 2 \mod 4$, *y por tanto las dos soluciones de la congruencia original son* $x \equiv 2, 6 \mod 8$.

El caso general no es tan simple. Puede ocurrir que una congruencia lineal no tenga soluciones o que tenga más de una, pero con una idea análoga utilizada en la demostración del teorema **[9.1]** puede demostrarse el siguiente teorema.

Teorema 9.4. *Sea* $d = (a : m)$. *Entonces la congruencia lineal* $ax \equiv b \mod m$ *tiene solución si y sólo si* $d \mid b$, *y en tal caso hay* d *soluciones para* x *dadas por:*

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \ldots, t + (d-1)\frac{m}{d}, \tag{9.3}$$

donde t *es la única solución de la congruencia:*

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}. \tag{9.4}$$

Ejemplo 9.5. *Resolver la ecuación* $30x \equiv 15 \mod 21$.

Resolución. *Observe que* $(30 : 21) = 3$ *y* 3 *divide a* 15, *por el teorema* **[9.4]** *la ecuación tiene solución y la cantidad de soluciones módulo* 21 *será igual a* $(21 : 30) = 3$.

Con la finalidad de hallar una solución particular, procederemos a dividir la congruencia por 3 *obteniendo* $10x \equiv 5 \mod 7$, *o de forma equivalente*

$$3x \equiv 5 \mod 7$$

cuya solución es $x \equiv 4 \mod 7$. *Luego las tres soluciones distintas módulo* 21 *son:* 4, 11 *y* 18.

EJERCICIOS

Ejercicio 9.1. *Escribir la solución general de la congruencia* $12x \equiv 9 \mod 15$

Ejercicio 9.2. *Resolver una congruencia es determinar si hay o no soluciones; en el caso que si tenga solución, determinarlas todos los* $x \in \mathbb{Z}$ *que satisfagan la congruencia. Resolver cada una de las siguientes congruencias.*

[A] $3x \equiv 5 \mod 7$ **[C]** $19y \equiv 42 \mod 50$ **[E]** $5x + 2 \equiv 5 \mod 7$ **[G]** $12x \equiv 9 \mod 27$

[B] $12u \equiv 15 \mod 22$ **[D]** $18v \equiv 42 \mod 50$ **[F]** $3v + 4 \equiv 5 \mod 6$ **[H]** $4y \equiv 3 \mod 7$

Ejercicio 9.3. *Encontrar el inverso multiplicativo de* 3 *módulo* 7*, es decir, encontrar un entero* a *que cumpla que* $a \cdot 3 \equiv 1 \mod 7$*.*

Ejercicio 9.4. *Encontrar el inverso multiplicativo de* 3*,* 4 *y* 5 *módulo* 13

Ejercicio 9.5. *Resuelva la congruencia* $2x \equiv 1 \mod m$*, donde* $m \in \mathbb{N}$*.*

Ejercicio 9.6. *Si* $a = 18726132117057$*, resolver la congruencia lineal* $a \equiv x \mod m$ *para* $m = 2, 3, 5, 9$ *y* 11*.*

Ejercicio 9.7. *Resolver las siguientes congruencias*

[A] $42x \equiv 90 \mod 156$ **[C]** $64x \equiv 897 \mod 1001$

[B] $87x \equiv 57 \mod 105$ **[D]** $108x \equiv 171 \mod 529$

9.3. Teorema chino del residuo

En ocasiones puede suceder que las congruencias de un sistema tengan cada una soluciones por separado, pero esto no implica que el sistema de congruencias tenga solución. Probaremos que un sistema de congruencias lineales que pueden resolverse por separado también se puede resolver simultáneamente si los módulos son primos relativos dos a dos.[1]

Teorema 9.6 (Teorema chino del residuo o Teorema chino del resto)**.** *Supongamos que* $m_1, m_2, \ldots, m_r$ *son enteros positivos primos relativos dos a dos, y sean* $b_1, b_2, \ldots, b_r$ *números enteros. Entonces el sistema*

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \quad \vdots \\ x \equiv b_r \mod m_r \end{cases} \tag{9.5}$$

tiene exactamente una solución módulo $m_1 \cdots m_r$*.*

Demostración. Sean $M = m_1 \cdots m_r$, $M_k = M/m_k$. Entonces $(m_k : M_k) = 1$. Por tanto, cada congruencia

$$M_k x \equiv 1 \mod m_k$$

tiene una única solución M'_k (a este M'_k se le suele llamar el inverso de M_k módulo m_k). Pongamos

$$x = b_1 M_1 M'_1 + \ldots + b_r M_r M'_r.$$

[1] Los números enteros $m_1, m_2, \ldots, m_n$ se dice que son **primos relativos dos a dos** si y sólo si $(m_i : m_j) = 1$ para todo $i \neq j$.

Puesto que $M_i \equiv 0 \mod m_k$ si $i \neq k$, tendremos

$$x \equiv b_k M_k M_k' \equiv b_k \mod m_k.$$

Por tanto x es solución del sistema **[9.5]**. Para probar la unicidad, sea y otra solución. Puesto que $x \equiv y \mod m_k$ para todo k, se tendrá gracias a la Propiedad **[Ñ]** que $x \equiv y \mod M$, como queríamos ver. □

Ejemplo (…continuación…)**.** *Volviendo al problema de la bicicleta discutido en la introducción, nos preguntábamos si es posible encontrar una regla que identifique cada residuo* x *módulo* 15 *con una única pareja de números enteros* $(a; b)$*, donde* $a = 0, 1, 2$ *y* $b = 0, 1, 2, 3, 4$*.*

Con la notación del teorema **[9.6]***, tenemos* $m_1 = 3$*,* $m_2 = 5$*,* $M = 15$*,* $M_1 = 5$*,* $M_2 = 3$*. Como* $(3 : 5) = 1$ *el sistema de congruencias* **[9.1]** *tiene solución y es equivalente al siguiente*

$$\begin{cases} 5M_1' \equiv 1 \mod 3 \\ 3M_2' \equiv 1 \mod 5. \end{cases}$$

El inverso multiplicativo de 5 *módulo* 3 *es* 2 *y el inverso multiplicativo de* 3 *módulo* 5 *también es* 2*, así*

$$\begin{cases} M_1' \equiv 2 \mod 3 \\ M_2' \equiv 2 \mod 5. \end{cases}$$

Por el teorema chino del residuo obtenemos la solución $x \equiv a \cdot 5 \cdot 2 + b \cdot 3 \cdot 2 \mod 15$*, es decir la relación explícita buscada es*

$$x \equiv 10a + 6b \mod 15.$$

Ejemplo 9.7. *Consideremos el sistema*

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 1 \mod 5 \\ x \equiv 4 \mod 7. \end{cases}$$

Con la notación del teorema **[9.6]***, tenemos* $M = 105$*,* $M_1 = 35$*,* $M_2 = 21$*,* $M_3 = 15$*. Por tanto, debemos resolver*

$$\begin{cases} 35M_1' \equiv 1 \mod 3 \\ 21M_2' \equiv 1 \mod 5 \\ 15M_3' \equiv 1 \mod 7, \end{cases}$$

cuya solución es $M_1' \equiv -1 \mod 3$*,* $M_2' \equiv 1 \mod 5$*,* $M_3' \equiv 1 \mod 7$*. Por tanto:*

$$x \equiv 2 \cdot 35 \cdot (-1) + 1 \cdot 21 \cdot 1 + 4 \cdot 15 \cdot 1 \mod 105 \qquad \Rightarrow \qquad x \equiv 11 \mod 105$$

es la solución al sistema.

Observación 9.8. *Un procedimiento alternativo en el ejemplo anterior consiste en escribir la primera congruencia como* $x = 2 + 3t$*, para* $t \in \mathbb{Z}$*. Al sustituir en las otras congruencias tenemos:*

$$\begin{cases} t \equiv 3 \mod 5 \\ t \equiv 3 \mod 7 \end{cases}$$

Repitiendo el mismo procedimiento sustituimos $t = 3 + 5s$ *y llegamos a* $s \equiv 0 \mod 7$*, es decir,* $s = 7k$*. Por tanto*

$$x = 2 + 3t = 2 + 3(3 + 5s) = 11 + 15s = 11 + 15(7k) = 11 + 105k,$$

y la solución de la congruencia es $x \equiv 11 \mod 105$*. La ventaja de este método es que puede usarse incluso cuando los módulos no son coprimos dos a dos.*

La demostración del siguiente corolario es una aplicación directa del teorema chino del residuo.

Corolario 9.9. *Sean* $m_1, m_2, \ldots, m_r$ *coprimos dos a dos,* $b_1, b_2, \ldots, b_r$ *enteros y* $a_1, a_2, \ldots, a_r$ *cumpliendo* $(a_i : m_i) = 1$*,* $i = 1, 2, \ldots, r$*. Entonces el sistema de congruencias lineales*

$$\begin{cases} a_1 x \equiv b_1 \mod m_1 \\ a_2 x \equiv b_2 \mod m_2 \\ \quad \vdots \\ a_r x \equiv b_r \mod m_r \end{cases}$$

tiene una única solución módulo el producto $m_1 \cdots m_r$*.*

9.4. Sistemas de congruencias lineales

En algunos de los ejercicios se observa que el problema de resolver la congruencia $ax \equiv b \mod m$ puede ser bastante laborioso si m es grande, debido a la cantidad de cálculos requeridos cuando se resuelve utilizando los métodos expuestos en las secciones anteriores. El siguiente teorema establece que si m se escribe como un producto de enteros $m_1, m_2, \ldots, m_n$ entonces la congruencia $ax \equiv b \mod m$ es equivalente (que tienen las mismas soluciones) al **sistema de congruencias** $ax \equiv b \mod m_i$, $i = 1, 2, \ldots, n$.

Teorema 9.10. *Sean* $m_1, m_2, \ldots, m_n$ *enteros positivos. Entonces el sistema*

$$\begin{cases} ax \equiv b \mod m_1 \\ ax \equiv b \mod m_2 \\ \quad \vdots \\ ax \equiv b \mod m_n \end{cases} \tag{9.6}$$

es equivalente a la congruencia $ax \equiv b \mod [m_1 : m_2 : \ldots : m_n]$.

Observación 9.11. *El teorema anterior junto con el teorema* **[9.4]** *dan un criterio para determinar si un sistema de congruencias tiene solución, el sistema* **[9.6]** *tiene solución si y sólo si* $(a : [m_1 : m_2 : \ldots : m_n]) \mid b$.

En el caso particular que los m_i *sean primos relativos dos a dos, el sistema* **[9.6]** *tiene solución si y sólo si* $(a : m_1 m_2 \cdots m_n) \mid b$*.*

Así pues, tenemos el siguiente resultado.

Teorema 9.12. *Si la factorización canónica de* m *es* $p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ *entonces la congruencia* $ax \equiv b \mod m$ *es equivalente al sistema de* r *congruencias*

$$ax \equiv b \mod p_i^{e_i}, \; i = 1, 2, \ldots, r.$$

Para comprender los teoremas anteriores estudiemos los siguientes ejemplos.

Ejemplo 9.13. *Resolver* $7x \equiv 6 \mod 100$

Resolución. *La factorización canónica de* 100 *es* $2^2 5^2$*, luego la congruencia es equivalente al sistema*

$$\begin{cases} 7x \equiv 6 \mod 25 \\ 3x \equiv 2 \mod 4 \end{cases}$$

La primera congruencia $x \equiv 8 \mod 25$ *tiene solución, las cuales son* $x = 8, 33, \boxed{58}, 83, \ldots$

La segunda congruencia $x \equiv 2 \mod 4$ *también tiene solución y sus soluciones están dadas por* $x = 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, \boxed{58}, 62, \ldots$

Así la solución al sistema está determinada por la solución común a cada congruencia $x \equiv 58 \mod 100$.

EJERCICIOS

Ejercicio 9.8. *Resolver los sistemas de congruencias*

[A]

$$\begin{cases} x \equiv 1 & \mod 4 \\ x \equiv 2 & \mod 3 \\ x \equiv 3 & \mod 5 \end{cases}$$

[B]

$$\begin{cases} 3x \equiv 6 & \mod 12 \\ 2x \equiv 5 & \mod 7 \\ 3x \equiv 1 & \mod 5 \end{cases}$$

[C]

$$\begin{cases} x \equiv 5 & \mod 12 \\ x \equiv 17 & \mod 20 \\ x \equiv 23 & \mod 42 \end{cases}$$

Ejercicio 9.9. *Mostrar que la conclusión del teorema* **[9.6]** *chino del residuo no necesariamente se cumple si los módulos* m_i *no son primos relativos.*

Ejercicio 9.10. *Resolver la congruencia* $91x \equiv 419 \mod 440$. *Sugerencia: Transformarla en un sistema*

Ejercicio 9.11. *Ahora planteamos un problema de la antigua China, que data del año 1275 d.C. "Encontrar un número tal que, al ser dividido por siete da uno como residuo, al ser dividido por ocho da dos como residuo y al ser dividido por nueve da tres como residuo".*

Ejercicio 9.12. *Dado el sistema*

$$\begin{cases} x \equiv 4 & \mod 8 \\ x \equiv a & \mod 6 \\ x \equiv -1 & \mod 15 \end{cases}$$

[A] *Determinar todos los posibles valores del parámetro* $a \in \mathbb{Z}$ *que hacen que el sistema tenga solución.*

[B] *En caso que el sistema tenga solución, demostrar que es independiente del parámetro* a.

[C] *En caso que el sistema tenga solución, resolver el sistema.*

Ejercicio 9.13. *Encontrar el menor entero positivo que deje residuo* $9, 8, \ldots, 2, 1$ *cuando se divide por* $10, 9, \ldots, 3, 2$, *respectivamente.*

Ejercicio 9.14. *Encontrar el menor entero positivo* n *tal que* $n/3$ *es un cubo perfecto,* $n/5$ *es una quinta potencia perfecta y* $n/7$ *es una séptima potencia perfecta.*

Bibliografía

[1] A. Adler y J.E. Coury. *The Theory of Numbers: A Text and Source Book of Problems*. Jones y Bartlett, 1995.

[2] D.M. Burton. *Elementary Number Theory*. Tata McGraw-Hill Publishing Company Limited, 2006. ISBN: 9780070616073.

[3] R. Dolores M. & Rodríguez. *Como enseñar divisibilidad*. Anaya, 1982.

[4] X. Jiagu. *Lecture Notes on Mathematical Olympiad Courses: For Junior Section*. Mathematical Olympiad series v. 2. World Scientific Publishing Company Pte Limited, 2010. ISBN: 9789814293570.

[5] M. Ruiz. *Introducción a la teoría de números enteros*. Universidad de El Salvador.

[6] H. Sermeño. *Introducción a la Matemática Abstracta*. Universidad de El Salvador.

[7] Viceministerio de Ciencia y Tecnología. *Resolución de problemas matemáticos*. Ministerio de Educación de El Salvador, 2014.

[8] F. Velásquez. *Problemas de Aritmética y cómo resolverlos*. Colección Racso, 1999.