

Teoría de números  
[para principiantes]

GUSTAVO  
RUBIANO

Teoría de números  
[para principiantes]

Luis R. Jiménez B.  
Jorge E. Gordillo A.  
Gustavo N. Rubiano O.  
PROFESORES

Universidad Nacional de Colombia  
Facultad de Ciencias  
Sede Bogotá

vi, 284 p. : 3 il.  
ISBN 958-701-372-7  
QA241.

1. Teoría de números

Luis R. Jiménez B.,  
Jorge E. Gordillo A.,  
Gustavo N. Rubiano O.

TEORÍA DE NÚMEROS [PARA PRINCIPIANTES], 2A. EDICIÓN.  
Universidad Nacional de Colombia, Sede Bogotá.  
Facultad de Ciencias, 2004

MATHEMATICS SUBJECT CLASSIFICATION 2000: 11-01.

© *Edición en castellano*: Luis R. Jiménez B., Jorge E. Gordillo A.,  
Gustavo N. Rubiano O.  
Universidad Nacional de Colombia.

Primera impresión, 2004

Impresión:  
Pro-Offset Editorial Ltda.  
Bogotá, D. C.  
COLOMBIA

---

Índice General

---

<b>Prólogo</b>	<b>ix</b>
<b>1 Números Naturales</b>	<b>1</b>
1.1 Axiomas de Peano . . . . .	1
1.2 Adición de números naturales . . . . .	2
1.3 Multiplicación de números naturales . . . . .	5
1.4 Orden entre números naturales . . . . .	7
1.5 Construcción de los números enteros . . . . .	10
1.6 Formas equivalentes al principio de inducción matemática . . . . .	13
<b>2 Divisibilidad</b>	<b>25</b>
2.1 Propiedades básicas . . . . .	25
2.2 Máximo Común Divisor MCD . . . . .	27

2.3	Algoritmo de Euclides . . . . .	29
2.4	Propiedades del Máximo Común Divisor . . . . .	33
2.5	Mínimo Común Múltiplo y generalizaciones . . . . .	39
2.6	Teorema fundamental de la aritmética . . . . .	46
2.7	Algunas propiedades de los números primos . . . . .	51
2.8	Algunas ecuaciones diofánticas . . . . .	58
<b>3</b>	<b>Funciones Aritméticas</b>	<b>64</b>
3.1	La función parte entera . . . . .	64
3.2	Las funciones número y suma de divisores . . . . .	70
3.3	Números perfectos, de Mersenne y de Fermat . . . . .	74
3.4	La función $\Phi$ de Euler . . . . .	78
3.5	Funciones multiplicativas . . . . .	86
3.6	La fórmula de inversión de Möbius . . . . .	90
<b>4</b>	<b>Congruencias</b>	<b>98</b>
4.1	Definición y propiedades básicas . . . . .	98
4.2	Criterios de Divisibilidad . . . . .	104
4.3	Aritmética módulo $n$ . . . . .	106
4.4	Los Teoremas de Euler y Fermat . . . . .	114
4.5	Congruencias lineales . . . . .	121
4.6	Ecuaciones Diofánticas lineales . . . . .	125
4.7	Sistemas de congruencias lineales . . . . .	127
4.8	El Teorema chino del residuo . . . . .	131

4.9	Congruencias de grado superior . . . . .	137
4.10	Congruencias con módulo una potencia de un primo . . . . .	140
4.11	Teoremas de Lagrange y Wilson . . . . .	147
<b>5</b>	<b>Residuos cuadráticos</b>	<b>153</b>
5.1	Congruencias de segundo grado con módulo primo . . . . .	153
5.2	Ley de la reciprocidad cuadrática . . . . .	160
5.3	El símbolo de Jacobi . . . . .	167
5.4	Potencias módulo $n$ y raíces primitivas . . . . .	172
5.5	Álgebra y teoría de números . . . . .	180
<b>6</b>	<b>Criptografía</b>	<b>194</b>
6.1	Nociones básicas . . . . .	194
6.2	Cifrados monográficos . . . . .	195
6.3	Cifrado en Bloques . . . . .	206
6.4	Cifrados Exponenciales . . . . .	213
6.4.1	Algoritmo para calcular $P^e$ módulo $p$ . . . . .	214
6.5	Sistemas de Clave Pública . . . . .	217
6.5.1	Sistema RSA . . . . .	219
6.5.2	Sistema de Rabin . . . . .	221
6.5.3	Sistema de la mochila . . . . .	225
<b>7</b>	<b>Fraciones continuas</b>	<b>230</b>
7.1	Fraciones continuas finitas . . . . .	231
7.2	Convergentes . . . . .	235

7.3	Fracciones continuas infinitas . . . . .	242
7.4	Fracciones continuas periódicas . . . . .	248
7.5	Aproximación de números irracionales . . . . .	253
	<b>Números primos menores que 10.000</b>	<b>257</b>
	<b>Respuestas y sugerencias</b>	<b>262</b>
	<b>Bibliografía</b>	<b>280</b>

---

## Prólogo

---

La segunda edición de este libro mantiene el mismo espíritu con que fue concebida la primera; es decir, se trata de un texto básico de iniciación al estudio de la Teoría de Números. La principal característica de esta nueva edición es la adición de un capítulo sobre Criptografía, que muestra una de las principales aplicaciones de la teoría desarrollada.

También se ha hecho una revisión cuidadosa de los temas tratados y de las correspondientes secciones de ejercicios, se han adicionado algunas secciones y se ha actualizado la bibliografía. Esperamos que estos cambios hagan el material más útil y atractivo para los estudiantes.

Finalmente queremos expresar nuestra gratitud a todas las personas que leyeron la primera edición, y nos hicieron llegar sus valiosos comentarios y sugerencias que tuvimos en cuenta para la preparación de la presente edición. En especial, manifestamos nuestro agradecimiento a los profesores Paz Morillo (E-UPB-TL; Barcelona) por *Mathematical Reviews* [MR 2000j:11001], y Gabriel D. Villa-Salvador (Cinvestav, México D. F.) por *Zentralblatt* [Zbl 0956.1101] quienes gentilmente evaluaron la edición original y nos motivaron para realizar esta nueva versión.

## Prólogo a la primera edición

En la formación de toda persona que se dedique a la enseñanza o al estudio de las matemáticas, o cualquier nivel, no puede faltar un curso de Teoría de números. Esta hermosa teoría, ha sido llamada por K. F. Gauss, la reina de las matemáticas. La simplicidad de su objeto, la elegancia y la diversidad de sus métodos, la formulación sencilla de numerosos problemas no resueltos, hacen de esta disciplina una de las áreas más fascinantes del universo matemático.

En este libro se ofrece una introducción breve y eficiente de los temas, que a nuestro modo de ver son fundamentales para iniciarse en el estudio de esta teoría. A lo largo de sus capítulos estudiamos detalladamente los siguientes tópicos: números naturales y enteros, divisibilidad y números primos, funciones numéricas, congruencias y fracciones continuas.

En el estudio de todos los temas, presentamos numerosos ejemplos y proponemos una buena cantidad de ejercicios, la mayoría de ellos con respuestas o sugerencias, que permiten al estudiante avanzar con mayor seguridad en la asimilación de los contenidos.

Con este libro, creemos llenar la necesidad de un texto claro, sencillo y económico, dirigido principalmente a los estudiantes de las carreras y licenciaturas de matemáticas ofrecidas por nuestras universidades.

Luis Rafael Jiménez Becerra  
Jorge Enrique Gordillo Ardila  
Gustavo Nevardo Rubiano Ortegón

Departamento de Matemáticas  
Universidad Nacional de Colombia  
Ciudad Universitaria, Bogotá, Colombia.  
mjimenez98@yahoo.com  
gnrubianoo@unal.edu.co  
Junio de 2004

---

## Números Naturales

---

### 1.1 Axiomas de Peano

El conjunto de los números naturales se puede caracterizar mediante los siguientes axiomas, introducidos por el matemático italiano Giuseppe Peano en 1899:

**A-1** Hay un elemento especial  $0 \in \mathbb{N}$ .

**A-2** Para todo  $n \in \mathbb{N}$  existe un único elemento  $n^+ \in \mathbb{N}$  llamado el sucesor de  $n$ .

**A-3** Para todo  $n \in \mathbb{N}$ ,  $n^+ \neq 0$ .

**A-4** Si  $n, m \in \mathbb{N}$  y  $n^+ = m^+$  entonces  $n = m$ .

**A-5** Si  $S$  es un subconjunto de  $\mathbb{N}$  tal que:

1.  $0 \in S$ ,
2.  $n^+ \in S$  siempre que  $n \in S$ , entonces  $S = \mathbb{N}$ .

En la formulación de los axiomas de Peano se supone de antemano la existencia del conjunto  $\mathbb{N}$ . El axioma **A-3** establece la existencia de un primer número natural que es 0. El axioma **A-4** indica que números naturales diferentes tienen sucesores diferentes.

El axioma **A-5** se conoce como *El Principio de Inducción Matemática* —abreviadamente, PIM—. En las aplicaciones de este principio la hipótesis  $n \in S$ , a partir de la cual se demuestra que  $n^+ \in S$ , se denomina *Hipótesis de Inducción*.

## 1.2 Adición de números naturales

**1.1 Definición.** Las siguientes ecuaciones definen la adición en  $\mathbb{N}$ . Para todo  $m, n \in \mathbb{N}$ :

$$\begin{aligned}m + 0 &= m, \\m + n^+ &= (m + n)^+.\end{aligned}$$

Como todo número natural distinto de cero es el sucesor de un número natural la adición resulta bien definida.

**1.2 Teorema.** *La adición de números naturales es asociativa, es decir: Para todo  $n, m, k \in \mathbb{N}$*

$$(n + m) + k = n + (m + k).$$

*Demostración.* Usaremos el axioma **A-5** —PIM—.

Sea  $S = \{k \in \mathbb{N} \mid (n + m) + k = n + (m + k) \text{ para todo } n, m \in \mathbb{N}\}$ .

1.  $0 \in S$  puesto que

$$(n + m) + 0 = n + m = n + (m + 0) \quad (\text{def. suma})$$

2. Supongamos que  $k \in S$ , es decir que para todo  $n, m \in \mathbb{N}$

$$(n + m) + k = n + (m + k).$$

Entonces,

$$\begin{aligned}
 (n + m) + k^+ &= [(n + m) + k]^+ && \text{(def. suma)} \\
 &= [n + (m + k)]^+ && \text{(hip. inducción)} \\
 &= n + (m + k)^+ && \text{(def. suma)} \\
 &= n + (m + k^+) && \text{(def. suma)}
 \end{aligned}$$

luego  $k^+ \in S$  y por **A-5**,  $S = \mathbb{N}$ . □

Para demostrar la conmutatividad, probamos primero:

**1.3 Lema.** *Para todo  $m \in \mathbb{N}$ ,  $0 + m = m$ .*

*Demostración.* Sea  $S = \{m \in \mathbb{N} \mid 0 + m = m\}$ .

1.  $0 \in S$ , puesto que  $0 + 0 = 0$  por definición de suma.
2. Supongamos que  $m \in S$ , es decir, que  $0 + m = m$ . Entonces:

$$\begin{aligned}
 0 + m^+ &= (0 + m)^+ && \text{(def. suma)} \\
 &= m^+ && \text{(hip. inducción)}
 \end{aligned}$$

Luego  $m^+ \in S$  y, por **A-5**,  $S = \mathbb{N}$ . □

**1.4 Lema.** *Para todo  $m, n \in \mathbb{N}$ ,  $m^+ + n = (m + n)^+$ .*

*Demostración.* Sea  $S = \{n \in \mathbb{N} \mid m^+ + n = (m + n)^+ \text{ para todo } m \in \mathbb{N}\}$ .

1.  $0 \in S$ , puesto que para todo  $m \in \mathbb{N}$

$$\begin{aligned}
 m^+ + 0 &= m^+ && \text{(def. suma)} \\
 &= (m + 0)^+ && \text{(def. suma)}
 \end{aligned}$$

2. Supongamos que  $n \in S$ , es decir, que para todo  $m \in \mathbb{N}$

$$m^+ + n = (m + n)^+.$$

Entonces para todo  $m \in \mathbb{N}$ , tenemos

$$\begin{aligned} m^+ + n^+ &= (m^+ + n)^+ && \text{(def. suma)} \\ &= [(m + n)^+]^+ && \text{(hip. inducción)} \\ &= (m + n^+)^+ && \text{(def. suma)} \end{aligned}$$

Así,  $n^+ \in S$  y, por **A-5**,  $S = \mathbb{N}$ .

□

**1.5 Teorema.** *La adición de números naturales es conmutativa: para todo  $m, n \in \mathbb{N}$ ,  $m + n = n + m$ .*

*Demostración.* Sea  $S = \{n \in \mathbb{N} \mid m + n = n + m \text{ para todo } m \in \mathbb{N}\}$ .

1.  $0 \in S$ , puesto que  $m + 0 = m = 0 + m$ .
2. Supongamos que  $n \in S$ . Entonces, para todo  $m \in \mathbb{N}$ ,

$$\begin{aligned} m + n^+ &= (m + n)^+ && \text{(def. suma)} \\ &= (n + m)^+ && \text{(hip. inducción)} \\ &= n^+ + m && \text{(Lema 1.4).} \end{aligned}$$

Así,  $n^+ \in S$  y, por **A-5**,  $S = \mathbb{N}$ .

□

**1.6 Teorema.** *Si  $n, m$  y  $k$  son números naturales tales que  $m + k = n + k$ , entonces  $m = n$ .*

*Demostración.* Sea

$$S = \{k \in \mathbb{N} \mid \text{si } m + k = n + k \text{ entonces } m = n \text{ para todo } m, n \in \mathbb{N}\}.$$

1.  $0 \in S$ , pues si  $n$  y  $m$  son naturales tales que  $m + 0 = n + 0$  por definición de suma concluimos que  $m = n$ .
2. Supongamos que  $k \in S$  y sean  $n, m \in \mathbb{N}$  tales que

$$m + k^+ = n + k^+.$$

Entonces,

$$(m + k)^+ = (n + k)^+ \quad (\text{def. suma})$$

luego, por **A-4**,  $m + k = n + k$  y, por la hipótesis de inducción,  $m = n$ .

Así,  $k^+ \in S$  y  $S = \mathbb{N}$ , por **A-5**.  $\square$

### 1.3 Multiplicación de números naturales

Las siguientes ecuaciones definen la multiplicación en  $\mathbb{N}$ . Para todo  $m, n \in \mathbb{N}$ ,

$$\begin{aligned} m0 &= 0, \\ mn^+ &= mn + m. \end{aligned}$$

Como todo número natural distinto de cero es el sucesor de otro número natural, la operación resulta bien definida.

**1.7 Teorema.** *La multiplicación es distributiva con respecto a la adición, es decir: para todo  $m, n, k \in \mathbb{N}$ ,  $m(n + k) = mn + mk$ .*

*Demostración.* Sea

$$S = \{k \in \mathbb{N} \mid m(n + k) = mn + mk \text{ para todo } m, n \in \mathbb{N}\}.$$

1.  $0 \in S$ . En efecto,

$$\begin{aligned} m(n + 0) &= mn && (\text{def. suma}) \\ &= mn + 0 && (\text{def. suma}) \\ &= mn + m0 && (\text{def. multiplicación}). \end{aligned}$$

2. Supongamos que  $k \in S$ .

Para todo  $m, n \in \mathbb{N}$ , tenemos

$$\begin{aligned} m(n + k^+) &= m(n + k)^+ && (\text{def. suma}) \\ &= m(n + k) + m && (\text{def. multiplicación}) \\ &= (mn + mk) + m && (\text{hip. inducción}) \\ &= mn + (mk + m) && (\text{Teorema 1.2}) \\ &= mn + mk^+ && (\text{def. multiplicación}) \end{aligned}$$

Así,  $k^+ \in S$  y, por **A-5**,  $S = \mathbb{N}$ . □

**1.8 Teorema.** *La multiplicación de números naturales es asociativa: para todo  $n, m, k \in \mathbb{N}$   $(mn)k = m(nk)$ .*

*Demostración.* Sea

$$S = \{k \in \mathbb{N} \mid (mn)k = m(nk) \text{ para todo } n, m \in \mathbb{N}\}$$

1.  $0 \in S$ . En efecto, la definición de multiplicación nos permite afirmar que

$$(mn)0 = 0 \text{ y también que } m(n0) = m0 = 0$$

2. Supongamos que  $k \in S$ . Para todo  $m, n \in \mathbb{N}$  tenemos:

$$\begin{aligned} (mn)k^+ &= (mn)k + mn && \text{(def. multiplicación)} \\ &= m(nk) + mn && \text{(hip. inducción)} \\ &= m(nk + n) && \text{(Teorema 1.7)} \\ &= m(nk^+) && \text{(def. multiplicación);} \end{aligned}$$

luego  $k^+ \in S$  y, por **A-5**,  $S = \mathbb{N}$ . □

**1.9 Teorema.** *La multiplicación de números naturales es conmutativa. Es decir: Para todo  $m, n \in \mathbb{N}$ ,  $mn = nm$ .*

Para demostrar el Teorema 1.9 es necesario probar antes los lemas siguientes:

**1.10 Lema.** *Para todo  $m \in \mathbb{N}$ , tenemos  $0m = 0$ .*

**1.11 Lema.** *Para todo  $m, n \in \mathbb{N}$ , tenemos  $m^+n = mn + n$ .*

Tanto la demostración de los Lemas 1.10, 1.11 como la del Teorema 1.9 las dejamos como ejercicio al lector.

---

## Ejercicios 1.1

---

1. Demostrar que todo número natural diferente de cero es de la forma  $n^+$  para algún  $n \in \mathbb{N}$ .
2. Demostrar que para todo  $n \in \mathbb{N}$ ,  $n^+ = n + 0^+$ .
3. Si  $m$  y  $n$  son números naturales tales que  $m + n = 0$ , probar que  $m = 0$  y  $n = 0$ .
4. Demostrar que si  $m, n \in \mathbb{N}$  entonces  $m + n \in \mathbb{N}$  y  $mn \in \mathbb{N}$ .
5. Probar que si  $n, m \in \mathbb{N}$  son tales que  $mn = 0$  entonces  $m = 0$ , o  $n = 0$ .
6. Demostrar los lemas 1.10 y 1.11 y el Teorema 1.9.

### 1.4 Orden entre números naturales

**1.12 Definición.** Dados  $m, n \in \mathbb{N}$  decimos que:

$$m \leq n \text{ si existe } p \in \mathbb{N} \text{ tal que } n = m + p.$$

Veamos que la relación  $\leq$  define un orden sobre  $\mathbb{N}$ . En efecto,

1. La relación  $\leq$  es reflexiva.

Para todo  $m \in \mathbb{N}$ ,  $m \leq m$  puesto que  $m = m + 0$  con  $0 \in \mathbb{N}$ .

2. La relación  $\leq$  es antisimétrica.

Si  $n, m$  son números naturales tales que  $m \leq n$  y  $n \leq m$ , entonces existen  $p, q \in \mathbb{N}$  tales que  $n = m + p$  y  $m = n + q$ . Luego,  $m = (m + p) + q = m + (p + q)$ . Por lo tanto,  $p + q = 0$  y, en consecuencia,  $p = q = 0$ , lo que implica  $m = n$ .

3. La relación es transitiva.

Si  $m, n, r \in \mathbb{N}$  son tales que  $m \leq n$  y  $n \leq r$ , entonces  $n = m + p$  y  $r = n + q$  donde  $p, q \in \mathbb{N}$ , y por lo tanto  $r = (m + p) + q = m + (p + q)$  donde  $p + q \in \mathbb{N}$ , luego  $m \leq r$ .

Como es usual, definimos  $m < n$  si  $m \leq n$  y  $m \neq n$ . Podemos observar como consecuencia de la definición que  $m < n$  si y solo si  $n = m + p^+$  para algún  $p \in \mathbb{N}$ .

**1.13 Teorema (Ley de la tricotomía).** *Dados  $m, n \in \mathbb{N}$  una y solo una de las siguientes afirmaciones es verdadera,*

$$m < n, \quad m = n, \quad n < m.$$

La demostración requiere la prueba del lema siguiente.

**1.14 Lema.** *Si  $m, n \in \mathbb{N}$  todas las afirmaciones siguientes son falsas:*

1.  $m < n$  y  $m = n$ .
2.  $n < m$  y  $n = m$ .
3.  $m < n$  y  $n < m$ .

*Demostración.* Si tuviéramos simultáneamente  $m < n$  y  $m = n$ , tendríamos  $n = m + p^+$ , donde  $p \in \mathbb{N}$  y  $m = n$ , lo que implicaría que  $p^+ = 0$ . Esto contradice el axioma **A-3**. Luego 1 es falsa.

Análogamente demostramos que 2 es falsa.

Ahora, si  $m < n$  y  $n < m$  tendríamos  $n = m + p^+$  y  $m = n + q^+$  lo que implicaría

$$n = (n + q^+) + p^+ = n + (q^+ + p^+) = n + (q^+ + p)^+$$

y en consecuencia  $(q^+ + p)^+ = 0$ , lo que contradice **A-3**, luego 3 es falsa.  $\square$

*Demostración.* (Del Teorema 1.13). Dados  $m, n \in \mathbb{N}$  veamos que se tiene al menos una de las afirmaciones.

Sea  $S = \{n \in \mathbb{N} \mid \text{para todo } m \in \mathbb{N} \text{ se tiene alguna de las relaciones } m < n, m = n, n < m\}$ .

1.  $0 \in S$ , ya que para todo  $m \neq 0$  tenemos  $0 < m$ .

2. Supongamos que  $n \in S$ . Sea  $m \in \mathbb{N}$ , como  $n \in S$  se presentan tres casos:

Caso 1.  $m < n$ . En este caso  $n = m + p^+$  donde  $p \in \mathbb{N}$  y por lo tanto,

$$\begin{aligned} n^+ &= n + 0^+ = (m + p^+) + 0^+ \\ &= m + (p^+ + 0^+) \\ &= m + (p^+ + 0)^+ \\ &= m + (p^+)^+ \end{aligned}$$

luego  $m < n^+$ .

Caso 2.  $m = n$ . En este caso  $n^+ = n + 0^+ = m + 0^+$ , es decir  $m < n^+$ .

Caso 3.  $n < m$ . En este caso  $m = n + p^+$  donde  $p \in \mathbb{N}$ . Si  $p = 0$  entonces  $m = n + 0^+ = n^+$ . Si  $p \neq 0$  entonces  $m = n + p^+ = n + (p + 0^+) = (n + 0^+) + p = n^+ + p$ , luego  $n^+ < m$ .

Hemos visto entonces que para todo  $m \in \mathbb{N}$ , se cumple alguna de las relaciones  $m < n^+$ ,  $m = n^+$ ,  $n^+ < m$ , en consecuencia  $n^+ \in S$  y por **A-5**,  $S = \mathbb{N}$ .

El lema demuestra que solamente se puede tener una de las afirmaciones  $m < n$ ,  $m = n$ ,  $n < m$  y así se termina la demostración del teorema.  $\square$

Otras propiedades del orden en  $\mathbb{N}$  serán enunciadas en los siguientes ejercicios.

---

## Ejercicios 1.2

---

Demostrar cada una de las siguientes afirmaciones:

1. Si  $n \in \mathbb{N}$  y  $n \neq 0$  entonces  $n \geq 1$ .

2. Para todo  $n \in \mathbb{N}$ ,  $n < n^+$ .
3. Si  $m, n \in \mathbb{N}$  con  $m < n$  y  $n < r$  entonces  $m < r$ .
4. Si  $n \in \mathbb{N}$  con  $m < n$  entonces para todo  $p \in \mathbb{N}$ ,  $m + p < n + p$ .
5. Si  $n \in \mathbb{N}$  con  $m < n$  entonces para todo  $p \neq 0$ ,  $mp < np$ .
6. Si  $m, n \in \mathbb{N}$  son tales que  $m < n$  entonces  $m^+ \leq n$ .
7. Si  $m, n, k \in \mathbb{N}$  son tales que  $m < n^+$  entonces  $m \leq n$ .
8. Si  $m, n, k \in \mathbb{N}$  son tales que  $mk = nk$  y  $k \neq 0$  entonces  $m = n$ .
9. La relación  $\leq$  definida sobre  $\mathbb{N}$  es una relación de orden total.

## 1.5 Construcción de los números enteros

Presentamos ahora de manera breve una de las formas de construir el conjunto de los números enteros a partir del conjunto de los números naturales.

Para todo número natural  $n \neq 0$  seleccionamos un nuevo símbolo que representamos por  $(-n)$  y definimos el conjunto de los números enteros así:

$$\mathbb{Z} = \{-n \mid n \in \mathbb{N}, n \neq 0\} \cup \mathbb{N}.$$

### ADICIÓN DE NÚMEROS ENTEROS

Definimos la adición en  $\mathbb{Z}$  mediante las siguientes reglas:

1. Si  $x, y \in \mathbb{N}$  definimos  $x + y$  usando la definición en  $\mathbb{N}$ .
2. Para todo  $x \in \mathbb{Z}$  definimos  $x + 0 = 0 + x = x$ .
3. Si  $m$  y  $n$  son números naturales diferentes de cero y  $m = n + k$  para algún  $k \in \mathbb{N}$ , definimos:

$$(a) \quad m + (-n) = (-n) + m = k.$$

$$(b) \quad (-m) + n = n + (-m) = \begin{cases} -k & \text{si } k \neq 0. \\ 0 & \text{si } k = 0. \end{cases}$$

$$(c) \quad (-m) + (-n) = -(m + n).$$

Observamos que dados  $x, y$  donde al menos uno de ellos no es un número natural, alguna de las alternativas (a), (b), o (c) define  $x + y$ .

La adición que acabamos de definir goza de las siguientes propiedades:

1. Si  $x, y, z \in \mathbb{Z}$  entonces  $(x + y) + z = x + (y + z)$ .
2. Si  $x, y \in \mathbb{Z}$  entonces  $x + y = y + x$ .
3. Para todo  $x \in \mathbb{Z}$ ,  $x + 0 = 0 + x = x$ .
4. Para todo  $x \in \mathbb{Z}$ , existe  $y \in \mathbb{Z}$  tal que  $x + y = 0$ .

Las pruebas de los enunciados 1 a 4 se dejan como ejercicios al lector. El elemento  $y$  de la propiedad (4) se denomina *el opuesto de  $x$*  y se denota  $(-x)$ . Usualmente escribimos  $x - y$  en vez de  $x + (-y)$ .

#### MULTIPLICACIÓN DE NÚMEROS ENTEROS

Definimos la multiplicación en  $\mathbb{Z}$  mediante las siguientes reglas:

1. Si  $x, y \in \mathbb{N}$  usamos la multiplicación definida en  $\mathbb{N}$ .
2. Para todo  $x \in \mathbb{Z}$ , definimos  $x0 = 0x = 0$ .
3. Si  $m, n$  son naturales diferentes de cero, definimos:
  - (a)  $(-m)n = n(-m) = -(mn)$ .
  - (b)  $(-m)(-n) = mn$ .

Nuevamente observamos que dados  $x, y$  distintos de cero donde al menos uno de ellos no es natural, alguna de las alternativas (a) o (b) define su producto.

A continuación enunciamos las propiedades fundamentales de la multiplicación de enteros.

1. Si  $x, y, z \in \mathbb{Z}$  entonces  $(xy)z = x(yz)$ .
2. Si  $x, y \in \mathbb{Z}$  entonces  $xy = yx$ .

3. Para todo  $x \in \mathbb{Z}$ ,  $x1 = x$ .
4. Para todo  $x, y, z \in \mathbb{Z}$ ,  $x(y + z) = xy + xz$ .
5. Si  $x, y \in \mathbb{Z}$  con  $x \neq 0$ ,  $y \neq 0$  entonces  $xy \neq 0$ .
6. Si  $x, y, z \in \mathbb{Z}$ ,  $z \neq 0$  son tales que  $xz = yz$  entonces  $x = y$ .

Las demostraciones de las afirmaciones anteriores son ejercicio para el lector.

### ORDEN EN LOS NÚMEROS ENTEROS

La relación definida por

$$x \leq y \text{ si y solo si } y - x \in \mathbb{N}$$

es una relación de orden total sobre  $\mathbb{Z}$ .

- Si  $x \leq y$  y  $x \neq y$  escribimos  $x < y$ .
- Si  $0 < x$  decimos que  $x$  es un *entero positivo*. Denotamos por  $\mathbb{Z}^+$  el conjunto de los enteros positivos.
- También usamos  $x > 0$  para decir que  $x$  es positivo.
- Los enteros  $x$  que satisfacen  $(-x) > 0$  se denominan *negativos*.
- También escribimos  $x < 0$  para decir que  $x$  es negativo.

El orden definido sobre  $\mathbb{Z}$  tiene las siguientes propiedades:

1. Si  $x, y \in \mathbb{Z}^+$  entonces  $x + y \in \mathbb{Z}^+$  y  $xy \in \mathbb{Z}^+$ .
2. Si  $x, y \in \mathbb{Z}$  entonces una y solo una de las siguientes afirmaciones es verdadera  $x < y$ ,  $x = y$ ,  $y < x$ .
3. Si  $x, y \in \mathbb{Z}$  son tales que  $x \leq y$  entonces para todo  $z$ ,  $x + z \leq y + z$ .
4. Si  $x, y, z, w \in \mathbb{Z}$  son tales que  $x \leq y$  y  $z \leq w$  entonces  $x + z \leq y + w$ .
5. Si  $x, y \in \mathbb{Z}$  son tales que  $x \leq y$  y  $z > 0$  entonces  $xz \leq yz$ .
6. Si  $x, y \in \mathbb{Z}$  son tales que  $x \leq y$  y  $z < 0$  entonces  $yz \leq xz$ .

El lector debe verificar que la relación  $\leq$  es en efecto una relación de orden total y demostrar además las propiedades enunciadas.

## 1.6 Formas equivalentes al principio de inducción matemática

Al enunciar los axiomas de Peano, indicamos que el axioma **A-5** se conoce con el nombre de Principio de Inducción Matemática y seguidamente vimos su fuerza en la demostración de varios resultados sobre las operaciones con números naturales. Nos proponemos ahora presentar algunas formas equivalentes y mostrar su aplicación en la prueba de enunciados matemáticos. En esta sección nos referiremos al axioma **A-5** como el PIM1.

**1.15 Teorema (Principio de buena ordenación (abreviadamente PBO)).** *Todo subconjunto no vacío  $S$  de números naturales posee un mínimo. Es decir, existe  $m \in S$  —  $m = \min S$  — tal que para todo  $s \in S$ ,  $m \leq s$ .*

*Demostración.* Utilizamos el PIM1. Sea

$$T = \{n \in \mathbb{N} \mid n \leq s \text{ para todo } s \in S\}.$$

Como  $S \neq \emptyset$  tenemos que  $T \neq \mathbb{N}$ , ya que si  $s' \in S$  entonces  $s' + 1 \notin T$ .

Además  $0 \in T$  y por PIM1 existe  $m \in T$  tal que  $m + 1 \notin T$ . Necesariamente  $m \in S$ , pues como  $m \leq s$  para todo  $s \in S$ , si  $m \notin S$  se tendría que  $m < s$  para todo  $s \in S$  por lo tanto  $m + 1 \leq s$  para todo  $s \in S$  y en consecuencia  $m + 1 \in T$  que es contradictorio. Por lo tanto  $m = \min S$ .  $\square$

Como una aplicación al PBO demostraremos un resultado fundamental del sistema de los números enteros denominado el *Algoritmo de la división*.

**1.16 Teorema (Algoritmo de la división).** *Sean  $a, b$  enteros con  $b > 0$ . Entonces existen enteros únicos  $q, r$  tales que*

$$a = bq + r \quad \text{con} \quad 0 \leq r < b.$$

*Demostración.* 1 Existencia. Sea  $S = \{a - bx \mid x \in \mathbb{Z} \text{ y } a - bx \geq 0\}$ . Veamos que  $S \neq \emptyset$ . Si  $a \geq 0$ ,  $a - b \cdot 0 = a \in S$ . Si  $a < 0$ , como  $b \geq 1$  tenemos que  $a - ab = a(1 - b) \geq 0$  y así  $a - ab \in S$ . Luego  $S \neq \emptyset$ .

Ahora por el PBO,  $S$  tiene un mínimo  $r$  y en consecuencia existe un entero  $q$  tal que

$$a - bq = r \quad \text{con} \quad 0 \leq r.$$

De otra parte, puesto que  $r = \min S$ , entonces

$$r - b = (a - bq) - b = a - (q + 1)b < 0,$$

y por tanto  $r < b$ .

2 Unicidad. Supongamos que  $a = bq + r = bq' + r'$  con  $0 \leq r < b$  y  $0 \leq r' < b$ . Si suponemos  $q' < q$  entonces  $q' + 1 \leq q$  y por lo tanto

$$r = a - bq \leq a - b(q' + 1) = (a - bq') - b = r' - b < 0,$$

que evidentemente es una contradicción.

Similarmente si suponemos  $q < q'$  obtenemos una contradicción. Luego necesariamente  $q = q'$  y también  $r = r'$ .  $\square$

Probaremos ahora, utilizando el PBO, una forma del principio de inducción denotado con PIM2 que nos permite iniciar la inducción desde cualquier número natural y utilizar una hipótesis de inducción más general.

**1.17 Teorema (PIM2).** *Sea  $a$  un número natural. Sea  $S$  un subconjunto de  $\{k \in \mathbb{N} \mid k \geq a\}$  que satisface:*

1.  $a \in S$ .
2. Para cada  $n > a$ ,  $n \in S$  siempre que  $k \in S$  para todo  $k \in \mathbb{N}$  tal que,  $a \leq k < n$ .

Entonces

$$S = \{k \in \mathbb{N} \mid k \geq a\}.$$

*Demostración.* La demostración es por contradicción. Supongamos que  $S \neq \{k \in \mathbb{N} \mid k \geq a\}$  y sea  $T = \{k \in \mathbb{N} \mid k \geq a\} - S$ . Luego  $T \neq \emptyset$  y por el PBO tiene un mínimo  $m$ .

Además, puesto que  $a \in S$  entonces  $m > a$  y para todo  $k$  tal que  $a \leq k < m$ , la minimalidad de  $m$  nos garantiza que  $k \in S$ , y por la condición 2 concluimos que  $m \in S$  lo cual es una contradicción.  $\square$

Antes de presentar alguna aplicación de PIM2 veamos algunas definiciones.

**1.18 Definición.** Sean  $a, b$  números enteros con  $a$  diferente de cero. Decimos que  $a$  divide a  $b$  si existe un entero  $c$  tal que  $b = ac$ . En tal caso escribimos  $a \mid b$ . Decimos también que  $a$  es un *divisor* de  $b$  o que  $b$  es un *múltiplo* de  $a$ .

Para indicar que  $a$  no divide a  $b$  escribimos  $a \nmid b$ . Es fácil verificar que para todo entero  $k$ ,  $1 \mid k$  y si  $k \neq 0$ ,  $k \mid k$ .

**1.19 Definición.** Un entero positivo  $p > 1$  se denomina un número *primo* si tiene exactamente dos divisores positivos a saber: 1 y  $p$ . Un entero positivo mayor que 1 que no es primo se denomina *compuesto*.

**1.20 Teorema.** *Todo entero mayor o igual que 2, o es primo o es un producto de números primos.*

*Demostración.* Sea  $S$  el conjunto de todos los números naturales que son primos o que pueden escribirse como producto de primos.

Claramente  $S \subseteq \{k \in \mathbb{N} \mid k \geq 2\}$  y además tenemos:

1.  $2 \in S$  porque 2 es un número primo.
2. Supongamos que  $n > 2$  y que  $k \in S$  para todo  $k$  tal que  $2 \leq k < n$ . Veamos que  $n \in S$ . Si  $n$  es primo entonces  $n \in S$ . Si  $n$  no es primo existen  $r$  y  $t$  tales que  $n = rt$  con  $2 \leq r < n$  y  $2 \leq t < n$  y por hipótesis ellos o son primos o productos de primos. En consecuencia  $n$  es producto de primos y así  $n \in S$ . El PIM2 nos afirma entonces que  $S = \{k \in \mathbb{N} \mid k \geq 2\}$ .  $\square$

Como otra aplicación de este principio vamos a estudiar la representación de todo entero positivo en base  $b$ , con  $b$  un número natural mayor que 1.

**1.21 Teorema.** *Sea  $b > 1$ . Todo número natural  $a > 0$  se representa de manera única en la forma:*

$$a = c_n b^n + c_{n-1} b^{n-1} + \dots + cb + c_0$$

donde  $n \geq 0$ ,  $c_n \neq 0$  y  $0 \leq c_i < b$  para todo  $i = 0, 1, 2, \dots, n$ .

*Demostración.* **1 Existencia.** Sea  $S$  el conjunto de enteros positivos que pueden escribirse en la forma mencionada. Es evidente que  $1 \in S$ . Supongamos que  $n > 1$  y que todo entero  $k$  tal que  $1 \leq k < n$  pertenece a  $S$ . Por el algoritmo de la división tenemos

$$n = qb + c_0 \text{ con } 0 \leq c_0 < b.$$

Como  $n > 1$  se observa que  $q \geq 0$ . Si  $q = 0$ ,  $n = c_0 \neq 0$  y así  $n \in S$ . Si  $q > 0$  evidentemente  $q < n$  y por la hipótesis de inducción  $q$  puede representarse en la forma:

$$q = c_m b^{m-1} + c_{m-1} b^{m-2} + \cdots + c_2 b + c_1$$

donde  $c_m \neq 0$  y  $0 \leq c_i < b$  para  $i = 1, 2, 3, \dots, m$ , por lo tanto:

$$n = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_1 b + c_0$$

y así  $n \in S$ . Por el PIM2,  $S = \{a \in N \mid a \geq 1\}$ , lo cual prueba la existencia de la representación.

**2 Unicidad.** Supongamos que  $a$  tiene dos representaciones a saber,

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0 = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0$$

donde  $c_n \neq 0$ ,  $d_m \neq 0$ ,  $0 \leq c_i < b$  y  $0 \leq d_j < b$  para todo  $i$  y todo  $j$ .

Por sustracción de las dos representaciones tenemos,

$$0 = e_0 + e_1 b + \cdots + e_s b^s$$

donde  $s$  es el mayor valor de  $k$  para el cual  $c_k \neq d_k$ , en particular  $e_s \neq 0$ .

Si  $s = 0$  obtenemos la contradicción  $e_0 = e_s = 0$ .

Si  $s > 0$  obtenemos  $|e_k| = |c_k - d_k| \leq b - 1$ ;  $0 \leq k \leq s - 1$  y como

$$e_s b^s = -(e_0 + e_1 b + \cdots + e_{s-1} b^{s-1})$$

entonces

$$\begin{aligned} b^s &\leq |e_s b^s| = |e_0 + e_1 b + \cdots + e_{s-1} b^{s-1}| \\ &\leq |e_0| + |e_1| b + \cdots + |e_{s-1}| b^{s-1} \\ &\leq (b-1)(1 + b + \cdots + b^{s-1}) = b^s - 1, \end{aligned}$$

que es también una contradicción. Concluimos que  $m = n$  y  $c_k = d_k$  para todo  $k$  tal que  $0 \leq k \leq n$ .  $\square$

El teorema anterior nos permite construir sistemas de símbolos para representar los números enteros positivos, así: Escogemos símbolos para representar los *dígitos* es decir, los enteros no negativos menores que  $b$  y reemplazamos el número,

$$c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0$$

por el símbolo

$$c_n c_{n-1} \cdots c_1 c_0.$$

El sistema que usamos comúnmente tiene base  $b = 10$  y se denomina el *sistema decimal*. En este sistema el símbolo 8375 representa el número

$$(8)(10)^3 + (3)(10)^2 + (7)(10)^1 + 5.$$

Si escogiésemos  $b = 8$ , el número cuya representación decimal es 8375 está representado por 20267 puesto que

$$8375 = (2)(8)^4 + (0)(8)^3 + (2)(8)^2 + (6)(8)^1 + 7.$$

El número  $b$  en el teorema se denomina la *base del sistema*. Cuando usamos una base diferente a 10, para indicar cuál, la escribimos como subíndice, así por ejemplo:

$$8375 = (20267)_8.$$

Cuando la base es mayor que 10 es necesario inventar símbolos para los dígitos  $11, 12, \dots, (b - 1)$ . Por ejemplo cuando la base es 16 —*sistema hexadecimal*— se establece:

$$10 = A, 11 = B, 12 = C, 13 = D, 14 = E, 15 = F.$$

Por ejemplo:

$$(40)_{16} = (4)(16)^1 + 0 = 64.$$

$$(7F)_{16} = (7)(16)^1 + F = (7)(16) + 15 = 127.$$

$$(FF)_{16} = (F)(16)^1 + F = (15)(16) + 15 = 255.$$

El sistema hexadecimal es especialmente usado en computadores al igual que el sistema en base 2, este último por la facilidad para describir situaciones físicas del tipo ‘ser o no ser’, ‘estar o no estar’.

Los cálculos y reglas para las operaciones de adición y multiplicación son esencialmente los mismos en cualquier sistema, ya que solo dependen

del carácter posicional de la notación y no de la base utilizada; por ejemplo las tablas de adición y multiplicación en base 5 son:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	10
2	2	3	4	10	11
3	3	4	10	11	12
4	4	10	11	12	13

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	11	13
3	0	3	11	14	22
4	0	4	13	22	31

Hallemos ahora  $(232)_5(141)_5$  usando las tablas:

$$\begin{array}{r}
 232 \\
 \times 141 \\
 \hline
 232 \\
 2033 \\
 232 \\
 \hline
 44312
 \end{array}$$

es decir  $(232)_5(141)_5 = (44312)_5$ .

Por una aplicación repetida del Algoritmo de la División podemos fácilmente encontrar la representación en base  $b$  de cualquier entero positivo  $a$ . Si dividimos  $a$  entre  $b$ , el cociente nuevamente entre  $b$  y así hasta obtener un cociente menor que  $b$  tenemos:

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 \leq r_1 < b, & q_1 \geq b \\
 q_1 &= bq_2 + r_2, & 0 \leq r_2 < b, & q_2 \geq b \\
 &\cdot \\
 &\cdot \\
 &\cdot \\
 q_{k-1} &= bq_k + r_k, & 0 \leq r_k < b, & q_k < b.
 \end{aligned}$$

Escribiendo además

$$q_k = 0b + r_{k+1}, \quad 0 < r_{k+1} < b$$

de las ecuaciones anteriores resulta inmediatamente que,

$$a = bq_1 + r_1$$

$$a = b(bq_2 + r_2) + r_1 = b^2q_2 + br_2 + r_1$$

·

·

·

$$a = b^k r_{k+1} + b^{k-1} r_k + \cdots + br_2 + r_1,$$

y por lo tanto,

$$a = (r_{k+1}r_k \cdots r_1)_b.$$

**1.22 Ejemplo.** Hallemos la representación de 756 en base 8:

$$\begin{array}{r} 756 \overline{) 8} \\ \underline{36} \quad 94 \\ \quad \underline{4} \quad 14 \quad 8 \\ \qquad \underline{6} \quad 11 \quad 8 \\ \qquad \qquad \underline{3} \quad 1 \quad 8 \\ \qquad \qquad \qquad \underline{1} \quad 0 \end{array}$$

Luego  $756 = (1364)_8$ .

Volviendo a las diferentes versiones del PIM tenemos la siguiente versión simplificada del Teorema 1.17.

**1.23 Teorema (PIM3).** Sea  $a$  un número natural fijo y

$$U = \{k \in \mathbb{Z} \mid k \geq a\}.$$

Sea  $S \subseteq U$  tal que:

1.  $a \in S$
2. Para cada  $n \geq a$ , si  $n \in S$  entonces  $n + 1 \in S$ .

Entonces  $S = U$ .

*Demostración.* Sea  $n > a$  y supongamos que  $k \in S$  para todo  $k$  tal que  $a \leq k < n$ . En particular se tiene entonces que  $n - 1 \in S$  y por la condición 2 de la hipótesis del teorema se sigue que  $n \in S$  y por PIM2,  $S = U$ .  $\square$

Finalmente veamos que PIM3 implica PIM1.

**1.24 Teorema.** *PIM3 implica PIM1.*

*Demostración.* Supongamos  $S \subseteq \mathbb{N}$  tal que (i)  $0 \in S$ , y (ii) Si  $n \in S$  entonces  $n + 1 \in S$ . Tenemos que probar que  $S = \mathbb{N}$ .

Sean,

$$T = \{x \in \mathbb{N} \mid x = a + s \text{ para algún } s \in S\},$$

$$U = \{x \in \mathbb{N} \mid x \geq a\}.$$

Entonces  $T \subseteq U$ , y además,

1.  $a \in T$  pues  $a = a + 0$  y  $0 \in S$ .
2. Si  $n \geq a$  es tal que  $n \in T$  entonces  $n = a + s$  con  $s \in S$  y por lo tanto  $n + 1 = (a + s) + 1 = a + (s + 1) \in T$ , puesto que  $s + 1 \in S$ .

En consecuencia por el PIM3,  $T = U$ .

Ahora, si  $n \in \mathbb{N}$  entonces  $n + a \geq a$  y como  $U = T$ ,  $n + a \in T$ ; es decir, existe  $s \in S$  tal que  $n + a = a + s$  y por lo tanto  $n = s$ , luego  $\mathbb{N} \subseteq S$  y por lo tanto  $S = \mathbb{N}$ .  $\square$

Si revisamos los resultados expresados en los teoremas 1.15, 1.17, 1.23 y 1.24 tenemos la siguiente cadena de implicaciones:

$$\begin{array}{ccc} \text{PIM1} & \longrightarrow & \text{PBO} \\ \uparrow & & \downarrow \\ \text{PIM3} & \longleftarrow & \text{PIM2} \end{array}$$

Es decir todas las proposiciones son equivalente y nos referiremos a cualquiera de ellas como el *Principio de Inducción Matemática*.

## Ejercicios 1.3

En los ejercicios 1 a 6 demuestre que la proposición es cierta para todo  $n \geq 1$ .

1.  $1 + 2 + 3 + \dots + n = n(n + 1)/2$ .
2.  $1^2 + 2^2 + \dots + n^2 = (1/6)n(n + 1)(2n + 1)$ .
3.  $1^3 + 2^3 + \dots + n^3 = (1/4)n^2(n + 1)^2$ .
4. Si  $r \neq 1$  entonces

$$1 + r + r^2 + \dots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

5.  $1^3 + 2^3 + \dots + (n - 1)^3 < \frac{n^4}{4} < 1^3 + 2^3 + \dots + n^3$ .
6.  $2^{2n+1} - 9n^2 + 3n - 2$  es divisible por 54.
7. Definimos los *números de Fermat* mediante la formula,

$$F_n = 2^{2^n} + 1 \text{ para } n = 0, 1, \dots$$

Pruebe que para todo  $n \geq 1$ ,  $F_0 F_1 \dots F_{n-1} + 2 = F_n$ .

Para representar la suma  $a_1 + a_2 + \dots + a_n$  de  $n$  números reales utilizamos el símbolo  $\sum_{i=1}^n a_i$  que definimos inductivamente de la siguiente forma:

$$\sum_{i=1}^1 a_i = a_1$$

y suponiendo que ya hemos definido  $\sum_{i=1}^n a_i$  para algún  $n \geq 1$  fijo, definimos

$$\sum_{i=1}^{n+1} a_i = \left( \sum_{i=1}^n a_i \right) + a_{n+1}.$$

Demostrar por inducción:

8.  $\sum_{i=1}^n (a_i + b_i) = \sum_{i=1}^n a_i + \sum_{i=1}^n b_i$ .
9.  $\sum_{i=1}^n (ca_i) = c \sum_{i=1}^n a_i$ .
10.  $\sum_{i=1}^n (a_i - a_{i-1}) = a_n - a_0$  (*Propiedad telescópica*).
11. Demostrar que

$$\sum_{j=1}^m \sum_{i=1}^n a_i b_j = \left( \sum_{i=1}^n a_i \right) \left( \sum_{j=1}^m b_j \right).$$

Para representar el producto de  $n$  números reales  $a_1, a_2, \dots, a_n$  utilizamos el símbolo  $\prod_{i=1}^n a_i$  que se define de manera análoga al de suma.

Demostrar por inducción:

12.  $\prod_{i=1}^n (a_i b_i) = \left( \prod_{i=1}^n a_i \right) \left( \prod_{i=1}^n b_i \right)$ .
13.  $\prod_{i=1}^n (ca_i) = c^n \prod_{i=1}^n a_i$ .
- 14.

$$\prod_{i=1}^n \left( \frac{a_i}{a_{i-1}} \right) = \frac{a_n}{a_0} \text{ si } a_i \neq 0 \text{ para } i = 0, 1, \dots, n.$$

El símbolo  $n!$  (leído ene factorial) se define inductivamente como sigue:  $0! = 1$  y para  $n \geq 1$ ,  $n! = n(n-1)!$ . Se observa fácilmente que

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n.$$

Además si  $n$  es un número natural y  $k$  es un entero arbitrario definimos el coeficiente binomial mediante:

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } 0 \leq k \leq n. \\ 0 & \text{en los demás casos.} \end{cases}$$

15. Demostrar la formula del triángulo de Pascal

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

para  $n \in \mathbb{N}$  y todo entero  $k$ .

Demostrar por inducción:

16. Los coeficientes binomiales son números naturales.
17. Si  $a$  y  $b$  son números reales diferentes de cero, para todo entero positivo  $n$  se tiene:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \quad (\text{Teorema del binomio})$$

18. Si  $b$  es un entero positivo fijo, todo entero  $n \geq 0$  puede escribirse en la forma  $n = bq + r$  con  $q$  y  $r$  enteros no negativos y  $0 \leq r < b$ .
19.  $(\frac{4}{3})^n > n$  para todo entero  $n \geq 7$ .
20. *Ley asociativa generalizada.* Sean  $a_1, a_2, \dots, a_n$  números reales con  $n \geq 3$ . Demuestre que dos maneras cualesquiera de sumar estos números tomados en ese orden, producen el mismo resultado.

21. Encontrar el error —si lo hay— en la siguiente demostración. Si no lo encuentra, compare con la realidad.

**Teorema.** *Todos los caballos son del mismo color.*

*Demostración.* Sea  $P_n$  la proposición: “Todos los caballos en un conjunto de  $n$  caballos, son del mismo color.”

- (a)  $P_1$  es verdadera.
- (b) Supongamos que  $P_k$  es verdadera y supongamos que  $c_1, c_2, c_3, \dots, c_{k+1}$  son los  $k+1$  caballos en un conjunto de  $k+1$  caballos.

Consideramos  $\{c_1, c_2, c_3, \dots, c_k\}$ . Por la hipótesis de inducción todos estos caballos son del mismo color. En el conjunto anterior reemplacemos  $c_k$  por  $c_{k+1}$  entonces en el conjunto resultante  $\{c_1, c_2, c_3, \dots, c_{k-1}, c_{k+1}\}$  todos los  $k$  caballos son del mismo color. Ahora  $c_1$  y  $c_k$  son del mismo color y también  $c_1$  y  $c_{k+1}$ , entonces todos los  $k+1$  caballos son del mismo color. Luego  $P_{k+1}$  es verdadera y por el PIM se concluye la afirmación del teorema.  $\square$

22. Demostrar que no hay números naturales entre 0 y 1.

*Sugerencia:* Utilizar el PBO y propiedades de orden de  $\mathbb{N}$ .

23. Demostrar que el PIM es equivalente a la siguiente afirmación:

Sea  $a \in \mathbb{Z}$  y sea  $S$  un subconjunto de  $\{k \in \mathbb{Z} \mid k \geq a\}$  tal que,

- (a)  $a \in S$ .
- (b)  $n + 1 \in S$  cada vez que  $n \in S$ .

Entonces  $S = \{k \in \mathbb{Z} \mid k \geq a\}$ .

Se define inductivamente la *sucesión de Fibonacci* mediante:

$$u_1 = u_2 = 1 \text{ y } u_{n+2} = u_{n+1} + u_n \text{ si } n \geq 1.$$

24. Demostrar que para todo entero positivo  $n$ ,

$$u_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right]$$

*Sugerencia:* Comprobar primero que los dos números  $a = \frac{1 + \sqrt{5}}{2}$  y

$b = \frac{1 - \sqrt{5}}{2}$  son raíces de la ecuación  $x^2 = x + 1$ .

El número  $\frac{1 + \sqrt{5}}{2}$  es llamado la *proporción áurea*.

25. Si establecemos  $u_0 = 0$ , entonces para todo entero  $m \geq 0$  y todo entero  $n \geq 0$  se tiene,

$$u_{n+m+1} = u_n u_m + u_{n+1} u_{m+1}.$$

26. Para todo entero  $n \geq 1$  y todo entero  $m \geq 1$  se tiene que  $u_n \mid u_{mn}$ .

27. Construir tablas para la adición y multiplicación en base 9 y calcular  $(4685)_9(3483)_9$ .

28. Expresar  $(400803)_9$  en el sistema de base 5 sin pasar por la base 10.

29. En un sistema numérico con base  $b$ , un número se escribe  $(34)_b$  y su cuadrado se escribe como  $(1552)_b$ . Cuál es el valor de  $b$ ?

30. ¿En qué base los números 479, 698 y 907 están en progresión aritmética?

## 2.1 Propiedades básicas

Ya en el capítulo anterior dimos significado a la expresión “ $a$  divide a  $b$ ” que escribimos así, “ $a \mid b$ ”.

Aun cuando algunas propiedades ya las enunciamos y probamos, recopilamos éstas y otras propiedades en el siguiente teorema.

**2.1 Teorema.** *Supongamos que  $a, b$  y  $c$  son números enteros. Entonces:*

1. Si  $a \neq 0$  entonces  $a \mid 0$ ,  $a \mid a$ ,  $a \mid (-a)$ .
2.  $1 \mid a$ ,  $(-1) \mid a$ .
3. Si  $a \mid b$  entonces  $a \mid bc$ .
4. Si  $a \mid b$  y  $b \mid c$  entonces  $a \mid c$ .
5. Si  $a \mid b$  y  $a \mid c$  entonces para todo  $x, y \in \mathbb{Z}$ ,  $a \mid (bx + cy)$ .

6. Si  $a \mid b$  y  $b \neq 0$  entonces  $|a| \leq |b|$ .

7. Si  $a \mid b$  y  $b \mid a$  entonces  $a = b$  o  $a = (-b)$ .

*Demostración.* (5) Si  $a \mid b$  y  $a \mid c$  entonces existen enteros  $r$  y  $s$  tales que  $b = ar$  y  $c = as$ , luego cualesquiera sean  $x, y$  enteros tenemos

$$bx + cy = (ar)x + (as)y = a(rx + sy),$$

luego  $a \mid (bx + cy)$ .

(6) Como  $a \mid b$  existe  $c \in \mathbb{Z}$  tal que  $b = ac$ . Puesto que  $b \neq 0$  entonces  $c \neq 0$  y por lo tanto  $|c| \geq 1$ , y en consecuencia  $|b| = |c| |a| \geq |a|$ .

(7) Por (6) tenemos  $|a| \leq |b|$  y  $|b| \leq |a|$  luego  $|a| = |b|$  y por lo tanto  $a = b$  o  $a = (-b)$ .  $\square$

**2.2 Ejemplo.** Para todo entero positivo  $m$ , el producto de  $m$  enteros consecutivos es divisible por  $m!$ .

En efecto, consideremos

$$(k+1)(k+2)(k+3)\cdots(k+m).$$

Si  $k \geq 0$ , tenemos,

$$\begin{aligned} \frac{(k+1)(k+2)\cdots(k+m)}{m!} &= \frac{k!(k+1)(k+2)\cdots(k+m)}{k!m!} \\ &= \frac{(k+m)!}{k!m!} = \binom{k+m}{m} \end{aligned}$$

luego,

$$(k+1)(k+2)\cdots(k+m) = \binom{k+m}{m} m!.$$

Si  $k < 0$  se presentan dos alternativas:

1. El producto es 0, en cuyo caso la parte (1) del Teorema 2.1 garantiza que este producto es divisible por  $m!$ .
2. El producto es distinto de 0, en cuyo caso se puede expresar, salvo por un signo, como el producto de enteros positivos consecutivos y se sigue del caso  $k \geq 0$ .

**2.3 Ejemplo.** Para todo entero positivo  $n$ ,  $(n!)^2$  divide a  $(2n)!$ . En efecto,  $(2n)! = 1 \cdot 2 \cdot 3 \cdots n(n+1)(n+2) \cdots (n+n) = n! \cdot (n+1)(n+2) \cdots (n+n)$ .

Por el ejemplo anterior  $(n+1)(n+2) \cdots (n+n) = t(n!)$ , por lo tanto

$$(2n)! = (n!)t(n!) = t(n!)^2.$$

## 2.2 Máximo Común Divisor MCD

**2.4 Definición.** Sean  $a$  y  $b$  enteros no ambos iguales a cero. El conjunto de todos los divisores comunes de  $a$  y  $b$  (un divisor común de  $a$  y  $b$  es un entero que divide a ambos números  $a$  y  $b$ ) es un conjunto finito de números enteros cuyo máximo se denomina el *Máximo Común Divisor* de  $a$  y  $b$ . Lo notamos  $\text{MCD}(a, b)$  o simplemente  $(a, b)$ .

Puesto que, si  $x \mid a$  entonces  $x \mid (-a)$ , es fácil observar que

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

**2.5 Teorema.** Sean  $a$  y  $b$  enteros no ambos iguales a cero. El  $\text{MCD}(a, b)$  es el menor entero positivo que pueda escribirse en la forma  $ax + by$  con  $x, y$  enteros.

*Demostración.* Supongamos que  $d = (a, b)$  y sea

$$S = \{z \in \mathbb{Z}^+ \mid z = ax + by \text{ con } x, y \in \mathbb{Z}\}.$$

$S \neq \emptyset$  puesto que  $z = a^2 + b^2 \in S$ . Luego por el PBO,  $S$  posee un mínimo, llamémoslo  $g$  que podemos escribir en la forma  $g = ax_0 + by_0$ . Probaremos que  $g = d = (a, b)$ . En efecto  $g$  es divisor común de  $a$  y  $b$ , pues si dividimos  $a$  entre  $g$  tenemos:

$$a = qg + r \text{ con } 0 \leq r < g$$

luego,

$$\begin{aligned} r &= a - qg \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + b(-qy_0) \\ &= ax' + by'. \end{aligned}$$

Ahora, si  $r \neq 0$  entonces  $r \in S$  lo cual contradice la minimalidad de  $g$ , en consecuencia  $r = 0$  y así  $g \mid a$ . Análogamente se verifica que  $g \mid b$ .

Como  $d = (a, b)$  y  $g$  es un divisor común entonces  $g \leq d$ .

De otra parte  $g = ax_0 + by_0$  y  $d \mid a$  y  $d \mid b$  luego  $d \mid g$  y como ambos números son positivos  $d \leq g$  y en consecuencia  $d = g$ .  $\square$

Es importante observar que los enteros  $x, y$  del teorema anterior no son únicos, en efecto si  $t \in \mathbb{Z}$  y  $(a, b) = ax_0 + by_0$  entonces  $(a, b) = a(x_0 + bt) + b(y_0 - at)$ .

También se ve claramente que por ser el mínimo de un conjunto, el MCD es único.

Igualmente es importante observar que el solo hecho de escribir un entero positivo  $d$ , en la forma  $d = ax + by$  no garantiza que  $d = (a, b)$ . Solamente podemos afirmar que  $(a, b) \mid d$ .

Por ejemplo,

$$4 = (6)(3) + (2)(-7) \text{ y sin embargo } (6, 2) = 2 \neq 4$$

**2.6 Teorema.** Sean  $a$  y  $b$  enteros no ambos cero. Entonces  $d = (a, b)$  si y solamente si  $d$  satisface las siguientes propiedades:

1.  $d > 0$ .
2.  $d \mid a$  y  $d \mid b$ .
3. Si  $f \mid a$  y  $f \mid b$  entonces  $f \mid d$ .

*Demostración.* Supongamos que  $d = (a, b)$ . Tenemos inmediatamente que  $d > 0$  y que  $d \mid a$  y  $d \mid b$ . Además  $d = ax + by$  para algún par de enteros  $x, y$  y si  $f \mid a$  y  $f \mid b$  entonces por el Teorema 2.1  $f \mid d$ .

Recíprocamente supongamos ahora que  $d$  satisface (1), (2) y (3) y supongamos que  $f$  es un divisor común de  $a$  y  $b$ ; entonces por (3)  $f \mid d$  y en consecuencia  $|f| \leq |d| = d$ , luego  $d$  es el mayor de los divisores comunes de  $a$  y  $b$ .  $\square$

**2.7 Teorema.** Si  $a = bq + r$  entonces  $(a, b) = (b, r)$

*Demostración.* Supongamos que  $d = (a, b)$  y  $d' = (b, r)$ . Como  $d \mid a$  y  $d \mid b$  entonces  $d \mid r = a - bq$  en consecuencia  $d \mid d'$ . Análogamente  $d' \mid a = bq + r$  y en consecuencia  $d' \mid d$ . Como  $d$  y  $d'$  son positivos entonces  $d = d'$ .  $\square$

## 2.3 Algoritmo de Euclides

Aun cuando hemos presentado criterios para decidir si un entero positivo es o no el máximo común divisor de dos enteros, no hemos presentado aún un procedimiento eficiente que nos permita encontrar el MCD de dos enteros dados  $a$  y  $b$ . Solucionamos ahora esta dificultad al presentar el denominado *Algoritmo de Euclides*. Euclides (365–300 AC) en su libro *Elementos*, dio este método para el cálculo del MCD.

Si  $0 < b < a$ , aplicamos el algoritmo de división y escribimos

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

Si  $r_1 = 0$  entonces  $b \mid a$  y  $(a, b) = b$ . Si no, aplicamos nuevamente el algoritmo para obtener

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

Si  $r_2 = 0$  entonces  $r_1 = (r_1, b) = (a, b)$ . Si no, repetimos el proceso, hasta llegar a lo sumo en  $b$  pasos a un residuo cero; obteniendo las siguientes ecuaciones:

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2} \\ r_{k-2} &= r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} &= r_kq_{k+1} + 0. \end{aligned}$$

La aplicación repetida del Teorema 2.7 nos permite afirmar que

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = r_k.$$

Puesto que  $(a, b) = (a, -b) = (-a, b) = (-a, -b)$  el algoritmo anterior permite encontrar el MCD de cualquier par de enteros.

También las ecuaciones precedentes nos permiten encontrar enteros  $x$  y  $y$  tales que  $(a, b) = ax + by$ .

**2.8 Ejemplo.** Encontrar  $(687, -234)$  y expresarlo como combinación lineal de 687 y  $-234$ .

Aplicando el Algoritmo de Euclides, tenemos,

$$687 = (234)(2) + 219$$

$$234 = (219)(1) + 15$$

$$219 = (15)(14) + 9$$

$$15 = (9)(1) + 6$$

$$9 = (6)(1) + 3$$

$$6 = (3)(2) + 0.$$

Por lo tanto,  $(687, -234) = (687, 234) = 3$ .

Además, empezando con la penúltima ecuación obtenemos,

$$3 = 9 - 6$$

$$6 = 15 - 9$$

$$9 = 219 - (15)(14)$$

$$15 = 234 - 219$$

$$219 = 687 - (2)(234),$$

y reemplazando los residuos sucesivamente tenemos,

$$3 = 9 - 6$$

$$= 9 - [15 - 9] = (2)(9) - 15$$

$$= 2[219 - (14)(15)] - 15 = (2)(219) - (29)(15)$$

$$= (2)(219) - 29[234 - 219] = (31)(219) - (29)(234)$$

$$= 31[687 - (2)(234)] - (29)(234)$$

$$= (31)(687) - (91)(234),$$

luego

$$(687, -234) = 3 = (31)(687) + (91)(-234).$$

El procedimiento que presentamos a continuación, conocido como *algoritmo extendido de Euclides*, se puede programar fácilmente en un computador y permite hallar el MCD de dos enteros y escribirlo como combinación lineal de ellos.

Sean  $0 < b < a$  enteros, y supongamos que tenemos las ecuaciones:

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ &\vdots \\ &\vdots \\ r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, & 0 < r_{k-1} < r_{k-2} \\ r_{k-2} &= r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1} \\ r_{k-1} &= r_kq_{k+1} + 0. \end{aligned}$$

Definimos  $x_0 = 0$ ,  $x_1 = 1$ ,  $y_0 = 1$ ,  $y_1 = -q_1$  y las fórmulas de recurrencia

$$\begin{aligned} x_i &= x_{i-2} - x_{i-1}q_i, \\ y_i &= y_{i-2} - y_{i-1}q_i, \end{aligned}$$

para  $i = 2, \dots, k$ .

Por el algoritmo euclideano sabemos que  $(a, b) = r_k$  y afirmamos que

$$r_k = ax_k + by_k.$$

Más generalmente, tenemos el siguiente teorema.

**2.9 Teorema.** *En las condiciones anteriormente descritas, tenemos:*

$$ax_i + by_i = r_i \tag{2.1}$$

para  $i = 1, 2, \dots, k$ .

*Demostración.* Sea  $S$  el conjunto de los  $i \in \mathbb{Z}$  tales que  $1 \leq i \leq k$  y para los cuales la afirmación (2.1) es cierta.

Cuando  $i = 1$  tenemos,

$$ax_1 + by_1 = (a)(1) + b(-q_1) = r_1$$

que es la ecuación con la cual comenzamos el algoritmos de Euclides.

Supongamos que (2.1) es cierta para  $i \leq j$  donde  $2 \leq j \leq k$ . Por las fórmulas de recurrencia tenemos:

$$\begin{aligned} ax_{j+1} + by_{j+1} &= a(x_{j-1} - x_j q_{j+1}) + b(y_{j-1} - y_j q_{j+1}) \\ &= (ax_{j-1} + by_{j-1}) - (ax_j + by_j)q_{j+1} \\ &= r_{j-1} - r_j q_{j+1}. \end{aligned}$$

Además, puesto que  $r_{j-1} = r_j q_{j+1} + r_{j+1}$  obtenemos  $ax_{j+1} + by_{j+1} = r_{j+1}$  y, por el PIM, la relación (2.1) es cierta para  $i = 1, 2, \dots, k$ .  $\square$

**2.10 Ejemplo.** Encontramos (1001, 275) y escribámoslo como combinación lineal de ellos.

$$\begin{aligned} 1001 &= (275)(3) + 176 \\ 275 &= (176)(1) + 99 \\ 176 &= (99)(1) + 77 \\ 99 &= (77)(1) + 22 \\ 77 &= (22)(3) + 11 \\ 22 &= (11)(2) + 0. \end{aligned}$$

Usando las fórmulas de recurrencia tenemos la siguiente tabla,

$i$	$q_i$	$x_i$	$y_i$
0	—	0	1
1	3	1	-3
2	1	-1	4
3	1	2	-7
4	1	-3	11
5	3	11	-40

por lo tanto,

$$(1001, 275) = 11 = (1001)(11) + (275)(-40).$$

## 2.4 Propiedades del Máximo Común Divisor

Hemos mostrado que si  $d = (a, b)$  entonces existen  $x, y$  enteros tales que  $d = ax + by$ . El siguiente teorema muestra el único caso en el que se da la equivalencia de las dos afirmaciones.

**2.11 Teorema.** Sean  $a$  y  $b$  enteros no ambos nulos. Entonces,

$$(a, b) = 1 \text{ si y solo si existen enteros } x, y \text{ tales que } 1 = ax + by$$

*Demostración.* Si  $(a, b) = 1$  el Teorema 2.5 garantiza la existencia de tales  $x, y$ . Recíprocamente, si existen  $x, y$  tales que  $1 = ax + by$  entonces  $(a, b) \mid 1$  y por lo tanto,  $(a, b) = 1$ .  $\square$

**2.12 Corolario.** Si  $d = (a, b)$ , entonces  $(\frac{a}{d}, \frac{b}{d}) = 1$ .

*Demostración.* Puesto que  $d = (a, b)$  existen enteros  $x, y$  tales que  $d = ax + by$ , por lo tanto, al dividir por  $d$  tenemos:

$$1 = \frac{d}{d} = \frac{a}{d}x + \frac{b}{d}y. \quad \square$$

**2.13 Definición.** Si  $a$  y  $b$  son enteros no ambos iguales a cero tales que  $(a, b) = 1$ , decimos que  $a$  y  $b$  son *primos relativos*. Más generalmente si  $a_1, a_2, \dots, a_n$  son enteros tales que para todo  $i$  y para todo  $j$  con  $i \neq j$ ,  $1 \leq i, j \leq n$  se tiene  $(a_i, a_j) = 1$ , decimos que  $a_1, a_2, \dots, a_n$  son *primos relativos dos a dos*.

**2.14 Teorema.** Si  $a \mid bc$  y  $(a, b) = 1$  entonces  $a \mid c$ .

*Demostración.* Como  $a \mid bc$  existe  $k$  tal que  $bc = ak$ . Como  $(a, b) = 1$  existen enteros  $x, y$  tales que  $ax + by = 1$ .

Por lo tanto,

$$c = c(ax + by) = acx + bcy = acx + aky = a(cx + ky)$$

es decir  $a \mid c$ .  $\square$

**2.15 Corolario.** Si  $p$  es primo y  $p \mid ab$  entonces  $p \mid a$ , o  $p \mid b$ .

*Demostración.* Si  $p \nmid a$  entonces  $(a, p) = 1$ , y por el teorema  $p \mid b$ .  $\square$

**2.16 Corolario.** Si  $p$  es primo y  $p \mid a_1 a_2 \dots a_n$ , entonces  $p \mid a_i$  para algún  $i$ ,  $1 \leq i \leq n$ .

*Demostración.* La demostración es por inducción.  $\square$

**2.17 Corolario.** Si  $p, p_1, p_2, \dots, p_n$  son números primos y

$$p \mid p_1 p_2 \dots p_n,$$

entonces  $p = p_i$  para algún  $i$ ,  $1 \leq i \leq n$ .

*Demostración.* La demostración es por inducción.  $\square$

**2.18 Teorema.** Si  $(a, b) = 1$  y  $(a, c) = 1$  entonces  $(a, bc) = 1$ .

*Demostración.* Puesto que  $(a, b) = 1$  y  $(a, c) = 1$  tenemos que,

$$1 = ax + by \text{ y también } 1 = ar + cs$$

con  $x, y, r, s$  enteros y por lo tanto

$$\begin{aligned} 1 &= (ax + by)(ar + cs) \\ &= a(xar + xsc + byr) + bc(ys) \end{aligned}$$

y en consecuencia  $(a, bc) = 1$ .  $\square$

**2.19 Corolario.** Si  $(a, b_i) = 1$  para  $i = 1, 2, \dots, n$  entonces

$$(a, b_1 b_2 \dots b_n) = 1.$$

*Demostración.* La demostración es por inducción.

Si  $n = 1$  es claro que  $(a, b_1) = 1$ .

Supongamos como hipótesis que, si  $(a, b_i) = 1$  para  $i = 1, 2, \dots, k$  entonces  $(a, b_1 b_2 \dots b_k) = 1$  y asumamos además, que  $(a, b_i) = 1$  para  $i = 1, 2, \dots, k, k + 1$ .

Aplicando el teorema con  $(a, b_1 b_2 \dots b_k) = 1$  y  $(a, b_{k+1}) = 1$  se sigue el resultado.  $\square$

Una aplicación de este corolario la observamos en el siguiente ejemplo.

**2.20 Ejemplo.** Si  $p$  es un número primo entonces  $p \mid \binom{p}{k}$  para todo  $k = 1, 2, \dots, (p-1)$ .

En efecto,

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-(k-1))}{k!}.$$

Como  $k < p$  tenemos  $(p, 1) = 1, (p, 2) = 1, \dots, (p, k) = 1$  y por el corolario,  $(p, 1 \cdot 2 \cdot 3 \cdots k) = 1$  es decir  $(p, k!) = 1$ . Puesto que  $\binom{p}{k}$  es un entero, tenemos,

$$k! \mid p(p-1)(p-2)\cdots(p-(k-1))$$

y como,

$$(k!, p) = 1$$

entonces,

$$k! \mid (p-1)\cdots(p-(k-1))$$

es decir,

$$(p-1)(p-2)\cdots(p-(k-1)) = k!t$$

para algún entero  $t$  y en consecuencia,

$$\binom{p}{k} = \frac{pk!t}{k!} = pt.$$

**2.21 Teorema.** Si  $a \mid c, b \mid c$  y  $(a, b) = 1$  entonces  $ab \mid c$ .

*Demostración.* Puesto que  $a \mid c$  y  $b \mid c$  existen enteros  $u$  y  $v$  tales que  $c = au = bv$ , de donde  $b \mid au$ . Como  $(a, b) = 1$  entonces  $b \mid u$ , es decir,  $u = br$  para algún  $r$ . En consecuencia,  $c = au = a(br) = (ab)r$  es decir  $ab \mid c$ .  $\square$

**2.22 Corolario.** Si  $a_1, a_2, \dots, a_n$  son enteros primos relativos dos a dos y para cada  $i, i = 1, 2, \dots, n, a_i \mid c$  entonces  $a_1 a_2 \dots a_n \mid c$ .

*Demostración.* La demostración es por inducción.  $\square$

**2.23 Teorema.** Si  $k \neq 0$  entonces  $(ka, kb) = |k|(a, b)$ .

*Demostración.* Basta probar el resultado para  $k > 0$ . Supongamos que  $d = (a, b)$  entonces  $kd \mid ka$  y  $kd \mid kb$  y por lo tanto  $kd \mid (ka, kb)$ .

Por otra parte,  $d = ax + by$  para algún par de enteros  $x, y$  luego  $kd = kax + kby$  y por lo tanto  $(ka, kb) \mid kd$ , luego  $kd = k(a, b) = (ka, kb)$ .  $\square$

**2.24 Ejemplo.** Si  $(a, b) = 1$  entonces  $(3a - b, 4a + b) = 1$  o  $7$ .

Supongamos que  $d = (3a - b, 4a + b)$ , entonces  $d \mid 3a - b$  y  $d \mid 4a + b$ ; por lo tanto,

$$d \mid [(3a - b) + (4a + b)] = 7a$$

y

$$d \mid [(-4)(3a - b) + 3(4a + b)] = 7b;$$

luego

$$d \mid (7a, 7b) = 7(a, b) = (7)(1) = 7,$$

y finalmente  $d = 1$  o  $d = 7$ .

**2.25 Ejemplo (Los números de Fibonacci).** Los *números de Fibonacci*, descubiertos por Leonardo Fibonacci<sup>1</sup> (1170–1240) se definen por las condiciones siguientes:

$$u_1 = 1, u_2 = 1 \text{ y para } n \geq 2, u_{n+1} = u_n + u_{n-1}.$$

Veamos, por inducción, que para  $n \geq 1$ ,  $(u_n, u_{n+1}) = 1$ . Si  $n = 1$ ,  $(u_1, u_2) = (1, 1) = 1$ .

Supongamos que  $(u_n, u_{n+1}) = 1$  y sea  $d = (u_{n+1}, u_{n+2})$ , entonces  $d \mid u_{n+1}$  y  $d \mid u_{n+2} = u_{n+1} + u_n$  y por lo tanto  $d \mid [(u_{n+1} + u_n) - u_{n+1}] = u_n$ .

Así,  $d \mid u_n$  y  $d \mid u_{n+1}$ . Luego  $d \mid (u_n, u_{n+1}) = 1$ , y claramente  $d = 1$ . Entonces por PIM, para todo  $n \geq 1$ ,  $(u_n, u_{n+1}) = 1$ .

**2.26 Ejemplo.** Sean  $m, n$  enteros positivos primos relativos. Veamos que

$$q = \frac{(m+n-1)!}{m!n!}$$

es un entero.

---

<sup>1</sup>Fibonacci fue quien introdujo al mundo occidental los números indú-arábigos, que hoy usamos, después de viajar con su padre a Bougie, una ciudad entre Argel y Tunez.

Si utilizamos el ejemplo 2.2 de este capítulo tenemos,

$$q = \frac{m!(m+1)(m+2)\cdots(m+n-1)}{m!n!} = \frac{t(n-1)!}{n!} = \frac{t}{n}$$

para algún entero  $t$ . Similarmente,

$$q = \frac{n!(n+1)(n+2)\cdots(n+m-1)}{m!n!} = \frac{s(m-1)!}{m!} = \frac{s}{m}$$

para algún entero  $s$ .

Por lo tanto  $\frac{t}{n} = \frac{s}{m}$  es decir  $tm = sn$ . Así,  $m \mid sn$  y como  $(m, n) = 1$  entonces  $m \mid s$  es decir  $s = mr$  con  $r$  entero y  $q = \frac{s}{m} = \frac{mr}{m} = r$ .

---

## Ejercicios 2.1

---

1. Probar que si  $a \mid b$  y  $c \mid d$  entonces  $ac \mid bd$ .
2. Probar que el producto de tres enteros consecutivos es divisible por 6. Si además el primero es par el producto es múltiplo de 24.
3. Probar que  $100 \mid (11^{10} - 1)$ .
4. Probar que para todo  $n \geq 1$ ,  $30 \mid n^5 - n$ .
5. Probar que si  $n = rs$  con  $r > 0$  y  $s > 0$  entonces  $(r!)^s \mid n!$ .
6. Sean  $n$  y  $m$  enteros positivos y  $a > 1$ . Probar que,

$$(a^n - 1) \mid (a^m - 1) \text{ si solo si } n \mid m.$$

7. Probar que todo cuadrado perfecto es de la forma  $4k$  o  $4k + 1$  para algún entero  $k$ .
8. Probar que si  $a$  y  $b$  son impares entonces  $a^2 + b^2$  no es un cuadrado perfecto.

9. Use el PBO para probar que todo entero mayor que uno tiene un factor primo.
10. Hallar el MCD de cada par de números y expresarlo como combinación lineal de ellos.

$$382 \text{ y } 26, \quad -275 \text{ y } 726, \quad 1137 \text{ y } 419, \quad -2947 \text{ y } -3997.$$

11. Usar el algoritmo extendido de Euclides para encontrar enteros tales que:

$$1426x + 343y = 3$$

$$630x + 132y = 12$$

$$936x + 666y = 18$$

$$4001x + 2689y = 4.$$

12. Probar que si  $(a, b) = c$  entonces  $(a^2, b^2) = c^2$ .
13. Probar que si  $(a, b) = 1$  entonces  $(a + b, ab) = 1$ .
14. Probar que si  $(a, b) = 1$  y  $c \mid b$  entonces  $(a, c) = 1$ .
15. Probar que si  $(a, b) = 1$  entonces  $(2a + b, a + 2b) = 1$  o  $3$ .
16. Probar que si  $(b, c) = 1$  entonces  $(a, bc) = (a, b)(a, c)$
17. Probar que si  $(a, b) = 1$  entonces para todo  $n$  y  $m$  enteros positivos,  $(a^m, b^n) = 1$ .
18. Probar que si  $d \mid nm$  y  $(n, m) = 1$  entonces  $d = d_1 d_2$  donde  $d_1 \mid m$ ,  $d_2 \mid n$  y  $(d_1, d_2) = 1$ .
19. Probar que no existen enteros  $x, y$  tales que

$$x + y = 200 \text{ y } (x, y) = 7.$$

20. Probar que existe un número infinito de pares de enteros  $x, y$  que satisfacen  $x + y = 203$  y  $(x, y) = 7$ .
21. Probar que si  $ad - bc = \pm 1$  entonces la fracción  $(a + b)/(c + d)$  es irreducible.
22. Evaluar  $(ab, p^4)$  y  $(a + b, p^4)$  si  $p$  es primo,  $(a, p^2) = p$  y  $(b, p^3) = p^2$ .
23.  Si  $p$  es un primo impar y  $(a, b) = 1$  probar que

$$(a + b, \frac{a^p + b^p}{a + b}) = 1 \text{ o } p.$$

24. Probar que para todo entero positivo  $n$ ,  $(u_{n+3}, u_n) = 1$  o igual 2.
25. Probar que si  $m = qn + r$  entonces  $(u_m, u_n) = (u_r, u_n)$ .
26. Probar que  $(u_n, u_m) = u_{(n,m)}$  para todo par de enteros positivos  $n, m$ .
27. Para todo par de entero positivos  $m$  y  $n$  probar que

$$u_n \mid u_m \text{ si y solo si } n \mid m.$$

28. 📖 Sean  $a, m, n$  enteros positivos con  $n \neq m$ . Probar que,

$$(a^{2^n} + 1, a^{2^m} + 1) = \begin{cases} 1 & \text{si } a \text{ es par} \\ 2 & \text{si } a \text{ es impar.} \end{cases}$$

29. 📖 Sea  $S := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$  donde  $n > 1$ . Probar que  $S$  no es un entero.

*Sugerencia:* Sea  $k$  el mayor entero tal que  $2^k \leq n$  y sea  $P$  el producto de todos los números impares menores o iguales a  $n$ . Probar que  $2^{k-1} \cdot P \cdot S$  es una suma cuyos términos a excepción de  $2^{k-1} \cdot P \cdot \frac{1}{2^k}$  son enteros.

## 2.5 Mínimo Común Múltiplo y generalizaciones

**2.27 Definición.** El menor múltiplo común positivo de dos enteros  $a$  y  $b$  no nulos se denomina el *Mínimo Común Múltiplo* de  $a$  y  $b$  y se denota  $\text{MCM}(a, b)$  o simplemente  $[a, b]$ .

Puesto que dados  $a$  y  $b$  enteros cualesquiera no nulos, los números  $ab$  y  $-ab$  son ambos múltiplos comunes de  $a$  y de  $b$  y uno de ellos es positivo, entonces el PBO garantiza la existencia y unicidad de  $[a, b]$ . En lo que sigue cuando mencionemos el  $[a, b]$  supondremos  $a$  y  $b$  diferentes de cero.

Es inmediato deducir de la definición que,

$$[a, b] = [-a, b] = [a, -b] = [-a, -b].$$

**2.28 Teorema.** Sean  $a, b$  son enteros no nulos. Entonces  $m = [a, b]$  si y solo si,

- (i)  $m > 0$ .
- (ii)  $a \mid m$  y  $b \mid m$ .
- (iii) Si  $n$  es un entero tal que  $a \mid n$  y  $b \mid n$  entonces  $m \mid n$ .

*Demostración.* Supongamos que  $m = [a, b]$ . Entonces  $m$  satisface (i) y (ii).

Para probar (iii) supongamos  $n \in \mathbb{Z}$  tal que  $a \mid n$  y  $b \mid n$  y dividamos  $n$  entre  $m$ , entonces

$$n = qm + r \quad \text{donde } 0 \leq r < m.$$

Si  $r > 0$  entonces  $r$  sería un múltiplo común de  $a$  y  $b$ , positivo y menor que  $m$ , lo que niega la minimalidad de  $m$ . Luego  $r = 0$  y por tanto  $m \mid n$ .

Supongamos ahora que  $m$  satisface (i), (ii), (iii) y supongamos que  $n$  es un múltiplo común de  $a$  y  $b$ . Entonces por (iii)  $m \mid n$  y en consecuencia  $m = |m| \leq |n|$  es decir que  $m$  es el menor de los múltiplos comunes positivos de  $a$  y  $b$ .  $\square$

El siguiente resultado proporciona un método para calcular el MCM.

**2.29 Teorema.** Sean  $a$  y  $b$  enteros no nulos. Entonces,

$$[a, b] = \frac{|ab|}{(a, b)}.$$

*Demostración.* Sea  $m = \frac{|ab|}{(a, b)}$ . Veamos que  $m$  satisface las condiciones (i), (ii), (iii) del teorema anterior. Evidentemente  $m > 0$ . Sea  $d = (a, b)$  entonces  $a = Ad$  y  $b = Bd$  donde  $(A, B) = 1$  y por lo tanto

$$m = \frac{|ab|}{d} = \frac{|a| |Bd|}{d} = |a| |B| = a(\pm B),$$

luego  $a \mid m$  y en forma similar se muestra que  $b \mid m$ .

Sea ahora  $n$  un entero tal que  $a \mid n$  y  $b \mid n$ , entonces existen enteros  $r$  y  $s$  tales que  $n = ar = bs$ . En consecuencia  $Adr = Bds$  y por lo tanto  $Ar = Bs$ . Así,  $B \mid Ar$  y como  $(A, B) = 1$  entonces  $B \mid r$  es decir  $r = Bt$ , para algún entero  $t$ .

Reemplazando tenemos  $n = ar = a(Bt) = (aB)t = \pm mt$ , es decir  $m \mid n$  y se completa la demostración.  $\square$

**2.30 Ejemplo.** Ya obtuvimos que  $(687, -234) = 3$ , por lo tanto,

$$[687, -234] = \frac{|(687)(-234)|}{3} = \frac{(687)(234)}{3} = 53586.$$

**2.31 Corolario.** Sean  $a$  y  $b$  enteros no nulos. Entonces  $a$  y  $b$  son primos relativos si y solamente si  $[a, b] = |ab|$ .

**2.32 Ejemplo.** Si se sabe que  $(a, b) = 18$  y  $[a, b] = 1512$  encontremos  $a$  y  $b$ .

Si  $(a, b) = 18$  entonces  $a = 18A$  y  $b = 18B$  donde  $(A, B) = 1$ . Por el Teorema 2.29,  $(18)(1512) = (18)^2 AB$  luego  $AB = 84$ , y salvo por el orden las posibilidades son,

$$A = 4 \quad B = 21, \quad A = 12 \quad B = 7, \quad A = 28 \quad B = 3, \quad A = 84 \quad B = 1.$$

Así los números buscados son, salvo por el orden,

$$\begin{array}{ll} a = 72 & b = 378 \\ a = 504 & b = 54 \end{array} \qquad \begin{array}{ll} a = 216 & b = 126 \\ a = 1512 & b = 18. \end{array}$$

**2.33 Ejemplo.** Sean  $a$  y  $b$  enteros positivos. El número de múltiplos de  $b$  en la sucesión  $a, 2a, 3a, \dots, ba$  es precisamente  $(a, b)$ .

Representemos por  $N$  dicho número. Si  $ka$  es uno de los múltiplos de  $b$  en la sucesión, entonces  $[a, b] \mid ka$  y por lo tanto existe  $t$  entero tal que,

$$ka = [a, b]t = \left( \frac{ab}{(a, b)} \right) t$$

de donde  $k = \left( \frac{b}{(a, b)} \right) t$  y como  $k \leq b$  tenemos  $t \leq (a, b)$  y por lo tanto,

$$N \leq (a, b). \tag{2.2}$$

De otra parte, si  $1 \leq t \leq (a, b)$  entonces  $\left( \frac{b}{(a, b)} \right) t \leq b$  y así

$$\left( \frac{bt}{(a, b)} \right) a = \left( \frac{at}{(a, b)} \right) b$$

es un elemento de la sucesión que es múltiplo de  $b$ , en consecuencia

$$N \geq (a, b). \quad (2.3)$$

De (2.2) y (2.3),  $N = (a, b)$  como queríamos demostrar.

Las nociones de máximo común divisor y mínimo común múltiplo pueden extenderse de manera natural a más de dos números. Así por ejemplo, si  $a_1, a_2, \dots, a_n$  son enteros no todos nulos, ellos tienen un máximo común divisor que representamos por  $\text{MCD}(a_1, a_2, \dots, a_n)$  o simplemente  $(a_1, a_2, \dots, a_n)$ . En forma análoga a los casos correspondientes para dos enteros se pueden demostrar los siguientes teoremas.

**2.34 Teorema.** Sean  $a_1, a_2, \dots, a_n$  números enteros no todos nulos. Si  $d = (a_1, a_2, \dots, a_n)$  entonces  $d$  es el menor entero positivo que puede escribirse en la forma

$$a_1x_1 + a_2x_2 + \dots + a_nx_n \quad \text{con } x_1, x_2, \dots, x_n \text{ enteros.}$$

*Demostración.* Ejercicio □

**2.35 Teorema.** Sean  $a_1, a_2, \dots, a_n$  enteros no todos nulos. Entonces  $d = (a_1, a_2, \dots, a_n)$  si y solo si  $d$  satisface:

(i)  $d > 0$ ,

(ii)  $d \mid a_1, d \mid a_2, \dots, d \mid a_n$ ,

(iii) Si  $f$  es tal que  $f \mid a_1, \dots, f \mid a_n$ , entonces  $f \mid d$ .

*Demostración.* Ejercicio □

Los enteros  $a_1, a_2, \dots, a_n$  se denominan *primos relativos* si su MCD es 1, o sea si  $(a_1, \dots, a_n) = 1$ ; en este caso también los denominamos *primos entre sí*. Es claro que si los enteros  $a_1, a_2, \dots, a_n$  son primos relativos dos a dos, también son primos entre sí, pero el recíproco no siempre es cierto. Por ejemplo  $(2, 4, 5) = 1$  y sin embargo  $(2, 4) = 2$ .

El mismo argumento del Teorema 2.11 nos permite afirmar que  $(a_1, a_2, \dots, a_n) = 1$  si y solo si existen enteros  $x_1, x_2, \dots, x_n$ , tales que  $a_1x_1 + \dots + a_nx_n = 1$ .

De otra parte, si  $a_1, a_2, \dots, a_n$  son enteros todos diferentes de cero ellos poseen un mínimo común múltiplo que notamos  $\text{MCM}(a_1, a_2, \dots, a_n)$  o simplemente  $[a_1, a_2, \dots, a_n]$ . También tenemos el siguiente teorema cuya demostración es enteramente análoga a la del Teorema 2.28.

**2.36 Teorema.** Sean  $a_1, a_2, \dots, a_n$  enteros diferentes de cero. Entonces:  $m = [a_1, a_2, \dots, a_n]$  si y solo si  $m$  satisface:

- (i)  $m > 0$ ,
- (ii)  $a_1 \mid m, a_2 \mid m, \dots, a_n \mid m$ ,
- (iii) Si  $n$  es tal que  $a_1 \mid n, a_2 \mid n, \dots, a_n \mid n$  entonces  $m \mid n$ .

*Demostración.* Ejercicio □

Para efectos del cálculo del MCD y el MCM de más de dos enteros podemos hacer uso de la formulas de recurrencia que nos proporcionan los siguientes teoremas.

**2.37 Teorema.** Si  $a_1, a_2, \dots, a_n$  son enteros no nulos donde  $n \geq 3$  entonces,

$$(a_1, a_2, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n)$$

*Demostración.* Supongamos que

$$d = (a_1, a_2, \dots, a_n) \text{ y } d' = ((a_1, \dots, a_{n-1}), a_n).$$

Como  $d \mid a_i$  para cada  $i = 1, \dots, n$  entonces  $d \mid (a_1, \dots, a_{n-1})$  y también  $d \mid a_n$ . Por lo tanto  $d \mid d'$ . Por otra parte,  $d' \mid (a_1, \dots, a_{n-1})$  y  $d' \mid a_n$  luego  $d' \mid a_i$  para cada  $i = 1, \dots, n$  y en consecuencia  $d' \mid d$ . Por lo tanto  $d = d'$ . □

Análogamente se demuestra el resultado siguiente.

**2.38 Teorema.** Si  $a_1, a_2, \dots, a_n$  son enteros no nulos, con  $n \geq 3$ . Entonces

$$[a_1, a_2, \dots, a_n] = [[a_1, \dots, a_{n-1}], a_n]$$

*Demostración.* Ejercicio. □

**2.39 Ejemplo.** Encontramos  $(308, 882, 2961)$  y expresémoslo como combinación lineal de los enteros dados.

$$882 = (308)(2) + 266$$

$$308 = (266)(1) + 42$$

$$266 = (42)(6) + 14$$

$$42 = (14)(3)$$

luego  $(308, 882) = 14$ .

Ahora,

$$2961 = (14)(211) + 7$$

$$14 = (7)(2)$$

luego  $(14, 2961) = 7$  y en consecuencia

$$(308, 882, 2961) = (14, 2961) = 7.$$

Además,

$$7 = 2961 - (14)(211),$$

$$14 = 266 - (42)(6)$$

$$= 266 - (308 - 266)(6)$$

$$= (7)(266) - (6)(308)$$

$$= (7)[882 - (308)(2)] - (6)(308)$$

$$= (7)(882) - (20)(308)$$

luego,

$$7 = 2961 - [7(882) - (20)(308)](211)$$

$$7 = 2961 + (882)(-1477) + (308)(4220).$$

Podemos calcular también  $[308, 882, 2961]$  :

$$[308, 882] = \frac{(308)(882)}{(308, 882)} = \frac{(308)(882)}{14} = 19404.$$

Puesto que  $(19404, 2961) = 63$  tenemos:

$$[19404, 2961] = (19404)(2961)/(63) = 911988$$

es decir,

$$\begin{aligned} [308, 882, 2961] &= [[308, 882], 2961] \\ &= [19404, 2961] \\ &= 911988. \end{aligned}$$

---

## Ejercicios 2.2

---

1. Probar que  $a \mid b$  si y solo si  $[a, b] = |b|$ .
2. Probar que si  $[a, b] = (a, b)$  y  $a > 0$ ,  $b > 0$  entonces  $a = b$ .
3. Probar que  $(a, b) = (a + b, [a, b])$ .
4. Probar que  $[ka, kb] = |k| [a, b]$ ,  $k \neq 0$ .
5. Si  $k$  es un múltiplo común de  $a$  y  $b$ , probar que

$$\frac{|k|}{\left(\frac{k}{a}, \frac{k}{b}\right)} = [a, b]$$

6. Sea  $d$  un entero positivo tal que  $d \mid a$  y  $d \mid b$ . Probar que,

$$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{[a, b]}{d}.$$

7. Sean  $d$  y  $g$  enteros positivos. Probar que existen enteros  $a$  y  $b$  tales que  $(a, b) = d$  y  $[a, b] = g$  si y solo si  $d \mid g$ .
8. Probar que la ecuación  $ax + by = c$  tiene soluciones enteras  $x, y$  si y solo si  $(a, b) \mid c$ .
9. Probar que  $(a, b) = (a, b, ax + by)$  para todo  $x, y$  enteros.
10. Hallar enteros  $a$  y  $b$  tales que  $a + b = 216$  y  $[a, b] = 480$ .
11. Hallar todos los números  $a$  y  $b$  que satisfacen  $(a, b) = 24$  y  $[a, b] = 1440$ .

12. Hallar  $(20n^2 + 19n + 4, 4n + 3)$  y  $[20n^2 + 19n + 4, 4n + 3]$  donde  $n$  es un entero positivo.
13. Calcular  $(4410, 1404, 8712)$  y expresarlo como combinación lineal de los números dados.
14. Hallar  $(112, 240, 192, 760)$  y expresarlo como combinación lineal de los números dados.
15. Hallar enteros  $x, y, z, w$  tales que  $75x + 111y + 87z + 120w = 6$ .
16. Si  $p$  y  $q$  son primos impares diferentes y  $n = pq$ , cuántos enteros en el conjunto  $2, 3, \dots, n$  son primos relativos con  $n$ ?
17. Probar que  $|abc| = (ab, ac, bc)[a, b, c]$ .
18. Probar que  $|abc| \geq (a, b, c)[a, b, c]$ .
19. Dar un ejemplo para ilustrar que  $(a, b, c)[a, b, c]$  no siempre es  $abc$ .
20. Demostrar los teoremas 2.34, 2.35, 2.36 y 2.38.

## 2.6 Teorema fundamental de la aritmética

La propiedad más importante de los números primos es la posibilidad de factorizar todo entero  $n > 1$  como producto de ellos y esta factorización resulta esencialmente única. Esta propiedad fue descubierta por los griegos hace más de dos milenios

**2.40 Teorema (Fundamental de la Aritmética, TFA).** *Todo entero  $n > 1$  o es primo, o se puede factorizar como producto de primos. Este producto es único salvo por el orden de los factores.*

*Demostración.* En el Teorema 1.20 ya probamos la primera parte. Basta ahora probar la unicidad de la factorización salvo el orden. Usaremos inducción sobre  $n$ . Para  $n = 2$  claramente la representación es única. Supongamos ahora que para todo entero  $k$  con  $2 \leq k < n$  la representación única y supongamos que,

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

donde  $p_i$  y  $q_i$  son primos con  $p_1 \leq p_2 \leq \dots \leq p_s$  y  $q_1 \leq q_2 \leq \dots \leq q_t$ .

Así,  $p_1 \mid q_1 q_2 \dots q_t$  y entonces  $p_1 = q_j$  para algún  $j$  por lo tanto  $q_1 \leq p_1$ . Análogamente  $q_1 \mid p_1 p_2 \dots p_s$  y entonces  $q_1 = p_i$  para algún  $i$  y por lo tanto  $p_1 \leq q_1$ . Lo anterior demuestra que  $p_1 = q_1$  y cancelando tenemos,

$$\frac{n}{p_1} = p_2 p_3 \dots p_s = q_2 q_3 \dots q_t.$$

Como  $\frac{n}{p_1} < n$  la hipótesis de inducción garantiza que estas dos representaciones de  $\frac{n}{p_1}$  son idénticas (hemos escogido un orden) y en consecuencia  $s = t$  y para cada  $i$ ,  $p_i = q_i$ . Por el PIM la prueba queda completa.  $\square$

**2.41 Ejemplo.** No existen dos enteros positivos tales que  $m^2 = 2n^2$ .

1.  $m \neq 1$  pues de otra forma tendríamos  $1 = 2n^2$ , lo que es imposible.
2.  $n \neq 1$ , puesto que si  $n = 1$  entonces  $m^2 = 2$  y si la representación de  $m$  como producto de primos es  $m = p_1 p_2 \dots p_k$  entonces

$$2 = (p_1 p_1)(p_2 p_2) \dots (p_k p_k)$$

que contradice el TFA pues en un miembro hay un número par de factores primos y en el otro un número impar de tales factores.

Sean  $m = p_1 p_2 \dots p_k$  y  $n = q_1 q_2 \dots q_t$  las factorizaciones de  $m$  y  $n$  en factores primos. Si  $m^2 = 2n^2$  entonces,

$$(p_1 p_1)(p_2 p_2) \dots (p_k p_k) = 2(q_1 q_1)(q_2 q_2) \dots (q_t q_t)$$

que contradice el TFA porque el factor dos aparece un número impar de veces en la factorización de la derecha y un número par en la izquierda. Es decir, NO existen enteros positivos  $m, n$  tales que  $m^2 = 2n^2$ .

Agrupando los primos iguales en la factorización de  $n$  debida al TFA obtenemos la siguiente forma,

$$n = \prod_{i=1}^k p_i^{n_i} \quad (2.4)$$

donde  $n_i > 0$  y  $p_i \neq p_j$  si  $i \neq j$ . Esta escritura la denominamos *la forma canónica, natural o normal* del entero  $n$ .

En las pruebas de algunos resultados intervienen varios enteros diferentes, sin embargo es conveniente adoptar representaciones similares a la forma canónica donde en algunos casos aceptamos exponentes cero a fin de utilizar el mismo conjunto de primos en las factorizaciones.

Así por ejemplo escribimos,

$$60 = 2^2 \cdot 3 \cdot 5, \quad 45 = 2^0 \cdot 3^2 \cdot 5, \quad 25 = 2^0 \cdot 3^0 \cdot 5^2$$

donde en todos los casos hemos utilizado los primos 2, 3, 5 en la factorización.

**2.42 Teorema.** *Sea  $n = \prod_{i=1}^k p_i^{n_i}$  la representación canónica de un entero  $n$  y sea  $d$  un entero positivo. Entonces  $d \mid n$  si y solo si*

$$d = \prod_{i=1}^k p_i^{d_i}$$

donde  $0 \leq d_i \leq n_i$  para cada  $i$ ,  $1 \leq i \leq k$ .

*Demostración.* Supongamos que  $d = \prod_{i=1}^k p_i^{d_i}$  donde  $0 \leq d_i \leq n_i$  entonces,

$$\begin{aligned} n &= \prod_{i=1}^k p_i^{n_i} \\ &= \prod_{i=1}^k p_i^{n_i - d_i + d_i} \\ &= \prod_{i=1}^k p_i^{n_i - d_i} \prod_{i=1}^k p_i^{d_i} \\ &= (c)(d) \end{aligned}$$

donde  $c = \prod_{i=1}^k p_i^{n_i - d_i}$  es un entero. Luego  $d \mid n$ .

Recíprocamente supongamos que  $d \mid n$ . Por definición, existe un entero  $c$ , positivo en este caso, tal que  $n = cd$ .

La unicidad de la representación canónica de  $n$  nos garantiza que los primos que aparecen en la factorización de  $c$  y  $d$  son los mismos que aparecen en la de  $n$ . Así,

$$d = \prod_{i=1}^k p_i^{d_i}, \quad c = \prod_{i=1}^k p_i^{c_i}, \quad n = \prod_{i=1}^k p_i^{n_i}$$

donde  $d_i \geq 0$ ,  $c_i \geq 0$  y  $n_i = d_i + c_i$  y entonces  $d$  tiene la forma mencionada.  $\square$

El TFA nos proporciona otra manera de calcular el MCD y el MCM de dos o más enteros. Veamos el caso de dos enteros.

**2.43 Teorema.** Sean  $a = \prod_{i=1}^k p_i^{a_i}$ ,  $b = \prod_{i=1}^k p_i^{b_i}$  donde  $p_i$  es primo para todo  $i$ , y  $a_i \geq 0$ ,  $b_i \geq 0$  para todo  $i$ . Entonces:

$$(a, b) = \prod_{i=1}^k p_i^{s_i} \quad y \quad [a, b] = \prod_{i=1}^k p_i^{t_i}$$

donde  $s_i = \min\{a_i, b_i\}$  y  $t_i = \max\{a_i, b_i\}$ .

*Demostración.* Sea  $d = \prod_{i=1}^k p_i^{s_i}$ . Veamos que  $d$  satisface las condiciones (1), (2), (3) del Teorema 2.6.

Claramente satisface (1).

Además, como  $0 \leq s_i \leq a_i$  y  $0 \leq s_i \leq b_i$  para cada  $i$ , por el teorema anterior  $d \mid a$  y  $d \mid b$ , así  $d$  satisface (2).

Finalmente si  $f \mid a$  y  $f \mid b$  entonces  $|f| = \prod_{i=1}^k p_i^{f_i}$  donde  $0 \leq f_i \leq a_i$  y  $0 \leq f_i \leq b_i$  para cada  $i$ , y entonces  $|f| \mid d$ . Luego  $f \mid d$  y así  $d$  satisface (3).

En forma similar, usando el Teorema 2.28, se demuestra el correspondiente resultado para el MCM.  $\square$

#### 2.44 Ejemplo.

$$\begin{aligned} 1800 &= 2^3 \cdot 3^2 \cdot 5^2 \\ 3780 &= 2^2 \cdot 3^3 \cdot 5 \cdot 7 \\ 4900 &= 2^2 \cdot 5^2 \cdot 7^2. \end{aligned}$$

Entonces,

$$\begin{aligned} (1800, 3780, 4900) &= 2^2 \cdot 3^0 \cdot 5 \cdot 7^0 = 20 \\ [1800, 3780, 4900] &= 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 = 264600. \end{aligned}$$

---

## Ejercicios 2.3

---

1. Sea  $n = \prod_{i=1}^k p_i^{n_i}$  con  $n_i > 0$  la representación canónica de  $n$ . Demostrar que  $n$  es un cuadrado perfecto si y solamente si  $n_i$  es par para cada  $i$ ,  $1 \leq i \leq k$ .
2. Sean  $a = \prod_{i=1}^k p_i^{a_i}$  y  $b = \prod_{i=1}^k p_i^{b_i}$  con  $a_i \geq 0$  y  $b_i \geq 0$ . Demostrar que  $(a, b) = 1$  si y solo si  $a_i b_i = 0$  para todo  $i$ ,  $1 \leq i \leq k$ .
3. Sean  $a, b$  enteros positivos primos entre sí. Probar que si  $ab = c^n$ ,  $n > 0$  entonces existen  $e$  y  $f$  enteros positivos tales que  $a = e^n$  y  $b = f^n$ .
4. Si  $(a, b) = p$  con  $p$  primo. ¿Cuáles son los posibles valores de  $(a^2, b)$  y de  $(a^2, b^3)$ ?
5. Probar que la ecuación  $m^2 = 12n^2$  no admite solución en los enteros.
6. Probar que la ecuación  $m^3 = 4n^3$  no admite solución en los enteros.
7. Hallar el MCD y el MCM de 1485, 5445 y 12375.
8. Hallar el MCD y el MCM de 392, 1764, 2646 y 8820.
9. Demostrar el resultado similar al de el Teorema 2.43 para tres enteros.

Supongamos que  $a, b, c$  son enteros positivos, probar que:

10.  $abc = (ab, ac, bc)[a, b, c]$ .
11.  $abc = (a, b, c)[ab, ac, bc]$ .
12.  $(a, [b, c]) = [(a, b), (a, c)]$ .
13. Si  $(a, b, c) \cdot [a, b, c] = abc$  entonces  $(a, b) = (a, c) = (b, c) = 1$ .

## 2.7 Algunas propiedades de los números primos

Dada la importancia de los números primos, nos gustaría poder determinar rápidamente si un entero positivo es o no un número primo.

Desafortunadamente no existen métodos generales que permitan decidir si un entero positivo es o no un primo y solo en casos especiales conocemos su naturaleza. En el Apéndice A al final del libro se encuentra un listado de los números primos menores que 10.000.

Un método simple y eficiente para enteros positivos relativamente pequeños es verificar si el entero dado tiene o no divisores primos menores que él. Puesto que si  $n = ab$  entonces  $a \leq \sqrt{n}$  o  $b \leq \sqrt{n}$  es suficiente determinar si algún primo menor o igual a  $\sqrt{n}$  es divisor de  $n$ .

**2.45 Ejemplo.** Veamos si 239 es o no un número primo. La raíz cuadrada de 239 esta entre 15 y 16 pues  $15^2 = 225$  y  $16^2 = 256$ , luego basta ver si alguno de los primos 2, 3, 5, 7, 11, o 13 son divisores de 239 y como ninguno de ellos lo es entonces 239 es primo.

Una técnica llamada *criba de Eratóstenes* en honor del matemático griego Eratóstenes (276-194 A.C.) proporciona un método eficiente aplicable a números relativamente pequeños para encontrar todos los primos menores o iguales a un entero  $n$  dado.

La técnica consiste en escribir la lista de todos los enteros desde 2 hasta  $n$  y comenzar a tachar todos los múltiplos de 2 mayores que 2; al terminar, el primer número no tachado distinto de 2 es 3 que es un número primo; luego tachamos todos los múltiplos de 3 mayores de 3; al terminar, el menor número no tachado mayor que 3 es 5 que es un número primo; tachamos enseguida todos los múltiplos de 5 mayores que 5 y continuamos el proceso hasta tachar todos los múltiplos de  $p$  mayores que  $p$  para todo primo  $p \leq \sqrt{n}$ .

Los enteros no tachados al terminar este procedimiento son los números primos menores o iguales a  $n$ .

La siguiente tabla muestra la criba para  $n = 90$  ( $\sqrt{90} < 10$ )

	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	68	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90

Observamos entonces que los números primos menores o iguales que 90 son: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89.

Una observación detenida de la criba permite ver que la distribución de los primos decrece de manera constante, lo que nos podría inducir a pensar que el número de primos es finito. Sin embargo Euclides demostró que el número de primos es infinito.

**2.46 Teorema.** *El número de primos es infinito.*

*Demostración.* —Dada por Euclides—. Supongamos que solo hay un número finito de primos,

$$p, p_2, \dots, p_n \text{ y sea } N = p_1 p_2 \dots p_n + 1.$$

Como  $N > 1$ , entonces  $N$  es primo o se expresa como producto de primos. Ya que  $N$  es mayor que cada uno de los primos  $p_i$  entonces  $N$  no es primo. Además ningún primo  $p_i$  divide a  $N$  pues si  $p_i \mid N$  entonces

$$p_i \mid (N - p_1 p_2 \dots p_n) = 1$$

lo que es imposible.

Esto contradice el TFA y por tanto el número de primos es infinito.  $\square$

Observamos también en la criba que todos los números primos diferentes de 2 y 3 aparecen en la primera y quinta columnas esto nos induce a pensar que todos los números primos mayores de 3, son de la forma  $6k + 1$  o  $6k + 5$ , afirmación que es cierta y de fácil verificación.

Igualmente observamos en la criba la aparición de un número aproximadamente igual de primos de la forma  $4k + 1$  y  $4k + 3$  lo que nos sugiere pensar que hay infinitos primos de estas formas. Todas estas conjeturas son resultados particulares de un teorema más general denominado *Teorema de Dirichlet* que enunciaremos sin prueba, porque esta requiere conocimientos del Análisis Complejo.

**2.47 Teorema (Dirichlet).** *Si  $(a, d) = 1$  con  $a$  y  $d$  enteros positivos, entonces hay un número infinito de primos de la forma  $a + kd$ .*

Una variación rutinaria del argumento de Euclides en el Teorema 2.46 nos permite probar un caso en particular como el siguiente teorema.

**2.48 Teorema.** *Hay infinitos primos de la forma  $6k + 5$ .*

*Demostración.* Puesto que  $6k + 5 = 6(k + 1) - 1$  basta demostrar que hay infinitos primos de la forma  $6k - 1$ .

Supongamos que solo hay un número finito de primos de esta forma y que ellos son  $p_1, p_2, \dots, p_n$ . Consideremos

$$N = 6(p_1 p_2 \dots p_n) - 1.$$

Como  $N > p_i$  para  $1 \leq i \leq n$  y  $N$  es de la forma  $6k - 1$ , entonces  $N$  debe ser compuesto y debe tener factores primos de la forma  $6t + 1$  o  $6t - 1$  y puesto que el producto de dos números de la forma  $6t + 1$  es de esta forma,  $N$  debe tener al menos un factor primo de la forma  $6t - 1$ , es decir, existe  $i$  tal que  $p_i \mid N$  y en consecuencia  $p_i \mid 1$  lo que es imposible. Luego hay infinitos primos de la forma  $6t - 1$  como queríamos demostrar.  $\square$

Aún con las observaciones anteriores la disposición de los primos en la sucesión natural es bastante irregular. El siguiente teorema demuestra que hay separaciones arbitrariamente grandes entre números primos.

**2.49 Teorema.** *Para cada entero positivo  $n$ , existen  $n$  enteros consecutivos todos compuestos.*

*Demostración.* Los enteros  $(n+1)! + 2$ ,  $(n+1)! + 3$ ,  $(n+1)! + 4, \dots$ ,  $(n+1)! + n$ ,  $(n+1)! + (n+1)$  son  $n$  enteros consecutivos, además para cada  $j$ ,  $2 \leq j \leq (n+1)$ ,  $j \mid ((n+1)! + j)$ . Luego todos son compuestos.  $\square$

Otra observación sobre las tablas de números primos es la existencia de muchas parejas de *primos gemelos* es decir parejas de la forma  $p, p+2$  donde ambos números son primos. Por ejemplo: 3,5; 5,7; 11,13; 29,31; 1000000000061, 1000000000063; 140737488353507, 140737488353509.

Todavía no hay respuesta sobre la existencia de finitas o infinitas parejas de primos gemelos.

Si hubiese un número finito de primos gemelos la serie  $\sum \frac{1}{q}$  donde  $q$  toma valores en el conjunto de los primos gemelos sería una suma finita y por lo tanto convergente. Viggo Brun (1885–1978) demostró en 1921 que efectivamente esta serie es convergente. De otra parte la serie  $\sum \frac{1}{p}$  donde  $p$  toma valores en el conjunto de todos los números primos es una serie divergente. La primera prueba de este resultado fue dada por Euler (1707–1783) en 1737 y la prueba que aquí presentamos se debe a J. A. Clarkson quien la dió en 1966.

**2.50 Teorema.** La serie  $\sum \frac{1}{p_n}$  donde  $p_n$  es el  $n$ -ésimo número primo, es divergente.

*Demostración.* Supongamos que la serie dada es convergente, entonces existe un entero positivo  $k$  tal que

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} \leq \frac{1}{2}.$$

Sea  $Q = p_1 p_2 \dots p_k$  y consideremos los números de la forma  $1 + nQ$  con  $n = 1, 2, \dots$ , cada uno de estos enteros no es divisible por los primos  $p_1, p_2, \dots, p_k$  y entonces sus factores primos se encuentran entre los primos  $p_{k+1}, p_{k+2}, \dots$ , por lo tanto para cada  $r \geq 1$ ,

$$\sum_{n=1}^r \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left( \sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t$$

ya que cada término de la suma del lado izquierdo está contenido en la suma del lado derecho. Además

$$\sum_{t=1}^{\infty} \left( \sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t \leq \sum_{t=1}^{\infty} \left( \frac{1}{2} \right)^t = 1,$$

es decir todas las sumas parciales de la serie  $\sum \frac{1}{1+nQ}$  son acotadas y por lo tanto ella converge, pero el criterio de comparación por paso al límite muestra que,

$$\sum \frac{1}{1+nQ} \quad \text{y} \quad \sum \frac{1}{n}$$

son asintóticamente iguales, luego

$$\sum \frac{1}{1+nQ} \quad \text{diverge pues} \quad \sum \frac{1}{n} \quad \text{diverge}.$$

En consecuencia  $\sum \frac{1}{p_n}$  es divergente.  $\square$

Un problema planteado con frecuencia es la necesidad de encontrar expresiones a partir de las cuales obtengamos números primos mediante la asignación de enteros positivos a cada una de las variables. Por ejemplo la fórmula  $n^2 + n + 41$  —dada por Euler— da un número primo por cada asignación que demos a  $n$  entre 1 y 39, sin embargo para  $n = 40$  resulta

$$40^2 + 40 + 41 = 40^2 + 2(40) + 1 = (40 + 1)^2$$

que obviamente no es primo. Mostramos ahora que ningún polinomio en una variable con coeficientes enteros es útil a este propósito, es decir:

**2.51 Teorema.** *Si  $f(x)$  es un polinomio no constante con coeficientes enteros, entonces  $f(n)$  es un número compuesto para infinitos valores del entero  $n$ .*

*Demostración.* Claramente el teorema es cierto si  $f(n)$  es compuesto para todo  $n \geq 1$ . Supongamos que existe  $n_0 \geq 1$  tal que  $f(n_0) = p$  con  $p$  primo. Como  $\lim_{n \rightarrow \infty} |f(n)| = \infty$  existe  $n$  tal que si  $n \geq n_1$  entonces  $|f(n)| > p$ . Consideremos  $h$  tal que  $n_0 + ph \geq n_1$  entonces

$$\begin{aligned} f(n_0 + ph) &= f(n_0) + (\text{múltiplos de } p) \\ &= p + (\text{múltiplos de } p) \\ &= Y \cdot p \end{aligned}$$

y así  $f(n_0 + ph)$  es compuesto.  $\square$

**Nota.** Un problema que ha concentrado la atención de los matemáticos desde tiempos inmemoriales, es el de encontrar formulas que generen todos los números primos. Sobre este tema hay una literatura extensa y solo mencionaremos el hecho notable de que se ha encontrado un polinomio de grado 25 con 26 variables y coeficientes enteros  $p(x_1, \dots, x_{26})$  tal que cada vez que  $x_1, \dots, x_{26}$  son enteros no negativos y  $p(x_1, x_2, \dots, x_{26}) > 0$  entonces  $p(x_1, \dots, x_{26})$  es primo, y más aún todos los números primos se obtienen como valores de este polinomio.

Sin embargo, observamos que este polinomio no es una formula mágica para calcular números primos.

Un problema famoso relacionado con los números primos, muy sencillo de enunciar pero no resuelto hasta la fecha (como es común en la teoría de números), es el conocido como la conjetura de Goldbach. Cristian Goldbach (1690-1764) fue un matemático ruso quien a mediados del siglo XVIII en una carta a Euler, le preguntó si era cierto o no, que todo entero positivo mayor que 1 se podía expresar como suma de a lo más tres números primos. Euler le respondió que el problema era muy difícil y que era equivalente al siguiente enunciado, conocido hoy día como la *Conjetura de Goldbach*: Todo entero positivo par mayor que 2 se puede expresar como la suma de dos números primos. En 1997, Jean-Marc Deshouillers, Yannik Saouter y Hermann Riele probaron que la conjetura es verdadera para todo entero positivo menor que  $10^{14}$ . recientemente, en 2003 el matemático portugués Tomas Oliveira verificó la validez de la conjetura para los enteros positivos menores que  $6 \times 10^6$ .

Finalmente enunciaremos el denominado *Teorema de los números primos*, uno de los más famosos de la teoría avanzada de números, que nos proporciona un estimativo sobre la distribución de los primos en la sucesión natural.

Definimos primero la función  $\pi(x)$  que asigna a cada entero positivo  $x$  el número de primos menores o iguales a  $x$ ,

$$\pi(1) = 0, \quad \pi(2) = 1, \quad \pi(3) = 2, \quad \pi(10) = 4.$$

Como ya hemos observado que la distribución de los primos es muy irregular, no existe una fórmula sencilla que defina  $\pi(n)$ . El *Teorema de los números primos* establece una aproximación asintótica de  $\pi(n)$ .

**2.52 Teorema (de los números primos).**

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1$$

La afirmación del teorema fue conjeturada de manera independiente por Gauss en 1792 y Legendre en 1798 pero sólo hasta 1896 J. Hadamard y C. de la Vallée Poussin demostraron el Teorema por primera vez utilizando teoría de funciones de variable compleja. En 1949 A. Selberg y P. Erdős dieron una demostración más elemental sin usar análisis complejo pero aún muy difícil para presentarla en estas notas. En 1997, D. Zagier presentó una prueba más corta, dada por Newmann [13].

---

## Ejercicios 2.4

---

1. Probar que todo primo de la forma  $3k + 1$  es de la forma  $6t + 1$ .
2. Probar que todo primo diferente de 2 o 3 es de la forma  $6k + 1$  o  $6k - 1$ .
3. Probar que todo entero de la forma  $3k + 2$  tiene un factor primo de la misma forma.
4. Probar que todo entero de la forma  $4k + 3$  tiene un factor primo de la misma forma.
5. Demostrar que existen infinitos primos de la forma  $4k + 3$ .
6. Si  $p, q$  son primos tales que  $p \geq q \geq 5$  entonces  $24 \mid p^2 - q^2$ .
7. Demostrar que 3, 5, 7 son los únicos primos triples. (Los únicos tales que  $p, p + 2$  y  $p + 4$  son todos primos).
8. Si  $2^n - 1$  es primo probar que  $n$  es primo.

9. Si  $2^n + 1$  es primo, probar que  $n$  es una potencia de dos.

*Sugerencia:* Si  $k$  es impar  $(x + 1) \mid (x^k + 1)$ .

10. Sean  $p$  y  $q$  primos diferentes de 2 y 3. Probar que si  $p - q$  es una potencia de dos entonces  $p + q$  es divisible por tres.

11. Hallar un suceso de veinte enteros consecutivos y compuestos.

## 2.8 Algunas ecuaciones diofánticas

Una ecuación de la forma  $p(x_1, x_2, \dots, x_n) = 0$  donde  $p(x_1, x_2, \dots, x_n)$  es un polinomio con coeficientes enteros y con las variables restringidas a tomar únicamente valores enteros se denomina una Ecuación Diofántica en honor al matemático griego Diofanto de Alejandría (200–284) quien por primera vez las estudió detalladamente en su libro *Arithmetica*.

El ejercicio 8 de la sección 2.2 nos da una condición necesaria y suficiente para que la ecuación  $ax + by = c$  tenga una solución en  $\mathbb{Z}$ . Estas ecuaciones las estudiaremos detalladamente en el capítulo 4.

Estudiaremos en esta sección dos casos particulares de la ecuación de Fermat,

$$x^n + y^n = z^n. \quad (2.5)$$

Fermat afirmó haber demostrado que para  $n \geq 3$  esta ecuación no tiene solución en  $\mathbb{Z} - \{0\}$ , sin embargo su demostración nunca fue conocida.

**Nota.** Muchos matemáticos estudiaron intensamente este problema, que se denominó *el último Teorema de Fermat*, dando origen a diferentes teorías matemáticas en su intento por resolverlo. En junio de 1993 el matemático inglés Andrew Wiles anunció la demostración del teorema como consecuencia de su prueba de la conjetura de Taniyama–Shimura para curvas elípticas semiestables.

Durante la revisión de la demostración de Wiles surgieron algunos problemas que finalmente fueron resueltos por el mismo Wiles y el matemático Richard Taylor, quienes en mayo de 1995 publicaron en los *Annals of Mathematics* los resultados que llevaron a la demostración definitiva del último Teorema de Fermat.

Para  $n = 2$  la ecuación (2.5) tiene solución en los enteros positivos, por ejemplo  $x = 3$ ,  $y = 4$ ,  $z = 5$ . Daremos enseguida una descripción completa de la solución en este caso.

Observamos primero que si  $(x, y, z)$  es una solución de (2.5) entonces  $(kx, ky, kz)$  donde  $k$  es un entero cualquiera, también lo es. En consecuencia es suficiente encontrar soluciones tales que  $(x, y, z) = 1$ . Estas soluciones se denominan *soluciones primitivas*. Más aún, es suficiente encontrar soluciones primitivas de enteros positivos pues las demás se obtienen de estas mediante cambios de signos. También es fácil observar que si  $(x, y, z)$  es una solución primitiva de la ecuación (2.5), con  $n = 2$ , entonces los enteros  $x, y, z$  son primos relativos dos a dos.

En efecto, si por ejemplo  $(x, y) = d > 1$  y  $p$  es un primo tal que  $p \mid d$ , entonces  $p \mid x$  y  $p \mid y$  luego  $p \mid x^2$  y  $p \mid y^2$  y por lo tanto  $p \mid (x^2 + y^2) = z^2$  y como  $p$  es primo  $p \mid z$ , en contradicción con el hecho  $(x, y, z) = 1$ . Similarmente se verifica que  $(x, z) = (y, z) = 1$ .

Finalmente observemos que exactamente uno de los números  $x$  o  $y$  de la solución debe ser impar, pues si los dos lo fueran,  $x^2 + y^2$  sería de la forma  $4k + 2$  y por un ejercicio anterior ningún cuadrado perfecto tiene esa forma.

**2.53 Teorema.** *Los enteros  $x, y, z$  con  $x$  impar son una solución primitiva y positiva de la ecuación  $x^2 + y^2 = z^2$  si y solamente si existen enteros positivos  $a$  y  $b$  tales que,*

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

donde  $a > b$ ,  $(a, b) = 1$  con  $a$  y  $b$  de distinta paridad.

*Demostración.* Un cálculo directo muestra que las fórmulas dadas proporcionan una solución primitiva y positiva de la ecuación

$$x^2 + y^2 = z^2.$$

Recíprocamente, supongamos que  $(x, y, z)$  es una solución primitiva y positiva, donde  $x$  es impar. Como  $(y, z) = 1$  entonces  $(z - y, z + y) = 1$  o  $2$  y puesto que  $y$  es par y  $z$  es impar  $(z - y, z + y) = 1$ ; por lo tanto de la ecuación

$$x^2 = z^2 - y^2 = (z - y)(z + y)$$

concluimos que  $(z - y)$  y  $(z + y)$  deben ser números impares y cuadrados perfectos, puesto que son positivos.

Supongamos entonces  $(z - y) = r^2$  y  $(z + y) = s^2$  donde  $r$  y  $s$  son impares y positivos y definamos

$$a = \frac{s + r}{2}, \quad b = \frac{s - r}{2}.$$

Se observa fácilmente que  $r = a - b$  y  $s = a + b$ . Por lo tanto,

$$z - y = (a - b)^2, \quad z + y = (a + b)^2$$

de donde,

$$z = \frac{((a - b)^2 + (a + b)^2)}{2} = a^2 + b^2$$

$$y = \frac{((a + b)^2 - (a - b)^2)}{2} = 2ab$$

$$x = (a - b)(a + b) = a^2 - b^2.$$

Puesto que  $y > 0$ ,  $a$  y  $b$  tienen el mismo signo y como  $s = a + b$  entonces  $a$  y  $b$  resultan positivos. Como  $r = a - b > 0$  entonces  $a > b$  y como  $s = a + b$  es impar entonces  $a$  y  $b$  tienen distinta paridad. Finalmente  $(a, b) = 1$  pues si  $p$  es un primo tal que  $p \mid a$  y  $p \mid b$  entonces  $p \mid x$ ,  $p \mid y$ ,  $p \mid z$  lo que contradice que  $(x, y, z) = 1$ .  $\square$

Usando el teorema podemos construir la siguiente tabla pequeña de soluciones primitivas y positivas de la ecuación  $x^2 + y^2 = z^2$ .

$a$	$b$	$x$	$y$	$z$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

Las soluciones enteras y positivas de la ecuación  $x^2 + y^2 = z^2$  se conocen también con el nombre de *Ternas Pitagóricas* en una clara alusión al conocido Teorema de Pitágoras.

Estudiamos ahora la ecuación

$$x^4 + y^4 = z^2. \quad (2.6)$$

**2.54 Teorema.** *La ecuación  $x^4 + y^4 = z^2$  no tiene solución en el conjunto de los números enteros diferentes de cero.*

*Demostración.* Es suficiente probar que no existen soluciones primitivas positivas.

Como en el caso de la ecuación (2.5) con  $n = 2$  se ve que si  $(x, y, z)$  es una solución primitiva de (2.6) entonces los enteros  $x, y, z$  son primos relativos dos a dos. Supongamos entonces que  $(x, y, z)$  es una solución primitiva tal que  $x > 0, y > 0, z > 0$  y  $z$  es mínimo. Además, sin perder generalidad, podemos suponer que  $x$  es impar y  $y$  es par. Escribiendo  $x^4 + y^4 = z^2$  en la forma

$$(x^2)^2 + (y^2)^2 = z^2,$$

por aplicación del Teorema 2.53 tenemos:

$$x^2 = a^2 - b^2, \quad y^2 = 2ab, \quad z = a^2 + b^2$$

donde  $a > b > 0$ ,  $a$  y  $b$  de paridad opuesta y  $(a, b) = 1$ . Si  $a$  fuese par y  $b$  impar, el número  $x^2 = a^2 - b^2$  sería de la forma  $4k - 1 = 4(k - 1) + 3$  con  $k > 0$ , lo que es imposible. Luego  $a$  es impar y  $b$  es par.

Aplicando nuevamente el Teorema 2.53 a la ecuación  $x^2 + b^2 = a^2$  tenemos que

$$x = u^2 - v^2, \quad b = 2uv, \quad a = u^2 + v^2$$

donde  $u > v > 0$ ,  $(u, v) = 1$  con  $u$  y  $v$  de distinta paridad. Como  $y^2 = 2ab$  entonces  $y^2 = 4uv(u^2 + v^2)$ .

Puesto que  $u, v$  y  $(u^2 + v^2)$  son primos relativos dos a dos (pruébelo), entonces cada uno de estos números debe ser un cuadrado perfecto; sea por ejemplo

$$u = r^2, \quad v = s^2, \quad u^2 + v^2 = t^2$$

donde podemos asumir que  $r, s$  y  $t$  son positivos. Además tenemos  $(r, s, t) = 1, t > 1$  y

$$r^4 + s^4 = t^2$$

y como  $z = a^2 + b^2 = t^4 + b^2 > t^4$ , entonces  $z > t$ .

De esta forma hemos encontrado una solución primitiva y positiva de (2.6) a saber  $(r, s, t)$  donde  $t < z$  lo que contradice la minimalidad de  $z$ , con lo cual queda demostrado el teorema.  $\square$

Una ligera variación de la demostración consiste en construir a partir de una solución primitiva y positiva de (2.6) una sucesión  $(x_n, y_n, z_n)$  de soluciones de dicha ecuación donde la sucesión  $(z_n)$  es estrictamente decreciente, lo cual es absurdo. Este procedimiento es denominado *método del descenso infinito* y es debido a Fermat.

**2.55 Corolario.** *La ecuación  $x^4 + y^4 = z^4$  no tiene solución en el conjunto de los enteros diferentes de cero.*

*Demostración.* Es suficiente observar que la ecuación puede escribirse en la forma

$$x^4 + y^4 = (z^2)^2$$

y aplicar el teorema.  $\square$

---

## Ejercicios 2.5

---

1. Probar que si  $n$  es una potencia de 2 mayor que 2, la ecuación  $x^n + y^n = z^n$  no tiene solución en el conjunto de los enteros diferentes de cero.
2. Encontrar todas las ternas pitagóricas  $(x, y, z)$  tales que  $1 \leq z < 30$ .
3. Probar que la conjetura de Fermat es cierta si y solo si para todo primo impar  $p$ , la ecuación  $x^p + y^p = z^p$  no tiene solución en el conjunto de los enteros diferentes de cero.
4. Hallar todas las ternas pitagóricas que estén en progresión aritmética.
5. Probar que  $(3, 4, 5)$  es la única terna pitagórica formada por enteros consecutivos.
6. Hallar todas las ternas pitagóricas que estén en progresión geométrica.
7. Probar que no existen enteros diferentes de cero tales que  $x^4 - y^4 = z^2$

8. Probar que toda solución primitiva  $(x, y, z)$  de la ecuación  $x^4 + y^4 = z^2$  es tal que  $x, y, z$  son primos relativos dos a dos.
9. Probar que el radio del círculo inscrito en un triángulo pitagórico es siempre un entero.

*Sugerencia:* Calcular el área del triángulo de dos formas diferentes.

---

## Funciones Aritméticas

---

### 3.1 La función parte entera

**3.1 Definición.** Sea  $x$  un número real. Existe un único entero que representamos por  $[x]$  que satisface la desigualdad

$$[x] \leq x < [x] + 1.$$

En otras palabras  $[x]$  es el mayor entero menor o igual que  $x$ . Al entero  $[x]$  lo denominamos *la parte entera de  $x$* .

**3.2 Teorema.** Sean  $x, y, z$  números reales cualesquiera, entonces:

- a)  $x - 1 < [x] \leq x$ .
- b) Si  $m$  es un entero y  $m \leq x$  entonces  $m \leq [x]$ .
- c) Si  $m$  es un entero y  $m > x$  entonces  $m \geq [x] + 1$ .
- d) Si  $x \leq y$  entonces  $[x] \leq [y]$ .

- e) Si  $z = x - [x]$  entonces  $0 \leq z < 1$ .
- f) Si  $n$  es un entero y  $x = n + z$  con  $0 \leq z < 1$  entonces  $[x] = n$ .
- g) Para todo entero  $n$ ,  $[x + n] = [x] + n$ .
- h)  $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$ .

i)

$$[x] + [-x] = \begin{cases} 0 & \text{si } x \in \mathbb{Z}, \\ -1 & \text{si } x \notin \mathbb{Z}. \end{cases}$$

- j) Si  $a = bq + r$  con  $0 \leq r < b$  entonces  $\left[\frac{a}{b}\right] = q$

- k) Para todo entero positivo  $n$ ,  $\left[\frac{x}{n}\right] = \frac{[x]}{n}$ .

*Demostración.* a) Es consecuencia inmediata de la definición.

- b) Si  $m + 1 > x$  entonces  $m \leq x < m + 1$  y  $m = [x]$  por definición. Si  $m + 1 \leq x$ , entonces  $m \leq x - 1 < [x]$  por la parte (a).

- c) Tenemos  $[x] \leq x$ . Luego si  $m > x$  entonces  $m > [x]$  y en consecuencia  $m \geq [x] + 1$  puesto que  $m$  y  $[x]$  son enteros.

- d) Ya que  $[x] \leq x$  obtenemos  $[x] \leq y$  y por (b),  $[x] \leq [y]$ .

- e) Es consecuencia inmediata de la definición.

- f) Como  $0 \leq z = x - n < 1$  entonces  $n \leq x < n + 1$  y por definición  $[x] = n$ .

- g) Por (e),  $x = [x] + z$  con  $0 \leq z < 1$ . Luego  $x + n = [x] + n + z$  y por (f)  $[x + n] = [x] + n$ .

- h) Claramente  $[x] + [y] \leq x + y$  y por (b)  $[x] + [y] \leq [x + y]$ . Además  $x = [x] + z$  y  $y = [y] + w$  donde  $0 \leq z, w < 1$ . Luego aplicando (g) tenemos  $[x + y] = [[x] + [y] + z + w] = [x] + [y] + [z + w] \leq [x] + [y] + 1$

- i) Si  $x \in \mathbb{Z}$  entonces  $(-x) \in \mathbb{Z}$  y por lo tanto  $[x] + [-x] = x + (-x) = 0$ . Si  $x \notin \mathbb{Z}$  entonces  $[x] < x < [x] + 1$  y por lo tanto  $-([x] + 1) < (-x) < -[x]$  que significa  $[-x] = -[x] - 1$ . En consecuencia  $[x] + [-x] = -1$ .

- j) Se deduce inmediatamente de (f).

k) Si dividimos  $[x]$  por  $n$  obtenemos  $[x] = qn + r$  donde  $0 \leq r < n$  y por lo tanto  $q = \lfloor [x]/n \rfloor$ . De otra parte  $x = [x] + z$  con  $0 \leq z < 1$  y entonces  $x = (qn + r) + z$  con  $0 \leq r + z < n$ . Por lo tanto  $(x/n) = q + (r + z)/n$  con  $0 \leq (r + z)/n < 1$  y en consecuencia  $[x/n] = q$ .  $\square$

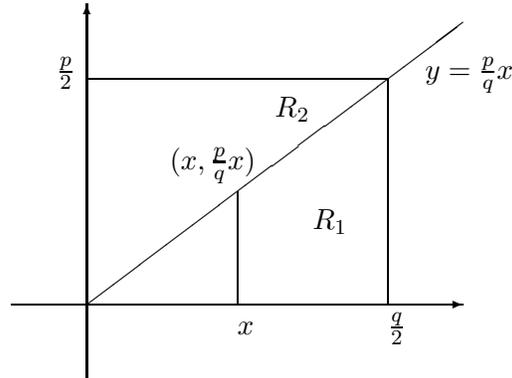
**3.3 Ejemplo.** Sea  $x$  un número real cualquiera. Veamos que  $[x + (1/2)]$  es el entero más próximo a  $x$ .

En efecto, sea  $n$  el entero más próximo a  $x$ , donde escogemos el mayor cuando hay dos enteros igualmente próximos. Tenemos entonces  $n = x + z$  con  $-(1/2) < z \leq (1/2)$ . Luego  $x + (1/2) = n + (1/2) - z$  con  $0 \leq (1/2) - z < 1$  y por (f) del teorema anterior,  $[x + (1/2)] = n$ .

**3.4 Ejemplo.** Sean  $p$  y  $q$  enteros positivos, impares y primos relativos. Veamos que,

$$\sum_{0 < x < \frac{q}{2}} \left\lfloor \frac{p}{q}x \right\rfloor + \sum_{0 < y < \frac{p}{2}} \left\lfloor \frac{q}{p}y \right\rfloor = \frac{p-1}{2} \frac{q-1}{2}.$$

Observemos la figura,



El número  $\frac{p-1}{2} \cdot \frac{q-1}{2}$  representa el número de puntos con coordenadas enteras en el interior del rectángulo. Sobre la diagonal no hay puntos de esta clase, pues si existieran  $x$  y  $y$  enteros tales que  $y = (p/q)x$  entonces  $qy = px$  es decir  $q \mid px$  y como  $(q, p) = 1$  entonces  $q \mid x$  lo que es imposible pues  $x < \frac{q}{2}$ .

De otra parte, para cada entero  $x$  el número de puntos en la región triangular  $R_1$  con primera coordenada  $x$  y coordenadas enteras es  $\lfloor \frac{p}{q}x \rfloor$ . Por

lo tanto el número de puntos en la región  $R_1$  con coordenadas enteras es

$$\sum_{0 < x < q/2} \left[ \frac{p}{q} x \right].$$

Similarmente, el número de puntos con coordenadas enteras en la región  $R_2$  es

$$\sum_{0 < y < p/2} \left[ \frac{q}{p} y \right]$$

y por lo tanto obtenemos,

$$\frac{(p-1)}{2} \cdot \frac{(q-1)}{2} = \sum_{0 < x < q/2} \left[ \frac{p}{q} x \right] + \sum_{0 < y < p/2} \left[ \frac{q}{p} y \right]$$

como queríamos probar.

**3.5 Teorema.** Sean  $n$  un entero positivo y  $p$  un número primo. Entonces  $p$  aparece en la representación canónica de  $n!$  con exponente

$$[n/p] + [n/p^2] + [n/p^3] + \cdots + [n/p^r]$$

donde  $r$  es tal que  $p^r \leq n < p^{r+1}$

*Demostración.* Para todo entero positivo  $k$ , los enteros positivos menores o iguales que  $n$  y divisibles por  $p^k$  son  $p^k, 2p^k, \dots, tp^k$  donde  $t$  es el mayor entero tal que  $t \leq (n/p^k)$  o sea  $t = [n/p^k]$ . Luego hay exactamente  $[n/p^k]$  múltiplos de  $p^k$  menores o iguales que  $n$ .

Si observamos que cada múltiplo de  $p^k$  lo es también de  $p, p^2, p^3, p^4, \dots, p^{k-1}$  y contamos su contribución  $k$  al exponente de  $p$  en la representación canónica de  $n!$ , una vez como múltiplo de  $p$ , otra vez como múltiplo de  $p^2$  y Así sucesivamente hasta contarla una vez como múltiplo de  $p^k$ , encontramos que el exponente de  $p$  en la representación canónica de  $n!$  es

$$[n/p] + [n/p^2] + [n/p^3] + \cdots + [n/p^r]$$

donde  $r$  es tal que  $p^r \leq n < p^{r+1}$ . □

Además si  $k > r$  entonces  $[n/p^k] = 0$  y podemos decir que el exponente con que aparece  $p$  en la representación canónica de  $n!$  es

$$\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right].$$

Podemos entonces escribir la siguiente fórmula notable para la representación canónica de  $n!$

$$n! = \prod_p p^{\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right]}$$

donde  $p$  varía sobre todos los números primos.

**3.6 Ejemplo.** El exponente con el cual aparece 7 en la factorización canónica de  $500!$  es

$$\left[ \frac{500}{7} \right] + \left[ \frac{500}{49} \right] + \left[ \frac{500}{343} \right] = 71 + 10 + 1 = 82.$$

El exponente con el cual 3 aparece en la representación canónica de  $500!$  es

$$\begin{aligned} & \left[ \frac{500}{3} \right] + \left[ \frac{500}{9} \right] + \left[ \frac{500}{27} \right] + \left[ \frac{500}{81} \right] + \left[ \frac{500}{243} \right] \\ & = 166 + 55 + 18 + 6 + 2 = 247. \end{aligned}$$

De lo anterior podemos deducir que la mayor potencia de 21 que divide a  $500!$  es  $\min(82, 247) = 82$ .

Cuando los números son grandes la propiedad (k) del Teorema 3.2 permite simplificar los cálculos, ya que con base en ella tenemos

$$\left[ \frac{n}{p^{k+1}} \right] = \left[ \frac{\left[ \frac{n}{p^k} \right]}{p} \right]$$

**3.7 Ejemplo.** Veamos que si  $a_1 + a_2 + \cdots + a_r = n$  donde  $a_i \geq 0$  entonces el coeficiente multinomial

$$\frac{n!}{a_1! a_2! a_3! \cdots a_r!}$$

es entero.

Es suficiente probar que todo primo  $p$  aparece en el denominador con un exponente menor que aquel con el cual aparece en el numerador.

El exponente con que  $p$  aparece en el numerador es

$$\sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right].$$

El exponente con que  $p$  aparece en el denominador es

$$\begin{aligned} & \sum_{k=1}^{\infty} \left[ \frac{a_1}{p^k} \right] + \sum_{k=1}^{\infty} \left[ \frac{a_2}{p^k} \right] + \cdots + \sum_{k=1}^{\infty} \left[ \frac{a_r}{p^k} \right] \\ &= \sum_{k=1}^{\infty} \left( \left[ \frac{a_1}{p^k} \right] + \left[ \frac{a_2}{p^k} \right] + \cdots + \left[ \frac{a_r}{p^k} \right] \right) \\ &\leq \sum_{k=1}^{\infty} \left[ \frac{a_1 + a_2 + \cdots + a_r}{p^k} \right] = \sum_{k=1}^{\infty} \left[ \frac{n}{p^k} \right] \end{aligned}$$

donde la desigualdad se tiene por la parte h) del Teorema 3.2. De esta forma queda probada nuestra afirmación.

---

## Ejercicios 3.1

---

1. Sean  $n$  y  $a$  enteros positivos. Probar que  $\left[ \frac{n}{a} \right]$  es el número de enteros de la sucesión  $1, 2, \dots, n$  que son divisibles por  $a$ .
2. Sea  $x$  un número real que no es punto medio de dos enteros probar que  $-[-x + \frac{1}{2}]$  es el entero más próximo a  $x$ .
3. Sean  $x, y$  números reales positivos. Probar que  $[x][y] \leq [xy]$ .
4. Hallar todos los números reales que satisfacen:
  - (a)  $[x] + [x] = [2x]$
  - (b)  $[x + \frac{1}{2}] + [x - \frac{1}{2}] = [2x]$ .
5. Probar que para todo número real  $x$ ,  $[x] + [x + \frac{1}{2}] = [2x]$ .  
*Sugerencia:* Escribir  $x = [x] + z$  y considerar  $0 \leq z < \frac{1}{2}$  y  $\frac{1}{2} \leq z < 1$ .
6. Probar que para todo número real  $x$ ,  $[x] + [x + \frac{1}{3}] + [x + \frac{2}{3}] = [3x]$ .

7. Probar que para todo número real  $x$ , y para todo entero positivo  $k$ ,
- $$[x] + [x + \frac{1}{k}] + [x + \frac{2}{k}] + \cdots + [x + \frac{k-1}{k}] = [kx].$$
8. ¿Cuál es el exponente de 5 en la representación canónica de 835!?  
¿Cuál el de 15?
9. ¿Con cuántos ceros termina la expansión decimal de 120!?
10. ¿Con cuántos ceros termina el desarrollo en base 3 de 100!?
- Sugerencia:* Escribir  $100! = 3^m b$  donde  $(b, 3) = 1$  y luego expresar  $b$  en la forma  $b = 3k + r$  con  $r = 1$  o  $r = 2$ .
11. Probar que  $3 \nmid \binom{91}{10}$
12. Si  $n$  es un entero positivo, probar que  $\frac{(2n)!}{(n!)^2}$  es un número par.
13. Para todo entero positivo  $n$ , probar que  $n!(n-1)!$  divide a  $(2n-2)!$
14. Sea  $n = p^a$  donde  $p$  es primo y  $a$  un entero positivo. Probar que:  
 $n \mid (n-1)!$  si y solamente si  $p$  es impar y  $a > 1$ , ó,  $p = 2$  y  $a > 2$ .

### 3.2 Las funciones número y suma de divisores

Las funciones que tienen como dominio el conjunto de los enteros positivos con valores en  $\mathbb{C}$  se denominan *funciones aritméticas* o *funciones numéricas*. En esta sección estudiaremos dos de ellas muy conocidas.

Si  $n$  es un entero positivo definimos las funciones  $\tau(n)$  y  $\sigma(n)$  así:

- $\tau(n)$  es el número de divisores positivos de  $n$ .
- $\sigma(n)$  es la suma de los divisores positivos de  $n$ .

Por ejemplo,  $\tau(1) = \sigma(1) = 1$ ,  $\tau(10) = 4$  y  $\sigma(10) = 1 + 2 + 5 + 10 = 18$ .

Como consecuencia del Teorema Fundamental de la Aritmética obtenemos los resultados siguientes.

**3.8 Teorema.** Si  $n = \prod_{i=1}^k p_i^{n_i}$  donde  $n_i > 0$  para cada  $i$ , es la representación canónica de un entero positivo  $n$ , entonces

$$\tau(n) = \prod_{i=1}^k (n_i + 1) \quad \text{y} \quad \sigma(n) = \prod_{i=1}^k \frac{p_i^{n_i+1} - 1}{p_i - 1}$$

*Demostración.* Por el Teorema 2.43,  $d$  es un divisor positivo de  $n$ , si y solo si,  $d = \prod_{i=1}^k p_i^{d_i}$  donde  $0 \leq d_i \leq n_i$  para cada  $i = 1, 2, \dots, k$ . Por el principio fundamental de conteo, podemos construir exactamente  $(n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$  de tales divisores. Es decir

$$\tau(n) = \prod_{i=1}^k (n_i + 1).$$

De otra parte, si observamos que cada divisor positivo de  $n$  aparece una y solamente una vez como sumando en el producto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{n_1}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{n_k})$$

concluimos que

$$\sigma(n) = \prod_{i=1}^k (1 + p_i + p_i^2 + \cdots + p_i^{n_i}),$$

y puesto que

$$1 + p_i + p_i^2 + \cdots + p_i^{n_i} = \frac{p_i^{n_i+1} - 1}{p_i - 1},$$

tenemos también que

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{n_i+1} - 1}{p_i - 1}. \quad \square$$

En el teorema anterior si  $p$  es un número primo tenemos,

$$\tau(p) = 1 + 1 = 2 \quad \text{y} \quad \sigma(p) = 1 + p = \frac{p^{1+1} - 1}{p - 1}.$$

Más generalmente, si  $p$  es primo y  $a$  es un entero positivo tenemos,

$$\tau(p^a) = a + 1 \quad \text{y} \quad \sigma(p^a) = 1 + p + p + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

**3.9 Ejemplo.** Encontramos el menor entero positivo que tiene 21 divisores positivos.

Como  $21 = 3 \times 7$ , el número buscado tiene la forma  $p^2q^6$  con  $p$  y  $q$  primos diferentes, o la forma  $p^{20}$  con  $p$  primo. Los números más pequeños que tienen estas formas son:

$$2^2 \times 3^6 = 2916$$

$$3^2 \times 2^6 = 576$$

$$2^{20} = 1048576$$

Por lo tanto 576 es el número buscado.

Busquemos una fórmula para el producto de los divisores positivos de un entero positivo  $n$ .

Supongamos que los divisores positivos de  $n$  son

$$d_1, d_2, \dots, d_{\tau(n)}$$

y su producto es

$$P = d_1 d_2 \dots d_{\tau(n)}. \quad (3.1)$$

Como los divisores positivos de  $n$  son también

$$\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_{\tau(n)}} \quad (3.2)$$

de (3.1) y (3.2) obtenemos

$$P^2 = n^{\tau(n)}.$$

Luego el producto buscado es  $P = n^{\frac{\tau(n)}{2}}$

**3.10 Definición.** Una función aritmética se llama *multiplicativa* si satisface la condición:

$$f(mn) = f(m)f(n), \text{ para todo } m, n \text{ enteros positivos tales que } (m, n) = 1.$$

Si  $f(mn) = f(m)f(n)$  para todo  $m, n$  enteros positivos, entonces  $f$  se llama *completamente multiplicativa*.

**3.11 Teorema.** Las funciones  $\tau$  y  $\sigma$  son multiplicativas.

*Demostración.* Supongamos que  $m$  y  $n$  son enteros positivos y primos relativos. Podemos escribir

$$n = \prod_{i=1}^k p_i^{n_i} \quad \text{y} \quad m = \prod_{j=1}^r q_j^{m_j}$$

donde los  $p_i$  y los  $q_j$  son primos distintos.

Tenemos,

$$\tau(mn) = \prod_{j=1}^r (m_j + 1) \cdot \prod_{i=1}^k (n_i + 1) = \tau(m)\tau(n)$$

y

$$\sigma(mn) = \prod_{j=1}^r \frac{q_j^{m_j+1} - 1}{q_j - 1} \cdot \prod_{i=1}^k \frac{p_i^{n_i+1} - 1}{p_i - 1} = \sigma(m)\sigma(n)$$

como queríamos probar.  $\square$

Ninguna de estas funciones es completamente multiplicativa, por ejemplo,

$$3 = \tau(4) \neq \tau(2)\tau(2) = (2)(2) = 4,$$

$$7 = \sigma(4) \neq \sigma(2)\sigma(2) = (3)(3) = 9.$$

Como ejemplos de funciones completamente multiplicativas podemos citar las definidas por la ecuación  $f(n) = n^k$  con  $k$  fijo.

---

## Ejercicios 3.2

---

1. Hallar el número de divisores positivos de 4320 y calcular su suma.
2. Probar que si  $\tau(n) = 2$ , entonces  $n$  es un número primo.
3. Hallar el menor entero positivo con 15 divisores positivos.

4. Hallar el menor entero positivo con 24 divisores positivos.
5. Si  $n$  es un entero positivo mayor que 1, probar que la ecuación  $\tau(x) = n$  tiene infinitas soluciones.
6. Si  $m$  y  $n$  son enteros positivos tales que  $(m, n) > 1$ , probar que  $\tau(mn) < \tau(m)\tau(n)$ .
7. Resolver la ecuación  $\sigma(x) = 36$ .  
*Sugerencia:* Descomponer 36 en factores que se puedan expresar en la forma  $1 + p + p^2 + \dots + p^k$  con  $p$  primo y usar una fórmula conveniente.
8. Hallar dos enteros positivos  $n$  que cumplan la condición  $\sigma(n) = 2n$ .
9. Si  $n$  es un entero positivo probar que la ecuación  $\sigma(x) = n$  tiene un número finito de soluciones.
10. Probar que el número de divisores positivos de un entero positivo  $n$  es impar si y solo si  $n$  es un cuadrado perfecto.
11. Si  $n = \prod_{i=1}^k p_i^{n_i}$  es la representación canónica de un entero positivo  $n$ , hallar una fórmula para calcular  $\sum_{d|n} d^2$

### 3.3 Números perfectos, de Mersenne y de Fermat

**3.12 Definición.** Un entero positivo  $n$  se denomina un *número perfecto* si  $\sigma(n) = 2n$ , es decir si es igual a la suma de todos sus divisores propios.

Los primeros números perfectos son 6, 28, 496, 8128, 33550336, 8589869056, 137438691328, 2305843008139952128, que se pueden factorizar como sigue

$$6 = 2(2^2 - 1)$$

$$28 = 2^2(2^3 - 1)$$

$$496 = 2^4(2^5 - 1)$$

$$8128 = 2^6(2^7 - 1)$$

$$33550336 = 2^{12}(2^{13} - 1)$$

$$8589869056 = 2^{16}(2^{17} - 1)$$

$$137438691328 = 2^{18}(2^{19} - 1)$$

$$2305843008139952128 = 2^{30}(2^{31} - 1)$$

La lista anterior nos sugiere que todo número perfecto par es de forma  $2^{p-1}(2^p - 1)$  donde ambos  $p$  y  $2^p - 1$  son números primos. Euclides en su libro IX de los *Elementos* demostró que todo número de esta forma es efectivamente un número perfecto, y Euler 2000 años más tarde demostró que todo número perfecto par tiene la forma mencionada.

**3.13 Teorema.** *Si  $2^p - 1$  es un número primo, entonces el número  $n = 2^{p-1}(2^p - 1)$  es perfecto.*

*Demostración.* Sea  $n = 2^{p-1}(2^p - 1)$  donde  $2^p - 1$  es primo. Entonces

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1}(2^p - 1)) \\ &= \sigma(2^{p-1})\sigma(2^p - 1) \\ &= (2^p - 1)/(2 - 1) \cdot (2^p - 1 + 1) \\ &= 2^p(2^p - 1) \\ &= 2n,\end{aligned}$$

por lo tanto  $n$  es un número perfecto.  $\square$

Demostremos ahora el recíproco.

**3.14 Teorema.** *Si  $n$  es un número perfecto par, entonces  $n$  es de la forma  $2^{p-1}(2^p - 1)$  donde  $2^p - 1$  es primo.*

*Demostración.* Supongamos que  $n$  es un número perfecto par. Podemos escribir  $n = 2^{p-1}r$  con  $p > 1$  y  $r$  impar positivo. Como  $n$  es perfecto tenemos

$$\begin{aligned}2n = 2^p r &= \sigma(n) \\ &= \sigma(2^{p-1})\sigma(r) \\ &= \frac{(2^p - 1)}{(2 - 1)}\sigma(r) \\ &= (2^p - 1)\sigma(r).\end{aligned}$$

Por lo tanto

$$\sigma(r) = 2^p \frac{r}{2^p - 1} = r + \frac{r}{2^p - 1} \quad (3.3)$$

Como  $2^p r = (2^p - 1)\sigma(r)$ , entonces  $(2^p - 1) \mid 2^p r$ , y puesto que  $(2^p - 1, 2^p) = 1$  tenemos que  $(2^p - 1) \mid r$  y en consecuencia  $\frac{r}{2^p - 1} \mid r$ . Como  $\sigma(r)$  es la suma

de todos los divisores positivos de  $r$ , se sigue de (3.3) que  $r$  tiene únicamente dos divisores positivos y que

$$\frac{r}{2^p - 1} = 1.$$

Luego  $r = 2^p - 1$  es primo y  $n$  es de la forma  $n = 2^{p-1}(2^p - 1)$ , como queríamos probar.  $\square$

**3.15 Teorema.** *Si un número de la forma  $2^p - 1$  es primo, entonces  $p$  es primo.*

*Demostración.* Supongamos que  $p$  no es primo es decir  $p = rs$  con  $1 < r, s < p$ . Por lo tanto

$$2^p - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \dots + 1)$$

de donde se deduce que  $2^p - 1$  no es primo. Esto contradice nuestra hipótesis, luego  $p$  debe ser primo.  $\square$

Los números de la forma  $2^p - 1$  donde  $p$  es primo se llaman *números de Mersenne* y se representan por  $M_p$ , en honor al monje francés Marin Mersenne (1588,1648) quien los estudió detalladamente en 1644 en su libro *Cogitata Physica-Mathematica*.

Los números de Mersenne que son primos se denominan primos de Mersenne y los primeros treinta y ocho<sup>1</sup> ocurren para  $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593$ . Éste último con más de dos millones de dígitos.

Un problema abierto es determinar si existen o no infinitos primos de Mersenne y por lo tanto infinitos números perfectos. Los dos últimos primos de Mersenne conocidos hasta la fecha son  $2^{13466917} - 1$  y  $2^{20996011} - 1$ ; fueron encontrados por Michael Cameron, el 14 de noviembre de 2001 y por Michael Shafer, el 17 de noviembre de 2003, respectivamente, en su trabajo dentro del proyecto de investigación *GIMPS* (Great Internet Mersenne Prime Search). El último de estos números tiene 6329430 dígitos y su escritura ocuparía un texto similar al que Ud. está leyendo.

---

<sup>1</sup>a abril de 2004.

Otro problema abierto es determinar si existe algún número perfecto impar. Todo lo que se sabe sobre este problema es que si existe algún número perfecto impar este debe ser mayor que  $10^{300}$ .

Fermat estudió los números de la forma  $2^{2^n} + 1$  para  $n = 0, 1, 2, \dots$  llamados *números de Fermat* y conjeturó en 1650 que siempre eran primos. La conjetura resulta cierta para los cinco primeros números de Fermat que son 3, 5, 17, 257 y 65537, sin embargo Euler demostró en 1732 que el sexto número de Fermat no es primo y se puede factorizar como

$$2^{2^5} + 1 = 2^{32} + 1 = (641)(6700417).$$

Hasta la fecha, no se conoce ningún *primo de Fermat* mayor que 65537. ¿Sólo hay cinco números primos de Fermat 3, 5, 17, 257 y 65537? ¿Existen infinitos primos de Fermat?

Es interesante mencionar que Gauss demostró que si  $p$  es un primo de Fermat entonces se puede construir con regla y compás un polígono regular de  $p$  lados. Más generalmente en un curso de Álgebra Abstracta, se demuestra el siguiente resultado: “*Se puede construir con regla y compás un polígono regular de  $n$  lados si y solo si todos los primos impares que dividen a  $n$  son primos de Fermat cuyos cuadrados no dividen a  $n$ .*”

---

## Ejercicios 3.3

---

1. Probar que todo número perfecto par termina en 6 o en 8.
2. Probar que ninguna potencia de un número primo es un número perfecto.
3. Probar que todo número perfecto par se puede escribir en la forma  $1 + 2 + 3 + \dots + n$  para algún entero positivo  $n$ .
4. Probar que un cuadrado perfecto no puede ser un número perfecto.

5. Sean  $a$  y  $n$  enteros positivos mayores que 1. Probar que si  $a^n - 1$  es primo entonces  $a = 2$  y  $n$  es primo.
6. Sean  $a$  y  $n$  enteros positivos mayores que 1. Probar que si  $a^n + 1$  es primo entonces  $a$  es par y  $n = 2^r$  para algún entero positivo  $r$ .
7. Si  $F_n$  representa el  $n$ -ésimo número de Fermat para  $n = 0, 1, \dots$  probar que  $F_0 F_1 \dots F_{n-1} + 2 = F_n$ .
8. Probar que si  $m$  y  $n$  son enteros no negativos diferentes, entonces  $(F_n, F_m) = 1$ .

### 3.4 La función $\Phi$ de Euler

**3.16 Definición.** Para cada entero positivo  $n$ , definimos  $\Phi(n)$  como el número de enteros positivos menores o iguales que  $n$  y primos relativos con  $n$ .

Como ejemplo tenemos la siguiente tabla de valores de  $\Phi(n)$

$n$ :	1	2	3	4	5	6	7	8	9	10
$\Phi(n)$ :	1	1	2	2	4	2	6	4	6	4

Algunas veces se designa a  $\Phi(n)$  con el nombre de *indicador* de  $n$  y con menos frecuencia con el de *totalizador* de  $n$ .

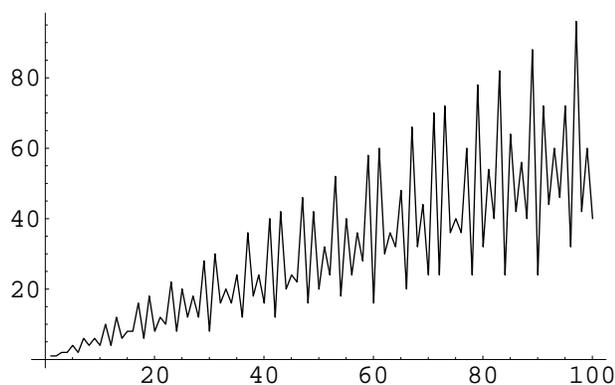


FIGURA 3.1. La función  $\Phi$  de Euler.

**3.17 Teorema.** Si  $p$  es un número primo y  $a$  es un entero positivo entonces

$$\Phi(p^a) = p^a - p^{a-1}.$$

*Demostración.* Los enteros positivos menores o iguales que  $p^a$  que no son primos relativos con  $p$  son precisamente los  $p^{a-1}$  múltiplos de  $p$ ,

$$1.p, 2.p, 3.p, \dots, p^{a-1}.p$$

Por lo tanto

$$\Phi(p^a) = p^a - p^{a-1}.$$

En particular, cuando  $a = 1$  obtenemos la fórmula

$$\Phi(p) = p - 1$$

para cada primo  $p$ . □

**3.18 Teorema.** Si  $(m, n) = 1$  entonces  $\Phi(mn) = \Phi(m)\Phi(n)$ .

*Demostración.* Si  $m = 1$  o  $n = 1$  el resultado es evidente. Luego podemos suponer que  $n$  y  $m$  son mayores que 1.

Supongamos que  $1 \leq x \leq mn$  con  $(x, mn) = 1$ . Por lo tanto  $(x, m) = 1$  y  $(x, n) = 1$  y por el algoritmo de la división podemos escribir

$$\begin{aligned} x &= qm + r, & 1 \leq r < m \\ x &= q'n + s, & 1 \leq s < n \end{aligned}$$

Como  $(x, m) = (r, m) = 1$  y  $(x, n) = (s, n) = 1$  según el Teorema 2.7, con cada  $x$  tal que  $1 \leq x \leq mn$  y  $(x, mn) = 1$  podemos asociar una pareja  $(r, s)$  tal que  $1 \leq r \leq m$  y  $(r, m) = 1$ ;  $1 \leq s \leq n$  y  $(s, n) = 1$ . En consecuencia por definición de  $\Phi$  tenemos

$$\Phi(mn) \leq \Phi(m)\Phi(n). \tag{3.4}$$

Recíprocamente, supongamos que  $(r, s)$  es una pareja de números tales que  $1 \leq r \leq m$ ,  $(r, m) = 1$  y  $1 \leq s \leq n$ ,  $(s, n) = 1$ . Como por hipótesis  $(m, n) = 1$  existen enteros  $x_0, y_0$  tales que

$$1 = mx_0 + ny_0$$

luego

$$r - s = mu + nv$$

donde  $u, v$  son enteros.

Dividiendo  $-u$  por  $n$  tenemos

$$-u = an + q, \quad 0 \leq q < n$$

y por lo tanto

$$\begin{aligned} r - s &= (-m)(-u) + nv \\ &= (-m)(an + q) + nv \\ &= -qm + (v - am)n \\ &= -qm + q'n, \end{aligned}$$

de donde

$$qm + r = q'n + s$$

Si llamamos  $x = qm + r = q'n + s$  tenemos:

1.  $1 \leq x \leq mn$ , ya que claramente  $x \geq 1$  y como  $q \leq n - 1$ ,  $r \leq m$  entonces  $qm + r \leq (n - 1)m + m = nm$ .
2. Por el Teorema 2.18,  $(x, mn) = 1$  ya que  $(x, m) = (r, m) = 1$  y  $(x, n) = (s, n) = 1$  según el Teorema 2.7.

De esta forma, con cada pareja de números  $(r, s)$  tales que  $1 \leq r \leq m$ ,  $(r, m) = 1$  y  $1 \leq s \leq n$ ,  $(s, n) = 1$ , podemos asociar un número  $x$  tal que  $1 \leq x \leq mn$  y  $(x, mn) = 1$ . En consecuencia se sigue que

$$\Phi(m)\Phi(n) \leq \Phi(mn) \tag{3.5}$$

De (3.4) y (3.5) concluimos que

$$\Phi(mn) = \Phi(m)\Phi(n). \quad \square$$

La aplicación del teorema anterior nos permite calcular  $\Phi(n)$  a partir de la descomposición canónica de  $n$  como producto de primos.

**3.19 Teorema.** Si  $n = \prod_{i=1}^k p_i^{n_i}$  es la representación canónica de un entero positivo  $n$ , entonces

$$\Phi(n) = \prod_{i=1}^k (p_i^{n_i} - p_i^{n_i-1})$$

o bien,

$$\Phi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

*Demostración.* Como  $\Phi$  es una función multiplicativa tenemos que

$$\begin{aligned} \Phi(n) &= \prod_{i=1}^k \Phi(p_i^{n_i}) \\ &= \prod_{i=1}^k (p_i^{n_i} - p_i^{n_i-1}). \end{aligned}$$

De otra parte,

$$\begin{aligned} \prod_{i=1}^k (p_i^{n_i} - p_i^{n_i-1}) &= \prod_{i=1}^k p_i^{n_i} \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^k p_i^{n_i} \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \\ &= n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

luego también

$$\Phi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

□

**3.20 Ejemplo.** Como  $18900 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7$ , tenemos

$$\begin{aligned} \Phi(18900) &= 18900 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) \\ &= 18900 \frac{1}{2} \frac{2}{3} \frac{4}{5} \frac{6}{7} \\ &= 4320. \end{aligned}$$

**3.21 Ejemplo.** Veamos que si  $3 \mid n$  entonces  $\Phi(3n) = 3\Phi(n)$ .

En efecto, como  $3 \mid n$ ,  $n$  tiene la forma  $n = 3^a m$  donde  $a \geq 1$  y  $(m, 3) = 1$ . Luego

$$\begin{aligned}\Phi(3n) &= \Phi(3^{a+1}m) \\ &= \Phi(3^{a+1})\Phi(m) \\ &= (3^{a+1} - 3^a)\Phi(m) \\ &= 3(3^a - 3^{a-1})\Phi(m) \\ &= 3\Phi(3^a)\Phi(m) \\ &= 3\Phi(3^a m) \\ &= 3\Phi(n).\end{aligned}$$

**3.22 Teorema.** Si  $n > 1$ , la suma de los enteros positivos menores o iguales que  $n$  y primos relativos con  $n$  es  $\frac{1}{2}n\Phi(n)$ .

*Demostración.* Sean  $m_1, m_2, m_3, \dots, m_{\Phi(n)}$  los enteros positivos menores o iguales que  $n$  y primos relativos con  $n$ . Su suma es

$$S = m_1 + m_2 + m_3 + \dots + m_{\Phi(n)}. \quad (3.6)$$

Como  $(m, n) = 1$  si y solo si  $(n - m, n) = 1$ , podemos expresar también todos los enteros positivos menores o iguales que  $n$  y primos relativos con  $n$  en la forma  $n - m_1, n - m_2, \dots, n - m_{\Phi(n)}$ , y por lo tanto su suma es

$$S = (n - m_1) + (n - m_2) + \dots + (n - m_{\Phi(n)}) \quad (3.7)$$

Sumando (3.6) y (3.7) tenemos,

$$\begin{aligned}2S &= n + n + \dots + n \quad (\Phi(n) \text{ veces}) \\ &= n\Phi(n)\end{aligned}$$

de donde

$$S = \frac{1}{2}n\Phi(n). \quad \square$$

**3.23 Teorema.** Para cada entero positivo  $n$ , tenemos

$$\sum_{d \mid n} \Phi(d) = n.$$

*Demostración.* Consideremos primero el número  $p^k$  cuyos divisores son  $1, p, p^2, \dots, p^k$ . Por el Teorema 3.17 tenemos que,

$$\begin{aligned} & \Phi(1) + \Phi(p) + \Phi(p^2) + \dots + \Phi(p^k) \\ &= 1 + (p-1) + (p^2-p) + \dots + (p^{k-1} - p^{k-2}) + (p^k - p^{k-1}) = p^k. \end{aligned}$$

Por lo tanto, si  $n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$  donde los primos son distintos, tenemos

$$n = \prod_{i=1}^r (1 + \Phi(p_i) + \dots + \Phi(p_i^{n_i})).$$

Desarrollando el producto y aplicando el Teorema 3.18, vemos que el producto consiste en la suma de todos los términos de la forma

$$\Phi(p_1^{t_1}) \Phi(p_2^{t_2}) \dots \Phi(p_r^{t_r}) = \Phi(d)$$

donde  $d = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$  con  $0 \leq t_i \leq n_i$  recorre precisamente todos los divisores de  $n$ , en virtud del Teorema 2.43. De esta forma hemos probado la fórmula deseada.  $\square$

Veamos como resolver la ecuación  $\Phi(x) = m$ . Si  $m = 1$ , las soluciones de la ecuación  $\Phi(x) = m$  son precisamente  $x = 1$  y  $x = 2$ . Por el ejercicio 4 de la sección 3.4, si  $m$  es un número impar mayor que 1 la ecuación no tiene solución. Estudiemos el caso cuando  $m$  es un entero par.

Supongamos que  $x = \prod_{i=1}^k p_i^{r_i}$  es la representación canónica de un entero positivo  $x$  que satisface la ecuación  $\Phi(x) = m$ . Por el Teorema 3.19 tenemos,

$$\prod_{i=1}^k (p_i^{r_i} - p_i^{r_i-1}) = m,$$

o sea

$$\prod_{i=1}^k p_i^{r_i-1} (p_i - 1) = m.$$

Por lo tanto si establecemos que

$$d_i = p_i - 1, \tag{3.8}$$

tenemos que

$$\prod_{i=1}^k p_i^{r_i-1} d_i = m \tag{3.9}$$

Podemos escribir (3.9) en la forma

$$\prod_{i=1}^k p_i^{r_i} \frac{d_i}{p_i} = m,$$

o sea

$$x \prod_{i=1}^k \frac{d_i}{p_i} = m,$$

de donde

$$x = \frac{m}{\prod_{i=1}^k d_i} \cdot \prod_{i=1}^k p_i. \quad (3.10)$$

Las ecuaciones (3.8), (3.9) y (3.10) establecen las condiciones siguientes sobre los  $d_i$ , que nos permiten determinar los valores del entero  $x$ :

1. Cada  $d_i + 1$  es un número primo.
2. Cada  $d_i$  es un divisor de  $m$ .
3. El número  $\frac{m}{\prod_{i=1}^k d_i}$  debe ser un entero cuya representación canónica solo puede contener primos que aparezcan en el producto  $\prod_{i=1}^k p_i$ .

**3.24 Ejemplo.** Resolvamos la ecuación  $\Phi(x) = 36$ .

Los divisores positivos de 36 son 1, 2, 3, 4, 6, 9, 12, 18 y 36. Los posibles valores de  $d_i$  son aquellos para los cuales  $d_i + 1$  es un primo, es decir 1, 2, 4, 6, 12, 18 y 36. Formamos los productos  $\prod d_i$  que sean menores o iguales que 36 y obtenemos 1, 2, 4, 6, 12, 18, 1·2, 1·4, 1·6, 1·12, 1·18, 1·36, 2·4, 2·6, 2·12, 2·18, 4·6, 1·2·4, 1·2·6, 1·2·12, 1·2·18, 1·4·6

Eliminamos de esta lista aquellos números para los cuales  $\frac{m}{\prod d_i} = \frac{36}{\prod d_i}$  no es un entero, es decir eliminamos 2·4, 2·12, 4·6, 1·2·4, 1·2·12 y 1·4·6. Con

los productos restantes hacemos una tabla en la forma siguiente:

$\prod d_i$	$\frac{36}{\prod d_i}$	$\prod p_i = \prod (d_i + 1)$	$x = \frac{36}{\prod d_i} \cdot \prod p_i$
1	$2^2 \cdot 3^2$	2	No
2	$2 \cdot 3^2$	3	No
4	$3^2$	5	No
6	$2 \cdot 3$	7	No
12	3	13	No
18	2	19	No
36	1	37	37
1·2	$2 \cdot 3^2$	2·3	108
1·4	$3^2$	2·5	No
1·6	$2 \cdot 3$	2·7	No
1·12	3	2·13	No
1·18	2	2·19	76
1·36	1	2·37	74
2·6	3	3·7	63
2·18	1	3·19	57
1·2·6	3	2·3·7	126
1·2·18	1	2·3·19	114

En la tabla eliminamos aquellos números donde  $\frac{36}{\prod d_i}$  contiene primos que no aparecen en  $\prod p_i$ , los hemos marcado con la palabra No. Los demás valores de  $x$  son las soluciones de la ecuación  $\Phi(x) = 36$ . Según la tabla las soluciones son 37, 108, 76, 74, 63, 57, 126 y 114.

---

## Ejercicios 3.4

---

1. Probar que  $\Phi(n^2) = n\Phi(n)$  para todo entero positivo  $n$ .
2. Probar que si  $n$  es impar  $\Phi(2n) = \Phi(n)$  y si  $n$  es par  $\Phi(2n) = 2\Phi(n)$ .

3. Hallar todos los enteros positivos  $n$ , que satisfacen la condición  $\Phi(2n) > \Phi(n)$ .
4. Probar que si  $n > 2$  entonces  $\Phi(n)$  es par.
5. Probar que si  $3 \nmid n$  entonces  $\Phi(3n) = 2\Phi(n)$ .
6. Hallar todos los enteros positivos  $n$  que satisfacen la condición  $\Phi(n) = n/2$ .
7. Hallar el número de enteros menores que 8400 y primos relativos con 4200.
8. Hallar una fórmula para calcular  $\Phi(n)$  cuando  $n$  es un número perfecto par.
9. Probar que el número de fracciones irreducibles, positivas, menores o iguales que 1 y con denominador menor o igual que  $n$  es  $\Phi(1) + \Phi(2) + \Phi(3) + \cdots + \Phi(n)$ .
10. Si todo primo que divide a  $n$ , también divide a  $m$ , probar que  $\Phi(nm) = n\Phi(m)$ .
11. Probar el Teorema 3.23 usando inducción sobre el número de factores primos que aparecen en la representación canónica de  $n$ .
12. Probar que existen infinitos primos utilizando el Teorema 3.19.
13. Si  $d = (m, n)$  probar que  $\Phi(mn) = \frac{d\Phi(m)\Phi(n)}{\Phi(d)}$ .
14. Resolver las ecuaciones  $\Phi(x) = 18$ ,  $\Phi(x) = 24$ ,  $\Phi(x) = 72$ , y  $\Phi(x) = 90$ .
15. Probar que  $\Phi(x) = 2p$  no tiene solución si  $p$  es primo y  $2p + 1$  es compuesto.

### 3.5 Funciones multiplicativas

Recordemos que una función aritmética se llama multiplicativa si  $f(mn) = f(m)f(n)$  para cada par de enteros positivos tales que  $(m, n) = 1$ . Estudiemos ahora algunas propiedades comunes a todas las funciones multiplicativas.

**3.25 Teorema.** Si  $f$  es una función multiplicativa diferente de la función cero, entonces  $f(1) = 1$ .

*Demostración.* Como  $f$  es diferente de la función cero, existe un entero positivo  $n$  tal que  $f(n) \neq 0$ . Como  $f$  es multiplicativa y  $(n, 1) = 1$  entonces  $f(n) = f(1 \cdot n) = f(1) \cdot f(n)$  y por lo tanto  $f(1) = 1$ .  $\square$

El producto  $fg$  y el cociente  $f/g$  de dos funciones aritméticas se definen mediante las fórmulas

$$(fg)(n) = f(n)g(n)$$

y

$$(f/g)(n) = f(n)/g(n), \text{ si } g(n) \neq 0$$

Es evidente que si  $f$  y  $g$  son funciones multiplicativas entonces  $fg$  y  $f/g$  también lo son.

**3.26 Teorema.** Supongamos que  $f$  es una función aritmética tal que  $f(1) = 1$ . Entonces  $f$  es multiplicativa si y solamente si

$$f\left(\prod_{i=1}^k p_i^{n_i}\right) = \prod_{i=1}^k f(p_i^{n_i})$$

para todos los primos  $p_i$  y todos los enteros  $n_i \geq 1$ .

*Demostración.* La demostración se sigue directamente de las definiciones usando el PIM y la dejamos como ejercicio.  $\square$

La utilidad del teorema anterior es que, reduce el cálculo del valor de una función multiplicativa en un número  $n$  arbitrario, al problema de calcularlo en las potencias de sus factores primos.

**3.27 Ejemplo.** Si sabemos de antemano que la función  $\sigma$  es multiplicativa, usando el teorema anterior tenemos que su valor en  $n = \prod_{i=1}^k p_i^{n_i}$  es,

$$\sigma(n) = \prod_{i=1}^k \sigma(p_i^{n_i})$$

y como

$$\sigma(p_i^{n_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{n_i} = \frac{p_i^{n_i+1} - 1}{p_i - 1}$$

obtenemos que

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{n_i+1} - 1}{p_i - 1}$$

como habíamos demostrado anteriormente.

**3.28 Teorema.** *Si  $f$  y  $g$  son funciones multiplicativas, también lo es la función  $F$  definida por*

$$F(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

*Demostración.* Sean  $m$  y  $n$  enteros positivos tales que  $(m, n) = 1$ . Por el ejercicio 18 de la sección de ejercicios 2.1, sabemos que  $d \mid mn$  si y solamente si  $d = d_1d_2$  donde  $d_1 \mid m$  y  $d_2 \mid n$ , donde además,  $(d_1, d_2) = 1$  y  $(m/d_1, n/d_2) = 1$ .

Por lo tanto tenemos,

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1d_2)g\left(\frac{mn}{d_1d_2}\right) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right) \sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right) \\ &= F(m)F(n). \end{aligned}$$

Así,  $F$  es una función multiplicativa. □

Un caso especial e importante del teorema anterior se obtiene cuando  $g$  es la función constante 1, es decir cuando  $g(n) = 1$  para todo entero positivo  $n$ . Concretamente tenemos:

**3.29 Corolario.** *Si  $f$  es una función multiplicativa entonces la función  $F$  definida por*

$$F(n) = \sum_{d|n} f(d)$$

*es también una función multiplicativa.*

**3.30 Ejemplo.** Como la función definida por  $f(d) = d^k$  donde  $k$  es un entero positivo es multiplicativa, por el corolario, la función definida por

$$\sigma_k(n) = \sum_{d|n} d^k$$

es también multiplicativa.

$\sigma_k(n)$  representa la suma de las potencias  $k$ -ésima de los divisores positivos de  $n$ . En particular  $\sigma_1(n) = \sigma(n)$ . Por el Teorema 3.26 si  $n = \prod_{i=1}^r p_i^{n_i}$  entonces,

$$\sigma_k(n) = \prod_{i=1}^r \sigma_k(p_i^{n_i})$$

y como

$$\sigma_k(p_i^{n_i}) = 1^k + p_i^k + p_i^{2k} + \cdots + p_i^{n_i k} = \frac{p_i^{(n_i+1)k} - 1}{p_i^k - 1}$$

concluimos que

$$\sigma_k(n) = \prod_{i=1}^r \frac{p_i^{(n_i+1)k} - 1}{p_i^k - 1}.$$

---

## Ejercicios 3.5

---

1. Demostrar el Teorema 3.26.
2. Si  $f$  y  $g$  son funciones multiplicativas, probar que  $fg$  y  $f/g$  son funciones multiplicativas. Suponga que el cociente esta bien definido.
3. Si  $f$  es multiplicativa y  $m \mid n$ , y  $(m, \frac{n}{m}) = 1$ . Probar que

$$f\left(\frac{n}{m}\right) = \frac{f(n)}{f(m)}$$

4. Si  $f$  es multiplicativa y  $n = \prod_{i=1}^k p_i^{n_i}$ , probar que

$$\sum_{d|n} f(d) = \prod_{i=1}^k (1 + f(p_i) + f(p_i^2) + \cdots + f(p_i^{n_i}))$$

5. Probar que  $\sum_{d|n} f(d) = \sum_{d|n} f(\frac{n}{d})$

6. Probar que  $\sum_{d|n} (\frac{1}{d}) = \frac{\sigma(n)}{n}$  para todo entero positivo  $n$ .

7. Si  $n$  es un número perfecto par, probar que  $\sum_{d|n} (\frac{1}{d}) = 2$ .

8. Si  $k \geq 1$ . Probar que  $\sigma_k(n)$  es impar si y solo si  $n$  es un cuadrado perfecto o el doble de un cuadrado perfecto.

9. Para  $n \geq 1$ , sea  $\tau_2(n) = \sum_{d|n} \tau(d)$ . Probar que  $\tau_2(n)$  es multiplicativa y encontrar una fórmula para  $\tau_2(n)$  en términos de la representación canónica de  $n$ .

10. Demostrar que  $d | n$  y  $b | \frac{n}{d}$  si y solo si  $b | n$  y  $d | \frac{n}{b}$ .

11. Probar que

$$\sum_{d|n} \sum_{b|\frac{n}{d}} f(d)g(b) = \sum_{b|n} \sum_{d|\frac{n}{b}} f(d)g(b)$$

12. Sean  $A = \{(d, c) : d | n \text{ y } c | d\}$  y  $B = \{(tc, c) : c | n \text{ y } t | (n/c)\}$ . Probar que  $A = B$ .

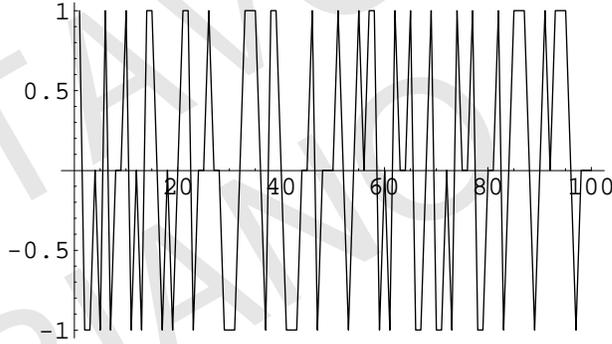
*Sugerencia:* Hacer  $d = tc$ .

### 3.6 La fórmula de inversión de Möbius

**3.31 Definición.** La función  $\mu$  de Möbius (fue introducida por Möbius (1832), y el primero en usar la notación  $\mu$  fue Mertens (1874)) se define mediante las ecuaciones,

$$\mu(1) = 1,$$

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n = p_1 p_2 \cdots p_k \text{ donde los } p_i \text{ son primos diferentes,} \\ 0 & \text{si } p^2 | n \text{ para algún primo } p. \end{cases}$$

FIGURA 3.2. La función  $\mu$ .

Como ejemplo tenemos la siguiente tabla:

$n$ :	1	2	3	4	5	6	7	8	9	10	11
$\mu(n)$ :	1	-1	-1	0	-1	1	-1	0	0	1	-1

**3.32 Teorema.** *La función  $\mu$  es multiplicativa y para todo  $n \geq 1$  se tiene que*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases} \quad (3.11)$$

*Demostración.* Si  $m = 1$  o  $n = 1$  se tiene inmediatamente que  $\mu(mn) = \mu(m) \cdot \mu(n)$ . Sean  $m$  y  $n$  enteros positivos tales que  $(m, n) = 1$  con representaciones canónicas

$$m = \prod_{i=1}^k p_i^{m_i} \text{ y } n = \prod_{j=1}^t q_j^{n_j}.$$

La representación canónica de  $mn$  es

$$mn = p_1^{m_1} \dots p_k^{m_k} q_1^{n_1} \dots q_t^{n_t}.$$

Si algún  $m_i > 1$  o algún  $n_j > 1$  entonces  $\mu(mn) = 0 = \mu(m)\mu(n)$ . Si todos los  $m_i$  y todos los  $n_j$  son iguales a 1 entonces  $\mu(m) = (-1)^k$ ,  $\mu(n) = (-1)^t$  y  $\mu(mn) = (-1)^{k+t}$ ; Así nuevamente  $\mu(mn) = \mu(m)\mu(n)$ . Por lo tanto hemos demostrado que  $\mu$  es una función multiplicativa.

La fórmula (3.11) es evidente si  $n = 1$ . Supongamos que  $n > 1$  y que la representación canónica de  $n$  es  $n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ . Los únicos términos no nulos en la suma ocurren cuando  $d = 1$  o cuando  $d$  es un producto de primos diferentes. Por lo tanto,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \dots + \mu(p_k) + \mu(p_1 p_2) + \dots + \mu(p_{k-1} p_k) + \\ &\quad + \dots + \mu(p_1 p_2 \dots p_k) \\ &= 1 + \binom{k}{1} (-1) + \binom{k}{2} (-1)^2 + \dots + \binom{k}{k} (-1)^k \\ &= (1 - 1)^k = 0. \end{aligned}$$

□

Como consecuencia de este teorema, podemos expresar una función multiplicativa  $f$  en términos de la función  $F$  definida en el Corolario 3.29, de la siguiente forma:

**3.33 Teorema (Fórmula de inversión de Möbius).** *Si  $f$  es una función numérica y  $F(n) = \sum_{d|n} f(d)$  para todo  $n \geq 1$ , entonces*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

*Demostración.* Tenemos,

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \left[ \mu(d) \sum_{b|\frac{n}{d}} f(b) \right] \\ &= \sum_{d|n} \sum_{b|\frac{n}{d}} \mu(d) f(b) \\ &= \sum_{b|n} \sum_{d|\frac{n}{b}} \mu(d) f(b) \quad (\text{¿por qué?}) \\ &= \sum_{b|n} \left[ f(b) \sum_{d|\frac{n}{b}} \mu(d) \right] \\ &= f(n), \end{aligned}$$

ya que por el teorema anterior, la suma interior en la última expresión es igual a cero, excepto en el caso en el cual  $b = n$ , cuando vale 1. □

Es interesante observar que el recíproco de este teorema también es cierto. Concretamente tenemos:

**3.34 Teorema.** *Si  $f$  y  $F$  son funciones numéricas tales que*

$$f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) \text{ para todo } n \geq 1,$$

*entonces  $F(n) = \sum_{d|n} f(d)$ .*

*Demostración.* Tenemos

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} \left[ \sum_{b|d} \mu(b)F\left(\frac{d}{b}\right) \right] \\ &= \sum_{d|n} \left[ \sum_{c|d} \mu\left(\frac{d}{c}\right) F(c) \right]. \end{aligned}$$

Haciendo  $d = tc$  y usando el ejercicio 12 de la sección 3.5, la última suma es igual a,

$$\begin{aligned} &= \sum_{tc|n} \sum_{c|n} \mu\left(\frac{tc}{c}\right) F(c) \\ &= \sum_{c|n} \sum_{tc|n} \mu(t)F(c) \\ &= \sum_{c|n} \sum_{t|\frac{n}{c}} \mu(t)F(c) \\ &= \sum_{c|n} \left[ F(c) \sum_{t|\frac{n}{c}} \mu(t) \right] \\ &= F(n). \quad (\text{por el Teorema 3.32}) \end{aligned}$$

□

En los dos últimos teoremas no se requiere que  $f$  y  $F$  sean funciones multiplicativas, sin embargo tenemos

**3.35 Teorema.** *Supongamos que  $f$  y  $F$  son funciones numéricas tales que  $F(n) = \sum_{d|n} f(d)$ . Tenemos:*

1. Si  $F$  es multiplicativa entonces  $f$  también es multiplicativa.
2. Si  $f$  es multiplicativa entonces  $F$  también es multiplicativa.

*Demostración.* 1. Por la fórmula de inversión de Möbius tenemos

$$f(n) = \sum_{d|n} \mu(d)F\left(\frac{n}{d}\right)$$

y como  $\mu$  y  $F$  son multiplicativas, se sigue del Teorema 3.28 que  $f$  también es multiplicativa.

2. Es precisamente el Corolario 3.29. □

Como aplicación de los resultados anteriores, vamos a deducir nuevamente las propiedades de la función de Euler.

**3.36 Lema.** Si  $m \mid n$  el número de enteros en el conjunto  $S = \{1, 2, 3, \dots, n\}$  que tienen con  $n$  como máximo común divisor a  $m$  es  $\Phi\left(\frac{n}{m}\right)$ .

*Demostración.* Los enteros en el conjunto  $S$  que son divisibles por  $m$  son precisamente

$$m, 2m, \dots, \left(\frac{n}{m}\right)m.$$

De otra parte sabemos que

$$(km, n) = (km, \left(\frac{n}{m}\right)m) = m(k, \left(\frac{n}{m}\right))$$

luego  $(km, n) = m$  si y solamente si  $(k, \left(\frac{n}{m}\right)) = 1$ . Por lo tanto el número de enteros en  $S$  que tienen con  $n$  como máximo común divisor a  $m$ , es el número de enteros en el conjunto  $\{1, 2, \dots, \left(\frac{n}{m}\right)\}$  que son primos relativos con  $\frac{n}{m}$ , es decir  $\Phi\left(\frac{n}{m}\right)$ . □

A continuación, daremos una demostración del Teorema 3.23 sin usar que  $\Phi$  es una función multiplicativa.

**3.37 Teorema.** Para todo entero positivo  $n$ , tenemos

$$\sum_{d|n} \Phi(d) = n.$$

*Demostración.* Sean  $d_1, d_2, \dots, d_{\tau(n)}$  los divisores positivos de  $n$ , y sean  $m_1, m_2, \dots, m_{\tau(n)}$  enteros positivos tales que

$$n = d_1 m_1 = d_2 m_2 = \dots = d_{\tau(n)} m_{\tau(n)}.$$

Cada entero en el conjunto  $S = \{1, 2, \dots, n\}$  tiene con  $n$  un único máximo común divisor que es alguno de los  $m_i$ . Por el lema anterior, el número de enteros en el conjunto  $S$  que tienen con  $n$  como máximo común divisor a  $m_i$  es  $\Phi(n/m_i)$ . Por lo tanto

$$n = \sum_{i=1}^{\tau(n)} \Phi(n/m_i) = \sum_{i=1}^{\tau(n)} \Phi(d_i) = \sum_{d|n} \Phi(d). \quad \square$$

Veamos ahora una nueva demostración del Teorema 3.18.

**3.38 Teorema.** *La función  $\Phi$  es multiplicativa.*

*Demostración.* Sabemos que la función  $F(n) = n$  es multiplicativa. Por el teorema anterior tenemos que

$$F(n) = n = \sum_{d|n} \Phi(d),$$

y por el Teorema 3.35, concluimos que  $\Phi$  es una función multiplicativa.

Si aplicamos la fórmula de inversión de Möbius a la fórmula

$$F(n) = n = \sum_{d|n} \Phi(d)$$

obtenemos que,

$$\Phi(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

En particular si  $n = p^a$  con  $p$  primo tenemos,

$$\begin{aligned} \Phi(p^a) &= p^a \sum_{d|p^a} \frac{\mu(d)}{d} \\ &= p^a \left[ \frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \dots + \frac{\mu(p^a)}{p^a} \right] \\ &= p^a \left( 1 - \frac{1}{p} \right) \quad (\text{por definición de } \mu) \\ &= p^a - p^{a-1}. \end{aligned}$$

Si la representación canónica de un entero positivo  $n$  es  $n = \prod_{i=1}^k p_i^{n_i}$ , como  $\Phi$  es multiplicativa, por el Teorema 3.26, tenemos que

$$\begin{aligned}\Phi(n) &= \prod_{i=1}^k \Phi(p_i^{n_i}) \\ &= \prod_{i=1}^k (p_i^{n_i} - p_i^{n_i-1})\end{aligned}$$

y hemos obtenido una nueva demostración del Teorema 3.19.  $\square$

---

## Ejercicios 3.6

---

1. Si  $n$  es un entero positivo probar que  $\prod_{i=0}^3 \mu(n+i) = 0$ .
2. Si  $n = \prod_{i=1}^k p_i^{n_i}$  es la representación canónica de  $n$ , probar que

$$\sum_{d|n} \mu(d)\tau(d) = (-1)^k.$$

3. Hallar una fórmula para evaluar  $\sum_{d|n} \mu(d)\sigma(d)$  en término de la representación canónica de  $n$ .
4. Si  $f(n) = \sum_{d|n} \mu(d)\Phi(d)$ , hallar una fórmula para evaluar  $f(n)$  en términos de la representación canónica de  $n$ .
5. Probar que para todo entero positivo  $n$ , se tiene que

$$\frac{n}{\Phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\Phi(d)}.$$

*Sugerencia:* Aplicar el Teorema 3.26 a la función multiplicativa  $f(n) = \sum_{d|n} \frac{\mu^2(d)}{\Phi(d)}$ .

6. Si  $n = \prod_{i=1}^k p_i^{n_i}$  es la representación canónica de  $n$ , probar que

$$\sum_{d|n} |\mu(d)| = 2^k.$$

7. Si  $f$  es una función multiplicativa y  $n = \prod_{i=1}^k p_i^{n_i}$ , probar que

$$\sum_{d|n} \mu(d)f(d) = \prod_{i=1}^k [1 - f(p_i)].$$

8. Deducir una fórmula para calcular  $\sum_{d|n} \mu(d)/d$ .

9. Probar que para todo entero positivo  $n$  se tiene que

$$\sum_{d|n} \mu(d)\tau(n/d) = 1.$$

10. Si para todo entero positivo  $n$  se tiene que  $n^2 = \sum_{d|n} g(d)$ , hallar una fórmula para evaluar  $g(n)$  en términos de la representación canónica de  $n$ .

11. Si  $\frac{1}{n} = \sum_{d|n} f(d)$ , hallar una fórmula para evaluar  $f(n)$  en términos de la representación canónica de  $n$ .

---

## Congruencias

---

### 4.1 Definición y propiedades básicas

**4.1 Definición.** Sean  $a$  y  $b$  enteros cualesquiera y  $n$  un entero positivo. Si  $n \mid (a - b)$  decimos que  $a$  y  $b$  son *congruentes módulo  $n$*  y escribimos

$$a \equiv b \pmod{n}.$$

si  $a$  no es congruente con  $b$  módulo  $n$ , escribimos

$$a \not\equiv b \pmod{n}.$$

**4.2 Ejemplo.** 1.  $23 \equiv 11 \pmod{12}$ .

2.  $1 \equiv -1 \pmod{2}$ .

3. Para todo par de enteros  $a$  y  $b$ , tenemos  $a \equiv b \pmod{1}$ .

4. Si  $d \mid n$  y  $a \equiv b \pmod{n}$  entonces  $a \equiv b \pmod{d}$ .

5.  $17 \not\equiv 10 \pmod{4}$ .

6. Si  $n \mid a$  entonces  $a \equiv 0 \pmod{n}$  y recíprocamente.

En lo que sigue del capítulo,  $n$  representa un entero positivo fijo.

Si  $a$  es un entero, el residuo de dividirlo por  $n$  caracteriza el comportamiento de  $a$  módulo  $n$  en el siguiente sentido.

**4.3 Teorema.** *Dos enteros  $a$  y  $b$  son congruentes módulo  $n$  si y solo si tienen el mismo residuo al dividirlos por  $n$ .*

*Demostración.* Supongamos que  $a \equiv b \pmod{n}$  y sea  $r$  el residuo de dividir  $b$  por  $n$ . Entonces, existe un entero  $k$  tal que  $a - b = kn$  y además  $b = qn + r$  con  $0 \leq r < n$ . En consecuencia,

$$\begin{aligned} a &= b + kn = (qn + r) + kn \\ &= (q + k)n + r. \end{aligned}$$

Como  $(q + k)$  es un entero observamos que  $a$  y  $b$  tienen el mismo residuo al dividirlos por  $n$ .

Recíprocamente, supongamos que  $a$  y  $b$  tienen el mismo residuo al dividirlos por  $n$ . Tenemos entonces

$$\begin{aligned} a &= q_1n + r \\ b &= q_2n + r, \end{aligned}$$

con  $0 \leq r < n$ . En consecuencia, restando término a término tenemos  $a - b = (q_1 - q_2)n$ , es decir  $a \equiv b \pmod{n}$ .  $\square$

Directamente de la definición tenemos el resultado siguiente.

**4.4 Teorema.** *La congruencia módulo  $n$  es una relación de equivalencia sobre  $\mathbb{Z}$ .*

*Demostración.* 1. *Reflexiva.* Para cualquier entero  $a$ ,  $n \mid (a - a) = 0$  es decir  $a \equiv a \pmod{n}$ .

2. *Simétrica.* Si  $a \equiv b \pmod{n}$  entonces  $n \mid (a - b)$  y por lo tanto  $n \mid -(a - b) = b - a$ , luego  $b \equiv a \pmod{n}$ .

3. *Transitiva.* Si  $a \equiv b \pmod{n}$  y  $b \equiv c \pmod{n}$  entonces  $n \mid (a - b)$  y  $n \mid (b - c)$ , por lo tanto  $n \mid \{(a - b) + (b - c)\} = a - c$ , es decir  $a \equiv c \pmod{n}$ .  $\square$

El comportamiento de la congruencia respecto de las operaciones definidas en  $\mathbb{Z}$  se concreta en el siguiente teorema.

**4.5 Teorema.** Si  $a \equiv b \pmod{n}$  y  $c \equiv d \pmod{n}$  entonces

1. Para todo par de enteros  $r$  y  $s$ ,  $ar + cs \equiv br + ds \pmod{n}$ .
2.  $a + c \equiv b + d \pmod{n}$ .
3.  $a - c \equiv b - d \pmod{n}$ .
4.  $ac \equiv bd \pmod{n}$ .
5. Para todo entero positivo  $k$ ,  $a^k \equiv b^k \pmod{n}$ .
6. Para todo entero  $r$ ,  $a + r \equiv b + r \pmod{n}$ .
7. Para todo entero  $r$ ,  $ar \equiv br \pmod{n}$ .

*Demostración.*

1. La hipótesis dice que  $n \mid (a - b)$  y  $n \mid (c - d)$  luego, por el Teorema 2.1 tenemos que  $n \mid \{r(a - b) + s(c - d)\} = (ar + cs) - (br + ds)$  y por lo tanto  $ar + cs \equiv br + ds \pmod{n}$ .
2. Se sigue de (1) tomando  $r = s = 1$ .
3. Se sigue de (1) tomando  $r = 1$  y  $s = -1$ .
4. Basta observar que  $ac - bd = (a - b)c + b(c - d)$ .
5. La demostración es por inducción sobre  $k$ .  
Para  $k = 1$  la afirmación es obvia. Además, si suponemos que  $a^k \equiv b^k \pmod{n}$ , puesto que  $a \equiv b \pmod{n}$  obtenemos aplicando 4) que  $a^{k+1} \equiv b^{k+1} \pmod{n}$ . Por el PIM el resultado es cierto para todo entero positivo  $k$ .
6. Es suficiente aplicar (2) a las congruencias  $a \equiv b \pmod{n}$  y  $r \equiv r \pmod{n}$ .

7. Se sigue de (1) tomando  $s = 0$ .  $\square$

**4.6 Corolario.** Si  $a \equiv b \pmod{n}$  y  $P(x)$  es un polinomio con coeficientes enteros, entonces  $P(a) \equiv P(b) \pmod{n}$ .

**4.7 Ejemplo.** Hallemos el residuo obtenido al dividir  $7^{135}$  por 8. Observemos que  $7^2 \equiv 1 \pmod{8}$ , luego por el Teorema 4.5 tenemos

$$7^{135} = (7^2)^{67} \cdot 7 = 1 \cdot 7 \equiv 7 \pmod{8},$$

y por el Teorema 4.3 el residuo de dividir  $7^{135}$  por 8 es el mismo de dividir 7 por 8, es decir 7.

**4.8 Ejemplo.** En el capítulo 3 afirmamos que el sexto número de Fermat  $2^{2^5} + 1$  no es primo pues se puede factorizar en la forma

$$2^{2^5} + 1 = (641)(6700417).$$

Veamos que efectivamente  $2^{2^5} + 1 \equiv 0 \pmod{641}$ . Puesto que,

$$2^{16} = 65536 = (102)(641) + 154$$

tenemos

$$2^{16} \equiv 154 \pmod{641},$$

y por lo tanto

$$2^{32} \equiv (154)^2 \pmod{641},$$

pero  $(154)^2 = 23716 = (36)(641) + 640$  y en consecuencia

$$2^{2^5} + 1 \equiv 0 \pmod{641}.$$

**4.9 Ejemplo.** Sean  $a$  y  $b$  enteros cualesquiera y  $p$  un número primo, veamos que

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

En efecto, por el Teorema del Binomio tenemos,

$$\begin{aligned} (a + b)^p &= \sum_{k=0}^p \binom{p}{k} a^{p-k} b^k \\ &= a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p, \end{aligned}$$

por lo tanto

$$(a+b)^p - (a^p + b^p) = \binom{p}{1} a^{p-1}b + \dots + \binom{p}{p-1} ab^{p-1} = tp,$$

puesto que los coeficientes binomiales  $\binom{p}{k}$  con  $k = 1, 2, \dots, p-1$  son divisibles por  $p$ . En consecuencia

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

**4.10 Teorema.** Sean  $n_1, n_2, \dots, n_r$  enteros positivos. Si para cada  $i = 1, \dots, r$ ,  $a \equiv b \pmod{n_i}$  entonces

$$a \equiv b \pmod{[n_1, \dots, n_r]}.$$

*Demostración.* Por hipótesis, para cada  $i = 1, \dots, r$   $n_i \mid (a-b)$  y por (3) del Teorema 2.37,  $[n_1, \dots, n_r] \mid (a-b)$  es decir,

$$a \equiv b \pmod{[n_1, \dots, n_r]}. \quad \square$$

**4.11 Corolario.** Si  $n_1, n_2, \dots, n_r$  son enteros positivos primos relativos dos a dos y para cada  $i = 1, \dots, r$ ,  $a \equiv b \pmod{n_i}$  entonces

$$a \equiv b \pmod{\prod_{i=1}^r n_i}.$$

Es necesario tener sumo cuidado cuando se trata de cancelar factores en las congruencias.

!No siempre  $ac \equiv bc \pmod{n}$  implica  $a \equiv b \pmod{n}$ !

Por ejemplo,

$$(6)(4) \equiv (3)(4) \pmod{6} \text{ pero } 6 \not\equiv 3 \pmod{6}.$$

El siguiente resultado nos indica como proceder en estos casos.

**4.12 Teorema.** Si  $ac \equiv bc \pmod{n}$  y  $d = (c, n)$  entonces

$$a \equiv b \pmod{\frac{n}{d}}.$$

*Demostración.* Por hipótesis  $n \mid (ac - bc)$  es decir  $c(a - b) = kn$  con  $k$  entero. De otra parte como  $d = (c, n)$  tenemos por el Corolario 2.12 que  $c = dC$  y  $n = dN$  donde  $(C, N) = 1$ . Por lo tanto tenemos  $dC(a - b) = kdN$  y entonces  $C(a - b) = kN$ . Luego  $N \mid C(a - b)$  y como  $(C, N) = 1$  entonces  $N \mid (a - b)$ . En otros términos  $a \equiv b \pmod{N}$  o sea  $a \equiv b \pmod{\frac{n}{d}}$ .  $\square$

**4.13 Corolario.** Si  $ac \equiv bc \pmod{n}$  y  $(c, n) = 1$  entonces  $a \equiv b \pmod{n}$ .

---

## Ejercicios 4.1

---

1. Probar que si  $a \equiv b \pmod{n}$  entonces  $(a, n) = (b, n)$ .
2. Probar que si  $ac \equiv bc \pmod{cn}$  entonces  $a \equiv b \pmod{n}$ .
3. Probar que para todo entero positivo  $n$ ,  $3^{2n+1} + 2^{n+2}$  es divisible por 7.
4. Probar que  $3^{105} + 4^{105} \equiv 0 \pmod{13}$ .
5. Probar que para todo entero  $a$ ,  $a^5 \equiv a \pmod{30}$ .
6. Si  $p$  es un primo impar probar que:
  - (a)  $1 + 2 + 3 + \dots + (p - 1) \equiv 0 \pmod{p}$ .
  - (b)  $1^2 + 2^2 + 3^2 + \dots + (p - 1)^2 \equiv 0 \pmod{p}$ .
  - (c)  $1^3 + 2^3 + 3^3 + \dots + (p - 1)^3 \equiv 0 \pmod{p}$ .
7. Si  $p$  es primo y  $n^2 \equiv 1 \pmod{p}$ , probar que  $n \equiv \pm 1 \pmod{p}$ .
8. Si  $f(x)$  es un polinomio con coeficientes enteros y  $f(a) \equiv k \pmod{n}$ , probar que para todo entero  $t$ ,  $f(a + tn) \equiv k \pmod{n}$ .
9. Probar que si  $2n + 1$  es un primo entonces los números  $1^2, 2^2, 3^2, \dots, n^2$  tienen residuos diferentes cuando los dividimos por  $2n + 1$ .

*Sugerencia:* La diferencia de dos de estos números no es divisible por  $2n + 1$ .

10. Hallar el dígito de las unidades de los números  $13^{13}$  y  $(5)(7)^{29} + (8)(9)^{72}$
11. Hallar el residuo obtenido al dividir  $6^{241}$  por 7 y el obtenido al dividir  $15^{168}$  por 13.

## 4.2 Criterios de Divisibilidad

Como una aplicación de las propiedades de las congruencias estudiadas en la sección anterior, vamos a deducir algunos de los criterios de divisibilidad de enteros, que conocemos desde la escuela elemental.

**4.14 Teorema.** *Un entero positivo expresado en forma decimal es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.*

*Demostración.* Todo entero positivo  $n$  lo podemos expresar en la forma

$$n = a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k,$$

donde  $0 \leq a_i < 10$  para cada  $i$  y  $k$  es un entero no negativo.

Si consideramos el polinomio con coeficientes enteros

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,$$

observamos que

$$P(10) = n, \quad P(1) = a_0 + a_1 + a_2 + \cdots + a_k.$$

Como  $10 \equiv 1 \pmod{3}$ , por el corolario 4.6 tenemos que

$$n \equiv a_0 + a_1 + a_2 + \cdots + a_k \pmod{3}.$$

Luego  $n - (a_0 + a_1 + \cdots + a_k) = 3t$  para algún entero  $t$ , y de esta igualdad concluimos que  $3 \mid n$  si y solo si  $3 \mid (a_0 + a_1 + \cdots + a_k)$ . Si notamos que todas las congruencias en la demostración anterior son válidas cuando el módulo es 9, tenemos también el criterio siguiente.  $\square$

**4.15 Teorema.** *Un entero positivo expresado en forma decimal es divisible por 9 si y solo si la suma de sus dígitos es divisible por 9.*

**4.16 Ejemplo.** El número 35.747.826 es divisible por 3 pues la suma de sus dígitos es

$$3 + 5 + 7 + 4 + 7 + 8 + 2 + 6 = 42$$

y 42 es divisible por 3. Sin embargo, como  $9 \nmid 42$  el número no es divisible por 9.

Como otra aplicación consideremos el siguiente criterio de divisibilidad por 4.

**4.17 Teorema.** *Un entero positivo con más de un dígito, expresado en forma decimal es divisible por 4, si y solo si, el número formado por sus dos últimos dígitos es divisible por 4.*

*Demostración.* Supongamos que la representación en base 10 del entero positivo  $n$  es

$$n = a_k 10^k + \cdots + a_1 10 + a_0,$$

entonces el número formado por sus dos últimos dígitos es

$$a_1 10 + a_0.$$

Como  $10^2 \equiv 0 \pmod{4}$ , por aplicación repetida de la propiedad 7) del Teorema 4.5 con  $r = 10$ , tenemos que  $10^3 \equiv 0 \pmod{4}$ ,  $10^4 \equiv 0 \pmod{4}$ ,  $\dots, 10^k \equiv 0 \pmod{4}$ . Por lo tanto

$$n \equiv a_1 10 + a_0 \pmod{4}.$$

Luego  $n - (a_1 10 + a_0) = 4k$  para algún entero  $k$ , y de esta ecuación concluimos que  $4 \mid n$  si y solo si  $4 \mid (a_1 10 + a_0)$ , como queríamos comprobar.  $\square$

**4.18 Ejemplo.** El número 624.746.872 es divisible por 4 pues  $4 \mid 72$ , en cambio el número 321658 no es divisible por 4 pues  $4 \nmid 58$ .

## Ejercicios 4.2

1. Sea  $n = a_0 + a_110 + a_210^2 + \cdots + a_k10^k$  la representación decimal del entero positivo  $n$ . Probar que  $n$  es divisible por 11, si y solo si,  $\sum_{i=0}^k (-1)^i a_i$  es divisible por 11.
2. A partir de la relación  $10^3 \equiv -1 \pmod{7}$ , deducir un criterio de divisibilidad por 7.
3. Probar que  $6 \mid n$  si y solo si  $2 \mid n$  y  $3 \mid n$ .
4. Con las notaciones del ejercicio 1, probar que  $8 \mid n$  si y solo si  $8 \mid (100a_2 + 10a_1 + a_0)$ .
5. Expresando los enteros positivos en el sistema de numeración con base 100, deducir un criterio de divisibilidad por 101.

4.3 Aritmética módulo  $n$ 

En el Teorema 4.4 vimos que la congruencia módulo  $n$  es una relación de equivalencia en el conjunto  $\mathbb{Z}$  de los números enteros. Para cada  $a \in \mathbb{Z}$ , representamos su clase de equivalencia por  $\bar{a}$ . Recordamos que  $\bar{a}$  esta definida por,

$$\begin{aligned}\bar{a} &= \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} \\ &= \{x \in \mathbb{Z} \mid x = a + kn, \text{ para algún } k \in \mathbb{Z}\}.\end{aligned}$$

Estas clases se llaman también *clases residuales módulo  $n$*  y sabemos que constituyen una partición del conjunto  $\mathbb{Z}$  de todos los enteros.

Veamos ahora que el conjunto cociente de  $\mathbb{Z}$  por esta relación esta formado precisamente por las clases  $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$ . En efecto, si  $a$  es un entero arbitrario, por el algoritmo de la división podemos representarlo en la forma  $a = qn + r$  con  $0 \leq r < n$ , luego  $a \equiv r \pmod{n}$  y en consecuencia  $\bar{a} = \bar{r}$ .

Se acostumbra a representar por  $\mathbb{Z}_n$  a este conjunto cociente y se le llama el *conjunto de los enteros módulo  $n$* . Tenemos por lo tanto que

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}.$$

Sobre  $\mathbb{Z}_n$  podemos definir una adición y una multiplicación mediante las fórmulas siguientes:

$$\begin{aligned}\overline{x} + \overline{y} &= \overline{x+y}, \\ \overline{x} \overline{y} &= \overline{xy}.\end{aligned}$$

Es decir, para sumar las clases residuales de  $x$  y de  $y$  tomamos un elemento de la clase de  $x$ , un elemento de la clase de  $y$ , los sumamos y tomamos la clase residual de esta suma. Similarmente se procede con la multiplicación. Estas operaciones resultan bien definidas en virtud de las propiedades 2 y 4 del Teorema 4.5.

**4.19 Ejemplo.** Las tablas de adición y multiplicación módulo 4 son:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

donde por comodidad hemos eliminado las barras.

**4.20 Teorema.** *La adición en  $\mathbb{Z}_n$  tiene las propiedades siguientes:*

- i.  $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$
- ii.  $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$
- iii. *Para cada  $\overline{a}$  existe  $\overline{x}$  tal que  $\overline{a} + \overline{x} = \overline{x} + \overline{a} = \overline{0}$*
- iv.  $\overline{a} + \overline{b} = \overline{b} + \overline{a}$

*Demostración.* Las propiedades i, ii y iv son consecuencia directa de las propiedades correspondientes para la adición ordinaria de enteros; por ejemplo

la propiedad asociativa se demuestra en la forma siguiente:

$$\begin{aligned}\bar{a} + (\bar{b} + \bar{c}) &= \overline{\bar{a} + \bar{b} + \bar{c}} \\ &= \overline{a + (b + c)} \\ &= \overline{(a + b) + c} \\ &= \overline{a + b} + \bar{c} \\ &= (\bar{a} + \bar{b}) + \bar{c}.\end{aligned}$$

De manera similar se demuestran ii y iv.

Para probar iii, es suficiente tomar  $x = n - a$ , pues en tal caso tenemos

$$\bar{a} + \overline{n - a} = \overline{a + (n - a)} = \bar{n} = \bar{0},$$

y

$$\overline{n - a} + \bar{a} = \overline{(n - a) + a} = \bar{n} = \bar{0}. \quad \square$$

El teorema anterior nos indica que  $\mathbb{Z}_n$  con la adición es un grupo conmutativo de acuerdo a las definiciones siguientes:

**4.21 Definición.** Un grupo  $(G, *)$  es un conjunto  $G$  provisto de una operación binaria  $*$  que satisface los axiomas siguientes:

G-1 La operación  $*$  es asociativa, es decir para todo  $a, b, c$  en  $G$  se tiene que  $a * (b * c) = (a * b) * c$ .

G-2 Existe un elemento  $e$  en  $G$  tal que  $a * e = e * a = a$  para todo  $a$  en  $G$ .

G-3 Para cada  $a$  en  $G$  existe un elemento  $a'$  en  $G$  tal que  $a * a' = a' * a = e$ .

El elemento  $e$  del axioma G-2 es único y se llama la identidad del grupo. Para cada  $a \in G$  el elemento  $a'$  del axioma 3 es también único y se llama el inverso de  $a$  con respecto a la operación  $*$ .

**4.22 Definición.** Un grupo  $G$  se llama *abeliano* o *conmutativo* si satisface la condición  $a * b = b * a$  para todo  $a$  y  $b$  en  $G$ .

**4.23 Ejemplo.** 1. De acuerdo al Teorema 4.20, el conjunto  $\mathbb{Z}_n$  con la adición que hemos definido entre clases residuales módulo  $n$ , es un grupo conmutativo donde la operación se representa por  $+$ , la identidad es  $\bar{0}$  y para cada  $\bar{a} \in \mathbb{Z}_n$  su inverso es  $\overline{n - a}$ .

2. El conjunto  $\mathbb{Z}$  con la adición es un grupo conmutativo, donde la identidad es el 0 y el inverso de cada  $n \in \mathbb{Z}$  es  $-n$ .
3. El conjunto  $\mathbb{R}^*$  de todos los números reales diferentes de cero, con la multiplicación usual como operación, es un grupo conmutativo, donde la identidad es el número 1 y para cada número real  $a \neq 0$ , su inverso es  $1/a$ .

**4.24 Teorema.** *La multiplicación en  $\mathbb{Z}_n$  tiene las propiedades siguientes:*

1.  $\overline{ab} = \overline{ba}$ .
2.  $\overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$ .
3.  $\overline{a}(\overline{b} + \overline{c}) = \overline{ab} + \overline{ac}$  y  $(\overline{b} + \overline{c})\overline{a} = \overline{ba} + \overline{ca}$ .
4.  $\overline{a}\overline{1} = \overline{1}\overline{a} = \overline{a}$ .

*Demostración.* De nuevo, las propiedades son consecuencia directa de las propiedades correspondientes para la multiplicación usual en los enteros. Como ejemplo demostramos la propiedad distributiva de la multiplicación con respecto a la adición. Tenemos

$$\begin{aligned}
 \overline{a}(\overline{b} + \overline{c}) &= \overline{a\overline{b+c}} \\
 &= \overline{a(b+c)} \\
 &= \overline{ab+ac} \\
 &= \overline{ab} + \overline{ac} \\
 &= \overline{ab} + \overline{ac}.
 \end{aligned}
 \quad \square$$

Los dos últimos teoremas, nos dicen que  $\mathbb{Z}_n$  con la adición y la multiplicación entre clases residuales módulo  $n$ , es un *anillo conmutativo con identidad*, de acuerdo a las definiciones siguientes.

**4.25 Definición.** Un *anillo*  $(A, +, \cdot)$  es un conjunto  $A$  provisto de dos operaciones  $+$  y  $\cdot$ , llamadas adición y multiplicación que satisface los axiomas siguientes:

A-1  $(A, +)$  es un grupo abeliano.

A-2 La multiplicación es asociativa.

A-3 Las dos operaciones están relación dadas por las propiedades distributivas

$$\begin{aligned}a(b + c) &= ab + ac \\(b + c)a &= ba + ca,\end{aligned}$$

para todo  $a, b, c \in A$ .

**4.26 Definición.** Un anillo donde la multiplicación es conmutativa se dice un *anillo conmutativo*. Un anillo que tiene una identidad para la multiplicación, que se representa usualmente por 1, es un *anillo con identidad*.

Ya hemos verificado que  $(\mathbb{Z}_n, +, \cdot)$  es un anillo conmutativo con identidad. La identidad de este anillo es precisamente  $\bar{1}$ . Este anillo se llama el *anillo de los enteros módulo  $n$* .

Como otro ejemplo de anillo, consideremos el conjunto  $A = \mathbb{R} \times \mathbb{R}$  con adición y multiplicación definidas por,

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d), \\(a, b) \cdot (c, d) &= (ac, bd).\end{aligned}$$

Una verificación directa nos muestra que  $(A, +, \cdot)$  es un anillo conmutativo con identidad  $(1, 1)$ . El elemento cero de este anillo es  $(0, 0)$ .

Observamos que en este anillo

$$(1, 0) \cdot (0, 1) = (0, 0)$$

aunque  $(1, 0)$  y  $(0, 1)$  son distintos de cero. Esta situación también se presenta en anillos tales como  $(\mathbb{Z}_6, +, \cdot)$  donde tenemos que

$$\bar{2} \cdot \bar{3} = \bar{0}$$

y ambos elementos  $\bar{2}$  y  $\bar{3}$  son diferentes de  $\bar{0}$ . Establecemos la definición siguiente.

**4.27 Definición.** Decimos que un anillo  $(A, +, \cdot)$  tiene *divisores de cero* si existen elementos  $a, b \in A$  distintos de cero pero tales que  $ab = 0$ .

Acabamos de ver que el anillo  $\mathbb{Z}_6$  tiene divisores de cero. También observamos que en este anillo no se cumple la ley cancelativa para la multiplicación, ya que tenemos por ejemplo:  $\bar{3} \cdot \bar{2} = \bar{3} \cdot \bar{4}$  pero  $\bar{2} \neq \bar{4}$ .

Este resultado no es casual, sino consecuencia del teorema siguiente.

**4.28 Teorema.** *Un anillo  $A$  satisface la ley cancelativa para la multiplicación a izquierda y a derecha, si y solo si,  $A$  no tiene divisores de cero.*

*Demostración.* Supongamos que  $A$  es un anillo sin divisores de cero. Si  $a, b, c \in A$  con  $a \neq 0$  y  $ab = ac$  entonces  $a(b - c) = 0$ . Como  $a \neq 0$  y el anillo no tiene divisores de cero, concluimos que  $b - c = 0$ , es decir que  $b = c$ . Luego se cumple la ley cancelativa a izquierda.

Similarmente se demuestra que se cumple la ley cancelativa a derecha.

Supongamos ahora que  $A$  satisface la ley cancelativa para la multiplicación. Si  $ab = 0$  con  $a \neq 0$ , tenemos  $ab = a0$  y cancelando  $a$ , obtenemos  $b = 0$ . Similarmente si  $ab = 0$  con  $b \neq 0$  tenemos  $ab = 0b$  y cancelando  $b$  tenemos  $a = 0$ . Luego  $A$  no tiene divisores de cero.  $\square$

**4.29 Definición.** *Un dominio de integridad es un anillo conmutativo, con identidad y sin divisores de cero.*

**4.30 Definición.** *Un cuerpo es un anillo conmutativo con identidad en el cual todo elemento distinto de cero tiene un inverso para la multiplicación.*

Los elementos inversibles para la multiplicación en un anillo con identidad se llaman las *unidades del anillo*. Por ejemplo en el anillo  $\mathbb{Z}$  de los números enteros, las unidades son 1 y  $-1$ . En un cuerpo las unidades son todos los elementos distintos de cero.

**4.31 Teorema.** *Todo cuerpo es un dominio de integridad.*

*Demostración.* Como un cuerpo es un anillo conmutativo con identidad, de acuerdo al Teorema 4.28, solo falta por demostrar que en un cuerpo es válida la ley cancelativa para la multiplicación.

Supongamos que  $a \neq 0$  y que  $ab = ac$ . Sea  $a'$  el inverso multiplicativo de  $a$ . Tenemos  $a'(ab) = a'(ac)$  es decir  $(a'a)b = (a'a)c$  luego  $1b = 1c$  con lo cual  $b = c$ .  $\square$

Volviendo a nuestro estudio de los enteros módulo  $n$ , tenemos el resultado siguiente.

**4.32 Teorema.** *En el anillo  $\mathbb{Z}_n$  los divisores de cero son precisamente los elementos  $\overline{m} \neq \overline{0}$  tales que  $m$  y  $n$  no son primos relativos.*

*Demostración.* Sea  $\overline{m} \neq \overline{0}$  y supongamos que  $m$  y  $n$  no son primos relativos. Entonces  $(m, n) = d$  con  $d > 1$  y tenemos

$$\overline{m(n/d)} = \overline{m(n/d)} = \overline{n(m/d)} = \overline{0}.$$

Como  $\overline{m} \neq \overline{0}$  y  $\overline{(n/d)} \neq \overline{0}$  pues  $d > 1$ , concluimos que  $\overline{m}$  es un divisor de cero en  $\mathbb{Z}_n$ .

Supongamos ahora que  $\overline{m} \in \mathbb{Z}_n$  con  $m$  y  $n$  primos relativos. Si  $\overline{mk} = \overline{0}$  entonces  $\overline{mk} = \overline{0}$  o sea  $mk \equiv 0 \pmod{n}$ . Luego  $n \mid mk$  y como  $(n, m) = 1$  entonces  $n \mid k$  y así  $k \equiv 0 \pmod{n}$ , o sea  $\overline{k} = \overline{0}$ . Por lo tanto  $\overline{m}$  no es divisor de cero.  $\square$

**4.33 Corolario.**  $\mathbb{Z}_n$  es un dominio de integridad si y solo si  $n$  es un número primo.

*Demostración.* Veamos primero que si  $n$  no es primo entonces  $\mathbb{Z}_n$  no es un dominio de integridad. Supongamos que  $n = ab$  con  $1 < a < n$  y  $1 < b < n$ . Tenemos entonces

$$\overline{ab} = \overline{ab} = \overline{n} = \overline{0},$$

con  $\overline{a} \neq \overline{0}, \overline{b} \neq \overline{0}$ . Luego  $\mathbb{Z}_n$  tiene divisores de cero y no es dominio de integridad.

Supongamos ahora que  $n$  es un número primo. Como  $n$  es primo relativo con cada uno de los enteros  $1, 2, \dots, n-1$ , por el Teorema 4.32,  $\mathbb{Z}_n$  no tiene divisores de cero y en consecuencia es un dominio de integridad.  $\square$

**4.34 Teorema.**  $\mathbb{Z}_n$  es un cuerpo si y solo si  $n$  es un número primo.

*Demostración.* Si  $n$  no es primo, por el corolario anterior  $\mathbb{Z}_n$  no es un dominio de integridad y por el Teorema 4.31  $\mathbb{Z}_n$  no es un campo.

Supongamos ahora que  $n$  es un número primo. Para probar que  $\mathbb{Z}_n$  es un campo, es suficiente probar que todo elemento distinto de cero en  $\mathbb{Z}_n$  es una unidad. Para ello, sea  $\overline{m} \in \mathbb{Z}_n$  con  $0 < m < n$ . Como  $m$  y  $n$  son primos relativos, por el Teorema 2.11 existen enteros  $r$  y  $s$  tales que

$$mr + ns = 1.$$

Por lo tanto tenemos

$$\overline{m} \overline{r} + \overline{n} \overline{s} = \overline{1},$$

y como  $\bar{n} = \bar{0}$ , nos queda

$$\bar{m}\bar{r} = \bar{1}.$$

De esta forma vemos que  $\bar{r}$  es el inverso multiplicativo de  $\bar{m}$  y  $\mathbb{Z}_n$  es un cuerpo como queríamos demostrar.  $\square$

---

## Ejercicios 4.3

---

1. Construir las tablas de adición y multiplicación, módulo 1, módulo 2, módulo 5, módulo 6, y módulo 7.
2. En  $\mathbb{Z}_7$  resolver las ecuaciones  $3x + 4 = 1$  y  $x^2 + 2x + 6 = 0$ .
3. En un anillo con identidad, ¿es el producto de dos unidades también una unidad?, ¿es la suma de dos unidades de nuevo una unidad?
4. Demostrar que el conjunto de las unidades de un anillo con identidad es un grupo, con la multiplicación del anillo como operación.
5. Sean  $a$  y  $n$  enteros positivos tales que  $n = ab$ . Probar que el conjunto  $A = \{\bar{0}, \bar{a}, \bar{2a}, \dots, \overline{(b-1)a}\}$  con la adición y la multiplicación de clases residuales módulo  $n$ , es un anillo.

*Sugerencia:* Hay que demostrar primero que  $A$  es cerrado para estas operaciones, es decir que la suma y la multiplicación módulo  $n$  de elementos de  $A$  es también un elemento de  $A$ .

Un conjunto  $C$  se llama un *sistema completo de residuos módulo  $n$* , si  $C$  contiene exactamente un elemento de cada clase residual módulo  $n$ .

6. Construir cuatro sistemas completos de residuos módulo 8.
7. Construir un sistema completo de residuos módulo 7 formado por números primos.

8. Probar que un conjunto  $C$  de enteros es un sistema completo de residuos módulo  $n$  si y solo si dos elementos cualesquiera de  $C$  no son congruentes módulo  $n$  y  $C$  tiene  $n$  elementos.
9. Probar que si  $C$  es un sistema completo de residuos módulo  $n$  y  $(a, n) = 1$  entonces, para todo  $b$  el conjunto  $C' = \{ax + b \mid x \in C\}$  también es un sistema completo de residuos módulo  $n$ .
10. Probar que si  $n > 2$ , el conjunto de enteros  $1^2, 2^2, \dots, n^2$  no es un sistema completo de residuos módulo  $n$ .

## 4.4 Los Teoremas de Euler y Fermat

**4.35 Definición.** Un subconjunto  $R$  del conjunto de los enteros se llama un *sistema reducido de residuos módulo  $n$*  si satisface las condiciones siguientes:

1.  $R$  tiene  $\Phi(n)$  elementos.
2. Para cada  $r \in R$  se tiene que  $(r, n) = 1$ ,
3. Los elementos de  $R$  son incongruentes módulo  $n$ .

**4.36 Ejemplo.** Si  $n = 8$ , los conjuntos  $\{1, 3, 5, 7\}$  y  $\{9, 3, -3, 23\}$  son sistemas reducidos de residuos módulo 8.

Si  $p$  es primo, el conjunto  $\{1, 2, 3, \dots, p-1\}$  es un sistema reducido de residuos módulo  $p$ . A partir de un sistema reducido de residuos módulo  $n$ , podemos construir una infinidad de tales sistemas aplicando el teorema siguiente.

**4.37 Teorema.** Si  $\{r_1, r_2, \dots, r_{\Phi(n)}\}$  es un sistema reducido de residuos módulo  $n$  y si  $(k, n) = 1$  entonces  $\{kr_1, kr_2, \dots, kr_{\Phi(n)}\}$  también es un sistema reducido de residuos módulo  $n$ .

*Demostración.* La condición 1 de la definición de sistema reducido es evidente. Como  $(r_i, n) = 1$  para cada  $i$  y  $(k, n) = 1$ , por el Teorema 2.18 se tiene que  $(kr_i, n) = 1$  para cada  $i$  y se cumple la condición 2.

Finalmente, no puede tenerse que dos de los números  $kr_i$  sean congruentes módulo  $n$ , ya que si  $kr_i \equiv kr_j \pmod{n}$  entonces  $r_i \equiv r_j \pmod{n}$  por

el Corolario 4.13, lo que contradice la hipótesis de que  $\{r_1, \dots, r_{\Phi(n)}\}$  es un sistema reducido de residuos módulo  $n$ . Por lo tanto, también se cumple la condición 3 de la definición y se tiene el teorema.  $\square$

La consecuencia más importante del teorema anterior es un resultado muy importante debido a Euler.

**4.38 Teorema (Teorema de Euler).** *Si  $(a, n) = 1$  entonces*

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

*Demostración.* Sea  $\{r_1, r_2, \dots, r_{\Phi(n)}\}$  un sistema reducido de residuos módulo  $n$ . Por el teorema anterior el conjunto  $\{ar_1, ar_2, \dots, ar_{\Phi(n)}\}$  es también un sistema reducido de residuos módulo  $n$ . Por lo tanto el producto de los enteros del primer conjunto es congruente al producto de los enteros del segundo conjunto. Luego

$$r_1 r_2 \cdots r_{\Phi(n)} \equiv a^{\Phi(n)} r_1 r_2 \cdots r_{\Phi(n)} \pmod{n}.$$

Como cada  $r_i$  es primo relativo con  $n$ , por el Corolario 4.13 podemos cancelar cada uno de los  $r_i$  y obtenemos

$$1 \equiv a^{\Phi(n)} \pmod{n}$$

como queríamos probar.  $\square$

**4.39 Corolario (Teorema de Fermat).** *Si  $p$  es un número primo y  $(a, p) = 1$ , entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Demostración.* Es consecuencia inmediata del Teorema de Euler, ya que  $\Phi(p) = p - 1$ .  $\square$

Una forma equivalente del Teorema de Fermat es el enunciado siguiente.

**4.40 Teorema.** *Si  $p$  es un número primo, entonces*

$$a^p \equiv a \pmod{p},$$

*para cualquier entero  $a$ .*

*Demostración.* Si  $p \nmid a$  entonces  $(a, p) = 1$  y por el corolario anterior

$$a^{p-1} \equiv 1 \pmod{p}.$$

Por 7 del Teorema 4.5, tenemos que

$$a^p \equiv a \pmod{p}.$$

Si  $p \mid a$ , tenemos que

$$a \equiv 0 \pmod{p} \quad \text{y} \quad a^p \equiv 0 \pmod{p},$$

y por las propiedades de la congruencia

$$a^p \equiv a \pmod{p}.$$

□

**4.41 Ejemplo.** Si  $p$  y  $q$  son primos diferentes veamos que

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Por el Teorema de Fermat tenemos

$$p^{q-1} \equiv 1 \pmod{q} \quad \text{y} \quad q^{p-1} \equiv 1 \pmod{p}.$$

De otra parte tenemos

$$p^{q-1} \equiv 0 \pmod{p} \quad \text{y} \quad q^{p-1} \equiv 0 \pmod{q},$$

luego

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q} \quad \text{y} \quad p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$$

y como  $p$  y  $q$  son primos relativos, por el Corolario 4.11, concluimos que

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

**4.42 Ejemplo.** Hallemos las dos últimas cifras en el desarrollo decimal del número  $27^{123}$ .

Si escribimos

$$27^{123} = a_k 10^k + \cdots + a_1 10 + a_0$$

con  $0 \leq a_i < 10$ , se trata de encontrar el número  $N$  formado por los dos últimos dígitos, es decir  $N = a_1 a_0$ . Es claro que este número  $N$  es el único que satisface

$$27^{123} \equiv N \pmod{100} \quad \text{y} \quad 0 \leq N < 100.$$

Por el Teorema de Euler tenemos que

$$27^{\Phi(100)} \equiv 1 \pmod{100}.$$

Como  $\Phi(100) = \Phi(5^2)\Phi(2^2) = (5^2 - 5)(2^2 - 2) = 40$ , la congruencia anterior es

$$27^{40} \equiv 1 \pmod{100}.$$

Por lo tanto

$$27^{123} = (27^{40})^3 27^3 \equiv 27^3 \pmod{100},$$

y como  $27^3 = 19.683$ , tenemos que

$$27^3 \equiv 83 \pmod{100}.$$

Luego el desarrollo decimal de  $27^{123}$  termina en 83.

El Teorema de Euler puede utilizarse también para resolver ciertas congruencias lineales. Tenemos el resultado siguiente.

**4.43 Teorema.** *Si  $(a, n) = 1$ , la solución de la congruencia lineal*

$$ax \equiv b \pmod{n},$$

es

$$x \equiv a^{\Phi(n)-1} b \pmod{n}.$$

*Demostración.* Por el Teorema de Euler tenemos

$$a^{\Phi(n)} \equiv 1 \pmod{n},$$

y por lo tanto

$$a^{\Phi(n)} b \equiv b \pmod{n}.$$

Luego la congruencia lineal toma la forma

$$ax \equiv a^{\Phi(n)} b \pmod{n},$$

de donde

$$x \equiv a^{\Phi(n)-1} b \pmod{n},$$

ya que  $(a, n) = 1$ . □

En la sección siguiente demostraremos que esta es la única solución incongruente de la congruencia lineal considerada.

Si  $G$  es un grupo finito, se llama *orden* de  $G$  al número de elementos de  $G$ . Se demuestra en teoría de grupos el resultado siguiente:

Si  $G$  es un grupo finito de orden  $n$  y  $a \in G$ , entonces  $a^n = e$ , donde  $a^n = a * a * \dots * a$ ,  $n$  veces, siendo  $*$  la operación en  $G$ .

Utilizando el resultado anterior y el ejercicio 4 de la sección precedente, obtenemos otras demostraciones de los teoremas de Fermat y Euler, que presentamos a continuación.

**4.44 Teorema (Teorema de Fermat).** *Si  $p$  es un número primo y  $(a, p) = 1$ , entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Demostración.* Como  $\mathbb{Z}_p$  es un cuerpo cuando  $p$  es primo, entonces el grupo de las unidades de  $\mathbb{Z}_p$  está formado por todos los elementos no nulos de  $\mathbb{Z}_p$  y tiene por lo tanto orden  $p - 1$ .

Si  $(a, p) = 1$  entonces  $\bar{a} \neq \bar{0}$  y en consecuencia  $\bar{a}$  es una unidad de  $\mathbb{Z}_p$ . Luego por el resultado mencionado

$$\bar{a}^{p-1} = \bar{1},$$

o equivalentemente

$$a^{p-1} \equiv 1 \pmod{p}.$$

Para demostrar el Teorema de Euler, necesitamos un lema previo. □

**4.45 Lema.** *El grupo de las unidades del anillo  $\mathbb{Z}_n$  está formado por todas las clases  $\bar{a}$  tales que  $(a, n) = 1$  y tiene orden  $\Phi(n)$ .*

*Demostración.* Supongamos que  $\bar{a}$  es una unidad de  $\mathbb{Z}_n$ . Luego existe  $\bar{b} \in \mathbb{Z}_n$  tal que  $\bar{a}\bar{b} = \bar{1}$ . Por lo tanto  $ab \equiv 1 \pmod{n}$  y tenemos que  $ab - 1 = qn$  para algún entero  $q$ . Luego  $ab - qn = 1$  y por el Teorema 2.11 concluimos que  $(a, n) = 1$ .

Recíprocamente, si  $(a, n) = 1$  por el Teorema 2.11 existe enteros  $b$  y  $q$  tales que  $ab - qn = 1$ . Luego  $ab \equiv 1 \pmod{n}$ , o sea  $\bar{a}\bar{b} = \bar{1}$  y por lo tanto  $\bar{a}$  es una unidad de  $\mathbb{Z}_n$ .

De esta forma hemos probado que en el anillo

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{(n-1)}\}$$

las unidades son precisamente las clases  $\overline{a}$  con  $(a, n) = 1$ , por lo tanto su número es  $\Phi(n)$ .  $\square$

**4.46 Teorema (Teorema de Euler).** *Si  $(a, n) = 1$  entonces*

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

*Demostración.* Como  $(a, n) = 1$ , por el Lema 4.45,  $\overline{a}$  es una unidad de  $\mathbb{Z}_n$ , y como el *orden del grupo* de unidades de este anillo es  $\Phi(n)$ , tenemos

$$(\overline{a})^{\Phi(n)} = \overline{1},$$

o equivalentemente

$$a^{\Phi(n)} \equiv 1 \pmod{n}.$$

$\square$

---

## Ejercicios 4.4

---

1. Probar que para todo entero  $n$ ,  $n^{12}$  es de la forma  $13k$  o de la forma  $13k + 1$ , para algún entero  $k$ .
2. Probar que para todo entero  $n$ ,  $n^8$  es de la forma  $17k$  o  $17k \pm 1$ , para algún entero  $k$ .
3. Probar que para todo entero  $a$ ,  $a^{561} \equiv a \pmod{561}$ .
4. Probar que si  $p$  es un número primo, entonces

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} + 1 \equiv 0 \pmod{p}.$$

5. Hallar en su desarrollo decimal

- (a) la última cifra de  $13^{1275}$ .  
(b) las dos últimas cifras de  $3^{400}$ .  
(c) las tres últimas cifras de  $7^{2407}$ .

6. Probar que para cualquier entero  $n$ ,  $n^{37} - n$  es divisible por 383838.

*Sugerencia:* Descomponer 383838 en factores primos.

7. Si  $p$  y  $q$  son primos diferentes, probar que

$$p^q + q^p \equiv (p + q) \pmod{pq}.$$

8. Probar que los números  $5, 5^2, 5^3, 5^4, 5^5$  y  $5^6$  forman un sistema reducido de residuos módulo 18.

9. Si  $p$  es un número primo y  $a^p \equiv b^p \pmod{p}$  probar que

$$a^p \equiv b^p \pmod{p^2}.$$

10. Probar que  $a^{4n+1} - a$  es divisible por 30 para todo entero  $a$  y todo entero positivo  $n$ .

11. Si  $p$  es un número primo y  $a, b$  son enteros positivos menores que  $p$ , probar que

$$a^{p-2} + a^{p-3}b + a^{p-4}b^2 + \dots + b^{p-2} \equiv 0 \pmod{p}.$$

12. Si  $p$  es un primo impar y  $p \nmid a$ , probar que

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

13. Si  $R$  es un anillo finito con identidad y  $a \in R$ , probar que  $a$  es una unidad de  $R$  o  $a$  es un divisor de cero.

*Sugerencia:* Si  $R = \{r_1, r_2, \dots, r_n\}$  y  $a$  no es divisor de cero demuestre que  $R = \{ar_1, ar_2, \dots, ar_n\}$

14. Utilice el ejercicio 13 para determinar las unidades de  $\mathbb{Z}_n$ .

## 4.5 Congruencias lineales

En Álgebra se estudian detalladamente las ecuaciones polinómicas y sus soluciones. En forma análoga podemos estudiar las congruencias polinómicas. En este estudio consideramos únicamente polinomios  $f(x)$  con coeficientes enteros.

Si  $a$  un entero tal que  $f(a) \equiv 0 \pmod{n}$ , decimos que  $a$  es una solución de la congruencia polinómica  $f(x) \equiv 0 \pmod{n}$ . Por el Corolario 4.6, si  $a \equiv b \pmod{n}$  también  $f(a) \equiv f(b) \pmod{n}$ , sin embargo no consideramos diferentes a estas soluciones que pertenecen a una misma clase de residuos módulo  $n$ . Cuando hablamos del número de soluciones de una congruencia polinómica nos referimos al número de soluciones incongruentes, es decir al número de soluciones obtenidas en el conjunto  $\{0, 1, 2, \dots, n-1\}$  o en cualquier otro sistema completo de residuos módulo  $n$ .

La congruencia  $f(x) \equiv 0 \pmod{n}$  se llama *lineal* cuando  $f(x)$  es un polinomio de grado uno. Toda congruencia lineal se puede escribir en la forma

$$ax \equiv b \pmod{n}.$$

Tenemos el resultado siguiente.

**4.47 Teorema.** *La congruencia lineal  $ax \equiv b \pmod{n}$  tiene solución si y solo si  $d \mid b$ , donde  $d = (a, n)$ .*

*Si la congruencia tiene solución, entonces tiene exactamente  $d$  soluciones incongruentes.*

*Demostración.* Dividimos la demostración en 5 partes:

1. Si  $d \mid b$ , hay una solución.
2. Si hay solución,  $d \mid b$ .
3. Si  $x_0$  es una solución entonces  $x_0 + k\frac{n}{d}$  es solución para todo entero  $k$ .
4. Todas las soluciones se encuentran entre las soluciones mencionadas en 3.
5. Las soluciones incongruentes son precisamente

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \dots, x_0 + \frac{(d-1)n}{d}.$$

Prueba de 1. Supongamos de  $d \mid b$ , luego  $b = cd$  para algún  $c$ . Como  $d = (a, n)$  por el Teorema 2.5 podemos expresar  $d$  en la forma  $d = ar + sn$ . Multiplicando por  $c$  obtenemos  $b = cd = car + csn$ .

Por lo tanto  $acr \equiv b \pmod{n}$  y  $cr$  es una solución de la congruencia lineal  $ax \equiv b \pmod{n}$ .

Prueba de 2. Supongamos que  $x_0$  es una solución de la congruencia lineal. Luego  $ax_0 \equiv b \pmod{n}$  y por lo tanto existe un entero  $k$  tal que  $ax_0 - b = kn$ . Como  $d \mid a$  y  $d \mid n$ , se sigue que  $d \mid b$  como habíamos mencionado.

Prueba de 3. Supongamos que  $x_0$  es una solución de la congruencia dada. Para todo entero  $k$  tenemos

$$a \left( x_0 + k \frac{n}{d} \right) = ax_0 + kn \left( \frac{a}{d} \right) \equiv ax_0 \equiv b \pmod{n},$$

puesto que  $d \mid a$ .

Prueba de 4. Supongamos que  $x_1$  es otra solución de la congruencia dada. Tenemos entonces

$$ax_1 \equiv b \equiv ax_0 \pmod{n},$$

y por el Teorema 4.12

$$x_1 \equiv x_0 \pmod{\frac{n}{d}}.$$

Luego existe un entero  $k$  tal que

$$x_1 = x_0 + k \frac{n}{d}.$$

Prueba de 5. Claramente las soluciones

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \dots, x_0 + (d-1)\frac{n}{d},$$

son incongruentes módulo  $n$ , puesto que dos cualesquiera de ellas no pueden diferir por un múltiplo de  $n$ . Además cada solución de la forma  $x_0 + kn/d$  es congruente módulo  $n$  con alguna de estas  $d$  soluciones, ya que por el algoritmo de la división podemos expresar a  $k$  en la forma  $k = qd + r$  con  $0 \leq r < d$ , y en consecuencia

$$\begin{aligned} x_0 + k \frac{n}{d} &= x_0 + (qd + r) \frac{n}{d} \\ &= x_0 + qn + r \frac{n}{d} \\ &\equiv x_0 + r \frac{n}{d} \pmod{n}. \end{aligned}$$

□

**4.48 Ejemplo.** Resolvamos la congruencia lineal  $32x \equiv 28 \pmod{36}$ .

Como  $(32, 36) = 4$  y  $4 \mid 28$ , la congruencia tiene 4 soluciones incongruentes.

Utilizando propiedades de las congruencias, la congruencia dada es equivalente a cada una de las congruencias siguientes

$$32x \equiv 28 \pmod{36}$$

$$8x \equiv 7 \pmod{9}$$

$$-x \equiv 7 \pmod{9}$$

$$x \equiv -7 \pmod{9}$$

$$x \equiv 2 \pmod{9}.$$

Por lo tanto las soluciones incongruentes son 2, 11, 20 y 29.

**4.49 Ejemplo.** Resolvamos la congruencia  $54x \equiv 168 \pmod{30}$ .

Como  $(54, 30) = 6$  y  $6 \mid 168$ , la congruencia tiene 6 soluciones incongruentes. Tenemos

$$54x \equiv 168 \pmod{30}$$

$$9x \equiv 28 \pmod{5}$$

$$4x \equiv 3 \pmod{5}$$

$$-x \equiv 3 \pmod{5}$$

$$x \equiv -3 \pmod{5}$$

$$x \equiv 2 \pmod{5}.$$

Luego las soluciones de la congruencia son 2, 7, 12, 17, 22 y 29.

El teorema siguiente nos permite reducir una congruencia lineal con módulo grande a una congruencia lineal con módulo más pequeño.

**4.50 Teorema.** Consideremos la congruencia lineal  $ax \equiv b \pmod{n}$ . Si  $y_0$  es una solución de la congruencia  $ny \equiv -b \pmod{a}$ , entonces el número

$$x_0 = \frac{ny_0 + b}{a}$$

es una solución de la congruencia original.

*Demostración.* Como  $y_0$  es solución de la congruencia  $ny \equiv -b \pmod{a}$ , entonces  $x_0$  es un entero y además

$$\begin{aligned} ax_0 &= a \frac{ny_0 + b}{a} \\ &= ny_0 + b \\ &\equiv b \pmod{n}. \end{aligned}$$

Luego  $x_0$  es solución de  $ax \equiv b \pmod{n}$ .  $\square$

**4.51 Ejemplo.** Resolvamos la congruencia  $245x \equiv 64 \pmod{9923}$ , usando el teorema anterior.

Por el teorema nos reducimos a resolver la congruencia

$$9923y \equiv -64 \pmod{245},$$

o sea

$$123y \equiv -64 \pmod{245}.$$

Nuevamente por el teorema, nos reducimos a resolver la congruencia

$$245z \equiv 64 \pmod{123},$$

o sea

$$\begin{aligned} 122z &\equiv 64 \pmod{123} \\ -z &\equiv 64 \pmod{123} \\ z &\equiv -64 \equiv 59 \pmod{123}. \end{aligned}$$

$$\text{Luego } y_0 = \frac{(245)(59) - 64}{123} = 117 \text{ y}$$

$$x_0 = \frac{(9923)(117) + 64}{245} = 4739.$$

Cuando apliquemos el teorema anterior a una congruencia  $ax \equiv b \pmod{n}$  donde  $(a, n) \nmid b$ , es claro que el proceso nos conduce a una congruencia que no tiene solución.

## 4.6 Ecuaciones Diofánticas lineales

Una *ecuación diofántica lineal* en 2 variables tiene la forma

$$ax + by = c,$$

donde  $a, b$  y  $c$  son enteros con  $ab \neq 0$ .

Determinar las soluciones de esta ecuación diofántica es equivalente a determinar las soluciones de alguna de las congruencias lineales

$$ax \equiv c \pmod{b} \quad \text{o} \quad by \equiv c \pmod{a}.$$

Según el Teorema 4.47, sabemos que existe solución si y solo si  $d \mid c$  donde  $d = (a, b)$ . Además si  $x_0$  es una solución de  $ax \equiv c \pmod{b}$ , sabemos que todas las demás soluciones de esta congruencia son de la forma

$$x = x_0 + k \frac{b}{d}.$$

A partir de la ecuación  $ax + by = c$ , podemos obtener los valores correspondientes de  $y$ . Cuando  $x = x_0$  obtenemos

$$y_0 = \frac{c - ax_0}{b}$$

y cuando  $x = x_0 + k \frac{b}{d}$  obtenemos

$$\begin{aligned} y &= \frac{c - a(x_0 + k \frac{b}{d})}{b} \\ &= \frac{c - ax_0}{b} - \frac{ka}{d} \\ &= y_0 - \frac{ka}{d}. \end{aligned}$$

Por lo tanto hemos demostrado el resultado siguiente.

**4.52 Teorema.** *La ecuación diofántica  $ax + by = c$  tiene solución, si y solo si,  $d \mid c$  donde  $d = (a, b)$ .*

*Además, si  $x_0$  y  $y_0$  es una solución particular de la ecuación, entonces todas las soluciones están dadas por las ecuaciones*

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

*donde  $k$  es un entero arbitrario.*

**4.53 Ejemplo.** Resolvamos la ecuación diofántica  $256x - 36y = 64$ .

La ecuación es equivalente a la congruencia

$$256x \equiv 64 \pmod{36}$$

o sea,

$$4x \equiv 28 \pmod{36}$$

$$x \equiv 7 \pmod{9}.$$

Luego  $x_0 = 7$  y  $y_0 = ((256)(7) - 64)/36 = 48$ . Como  $(256, -36) = 4$ , la solución general es

$$x = 7 + k(-36/4) = 7 - 9k$$

$$y = 48 - k(256/4) = 48 - 64k,$$

donde  $k$  es un entero arbitrario.

**4.54 Ejemplo.** Un comerciante compró lápices y borradores por \$2.490. Si cada lápiz costo \$29 y cada borrador costó \$33, ¿cuántos lápices y cuántos borradores compró?

*Solución:* Llamemos  $x$  al número de lápices y  $y$  al número de borradores que el comerciante compró. Tenemos que resolver la ecuación

$$29x + 33y = 2.490,$$

sujeta a las condiciones  $x > 0$  y  $y > 0$ .

La ecuación es equivalente a

$$29x \equiv 2.490 \pmod{33},$$

o sea

$$-4x \equiv 15 \pmod{33}$$

$$-32x \equiv 120 \pmod{33}$$

$$x \equiv 21 \pmod{33}.$$

Luego  $x_0 = 21$  y  $y_0 = \frac{2490 - (29)(21)}{33} = 57$ . Como  $(29, 33) = 1$ , la solución general de la ecuación es

$$x = 21 + 33k$$

$$y = 57 - 29k,$$

donde  $k$  es un entero arbitrario.

Si queremos que  $x > 0$  y  $y > 0$  tenemos

$$21 + 33k > 0 \quad \text{y} \quad 57 - 29k > 0.$$

Luego  $k > \frac{-21}{33}$  y  $k < \frac{57}{29}$ . Los valores enteros de  $k$  que cumplen ambas condiciones son  $k = 0$  y  $k = 1$ .

Si  $k = 0$  obtenemos  $x = 21, y = 57$ .

Si  $k = 1$  obtenemos  $x = 54, y = 28$ .

Por lo tanto el comerciante compró 21 lápices y 57 borradores, o 54 lápices y 28 borradores.

## 4.7 Sistemas de congruencias lineales

Los sistemas formados por varias congruencias lineales se resuelven en forma similar a la utilizada en álgebra elemental para resolver sistemas de ecuaciones lineales. Nos vamos a limitar a estudiar el caso en que tenemos el mismo número de congruencias y de incógnitas, donde todas las congruencias tienen el mismo módulo.

El caso más frecuente se presenta cuando tenemos un sistema formado por dos congruencias con dos incógnitas de la forma

$$\begin{aligned} ax + by &\equiv e \pmod{m} \\ cx + dy &\equiv f \pmod{m}, \end{aligned} \tag{4.1}$$

donde  $a, b, c, d, e$  y  $f$  son enteros arbitrarios y  $m$  es un entero positivo.

El siguiente resultado nos presenta una condición suficiente para poder resolver un sistema de la forma anterior.

**4.55 Teorema.** *Si los enteros  $a, b, c, d, e, f$  y  $m$  satisfacen la condición  $(D, m) = 1$ , donde  $D = ad - bc$ , entonces el sistema de congruencias (4.1), tiene solución única módulo  $m$  dada por*

$$\begin{aligned} x &\equiv D'(de - bf) \pmod{m} \\ y &\equiv D'(af - ce) \pmod{m}, \end{aligned}$$

donde  $D'$  es el inverso de  $D$  módulo  $m$ .

*Demostración.* Multiplicando la primera congruencia del sistema por  $d$  y la segunda por  $b$  obtenemos

$$adx + bdy \equiv de \pmod{m}$$

$$bcx + bdy \equiv bf \pmod{m}.$$

Restando la segunda congruencia de la primera encontramos

$$(ad - bc)x \equiv de - bf \pmod{m},$$

o sea

$$Dx \equiv de - bf \pmod{m},$$

puesto que  $D = ad - bc$ .

Multiplicando por el inverso  $D'$  de  $D$  módulo  $m$ , obtenemos

$$x \equiv D'(de - bf) \pmod{m}.$$

En forma similar podemos ver que

$$y \equiv D'(af - ce) \pmod{m}.$$

□

**4.56 Ejemplo.** Resolvamos el sistema

$$11x + 8y \equiv 3 \pmod{14}$$

$$3x + 5y \equiv 8 \pmod{14}.$$

Como  $11 \cdot 5 - 8 \cdot 3 = 31$  y  $(31, 14) = 1$ , el sistema tiene solución. En lugar de aplicar directamente las fórmulas obtenidas en el teorema, aplicamos el procedimiento utilizado en su demostración.

Multiplicando la primera congruencia por 5 y la segunda por 8 tenemos

$$55x + 40y \equiv 15 \pmod{14}$$

$$24x + 40y \equiv 64 \pmod{14}.$$

Restando la segunda congruencia de la primera nos queda

$$31x \equiv -49 \pmod{14},$$

y reduciendo módulo 14 obtenemos

$$3x \equiv 7 \pmod{14}.$$

Multiplicando por 5 que es el inverso de 3 módulo 14 tenemos

$$5 \cdot 3x \equiv 5 \cdot 7 \pmod{14},$$

o sea

$$x \equiv 7 \pmod{14}.$$

Similarmente si multiplicamos la primera congruencia por 3 y la segunda por 11 tenemos

$$33x + 24y \equiv 9 \pmod{14}$$

$$33x + 55y \equiv 88 \pmod{14}.$$

Restando la primera congruencia de la segunda nos queda

$$31y \equiv 79 \pmod{14},$$

y reduciendo módulo 14 obtenemos

$$3y \equiv 9 \pmod{14}.$$

Multiplicando por 5 que es el inverso de 3 módulo 14 tenemos

$$5 \cdot 3y \equiv 5 \cdot 9 \pmod{14},$$

o sea

$$y \equiv 3 \pmod{14}.$$

Por lo tanto la solución del sistema esta dada por todas las parejas  $(x, y)$  que satisfacen

$$x \equiv 7 \pmod{14}, \quad y \equiv 3 \pmod{14}.$$

La solución de sistemas de  $n$  congruencias con  $n$  incógnitas, se puede efectuar por eliminación sucesiva de las incógnitas, como en el caso de los sistemas de ecuaciones lineales. Sin embargo, esta teoría se puede tratar de una manera más adecuada utilizando el concepto de matrices. Un estudio detallado de estos temas se puede consultar en la referencia bibliográfica [11].

---

## Ejercicios 4.5

---

Resolver cada una de las congruencias siguientes:

1.  $3x \equiv 15 \pmod{18}$ .
2.  $24x \equiv 62 \pmod{110}$ .
3.  $16x \equiv 43 \pmod{71}$ .
4.  $32x \equiv 64 \pmod{36}$ .
5.  $5x \equiv 8 \pmod{30}$ .
6.  $70x \equiv 30 \pmod{182}$ .
7.  $126x \equiv 38 \pmod{12575}$ .
8.  $425x \equiv 846 \pmod{863}$ .
9.  $723x \equiv 318 \pmod{1461}$ .
10.  $561x \equiv 407 \pmod{901}$ .

Hallar la solución general de las ecuaciones diofánticas siguientes:

11.  $10x + 14y = 8$ .
12.  $18x - 42y = 57$ .
13.  $20y - 15x = 100$ .
14.  $12x + 21y = 44$ .
15.  $64x + 13y = 907$ .
16. Un hombre cambió un cheque por cierta cantidad de dinero. El cajero equivocadamente intercambio el número de pesos con el número de centavos. Al revisar la cantidad recibida el hombre observó que tenía el doble de la cantidad por la cual había girado el cheque mas dos centavos. Por que valor fue girado el cheque?

17. Una señora compró 100 frutas por \$5.000. Las ciruelas le costaron a \$25, las manzanas a \$150 y las pitahayas a \$500. Cuántas frutas de cada clase compró?
18. La entrada a cierto museo vale \$900 para adultos y \$375 para niños. Cierta día en que asistieron más adultos que niños se recaudaron \$45.000. Cuántos adultos y cuántos niños asistieron al museo? *Nota:* Hay varias respuestas posibles.

Resolver cada uno de los siguientes sistemas de congruencias lineales:

19.  $4x + 5y \equiv 7 \pmod{17}$   
 $7x + 12y \equiv 4 \pmod{17}$ .
20.  $7x + 10y \equiv 5 \pmod{24}$   
 $16x + 15y \equiv 16 \pmod{24}$ .
21.  $x + 2y + 16z \equiv 4 \pmod{19}$   
 $x + 3y + z \equiv 11 \pmod{19}$   
 $2x + 5y + 15z \equiv 13 \pmod{19}$ .

22. Consideremos el sistema de congruencias lineales

$$\begin{aligned} ax + by &\equiv e \pmod{m} \\ cx + dy &\equiv f \pmod{m}, \end{aligned}$$

$$\text{y sean } D = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc, \quad D_1 = \begin{vmatrix} e & b \\ f & d \end{vmatrix} = ed - bf \text{ y } D_2 = \begin{vmatrix} a & e \\ c & f \end{vmatrix} = af - ec.$$

Probar que si  $(D, m) \mid D_1$  y  $(D, m) \mid D_2$ , entonces el sistema de tiene  $(D, m)$  soluciones incongruentes módulo  $m$ .

## 4.8 El Teorema chino del residuo

Vamos a estudiar cierta clase de sistemas de congruencias lineales, que fueron conocidos desde la antigüedad por los Chinos, y que nos servirán más adelante para resolver congruencias de grado mayor que uno.

**4.57 Teorema (Teorema Chino del residuo).** Sean  $m_1, m_2, \dots, m_r$  enteros positivos primos relativos dos a dos, y sean  $a_1, a_2, \dots, a_r$  enteros arbitrarios. Entonces el sistema de congruencia lineales

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

tiene solución única módulo  $m = \prod_{i=1}^r m_i$ .

*Demostración.* Para  $i = 1, 2, \dots, r$  sea  $M_i = \frac{m}{m_i} = \prod_{j \neq i} m_j$ . Entonces  $(M_i, m_i) = 1$  para todo  $i$ .

Por el Teorema 4.47 existen soluciones únicas para las congruencia lineales

$$M_i x \equiv 1 \pmod{m_i},$$

para  $i = 1, 2, \dots, r$ . Es decir existen enteros  $b_1, b_2, \dots, b_r$  tales que

$$M_1 b_1 \equiv 1 \pmod{m_1}, M_2 b_2 \equiv 1 \pmod{m_2}, \dots, M_r b_r \equiv 1 \pmod{m_r}.$$

Por lo tanto,

$$M_1 b_1 a_1 \equiv a_1 \pmod{m_1}, M_2 b_2 a_2 \equiv a_2 \pmod{m_2}, \dots, M_r b_r a_r \equiv a_r \pmod{m_r}$$

y si establecemos

$$x_0 = \sum_{i=1}^r M_i b_i a_i,$$

tenemos que  $x_0 \equiv a_i \pmod{m_i}$  para todo  $i$ , puesto que  $M_i \equiv 0 \pmod{m_j}$  para  $j \neq i$ . En consecuencia,  $x_0$  es una solución del sistema de congruencias.

Supongamos ahora que  $x_1$  y  $x_0$  son dos soluciones del sistema. Entonces

$$x_1 \equiv a_i \equiv x_0 \pmod{m_i},$$

para  $i = 1, 2, \dots, r$  y por el Corolario 4.11 concluimos que  $x_1 \equiv x_0 \pmod{m}$  donde  $m = \prod_{i=1}^r m_i$ . Por consiguiente, la solución es única módulo  $m$ .  $\square$

**4.58 Ejemplo.** Resolvamos el sistema de congruencias lineales

$$\begin{aligned}x &\equiv 2 \pmod{3} \\x &\equiv 6 \pmod{5} \\x &\equiv 7 \pmod{7} \\x &\equiv 10 \pmod{8}.\end{aligned}$$

En este caso tenemos:

$$\begin{aligned}m_1 &= 3 & M_1 &= 280 & a_1 &= 2, \\m_2 &= 5 & M_2 &= 168 & a_2 &= 6, \\m_3 &= 7 & M_3 &= 120 & a_3 &= 7, \\m_4 &= 8 & M_4 &= 105 & a_4 &= 10.\end{aligned}$$

Debemos resolver las congruencias  $M_i x \equiv 1 \pmod{m_i}$ , es decir las congruencias  $280x \equiv 1 \pmod{3}$ ,  $168x \equiv 1 \pmod{5}$ ,  $120x \equiv 1 \pmod{7}$  y  $105x \equiv 1 \pmod{8}$ . La primera congruencia se reduce a  $x \equiv 1 \pmod{3}$ , luego  $b_1 = 1$ . La segunda congruencia se reduce a  $3x \equiv 1 \pmod{5}$  y  $b_2 = 2$ ; la tercera se reduce a  $x \equiv 1 \pmod{7}$  y  $b_3 = 1$ . Finalmente la cuarta congruencia se reduce a  $x \equiv 1 \pmod{8}$  y  $b_4 = 1$ .

Por lo tanto la solución deseada es

$$x_0 = \sum_{i=1}^r M_i b_i a_i = (280)(1)(2) + (168)(2)(6) + (120)(1)(7) + (105)(1)(10) = 4466.$$

Esta solución es única módulo  $(3)(5)(7)(8) = 840$ , luego la menor solución del sistema es  $4466 - (5)(840) = 266$ .

El método anterior no es el más práctico para resolver sistemas de congruencias, la manera más fácil de proceder es como sigue.

Como  $x \equiv 2 \pmod{3}$ , entonces  $x = 2 + 3a$  donde  $a$  es un entero. Sustituyendo en la segunda congruencia tenemos,

$$\begin{aligned}2 + 3a &\equiv 6 \pmod{5} \\3a &\equiv 4 \pmod{5} \\21a &\equiv 28 \pmod{5} \\a &\equiv 3 \pmod{5}.\end{aligned}$$

Si  $a \equiv 3 \pmod{5}$ , entonces  $a = 3 + 5b$  y  $x = 2 + 3a = 2 + 3(3 + 5b) = 11 + 15b$  donde  $b$  es un entero. Sustituyendo en la tercera congruencia del sistema tenemos

$$\begin{aligned} 11 + 15b &\equiv 7 \pmod{7} \\ 15b &\equiv -4 \pmod{7} \\ b &\equiv 3 \pmod{7}. \end{aligned}$$

Si  $b \equiv 3 \pmod{7}$ , entonces  $b = 3 + 7c$  y  $x = 11 + 15(3 + 7c) = 56 + 105c$ , donde  $c$  es un entero. Sustituyendo en la cuarta congruencia del sistema tenemos

$$\begin{aligned} 56 + 105c &\equiv 10 \pmod{8} \\ 105c &\equiv -46 \pmod{8} \\ c &\equiv 2 \pmod{8}. \end{aligned}$$

Si  $c \equiv 2 \pmod{8}$ , entonces  $c = 2 + 8d$  y  $x = 56 + 105(2 + 8d) = 266 + 840d$ , donde  $d$  es un entero.

Por lo tanto la solución del sistema es  $x \equiv 266 \pmod{840}$ .

**4.59 Ejemplo.** Una banda de 13 piratas encontró cierto número de monedas de oro. Al distribuirlas equitativamente les sobraron 8 monedas. Debido a una fiebre murieron dos de los piratas y al hacer un nuevo reparto de monedas, les sobraron 3. Por peleas entre ellos murieron 3 más y en un último reparto le sobraron 5 monedas. Hallar el menor número de monedas que encontraron.

*Solución.* Representemos por  $x$  el número de monedas encontradas. Tenemos el sistema,

$$\begin{aligned} x &\equiv 8 \pmod{13} \\ x &\equiv 3 \pmod{11} \\ x &\equiv 5 \pmod{8}. \end{aligned}$$

Como  $x \equiv 8 \pmod{13}$ , entonces  $x = 8 + 13a$ . Reemplazando en la segunda congruencia tenemos,

$$\begin{aligned} 8 + 13a &\equiv 3 \pmod{11} \\ 13a &\equiv -5 \pmod{11} \\ 2a &\equiv 6 \pmod{11} \\ a &\equiv 3 \pmod{11}. \end{aligned}$$

Como  $a \equiv 3 \pmod{11}$ , entonces  $a = 3 + 11b$  y  $x = 8 + 13(3 + 11b) = 47 + 143b$ . Sustituyendo en la tercera congruencia tenemos

$$\begin{aligned} 47 + 143b &\equiv 5 \pmod{8} \\ 143b &\equiv -42 \pmod{8} \\ 7b &\equiv 6 \pmod{8} \\ -b &\equiv 6 \pmod{8} \\ b &\equiv -6 \pmod{8} \\ b &\equiv 2 \pmod{8}. \end{aligned}$$

Como  $b \equiv 2 \pmod{8}$ , entonces  $b = 2 + 8c$  y por lo tanto  $x = 47 + 143b = 47 + 143(2 + 8c) = 333 + 1144c$ . Luego el número mínimo de monedas que encontraron los piratas fue 333.

El teorema siguiente es una generalización del Teorema Chino del Residuo, su demostración la dejamos como ejercicio.

**4.60 Teorema.** Sean  $m_1, m_2, \dots, m_r$  enteros positivos y sean  $a_1, a_2, \dots, a_r$  enteros arbitrarios. Entonces el sistema de congruencias lineales,

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

tiene solución si y solo si

$$(m_i, m_j) \mid (a_i - a_j),$$

para todo  $i, j$  con  $i \neq j$ .

Además cuando hay solución, esta es única módulo  $[m_1, m_2, \dots, m_r]$ .

---

## Ejercicios 4.6

---

Resolver los siguientes sistemas de congruencias lineales

1.  $x \equiv 2 \pmod{3}$   
 $x \equiv 5 \pmod{7}$   
 $x \equiv 5 \pmod{8}$ .
2.  $x \equiv 3 \pmod{5}$   
 $x \equiv 6 \pmod{7}$   
 $x \equiv 4 \pmod{9}$   
 $x \equiv 8 \pmod{11}$ .
3.  $x \equiv 2 \pmod{7}$   
 $x \equiv 6 \pmod{9}$   
 $x \equiv 9 \pmod{14}$ .
4. Hallar el menor entero positivo que deja restos 2, 7 y 10 cuando se divide por 3, 10 y 13.
5. Un niño recogió en una piñata cierto número de dulces. Al contarlos de tres en tres le sobraron 2. Al contarlos de cuatro en cuatro le sobraron 3 y al contarlos de a cinco le sobró 1. Si el niño recogió menos de 20 dulces, ¿cuántos dulces recogió?
6. Hay una pila de ladrillos. Si se divide la pila en dos partes sobra un ladrillo, si se divide en tres partes sobran 2 ladrillos, cuando se divide en 4 partes sobran 3 ladrillos, si se divide en doce partes sobran 11 ladrillos, pero cuando se divide en trece partes no sobran ladrillos. ¿Cuál es el menor número de ladrillos que puede haber en la pila?
7. Probar que para todo entero positivo  $n$ , existen  $n$  enteros consecutivos  $a_1, a_2, \dots, a_n$  tales que  $p_i \mid a_i$  donde  $p_i$  representa el  $i$ -ésimo primo.
8. Demostrar que para cada entero positivo  $n$ , se pueden encontrar  $n$  enteros consecutivos divisibles por cuadrados perfectos.

## 4.9 Congruencias de grado superior

Como una aplicación del teorema chino del residuo tenemos la siguiente simplificación para resolver congruencias polinómicas con módulo compuesto.

**4.61 Teorema.** Sean  $m_1, m_2, \dots, m_r$  enteros positivos primos relativos dos a dos y sea  $m = \prod_{i=1}^r m_i$ . Entonces toda solución de la congruencia polinómica  $f(x) \equiv 0 \pmod{m}$  es una solución del sistema de congruencias,

$$\begin{aligned} f(x) &\equiv 0 \pmod{m_1} \\ f(x) &\equiv 0 \pmod{m_2} \\ &\vdots \\ f(x) &\equiv 0 \pmod{m_r}, \end{aligned}$$

y recíprocamente. Además si  $N$  es el número de soluciones de la congruencia  $f(x) \equiv 0 \pmod{m}$  y  $N_i$  es el número de soluciones de la congruencia  $f(x) \equiv 0 \pmod{m_i}$  para  $i = 1, 2, \dots, r$ , entonces

$$N = N_1 N_2 \dots N_r.$$

*Demostración.* Supongamos que  $f(a) \equiv 0 \pmod{m}$ . Como  $m_i \mid m$ , tenemos que  $f(a) \equiv 0 \pmod{m_i}$  para cada  $i$ . Así, toda solución de  $f(x) \equiv 0 \pmod{m}$  es también solución del sistema.

Supongamos ahora que  $a$  es una solución del sistema. Entonces  $f(a) \equiv 0 \pmod{m_i}$  para cada  $i$  y puesto que los  $m_i$  son primos relativos dos a dos, por el Corolario 4.11 tenemos que  $f(a) \equiv 0 \pmod{m}$ . Luego  $a$  es solución de la congruencia  $f(x) \equiv 0 \pmod{m}$ .

Supongamos que para cada  $i = 1, 2, \dots, r$   $a_i$  es una solución de la congruencia  $f(x) \equiv 0 \pmod{m_i}$ . Por el Teorema Chino del residuo, existe un entero  $a$  tal que

$$\begin{aligned} a &\equiv a_1 \pmod{m_1} \\ a &\equiv a_2 \pmod{m_2} \\ &\vdots \\ a &\equiv a_r \pmod{m_r}, \end{aligned}$$

y  $a$  es único módulo  $m$ . Por lo tanto para cada  $i = 1, 2, \dots, r$  tenemos

$$f(a) \equiv f(a_i) \equiv 0 \pmod{m_i},$$

y por la primera parte del teorema,  $a$  es solución de la congruencia  $f(x) \equiv 0 \pmod{m}$ . Como de esta forma podemos construir todas las soluciones de  $f(x) \equiv 0 \pmod{m}$ , y podemos elegir  $a_1$  de  $N_1$  formas,  $a_2$  de  $N_2$  formas y así sucesivamente el número  $N$  de soluciones de la congruencia polinómica es precisamente

$$N = N_1 N_2 \dots N_r,$$

como queríamos probar.

Si  $m$  tiene la representación canónica

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

podemos tomar  $m_i = p_i^{\alpha_i}$  en el teorema anterior y vemos que el problema de resolver una congruencia polinómica con módulo compuesto, se reduce a resolver congruencias cuyos módulos son potencias de números primos.  $\square$

**4.62 Ejemplo.** Resolvamos la congruencia  $3x^2 + 4x + 5 \equiv 0 \pmod{60}$ .

Como  $60 = 3 \cdot 4 \cdot 5$ , resolvemos primero cada una de las congruencias

$$3x^2 + 4x + 5 \equiv 0 \pmod{3}$$

$$3x^2 + 4x + 5 \equiv 0 \pmod{4}$$

$$3x^2 + 4x + 5 \equiv 0 \pmod{5}.$$

Por verificación directa vemos que la solución de la primera congruencia es 1, que las soluciones de la segunda congruencia son 1 y 3, y que las soluciones de la tercer congruencia son 0 y 2. Por lo tanto las soluciones de la congruencia original son las soluciones de los 4 sistemas

$$\begin{array}{cccc} x \equiv 1 \pmod{3} & x \equiv 1 \pmod{3} & x \equiv 1 \pmod{3} & x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{4} & x \equiv 1 \pmod{4} & x \equiv 3 \pmod{4} & x \equiv 3 \pmod{4} \\ x \equiv 0 \pmod{5} & x \equiv 2 \pmod{5} & x \equiv 0 \pmod{5} & x \equiv 2 \pmod{5}. \end{array}$$

Resolviendo cada uno de estos sistemas por el método de la sección anterior, encontramos que las soluciones buscadas son 25, 37, 55 y 7.

El Teorema Chino del residuo y su generalización también nos ofrecen un método para resolver sistemas arbitrarios de congruencias simultáneas.

El método consiste en resolver por separado cada una de las congruencias del sistema y luego mediante utilización de estos teoremas construir las soluciones del sistema como en el caso previamente estudiado. Veamos unos ejemplos.

**4.63 Ejemplo.** Resolver el sistema

$$\begin{aligned}2x &\equiv 5 \pmod{7} \\2x &\equiv 4 \pmod{6} \\x &\equiv 6 \pmod{8}.\end{aligned}$$

*Solución:* Si resolvemos separadamente cada una de las congruencias del sistema obtenemos 6 como solución de la primera congruencia, 2 y 5 como soluciones incongruentes de la segunda congruencia y 6 como solución de la tercera.

Consideremos ahora cada uno de los sistemas

$$\begin{array}{ll}x \equiv 6 \pmod{7} & x \equiv 6 \pmod{7} \\x \equiv 2 \pmod{6} & y \quad x \equiv 5 \pmod{6} \\x \equiv 6 \pmod{8} & x \equiv 6 \pmod{8}.\end{array}$$

Por el Teorema 4.60 el primer sistema tiene solución y al resolverlo obtenemos  $x \equiv 62 \pmod{168}$ .

Por el mismo teorema el segundo sistema no tiene solución. Luego la única solución del sistema en consideración es  $x \equiv 62 \pmod{168}$ .

**4.64 Ejemplo.** Resolvamos el sistema

$$\begin{aligned}2x^2 + 3x + 1 &\equiv 0 \pmod{5} \\3x + 4 &\equiv 0 \pmod{14}.\end{aligned}$$

Por verificación directa tenemos que 2 y 4 son las soluciones incongruentes de la primera congruencia. Resolviendo la segunda congruencia, obtenemos 8 como solución.

Consideremos ahora los sistemas

$$\begin{array}{ll}x \equiv 2 \pmod{5} & x \equiv 4 \pmod{5} \\x \equiv 8 \pmod{14} & x \equiv 8 \pmod{14}.\end{array}$$

Resolviéndolos, obtenemos para el sistema original las soluciones 22 y 64 módulo 70.

## Ejercicios 4.7

Resolver cada una de las congruencias siguientes:

1.  $x^2 + 3x + 2 \equiv 0 \pmod{15}$ .
2.  $2x^3 + 3x^2 + x + 30 \equiv 0 \pmod{42}$ .
3.  $x^4 + x^2 + 40 \equiv 0 \pmod{105}$ .

Resolver cada uno de los sistemas de congruencias siguientes,

4. 
$$\begin{aligned} 2x^2 + 4x + 4 &\equiv 0 \pmod{5} \\ 2x + 6 &\equiv 0 \pmod{11}. \end{aligned}$$
5. 
$$\begin{aligned} x^3 + x + 2 &\equiv 0 \pmod{10} \\ 5x + 2 &\equiv 0 \pmod{9} \end{aligned}$$
6. 
$$\begin{aligned} 3x &\equiv 5 \pmod{8} \\ 2x + 2 &\equiv 0 \pmod{4} \\ 4x + 3 &\equiv 0 \pmod{7}. \end{aligned}$$

#### 4.10 Congruencias con módulo una potencia de un primo

Hemos visto que el problema de resolver la congruencia polinómica

$$f(x) \equiv 0 \pmod{m}$$

se reduce al problema de resolver el sistema de congruencias

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \quad (i = 1, 2, \dots, r),$$

donde la representación canónica de  $m$  es  $m = \prod_{i=1}^r p_i^{\alpha_i}$ .

Veremos ahora que el problema puede reducirse aun más, a la solución de congruencias con módulo primo, junto con la solución de algunas congruencias lineales. Empezamos con un resultado preliminar

**4.65 Lema.** Si  $f(x)$  es un polinomio con coeficientes enteros entonces

$$f(a+h) = f(a) + hf'(a) + h^2q$$

donde  $a, h$  y  $q$  son enteros, y  $f'(a)$  es la derivada de  $f(x)$  evaluada en  $a$ .

*Demostración.* Supongamos que

$$f(x) = \sum_{k=0}^n c_k x^k.$$

Entonces,

$$\begin{aligned} f(a+h) &= \sum_{k=0}^n c_k (a+h)^k \\ &= c_0 + c_1(a+h) + \sum_{k=2}^n c_k (a+h)^k \\ &= c_0 + c_1(a+h) + \sum_{k=2}^n c_k \left( \sum_{j=0}^k \binom{k}{j} a^{k-j} h^j \right) \\ &= c_0 + c_1(a+h) + \sum_{k=2}^n c_k (a^k + ka^{k-1}h + h^2q_k) \end{aligned}$$

donde

$$q_k = \sum_{j=2}^k \binom{k}{j} a^{k-j} h^{j-2},$$

en un entero. Por lo tanto

$$\begin{aligned} f(a+h) &= \sum_{k=0}^n c_k a^k + h \sum_{k=1}^n k c_k a^{k-1} + h^2 \sum_{k=2}^n c_k q_k \\ &= f(a) + hf'(a) + h^2q, \end{aligned}$$

donde  $q$  es un entero. □

Consideremos ahora la congruencia polinómica

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{4.2}$$

donde  $\alpha \geq 2$ .

Supongamos que  $a$  es una solución de la congruencia (4.1) tal que

$$0 \leq a < p^\alpha.$$

Esta solución también satisface la congruencia

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}. \quad (4.3)$$

Si dividimos  $a$  por  $p^{\alpha-1}$  podemos escribir

$$a = qp^{\alpha-1} + r, \text{ con } 0 \leq r < p^{\alpha-1}.$$

Como  $r \equiv a \pmod{p^{\alpha-1}}$ , entonces  $r$  es también solución de la congruencia (4.2). Decimos que la solución  $r$  es generada por la solución  $a$ .

Hemos visto que toda solución  $a$  de la congruencia (4.1) en el intervalo  $0 \leq a < p^\alpha$  genera una solución  $r$  de la congruencia (4.2) en el intervalo  $0 \leq r < p^{\alpha-1}$ .

Supongamos ahora que empezamos con una solución  $r$  de la congruencia (4.2) en el intervalo  $0 \leq r < p^{\alpha-1}$  y nos preguntamos si es posible encontrar una solución  $a$  de la congruencia (4.1) en el intervalo  $0 \leq a < p^\alpha$ , que genere a  $r$ . Cuando esto es posible decimos que  $r$  se puede levantar de  $p^{\alpha-1}$  a  $p^\alpha$ . El teorema siguiente nos indica que la posibilidad de levantar  $r$  de  $p^{\alpha-1}$  a  $p^\alpha$  depende de  $f(r)$  módulo  $p^\alpha$  y de  $f'(r)$  módulo  $p$ .

**4.66 Teorema.** *Supongamos que  $\alpha \geq 2$  y que  $r$  es una solución de la congruencia*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

*tal que  $0 \leq r < p^{\alpha-1}$ . Tenemos:*

1. *Si  $f'(r) \not\equiv 0 \pmod{p}$ ,  $r$  puede levantarse de manera única de  $p^{\alpha-1}$  a  $p^\alpha$ , es decir existe un único entero  $a$  en el intervalo  $0 \leq a < p^\alpha$  que genera a  $r$  y satisface la congruencia*

$$f(x) \equiv 0 \pmod{p^\alpha}.$$

2. *Si  $f'(r) \equiv 0 \pmod{p}$  y  $f(r) \equiv 0 \pmod{p^\alpha}$ ,  $r$  puede levantarse de  $p^{\alpha-1}$  a  $p^\alpha$  de  $p$  formas diferentes.*
3. *Si  $f'(r) \equiv 0 \pmod{p}$  y  $f(r) \not\equiv 0 \pmod{p^\alpha}$ ,  $r$  no puede levantarse de  $p^{\alpha-1}$  a  $p^\alpha$ .*

*Demostración.* Aplicando el lema con  $a = r$  y  $h = tp^{\alpha-1}$  donde  $t$  es un entero que vamos a determinar, tenemos

$$\begin{aligned} f(r + tp^{\alpha-1}) &= f(r) + tp^{\alpha-1}f'(r) + t^2p^{2\alpha-2}q \\ &\equiv f(r) + tp^{\alpha-1}f'(r) \pmod{p^\alpha}, \end{aligned}$$

ya que  $2\alpha - 2 \geq \alpha$  puesto que  $\alpha \geq 2$ .

Como  $r$  es solución de la congruencia  $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ , podemos escribir  $f(r) = kp^{\alpha-1}$  y la congruencia se convierte en

$$f(r + tp^{\alpha-1}) \equiv (k + tf'(r))p^{\alpha-1} \pmod{p^\alpha},$$

o sea

$$f(r + tp^{\alpha-1}) \equiv \left( \frac{f(r)}{p^{\alpha-1}} + tf'(r) \right) p^{\alpha-1} \pmod{p^\alpha},$$

Por lo tanto el número

$$a = r + tp^{\alpha-1}$$

es solución de la congruencia  $f(x) \equiv 0 \pmod{p^\alpha}$  si y solo si  $t$  es solución de la congruencia lineal

$$tf'(r) + \frac{f(r)}{p^{\alpha-1}} \equiv 0 \pmod{p}. \quad (4.4)$$

Si  $f'(r) \not\equiv 0 \pmod{p}$ , por el Teorema 4.47 la congruencia (4.3) tiene solución única  $t$  módulo  $p$  y si escogemos  $t$  tal que  $0 \leq t < p$  entonces el número  $a$  es una solución de  $f(x) \equiv 0 \pmod{p^\alpha}$  tal que  $0 \leq a < p^\alpha$ . Esto demuestra la parte 1.

Si  $f'(r) \equiv 0 \pmod{p}$ , la congruencia (4.3) tiene solución si y solo si  $f(r) \equiv 0 \pmod{p^\alpha}$ .

Si  $f(r) \equiv 0 \pmod{p^\alpha}$  los  $p$  valores  $t = 0, 1, \dots, p-1$  dan origen a  $p$  soluciones  $a$  de la congruencia  $f(x) \equiv 0 \pmod{p^\alpha}$  que generan a  $r$  y tales que  $0 \leq a < p^\alpha$ . Esto demuestra la parte 2.

Si  $f(r) \not\equiv 0 \pmod{p^\alpha}$  la congruencia (4.3) no tiene solución y no se pueden encontrar ningún valor de  $t$  que convierta a  $a$  en solución de  $f(x) \equiv 0 \pmod{p^\alpha}$ , quedando así demostrado 3 y el teorema.  $\square$

El teorema anterior proporciona un método para resolver congruencias polinómicas con módulo una potencia de un primo, reduciendo el problema

a la solución de congruencias de la forma

$$f(x) \equiv 0 \pmod{p}.$$

A partir de las soluciones de esta última congruencia, construimos como se indica en la demostración del teorema las soluciones de la congruencia

$$f(x) \equiv 0 \pmod{p^2}.$$

Luego, a partir de las soluciones de esta congruencia construimos las soluciones de la congruencia

$$f(x) \equiv 0 \pmod{p^3},$$

y así sucesivamente.

**4.67 Ejemplo.** Usemos el teorema anterior para resolver la congruencia

$$7x^4 + 19x + 25 \equiv 0 \pmod{27}.$$

En este caso  $f(x) = 7x^4 + 19x + 25$  y  $f'(x) = 28x^3 + 19$ .

1. Comenzamos resolviendo la congruencia  $f(x) \equiv 0 \pmod{3}$ . Por verificación directa vemos que su única solución es  $x = 1$ .
2. Para encontrar las soluciones de  $f(x) \equiv 0 \pmod{9}$  usamos el teorema con  $p = 3$ ,  $\alpha = 2$  y  $r = 1$ .  
El número  $a = r + tp^{\alpha-1} = 1 + 3t$  es solución de  $f(x) \equiv 0 \pmod{9}$  si  $t$  es solución de la congruencia lineal

$$tf'(r) + \frac{f(r)}{p^{\alpha-1}} \equiv 0 \pmod{p}.$$

Como  $f(1) = 51$  y  $f'(1) = 47$ , la congruencia anterior toma la forma

$$47t + 17 \equiv 0 \pmod{3}$$

Resolviéndola tenemos

$$\begin{aligned} 2t + 2 &\equiv 0 \pmod{3} \\ 2t &\equiv -2 \pmod{3} \\ -t &\equiv -2 \pmod{3} \\ t &\equiv 2 \pmod{3} \end{aligned}$$

Luego  $a = 1 + (3)(2) = 7$  es la solución de  $f(x) \equiv 0 \pmod{9}$ .

3. Para encontrar las soluciones de  $f(x) \equiv 0 \pmod{27}$  aplicamos nuevamente el teorema con  $p = 3, \alpha = 3$  y  $r = 7$ .

Tenemos que  $a = 7 + t(3^2)$  es solución de la congruencia  $f(x) \equiv 0 \pmod{27}$  si  $t$  es solución de la congruencia lineal

$$tf'(7) + f(7)/3^2 \equiv 0 \pmod{3}.$$

Como  $f(7) = 16965$  y  $f'(7) = 9623$ , la congruencia lineal se convierte en

$$9623t + 1885 \equiv 0 \pmod{3}$$

Resolviendo tenemos,

$$2t + 1 \equiv 0 \pmod{3}$$

$$2t \equiv -1 \pmod{3}$$

$$-t \equiv -1 \pmod{3}$$

$$t \equiv 1 \pmod{3}$$

Por lo tanto la solución de la congruencia  $f(x) \equiv 0 \pmod{27}$  es  $a = 7 + (1)(3^2) = 16$ .

Veamos otro ejemplo.

**4.68 Ejemplo.** Resolvamos la congruencia  $x^2 + 2x + 2 \equiv 0 \pmod{25}$ .

En este caso  $f(x) = x^2 + 2x + 2$  y  $f'(x) = 2x + 2$ .

1. Por verificación directa vemos que las soluciones de  $x^2 + 2x + 2 \equiv 0 \pmod{5}$  son 1 y 2.
2. Aplicando el teorema con  $p = 5, \alpha = 2$  y  $r = 1$  tenemos que  $a = 1 + t5$  es una solución de  $f(x) \equiv 0 \pmod{25}$  si  $t$  es solución de la congruencia

$$tf'(1) + f(1)/5 \equiv 0 \pmod{5}.$$

Como  $f(1) = 5$  y  $f'(1) = 4$  esta congruencia toma la forma

$$4t + 1 \equiv 0 \pmod{5}$$

Resolviéndola tenemos

$$4t \equiv -1 \pmod{5}$$

$$-t \equiv -1 \pmod{5}$$

$$t \equiv 1 \pmod{5}.$$

Por lo tanto una solución de  $f(x) \equiv 0 \pmod{25}$  es  $a = 1 + 1(5) = 6$ .

Aplicando ahora el teorema con  $p = 5$ ,  $\alpha = 2$  y  $r = 2$ , tenemos que  $a = 2 + t5$  es solución de  $f(x) \equiv 0 \pmod{25}$  si  $t$  es solución de

$$tf'(2) + f(2)/5 \equiv 0 \pmod{5}.$$

Como  $f(2) = 10$  y  $f'(2) = 6$ , esta congruencia se convierte en

$$6t + 2 \equiv 0 \pmod{5}.$$

Resolviéndola

$$6t \equiv -2 \pmod{5}$$

$$t \equiv -2 \equiv 3 \pmod{5}.$$

Luego otra solución de  $f(x) \equiv 0 \pmod{25}$  es  $a = 2 + 3(5) = 17$ . En total las soluciones incongruentes de  $x^2 + 2x + 2 \equiv 0 \pmod{25}$  son 6 y 17.

---

## Ejercicios 4.8

---

Resolver cada una de las congruencias siguientes:

1.  $2x^3 + 12x^2 + 9x + 90 \equiv 0 \pmod{125}$ .
2.  $6x^4 + 7x^3 + 21x + 16 \equiv 0 \pmod{25}$ .
3.  $2x^3 + x^2 - 7x + 3 \equiv 0 \pmod{27}$ .
4.  $x^3 + x^2 - 5 \equiv 0 \pmod{343}$ .
5.  $x^3 + x^2 - x + 15 \equiv 0 \pmod{200}$ .

## 4.11 Teoremas de Lagrange y Wilson

En la sección anterior vimos que el problema de resolver una congruencia polinómica de la forma

$$f(x) \equiv 0 \pmod{p^\alpha},$$

con  $p$  primo, se reduce en últimas a resolver la congruencia

$$f(x) \equiv 0 \pmod{p}$$

Veamos ahora algunas propiedades de estas congruencias. Una primera simplificación nos indica que el polinomio  $f(x)$  puede remplazarse por un polinomio de grado a lo más  $p - 1$ , de acuerdo con el teorema siguiente.

**4.69 Teorema.** *Si el grado  $n$  de  $f(x)$  es mayor o igual a  $p$ , entonces existe un polinomio  $r(x)$  de grado a lo más  $p - 1$ , de tal forma que  $r(x) \equiv 0 \pmod{p}$  y  $f(x) \equiv 0 \pmod{p}$  tienen las mismas soluciones.*

*Demostración.* Dividiendo  $f(x)$  por  $x^p - x$  obtenemos polinomios  $q(x)$  y  $r(x)$  con coeficientes enteros y con  $r(x)$  de grado a lo más  $p - 1$ , tales que

$$f(x) = q(x)(x^p - x) + r(x).$$

Por el Teorema de Fermat, se tiene que  $a^p \equiv a \pmod{p}$ , para todo entero  $a$ . Por lo tanto se sigue que

$$f(a) \equiv r(a) \pmod{p},$$

para todo entero  $a$ .

En consecuencia,  $f(a) \equiv 0 \pmod{p}$  si y solo si  $r(a) \equiv 0 \pmod{p}$ , y las congruencias  $f(x) \equiv 0 \pmod{p}$  y  $r(x) \equiv 0 \pmod{p}$  tienen las mismas soluciones.  $\square$

**4.70 Ejemplo.** Reduzcamos la congruencia

$$3x^{10} + 2x^9 - 4x^6 - x^5 + 2x^2 - x \equiv 0 \pmod{5},$$

a una congruencia polinómica equivalente de grado a lo más 4.

Dividiendo el polinomio dado por  $x^5 - x$  tenemos,



Supongamos que el teorema es cierto para polinomios de grado  $n - 1$ . Consideremos un polinomio  $f(x)$  de grado  $n$  y escojamos una solución  $a$  de la congruencia  $f(x) \equiv 0 \pmod{p}$ . Podemos escribir

$$f(x) = (x - a)g(x) + r,$$

con  $r$  constante y  $g(x)$  un polinomio de grado  $n - 1$  con coeficientes enteros y coeficiente principal  $a_n$ .

De la ecuación anterior tenemos  $f(a) = r$  y como  $f(a) \equiv 0 \pmod{p}$ , entonces  $r \equiv 0 \pmod{p}$  y para todo  $x$  tenemos que

$$f(x) \equiv (x - a)g(x) \pmod{p}. \quad (4.5)$$

Por la hipótesis de inducción de inducción la congruencia  $g(x) \equiv 0 \pmod{p}$  tiene a lo más  $n - 1$  soluciones incongruentes. Supongamos que ellas son  $c_1, \dots, c_r$  con  $r \leq n - 1$ . Si  $c$  es un número tal que  $f(c) \equiv 0 \pmod{p}$ , entonces de (4.4)

$$(c - a)g(c) \equiv 0 \pmod{p},$$

así que

$$c \equiv a \pmod{p},$$

o

$$g(c) \equiv 0 \pmod{p}.$$

En el último caso  $c = c_i$  para algún  $i$  con  $1 \leq i \leq r$  y la congruencia  $f(x) \equiv 0 \pmod{p}$  tiene a lo más  $r + 1 \leq n$  soluciones. Luego el teorema es verdadero por el principio de inducción matemática.  $\square$

**4.72 Corolario.** Si  $f(x) = a_0 + a_1x + \dots + a_nx^n$  es un polinomio de grado  $n$  con coeficientes enteros, y si la congruencia

$$f(x) \equiv 0 \pmod{p},$$

con  $p$  primo, tiene más de  $n$  soluciones, entonces todos los coeficientes de  $f(x)$  son divisibles por  $p$ .

*Demostración.* Supongamos que no todos los coeficientes son divisibles por  $p$ . Sea  $k$  el mayor índice tal que  $p \nmid a_k$ . Luego  $k \leq n$  y la congruencia  $f(x) \equiv 0 \pmod{p}$  se reduce a

$$a_0 + a_1x + \dots + a_kx^k \equiv 0 \pmod{p}.$$

Como esta última congruencia tiene más de  $k$  soluciones, se contradice el Teorema de Lagrange. Por lo tanto todos los coeficientes de  $f(x)$  deben ser divisibles por  $p$ .  $\square$

Otro corolario importante del Teorema de Lagrange es el Teorema de Wilson que proporciona una condición necesaria para que un número sea primo.

**4.73 Teorema (Teorema de Wilson).** *Para todo número primo  $p$  se tiene que*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

*Demostración.* Consideremos el polinomio de grado  $p-2$  definido por

$$f(x) = (x-1)(x-2)\dots(x-p+1) - (x^{p-1} - 1).$$

Por el Teorema de Fermat, cada uno de los números  $1, 2, \dots, p-1$  es una solución de la congruencia  $f(x) \equiv 0 \pmod{p}$ . Por el corolario anterior los coeficientes de  $f(x)$  son divisibles por  $p$ , en particular el término constante

$$f(0) = (-1)^{p-1}(p-1)! + 1,$$

es divisible por  $p$ , o sea

$$(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p}.$$

Si  $p$  es impar  $(-1)^{p-1} = 1$ , y si  $p = 2$ ,  $(-1)^{p-1} = -1 \equiv 1 \pmod{p}$ . Luego en cualquier caso

$$(p-1)! + 1 \equiv 0 \pmod{p}. \quad \square$$

El recíproco del Teorema de Wilson también es cierto y dejamos su demostración como ejercicio.

**4.74 Ejemplo.** Sea  $p$  un número primo y  $a, b$  enteros no negativos tales que  $a + b = p - 1$ . Veamos que  $a!b! \equiv (-1)^{b+1} \pmod{p}$ .

Tenemos

$$p-1 \equiv -1 \pmod{p}$$

$$p-2 \equiv -2 \pmod{p}$$

.

.

.

$$p-b \equiv -b \pmod{p}.$$

por lo tanto

$$(p-1)(p-2)\dots(p-b) \equiv (-1)^b b! \pmod{p}.$$

Multiplicando por  $[p - (b + 1)]! = a!$ , nos queda

$$(p-1)! \equiv (-1)^b a! b! \pmod{p},$$

que por el Teorema de Wilson se convierte en

$$-1 \equiv (-1)^b a! b! \pmod{p},$$

multiplicando por  $(-1)^b$  obtenemos finalmente

$$(-1)^{b+1} \equiv a! b! \pmod{p}.$$

---

## Ejercicios 4.9

---

En los ejercicios 1 y 2 reducir la congruencia polinómica a una congruencia de grado menor que el módulo.

1.  $4x^8 + 3x^6 + 3x^5 + 3x^4 + 4x^2 + x \equiv 0 \pmod{5}$ .
2.  $4x^{12} + 6x^{10} + 5x^8 + 6x^4 + 5x^3 + 5 \equiv 0 \pmod{7}$ .
3. Demostrar que si  $(a_n, p) = 1$ , la congruencia polinómica

$$a_0 + a_1x + \dots + a_nx^n \equiv 0 \pmod{p},$$

es equivalente a una congruencia polinómica de grado  $n$  con coeficiente principal igual a 1.

4. Demostrar el recíproco del Teorema de Wilson.

5. Demostrar el Teorema de Wilson para  $p \geq 5$  considerando los pares de números  $k, j$  de la sucesión  $2, 3, \dots, p-2$  que satisfacen la condición  $kj \equiv 1 \pmod{p}$ .

*Sugerencia:* Demostrar que para todo  $k$  en dicha sucesión la congruencia  $kx \equiv 1 \pmod{p}$  tiene exactamente una solución incongruente  $j$  en la sucesión.

6. Si  $p$  es un primo probar que

$$(p-1)! \equiv p-1 \pmod{\frac{(p-1)p}{2}}.$$

7. Si  $p$  es un primo impar tal que  $p \equiv 1 \pmod{4}$ , probar que  $x^2 \equiv -1 \pmod{p}$  tiene solución.

*Sugerencia:* Use el resultado del último ejemplo.

8. Demostrar que si  $p$  es primo y  $d \mid (p-1)$  entonces la congruencia  $x^d \equiv 1 \pmod{p}$  tiene exactamente  $d$  soluciones incongruentes.

---

## Residuos cuadráticos

---

En este capítulo estudiaremos las congruencias de segundo grado con módulo primo, analizaremos la noción de residuo cuadrático y demostraremos la conocida ley de la reciprocidad cuadrática de Gauss. También estudiaremos las nociones de orden módulo un entero positivo y de raíz primitiva. Finalmente ilustraremos como se puede deducir resultados importantes de teoría de números utilizando nociones de Algebra Abstracta.

### 5.1 Congruencias de segundo grado con módulo primo

Vimos en el capítulo anterior que la solución de congruencias polinómicas se reduce a la solución de congruencias con módulo primo; por tal razón en el estudio que vamos a realizar de las congruencias de segundo grado o cuadráticas, nos limitaremos al caso en que el módulo es un número primo.

Una *congruencia cuadrática* con módulo primo  $p$  tiene la forma,

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad \text{con } (a, p) = 1 \quad (5.1)$$

Si  $p = 2$ , la congruencia toma alguna de las formas,

$$\begin{aligned} x^2 &\equiv 0 \pmod{2}, & x^2 + 1 &\equiv 0 \pmod{2}, \\ x^2 + x &\equiv 0 \pmod{2}, & x^2 + x + 1 &\equiv 0 \pmod{2}, \end{aligned}$$

y la solución de cada una de estas congruencias se puede encontrar inmediatamente por inspección. Supondremos por lo tanto que  $p$  es un primo impar. Puesto que  $(4a, p) = 1$ , la congruencia (5.1) es equivalente con la congruencia

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

y por lo tanto con la congruencia

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}.$$

Hagamos  $b^2 - 4ac = d$  y  $X = 2ax + b$ . Entonces podemos escribir la congruencia anterior en la forma

$$X^2 \equiv d \pmod{p}. \tag{5.2}$$

Si la congruencia (5.2) no tiene solución, la congruencia (5.1) tampoco tiene solución. Si  $u$  es una solución de la congruencia (5.2), es decir si  $u$  satisface  $u^2 \equiv d \pmod{p}$  entonces el entero  $x_0$  que es una solución de la congruencia lineal

$$2ax + b \equiv u \pmod{p} \tag{5.3}$$

es una solución de la congruencia (5.1). Recíprocamente, si  $x_0$  es una solución de la congruencia (5.1), entonces  $2ax_0 + b \equiv u \pmod{p}$  donde  $u$  es una solución de la congruencia (5.2). Como la congruencia lineal (5.3) tiene exactamente una solución para cada valor de  $u$  en virtud del Teorema 4.47, vemos que hay una correspondencia biyectiva entre las soluciones de (5.1) y las soluciones de (5.2). Por lo tanto el problema de resolver congruencias de grado dos se reduce al problema de resolver congruencias de la forma

$$x^2 \equiv a \pmod{p}.$$

Por el Teorema de Lagrange, la congruencia anterior tiene a lo más dos soluciones incongruentes módulo  $p$ . Además, si  $x_0$  es una solución de la congruencia, entonces la otra solución es  $p - x_0$  ya que

$$(p - x_0)^2 \equiv x_0^2 \pmod{p}.$$

**5.1 Ejemplo.** Resolvamos la congruencia cuadrática

$$5x^2 - 6x + 2 \equiv 0 \pmod{13}.$$

La congruencia dada es equivalente a la congruencia

$$100x^2 - 120x + 40 \equiv 0 \pmod{13},$$

es decir a la congruencia

$$(10x - 6)^2 \equiv -4 \pmod{13}.$$

Si hacemos  $X = 10x - 6$ , tenemos la congruencia

$$X^2 \equiv -4 \pmod{13}.$$

Por verificación directa, encontramos que 3 y  $13 - 3 = 10$  son las soluciones de esta congruencia. Ahora, resolvemos las congruencias

$$10x - 6 \equiv 3 \pmod{13} \quad y \quad 10x - 6 \equiv 10 \pmod{13}.$$

Tenemos

$$\begin{array}{ll} 10x - 6 \equiv 3 \pmod{13} & y \quad 10x - 6 \equiv 10 \pmod{13} \\ 10x \equiv 9 \pmod{13} & 10x \equiv 16 \pmod{13} \\ -3x \equiv 9 \pmod{13} & 5x \equiv 8 \pmod{13} \\ -x \equiv 3 \pmod{13} & -8x \equiv 8 \pmod{13} \\ x \equiv -3 \equiv 10 \pmod{13} & -x \equiv 1 \pmod{13} \\ & x \equiv -1 \equiv 12 \pmod{13}. \end{array}$$

Por lo tanto las soluciones de las congruencias dadas son  $x \equiv 10 \pmod{13}$  y  $x \equiv 12 \pmod{13}$ .

Continuando con el estudio de la congruencia de la forma

$$x^2 \equiv a \pmod{p},$$

observamos primero que si  $a \equiv 0 \pmod{p}$ , esta congruencia tiene como única solución, la solución trivial  $x = 0$ ; por tal razón nos interesamos únicamente en el caso en que  $a \not\equiv 0 \pmod{p}$ . Si la congruencia tiene solución deberíamos decir que el número  $a$  es un cuadrado módulo  $p$ , pero históricamente se ha dicho es que el número  $a$  es un residuo cuadrático módulo  $p$ . Establezcamos de manera precisa la definición.

**5.2 Definición.** Sea  $p$  un primo impar y  $a$  un entero tal que  $(a, p) = 1$ . Si la congruencia

$$x^2 \equiv a \pmod{p}$$

tiene solución, decimos que  $a$  es un *residuo cuadrático* módulo  $p$ .

**5.3 Ejemplo.** Como los residuos cuadráticos módulo  $p$ , son precisamente los cuadrados módulo  $p$ , vemos que si  $p = 7$ , los residuos cuadráticos módulo 7 son 1, 4 y 2 ya que,

$$1^2 \equiv 6^2 \equiv 1 \pmod{7}, \quad 2^2 \equiv 5^2 \equiv 4 \pmod{7} \quad \text{y} \quad 3^2 \equiv 4^2 \equiv 2 \pmod{7}.$$

En general si  $(a, p) = 1$ , se sigue de la definición que  $a^2$  es un residuo cuadrático módulo  $p$ .

Para facilitar el estudio de los residuos cuadráticos introducimos el *símbolo de Legendre* mediante la definición siguiente

**5.4 Definición.** Si  $p$  es un primo impar y  $(a, p) = 1$ , definimos el *símbolo de Legendre*  $(a|p)$  mediante las ecuaciones

$$(a|p) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático módulo } p \\ -1 & \text{si } a \text{ no es un residuo cuadrático módulo } p \end{cases}$$

El símbolo de Legendre se representa con frecuencia por la notación  $\left(\frac{a}{p}\right)$ .

**5.5 Ejemplo.** 1.  $(1|7) = (2|7) = (4|7) = 1$ .

2.  $(3|7) = (5|7) = (6|7) = -1$ .

3. Si  $(a, p) = 1$  entonces  $(a^2|p) = 1$ . En particular  $(1|p) = 1$ .

**5.6 Teorema.** Sea  $p$  un primo impar. Entonces,

1. Si  $(a, p) = (b, p) = 1$  y  $a \equiv b \pmod{p}$  entonces  $(a|p) = (b|p)$ .

2. Hay exactamente  $\frac{p-1}{2}$  residuos cuadráticos módulo  $p$  incongruentes.

*Demostración.* 1 Es evidente. Además por 1, para determinar los residuos cuadráticos incongruentes nos podemos limitar al conjunto  $1, 2, \dots, p-1$ . La demostración de 2 consiste en probar que cada residuo cuadrático en el

conjunto  $1, 2, \dots, p-1$  es congruente módulo  $p$  con exactamente uno de los números

$$1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2.$$

Primero que todo observamos que los números en la colección anterior son todos diferentes módulo  $p$ . En efecto, si  $x^2 \equiv y^2 \pmod{p}$  con  $1 \leq x \leq \frac{p-1}{2}$ ,  $1 \leq y \leq \frac{p-1}{2}$  entonces,

$$(x-y)(x+y) \equiv 0 \pmod{p}$$

y por lo tanto,

$$x-y \equiv 0 \pmod{p} \text{ ,o, } x+y \equiv 0 \pmod{p},$$

pero como  $p > x+y$ , la segunda probabilidad no se presenta y en consecuencia

$$x \equiv y \pmod{p}.$$

Además, como

$$(p-k)^2 \equiv k^2 \pmod{p},$$

los cuadrados de los números  $1, 2, \dots, \frac{p-1}{2}$  son congruentes con los cuadrados de los números  $\frac{p+1}{2}, \dots, p-1$ . Por lo tanto todo residuo cuadrático en  $1, 2, \dots, p-1$  es congruente módulo  $p$  a exactamente uno de los números en la colección  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ , lo que completa la demostración.

El Teorema de Fermat nos dice que si  $(a, p) = 1$  entonces tenemos  $a^{p-1} \equiv 1 \pmod{p}$ , o sea  $a^{p-1} - 1 \equiv 0 \pmod{p}$ . Como

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

tenemos que

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

□

El criterio siguiente debido a Euler, nos dice que el valor obtenido en la congruencia anterior es 1 cuando  $(a|p) = 1$  y es  $-1$  cuando  $(a|p) = -1$ .

**5.7 Teorema (Criterio de Euler).** *Si  $p$  es un primo impar y  $(a, p) = 1$ , entonces*

$$a^{\frac{p-1}{2}} \equiv (a|p) \pmod{p}.$$

*Demostración.* Acabamos de ver que todo entero  $a$  satisface alguna de las congruencias

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{o,} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Además no puede satisfacer simultáneamente las dos, pues en tal caso se tendría que  $p \mid 2$ , lo cual es imposible ya que  $p$  es un primo impar.

Si  $(a|p) = 1$ , entonces existe una  $x_0$  tal que  $x_0^2 \equiv a \pmod{p}$  y por lo tanto

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod{p},$$

luego en este caso tenemos que  $a^{\frac{p-1}{2}} \equiv (a|p) \pmod{p}$ . El razonamiento anterior también nos muestra que todo residuo cuadrático módulo  $p$  es solución de la congruencia

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

y por el Teorema de Lagrange, concluimos que los  $\frac{p-1}{2}$  residuos cuadráticos son precisamente todas las soluciones de esta congruencia. Por lo tanto, si un número  $a$  no es residuo cuadrático, es decir si  $(a|p) = -1$ , entonces  $a$  satisface la congruencia

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

y también en este caso tenemos que  $a^{\frac{p-1}{2}} \equiv (a|p) \pmod{p}$  □

En el teorema siguiente, resumimos las propiedades principales del símbolo de Legendre.

**5.8 Teorema.** *Sea  $p$  un primo impar y sean  $a$  y  $b$  enteros primos relativos con  $p$ . Entonces:*

1. *Si  $a \equiv b \pmod{p}$  entonces  $(a|p) = (b|p)$ .*
2.  *$(a^2|p) = 1$ .*

3.  $(1|p) = 1$ .
4.  $(a|p) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .
5.  $(a|p)(b|p) = (ab|p)$ .
6.  $(-1|p) = (-1)^{\frac{p-1}{2}}$ .

*Demostración.* 1 es la parte 1 del Teorema 5.6, 2 y 3 son evidentes, 4 es el criterio de Euler. Una prueba de 5 es la siguiente: aplicando el criterio de Euler tenemos

$$(a|p)(b|p) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv (ab|p) \pmod{p},$$

y como  $(a|p)(b|p) = \pm 1$ ,  $(ab|p) = \pm 1$  y  $p > 2$  se sigue que  $(a|p)(b|p) = (ab|p)$ . Finalmente 6 se deduce de 4 cuando  $a = -1$ .  $\square$

**5.9 Corolario.** Si  $p$  es un primo impar tal que  $(a, p) = 1$  y la representación canónica de  $a$  como producto de primos es  $a = \prod_{i=1}^k p_i^{a_i}$ , entonces

$$(a|p) = \prod_{i=1}^k \left(\frac{p_i}{p}\right)^{a_i}.$$

*Demostración.* El resultado es consecuencia directa de la propiedad 5 del teorema.  $\square$

---

## Ejercicios 5.1

---

1. Resolver cada una de las siguientes congruencias:

- (a)  $5x^2 + x + 1 \equiv 0 \pmod{11}$ .
- (b)  $6x^2 + 7x - 15 \equiv 0 \pmod{23}$ .
- (c)  $4x^2 + 4x + 18 \equiv 0 \pmod{19}$ .
- (d)  $3x^2 - 4x + 10 \equiv 0 \pmod{13}$ .

(e)  $3x^2 + 9x + 20 \equiv 0 \pmod{28}$ .

2. Hallar todos los residuos cuadráticos módulo 13.
3. Hallar  $(a|p)$  cuando  $a = \pm 1, \pm 2, \pm 3$  y  $p = 11$ .
4. Sea  $p$  un primo impar y sean  $a$  y  $b$  enteros tales que  $(a, p) = (b, p) = 1$ . Probar que si las congruencias  $x^2 \equiv a \pmod{p}$  y  $x^2 \equiv b \pmod{p}$  no tienen solución, entonces la congruencia  $x^2 \equiv ab \pmod{p}$  tiene solución
5. Sea  $p$  un primo tal que  $p \equiv 1 \pmod{4}$ . Probar que  $a$  es un residuo cuadrático módulo  $p$  si y solo si  $p - a$  es un residuo cuadrático módulo  $p$ .
6. Sea  $p$  un primo tal que  $p \equiv 3 \pmod{4}$ . Probar que  $a$  es un residuo cuadrático módulo  $p$  si y solo si  $p - a$  no es residuo cuadrático módulo  $p$ .
7. Sea  $p$  un primo impar tal que  $(a, p) = 1$ . Probar que la congruencia  $ax^2 + bx + c \equiv 0 \pmod{p}$  tiene dos, una o ninguna soluciones, según que  $b^2 - 4ac$  sea un residuo cuadrático, sea congruente a cero, o no sea un residuo cuadrático módulo  $p$ .
8. Probar que la congruencia  $x^2 + 1 \equiv 0 \pmod{p}$  tiene solución si y solo si  $p$  es un primo de la forma  $4m + 1$ .
9. Probar que hay infinitos primos de la forma  $4m + 1$ .  
*Sugerencia:* Suponer que solo hay un número finito  $p_1, p_2, \dots, p_k$  de primos de esta forma, considerar el número  $N = 4p_1^2 p_2^2 \dots p_k^2 + 1$  y aplicar el ejercicio 8.
10. Sea  $p$  un primo impar. Probar que para todo entero positivo  $n$ , la congruencia  $x^2 \equiv p \pmod{p^n}$  tiene dos o ninguna soluciones, según  $a$  sea o no sea un residuo cuadrático módulo  $p$ . *Sugerencia:* usar el Teorema 4.64.

## 5.2 Ley de la reciprocidad cuadrática

La ley de la reciprocidad cuadrática es un resultado notable que proporciona un método práctico para determinar el carácter cuadrático de un número.

Esta ley fue establecida por primera vez por Euler en una forma muy complicada y redescubierta por Legendre, quien la demostró parcialmente en 1785. Gauss descubrió esta ley independientemente a la edad de 18 años en 1796, y presentó su primera demostración completa.

Empezaremos desarrollando unos resultados preliminares.

**5.10 Teorema (Lema de Gauss).** *Sea  $p$  un primo impar y sea  $a$  un entero tal que  $(a, p) = 1$ . Sea  $S$  el conjunto formado por los menores residuos positivos módulo  $p$  de los números*

$$a, 2a, 3a, \dots, \frac{p-1}{2}a.$$

*Si  $k$  representa el número de residuos que son mayores que  $\frac{p}{2}$ , entonces*

$$(a|p) = (-1)^k.$$

*Demostración.* Definimos  $t$  por  $k + t = \frac{p-1}{2}$  y representemos los elementos de  $S$  por  $a_1, a_2, \dots, a_t, b_1, b_2, \dots, b_k$  donde  $a_i < \frac{p}{2}$  para cada  $i$  y  $b_j > \frac{p}{2}$  para cada  $j$ .

Veamos primero dos observaciones. La primera es que todos los elementos de  $S$  son incongruentes módulo  $p$  y por lo tanto diferentes. En efecto, si  $m_1 \neq m_2$  y  $m_1 a \equiv m_2 a \pmod{p}$  entonces  $p \mid (m_1 - m_2)a$  y como  $(a, p) = 1$  entonces  $p \mid (m_1 - m_2)$  lo cual es imposible porque  $0 < m_1, m_2 \leq \frac{p-1}{2}$ .

La segunda es que  $a_i \neq p - b_j$  para todo  $i$  y todo  $j$ . En efecto, si  $a_i = p - b_j$  entonces  $a_i + b_j \equiv 0 \pmod{p}$ , y como  $a_i = m_i a$ ,  $b_j = m_j a$  para ciertos enteros  $m_i$  y  $m_j$  con  $m_i \neq m_j$ , entonces tendríamos  $m_i a + m_j a \equiv 0 \pmod{p}$ . Luego  $p \mid (m_i + m_j)a$  y como  $(a, p) = 1$ ,  $p \mid (m_i + m_j)$  lo que es imposible porque  $2 < m_i + m_j \leq p - 1$ .

Como  $\frac{p}{2} < b_j < p$  se tiene que  $0 < p - b_j < \frac{p}{2}$  para cada  $j$ , y de las dos observaciones anteriores concluimos que los  $\frac{p-1}{2}$  números  $p - b_1, p - b_2, \dots, p - b_k, a_1, a_2, \dots, a_t$  son todos diferentes, luego ellos son simplemente

los números  $1, 2, \dots, \frac{p-1}{2}$  en algún orden. Por lo tanto tenemos,

$$\begin{aligned} 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} &\equiv (p-b_1)(p-b_2) \cdots (p-b_k) a_1 a_2 \cdots a_t \pmod{p} \\ &\equiv (-b_1)(-b_2) \cdots (-b_k) a_1 a_2 \cdots a_t \pmod{p} \\ &\equiv (-1)^k b_1 b_2 \cdots b_k a_1 a_2 \cdots a_t \pmod{p}, \end{aligned}$$

y como

$$b_1 b_2 \cdots b_k a_1 \cdots a_t = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot a^{\frac{p-1}{2}},$$

tenemos

$$\frac{p-1}{2}! \equiv (-1)^k \frac{p-1}{2}! a^{\frac{p-1}{2}} \pmod{p},$$

multiplicando por  $(-1)^k$  y cancelando  $\frac{p-1}{2}!$  obtenemos

$$(-1)^k \equiv a^{\frac{p-1}{2}} \pmod{p},$$

que por el criterio de Euler se puede escribir en la forma

$$(-1)^k \equiv (a|p) \pmod{p}.$$

Como  $(-1)^k$  y  $(a|p)$  toman solo los valores  $\pm 1$ , se sigue de la congruencia anterior que

$$(a|p) = (-1)^k,$$

como queríamos probar.  $\square$

**5.11 Teorema.** Sea  $p$  un primo impar y sea  $a$  un entero tal que  $(a, p) = 1$ . Sea

$$M = \left[ \frac{a}{p} \right] + \left[ \frac{2a}{p} \right] + \cdots + \left[ \frac{1}{2} \frac{(p-1)a}{p} \right],$$

entonces

1. Si  $a$  es impar,  $(a|p) = (-1)^M$ .
2.  $(2|p) = (-1)^{\frac{p^2-1}{8}}$ .

*Demostración.* Sean  $r_1, r_2, \dots, r_{\frac{p-1}{2}}$  los menores residuos positivos módulo  $p$  de los números

$$a, 2a, 3a, \dots, \frac{p-1}{2}a.$$

Por el Teorema 3.2 —parte  $j$ — tenemos

$$\begin{aligned} a &= p[a/p] + r_1, \\ 2a &= p[2a/p] + r_2, \\ &\vdots \\ &\vdots \\ &\vdots \\ \frac{p-1}{2}a &= p\left[\frac{1}{2}\frac{(p-1)a}{p}\right] + r_{\frac{p-1}{2}}. \end{aligned}$$

Sumando estas ecuaciones y teniendo en cuenta que

$$1 + 2 + 3 + \dots + \frac{p-1}{2} = \frac{p^2-1}{8},$$

obtenemos

$$\frac{p^2-1}{8}a = pM + r_1 + r_2 + \dots + r_{\frac{p-1}{2}}.$$

Con las notaciones del lema de Gauss podemos escribir la ecuación anterior en la forma

$$\frac{p^2-1}{8}a = pM + (a_1 + a_2 + \dots + a_t) + (b_1 + b_2 + \dots + b_k). \quad (5.4)$$

De otra parte vimos en la demostración del lema de Gauss que los números  $p - b_1, \dots, p - b_k, a_1, \dots, a_t$  son simplemente los números  $1, 2, \dots, \frac{p-1}{2}$  en algún orden, por lo tanto

$$1 + 2 + \dots + \frac{p-1}{2} = kp - b_1 - \dots - b_k + a_1 + \dots + a_t$$

o sea

$$\frac{p^2-1}{8} = kp - b_1 - \dots - b_k + a_1 + \dots + a_t. \quad (5.5)$$

Restando (5.5) de (5.4) obtenemos

$$\frac{p^2-1}{8}(a-1) = p(M-k) + 2b_1 + \dots + 2b_k,$$

y como  $p$  es impar

$$\frac{p^2-1}{8}(a-1) \equiv (M-k) \pmod{2}. \quad (5.6)$$

Si  $a$  es impar, la congruencia anterior implica que  $M \equiv k \pmod{2}$  y por el Lema de Gauss tenemos,

$$(-1)^M = (-1)^k = (a|p).$$

Si  $a = 2$  entonces  $M = 0$  puesto que  $\left[\frac{2j}{p}\right] = 0$  para  $1 \leq j \leq \frac{p-1}{2}$  ya que para tales casos  $2 \leq 2j < p$ . Luego de (5.6) tenemos

$$\frac{p^2 - 1}{8} \equiv -k \equiv k \pmod{2}$$

y como antes, por el Lema de Gauss

$$(2|p) = (-1)^{\frac{p^2-1}{8}}$$

□

Estamos listos para demostrar el resultado principal.

**5.12 Teorema (Ley de la reciprocidad cuadrática).** *Si  $p$  y  $q$  son primos impares diferentes, entonces*

$$(p|q)(q|p) = (-1)^{\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)}$$

*Demostración.* Sean

$$M = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{1}{2} \frac{(p-1)q}{p}\right]$$

y

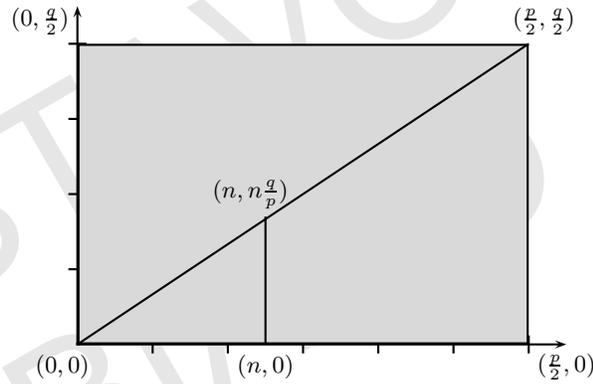
$$N = \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{1}{2} \frac{(q-1)p}{q}\right].$$

Por el teorema anterior tenemos que

$$(p|q)(q|p) = (-1)^M (-1)^N = (-1)^{M+N},$$

y es suficiente demostrar que  $M + N = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ .

Consideremos el rectángulo  $R$  en el plano cuyos vértices son  $(0, 0)$ ,  $(\frac{p}{2}, 0)$ ,  $(\frac{p}{2}, \frac{q}{2})$ ,  $(\frac{p}{2}, \frac{q}{2})$  sin incluir su frontera,



Si llamamos *punto reticular* a un punto  $(x, y)$  que tiene ambas coordenadas enteras, vemos que el rectángulo contiene  $\frac{1}{2}(p-1)\frac{1}{2}(q-1)$  puntos reticulares. Observamos también que sobre la diagonal que une  $(0, 0)$  con  $(\frac{p}{2}, \frac{q}{2})$  no hay puntos reticulares.

En efecto, como la ecuación de la recta que une estos puntos es  $py = qx$ , si hubiera un punto reticular sobre la recta tendríamos que  $p \mid qx$  y como  $(p, q) = 1$  entonces  $p \mid x$ , pero esto es imposible porque  $x < \frac{p}{2}$ .

De otra parte, para todo entero positivo  $n$ , el número de puntos reticulares sobre la recta vertical que pasa por  $(n, 0)$  y que se encuentran por debajo de la diagonal es  $\left[ \frac{nq}{p} \right]$ . Por lo tanto, el número de puntos reticulares en el rectángulo  $R$  que están por debajo de la diagonal es precisamente  $M$ . Similarmente, el número de puntos reticulares en el rectángulo  $R$  que están por encima de la diagonal es  $N$ , y por lo tanto  $N + M = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ , como queríamos demostrar.  $\square$

Como  $(q|p) = \pm 1$ , entonces  $(q|p)^2 = 1$  y podemos expresar la ley de la reciprocidad cuadrática en la forma

$$(p|q) = (q|p)(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)},$$

que es más conveniente para estudiar el carácter cuadrático de un entero.

**5.13 Ejemplo.** Determinar si 60 es un residuo cuadrático módulo 239.

Como  $60 = 2^2 \cdot 3 \cdot 5$ , entonces

$$(60|239) = (2|239)^2(3|239)(5|239) = (3|239)(5|239)$$

pero

$$\begin{aligned}(3|239) &= (239|3)(-1)^{\frac{1}{2}(238)\frac{1}{2}(2)} = -(239|3) \\ &= -(2|3) = -(-1) = 1\end{aligned}$$

y

$$\begin{aligned}(5|239) &= (239|5)(-1)^{\frac{1}{2}(238)\frac{1}{2}(4)} = (239|5) \\ &= (4|5) = (2|5)^2 = 1.\end{aligned}$$

Por lo tanto,  $(60|239) = 1$  y así, 60 es un residuo cuadrático módulo 239.

**5.14 Ejemplo.** Determinemos el carácter cuadrático de  $(3|p)$  para todo primo impar  $p$ .

Tenemos

$$(3|p) = (p|3)(-1)^{\frac{1}{2}(2)\frac{1}{2}(p-1)} = (p|3)(-1)^{\frac{p-1}{2}},$$

además

$$(p|3) = \begin{cases} (1|3) = 1 & \text{si } p \equiv 1 \pmod{3} \\ (2|3) = -1 & \text{si } p \equiv 2 \pmod{3}, \end{cases}$$

y

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

Por lo tanto

$$(3|p) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{3} \text{ y } p \equiv 1 \pmod{4} \\ 1 & \text{si } p \equiv 2 \pmod{3} \text{ y } p \equiv 3 \pmod{4} \\ -1 & \text{si } p \equiv 1 \pmod{3} \text{ y } p \equiv 3 \pmod{4} \\ -1 & \text{si } p \equiv 2 \pmod{3} \text{ y } p \equiv 1 \pmod{4}. \end{cases}$$

Usando el Teorema Chino del Residuo, tenemos finalmente que

$$(3|p) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{12} \\ -1 & \text{si } p \equiv \pm 5 \pmod{12}. \end{cases}$$

### 5.3 El símbolo de Jacobi

Para simplificar los cálculos necesarios para determinar si un número compuesto es un residuo cuadrático, utilizamos una extensión del símbolo de Legendre introducida por Jacobi. Recordemos que la segunda entrada  $p$  en el símbolo de Legendre  $(a|p)$  debe ser un primo impar. Jacobi generalizó este símbolo a fin de permitir entradas que sean números impares pero no necesariamente primos.

**5.15 Definición.** Si  $P$  es un entero positivo impar cuya representación canónica es,

$$P = \prod_{i=1}^k p_i^{\alpha_i}$$

definimos el *símbolo de Jacobi*  $(a|P)$  para todo entero  $a$  tal que  $(a, P) = 1$ , mediante la ecuación

$$(a|P) = \prod_{i=1}^k (a|p_i)^{\alpha_i}$$

donde  $(a|p_i)$  es el símbolo de Legendre. Además definimos  $(a|1) = 1$ .

Observamos que el símbolo de Jacobi coincide con el símbolo de Legendre cuando  $P$  es un número primo, lo que justifica el uso de la misma notación para ambos símbolos. También es claro que  $(a|P) = \pm 1$ , pero no es cierto en general que si  $(a|P) = 1$  entonces  $a$  es un residuo cuadrático módulo  $P$ , en el sentido de que la congruencia  $x^2 \equiv a \pmod{P}$  tiene solución.

Por ejemplo  $(5|9) = 1$  pero  $x^2 \equiv 5 \pmod{9}$  no tiene solución.

El símbolo de Jacobi tiene propiedades similares al símbolo de Legendre como veremos en los teoremas siguientes.

**5.16 Teorema.** *Sea  $P$  un entero positivo impar y sean  $a$  y  $b$  enteros primos relativos con  $P$ . Entonces*

1. Si  $a \equiv b \pmod{P}$  entonces  $(a|P) = (b|P)$ .
2.  $(a^2|P) = 1$ .
3.  $(1|P) = 1$ .
4.  $(a|P)(b|P) = (ab|P)$ .

5. Si la representación canónica de  $a$  es  $a = \prod_{i=1}^k p_i^{a_i}$  entonces  
 $(a|P) = \prod_{i=1}^k (p_i|P)^{a_i}$ .

*Demostración.* Las propiedades mencionadas son consecuencia directa de la propiedad del símbolo de Legendre demostradas en el Teorema 5.8. Dejamos su verificación al lector.  $\square$

**5.17 Teorema.** Sea  $P$  un entero positivo impar. Entonces,

1.  $(-1|P) = (-1)^{\frac{P-1}{2}}$
2.  $(2|P) = (-1)^{\frac{P^2-1}{8}}$

*Demostración.* Sea  $P = p_1 p_2 \dots p_s$  donde los  $p_i$  son primos no necesariamente diferentes. Tenemos,

$$\begin{aligned} (-1|P) &= (-1|p_1)(-1|p_2) \dots (-1|p_s) \\ &= (-1)^{\frac{p_1-1}{2}} (-1)^{\frac{p_2-1}{2}} \dots (-1)^{\frac{p_s-1}{2}} = (-1)^k \end{aligned}$$

donde  $k = \sum_{i=1}^s \frac{p_i-1}{2}$ . Podemos escribir

$$\begin{aligned} P &= (1 + (p_1 - 1))(1 + (p_2 - 1)) \dots (1 + (p_s - 1)) \\ &= 1 + \sum_{i=1}^s (p_i - 1) + \sum_{i \neq j} (p_i - 1)(p_j - 1) + \dots \\ &= 1 + 2k + 4t, \end{aligned}$$

porque cada una de las sumas después de la primera es divisible por 4, en virtud de que cada factor  $p_i - 1$  es par. Luego

$$P \equiv 1 + 2k \pmod{4}$$

y

$$\frac{P-1}{2} \equiv k \pmod{2}.$$

Por lo tanto

$$(-1|P) = (-1)^k = (-1)^{\frac{P-1}{2}}.$$

Similarmente, tenemos

$$\begin{aligned}(2|P) &= (2|p_1)(2|p_2) \cdots (2|p_s) \\ &= (-1)^{\frac{p_1^2-1}{8}} (-1)^{\frac{p_2^2-1}{8}} \cdots (-1)^{\frac{p_s^2-1}{8}} = (-1)^h,\end{aligned}$$

con  $h = \sum_{i=1}^s \frac{p_i^2-1}{8}$ . Por lo tanto

$$\begin{aligned}P^2 &= (1 + (p_1^2 - 1))(1 + (p_2^2 - 1)) \cdots (1 + (p_s^2 - 1)) \\ &= 1 + \sum_{i=1}^s (p_i^2 - 1) + \sum_{i \neq j} (p_i^2 - 1)(p_j^2 - 1) + \cdots \\ &= 1 + 8h + 64t,\end{aligned}$$

porque cada una de las sumas después de la primera es divisible por 64, ya que cada factor  $p_i^2 - 1$  es divisible por 8. Luego

$$P^2 \equiv 1 + 8h \pmod{64}$$

y

$$\frac{P^2 - 1}{8} \equiv h \pmod{8}.$$

Por lo tanto

$$(2|P) = (-1)^h = (-1)^{\frac{P^2-1}{8}}.$$

□

### 5.18 Teorema (Ley de la reciprocidad para el símbolo de Jacobi).

Sean  $P$  y  $Q$  enteros impares positivos tales que  $(P, Q) = 1$ . Entonces

$$(P|Q)(Q|P) = (-1)^r$$

con  $r = \frac{1}{2}(P-1)\frac{1}{2}(Q-1)$ .

*Demostración.* Sean  $P = p_1 p_2 \cdots p_s$  y  $Q = q_1 q_2 \cdots q_t$  donde los  $p_i$  y los  $q_j$  son primos no necesariamente diferentes. Tenemos

$$(P|Q)(Q|P) = \prod_i \prod_j (p_i|q_j)(q_j|p_i) = (-1)^r,$$

donde

$$r = \sum_i \sum_j \frac{1}{2}(p_i - 1) \cdot \frac{1}{2}(q_j - 1),$$

en virtud de la ley de la reciprocidad cuadrática aplicada a cada factor. En la demostración del teorema anterior, vimos que

$$\sum_{i=1}^s \frac{p_i - 1}{2} \equiv \frac{1}{2}(P - 1) \pmod{2}$$

y se tiene una congruencia similar para  $\sum_{j=1}^t \frac{q_j - 1}{2}$ .

Por lo tanto

$$r \equiv \frac{1}{2}(P - 1) \frac{1}{2}(Q - 1) \pmod{2},$$

lo que implica que

$$(-1)^r = (-1)^{\frac{1}{2}(P-1)\frac{1}{2}(Q-1)},$$

como queríamos demostrar.  $\square$

La ventaja principal del símbolo de Jacobi es que permite evaluar fácilmente el símbolo de Legendre como se ilustra en los ejemplos siguientes

### 5.19 Ejemplo.

$$(420|631) = (4|631)(105|631) = (105|631).$$

Para evaluar  $(105|631)$  usando el símbolo de Legendre debemos escribir

$$(105|631) = (3|631)(5|631)(7|631)$$

y aplicar la ley de la reciprocidad cuadrática a cada factor de la derecha. Usando el símbolo de Jacobi los cálculos son más simples pues tenemos

$$(105|631) = (631|105) = (1|105) = 1$$

### 5.20 Ejemplo.

Determinemos el carácter de  $-216$  con respecto al primo  $839$ .

Tenemos

$$\begin{aligned} (-216|839) &= (-1|839)(4|839)(27|839) \\ &= -(27|839) = (839|27) = (2|27) = -1 \end{aligned}$$

---

## Ejercicios 5.2

---

1. Hallar todos los primos  $p$  tales que  $(10|p) = 1$ .
2. Hallar todos los primos  $p$  tales que  $(7|p) = -1$ .
3. Para que primos impares  $p$  es  $(-3|p) = 1$
4. Probar que 2 es un residuo cuadrático módulo el primo impar  $p$  si y solo si  $p \equiv \pm 1 \pmod{8}$  y 2 no es un residuo cuadrático módulo  $p$  si y solo si  $p \equiv \pm 3 \pmod{8}$ .
5. ¿Cuáles de las congruencias siguientes tienen solución?
  - (a)  $x^2 \equiv 7 \pmod{257}$ .
  - (b)  $x^2 \equiv 219 \pmod{383}$ .
  - (c)  $x^2 \equiv -10 \pmod{191}$ .
  - (d)  $x^2 \equiv 5 \pmod{1231}$ .
6. Determinar el carácter cuadrático de los números 327 y  $-532$  módulo el primo 977.
7. Sea  $m$  un entero positivo impar y sea  $p_1, p_2, \dots, p_s$  los divisores primos de  $m$ . Sea  $a$  un entero tal que  $(a, m) = 1$ . Probar que  $x^2 \equiv a \pmod{m}$  tiene solución si y solo si  $(a|p_i) = 1$  para  $i = 1, 2, \dots, s$ .
8. Determinar si la congruencia  $x^2 \equiv 327 \pmod{2821}$  tiene solución.  
*Sugerencia:*  $2821 = 7 \cdot 13 \cdot 31$
9. Evaluar usando el símbolo de Legendre  $(129|283)$  y  $(640|277)$ .
10. Evaluar usando el símbolo de Jacobi  $(226|563)$  y  $(-416|977)$ .
11. Sea  $P$  un entero positivo impar. Sean  $a$  y  $b$  enteros tales que  $(a, P) = 1$  y  $(b, P) = 1$ . Probar las siguientes propiedades del símbolo de Jacobi:
  - (a)  $(-1|P) = 1$  si y solo si  $P \equiv 1 \pmod{4}$ .
  - (b)  $(2|P) = 1$  si y solo si  $P \equiv \pm 1 \pmod{8}$ .
  - (c)  $(ab^2|P) = (a|P)$ .

12. Sean  $P$  y  $Q$  enteros positivos impares tales que  $(P, Q) = 1$ . Probar que:
- (a)  $(P|Q) = (-Q|P)$  si y solo si  $P \equiv Q \equiv 3 \pmod{4}$
  - (b)  $(a|P)(a|Q) = (a|PQ)$  donde  $(a, P) = (a, Q) = 1$ .
  - (c)  $(P|Q^2) = 1$ .

## 5.4 Potencias módulo $n$ y raíces primitivas

En las secciones anteriores estudiamos detalladamente las congruencias cuadráticas de la forma  $x^2 \equiv a \pmod{p}$  con  $p$  un número primo y  $a$  un entero tal que  $(a, p) = 1$ . En esta sección estudiaremos algunos resultados sobre las congruencias más generales de la forma  $x^m \equiv a \pmod{p}$ .

**5.21 Definición.** Sean  $p$  un primo impar,  $a$  un entero tal que  $(a, p) = 1$  y  $m$  un entero positivo. Si la congruencia

$$x^m \equiv a \pmod{p}$$

tiene solución, decimos que  $a$  es una *potencia  $m$ -ésima módulo  $p$* .

**5.22 Ejemplo.** Sea  $p = 7$ . Como  $(\pm 1)^4 \equiv 1 \pmod{7}$ ,  $(\pm 2)^4 \equiv 2 \pmod{7}$  y  $(\pm 3)^4 \equiv 4 \pmod{7}$ , entonces las potencias cuartas módulo 7 son precisamente 1, 2 y 4.

Del criterio de Euler se deduce que una condición necesaria y suficiente para que la congruencia cuadrática  $x^2 \equiv a \pmod{p}$  tenga solución es que  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ . Es natural buscar una condición similar para que una congruencia de la forma  $x^m \equiv a \pmod{p}$  tenga solución. Para encontrar esta condición debemos primero estudiar las congruencias de la forma  $a^k \equiv 1 \pmod{n}$  con  $(a, n) = 1$ .

Por el Teorema de Euler, sabemos que si  $(a, n) = 1$  entonces  $a^{\Phi(n)} \equiv 1 \pmod{n}$  y por lo tanto podemos establecer la definición siguiente.

**5.23 Definición.** Sea  $n$  un entero positivo y  $a$  un entero tal que  $(a, n) = 1$ . El menor entero positivo  $k$  tal que  $a^k \equiv 1 \pmod{n}$  se llama *orden de  $a$  módulo  $n$*  y lo representamos por la notación  $\text{ord}_n a$ .

Si  $\text{ord}_n a = k$ , también se acostumbra a decir que  $a$  pertenece al exponente  $k$  módulo  $n$ .

Si  $a^h \equiv 1 \pmod{n}$  con  $h$  un entero positivo entonces  $a^h - 1 = tn$  para algún entero  $t$ , luego  $a^h - tn = 1$  y por el Teorema 2.11,  $(a, n) = 1$ . Esta observación nos indica que la definición anterior solo tiene sentido cuando  $a$  y  $n$  son primos relativos. Observamos también que si  $(a, n) = 1$  y  $a \equiv b \pmod{n}$  entonces  $\text{ord}_n a = \text{ord}_n b$ .

**5.24 Ejemplo.** Si  $n = 10$  los enteros primos relativos con 10 y menores que 10 son 1, 3, 7 y 9. Tenemos la tabla siguiente de potencias:

$a$	$a^2$	$a^3$	$a^4$
1			
3	9	7	1
7	9	3	1
9	1		

Por lo tanto  $\text{ord}_{10} 1 = 1$ ,  $\text{ord}_{10} 3 = \text{ord}_{10} 7 = 4$  y  $\text{ord}_{10} 9 = 2$ . Observamos que en cada caso  $\text{ord}_{10} a \mid 4 = \Phi(10)$ . En general  $\text{ord}_n a \mid \Phi(n)$ , como se deduce del teorema siguiente.

**5.25 Teorema.** Si  $a^t \equiv 1 \pmod{n}$  entonces  $\text{ord}_n a \mid t$

*Demostración.* Supongamos que  $\text{ord}_n a = k$ . Por el algoritmo de la división podemos escribir  $t$  en la forma  $t = qk + r$  con  $0 \leq r < k$ . Por lo tanto

$$a^t = a^{qk+r} = (a^k)^q a^r \equiv a^r \equiv 1 \pmod{n},$$

puesto que  $a^k \equiv 1 \pmod{n}$ .

Si  $r$  fuera diferente de 0, se tendría una contradicción con la minimalidad de  $k$ . En consecuencia  $r = 0$  y  $k \mid t$  como queríamos demostrar.  $\square$

**5.26 Corolario.** Si  $a$  es un entero primo relativo con  $n$ , entonces

$$\text{ord}_n a \mid \Phi(n).$$

*Demostración.* Por el Teorema de Euler  $a^{\Phi(n)} \equiv 1 \pmod{n}$ , luego el resultado es consecuencia directa del teorema.  $\square$

**5.27 Corolario.** Supongamos que  $\text{ord}_n a = k$ . Entonces

$$a^i \equiv a^j \pmod{n} \quad \text{si y solo si} \quad i \equiv j \pmod{k}.$$

*Demostración.* Si  $i \equiv j \pmod{k}$  entonces  $i = j + qk$  para algún entero  $q$  y por lo tanto

$$a^i = a^{j+qk} = a^j (a^k)^q \equiv a^j \pmod{n}$$

puesto que  $a^k \equiv 1 \pmod{n}$ .

Recíprocamente, supongamos que  $a^i \equiv a^j \pmod{n}$ . Sin perder generalidad podemos asumir que  $i \geq j$ . Como  $(a, n) = 1$  podemos cancelar repetidamente  $a$  hasta obtener  $a^{i-j} \equiv 1 \pmod{n}$ . Por el teorema  $k \mid i - j$  o sea  $i \equiv j \pmod{k}$ .  $\square$

El teorema siguiente nos relaciona el orden de una potencia positiva de  $a$  módulo  $n$ , con el orden de  $a$  módulo  $n$ .

**5.28 Teorema.** Si  $\text{ord}_n a = k$  entonces para todo entero positivo  $m$

$$\text{ord}_n a^m = \frac{k}{(m, k)}.$$

*Demostración.* Sean  $d = (m, k)$  y  $h = \text{ord}_n a^m$ . Como  $a^k \equiv 1 \pmod{n}$  tenemos

$$(a^m)^{\frac{k}{d}} = (a^k)^{\frac{m}{d}} \equiv 1 \pmod{n},$$

luego por el Teorema 5.25

$$h \left| \frac{k}{d}. \quad (5.7)$$

Como  $(a^m)^h \equiv 1 \pmod{n}$  entonces  $k \mid mh$  y en consecuencia

$$\frac{k}{d} \left| \frac{m}{d} h.$$

Por el Corolario 2.12 sabemos que  $\left(\frac{k}{d}, \frac{m}{d}\right) = 1$ , luego concluimos que

$$\frac{k}{d} \left| h. \quad (5.8)$$

De (5.7) y (5.8) obtenemos  $h = \frac{k}{d}$  que es el resultado deseado.  $\square$

**5.29 Ejemplo.** Como  $\text{ord}_{10}3 = 4$  entonces

$$\text{ord}_{10}3^2 = \frac{4}{(2,4)} = \frac{4}{2} = 2,$$

$$\text{ord}_{10}7 = \text{ord}_{10}3^3 = \frac{4}{(3,4)} = \frac{4}{1} = 4.$$

**5.30 Teorema.** Sea  $p$  un número primo. Si existe un entero  $a$  tal que  $\text{ord}_p a = h$ , entonces existen exactamente  $\Phi(h)$  enteros incongruentes módulo  $p$  que tienen orden  $h$  módulo  $p$ .

*Demostración.* Como  $a^h \equiv 1 \pmod{p}$  entonces los números  $a, a^2, \dots, a^h$  son soluciones de la congruencia  $x^h \equiv 1 \pmod{p}$ . Además estos números son incongruentes módulo  $p$ , ya que si  $a^i \equiv a^j \pmod{p}$  con  $1 \leq i < j \leq h$ , por el corolario 5.27 se tendría que  $i \equiv j \pmod{h}$  y  $h \mid (i - j)$ ; pero esto es una contradicción porque  $0 < j - i < h$ .

Por el Teorema de Lagrange concluimos que los números  $a, a^2, \dots, a^h$  son todas las soluciones incongruentes de la congruencia  $x^h \equiv 1 \pmod{p}$ .

Por el Teorema 5.28,  $\text{ord}_p a^m = \frac{h}{(m,h)}$  y en consecuencia  $\text{ord}_p a^m = h$  si y solo si  $(m, h) = 1$ . Por lo tanto hay exactamente  $\Phi(h)$  enteros incongruentes que tienen orden  $h$  módulo  $p$ , que son precisamente las potencias  $a^m$  con  $(h, m) = 1$ .  $\square$

**5.31 Ejemplo.** Si  $p = 17$ ,  $\text{ord}_{17}4 = 4$ . Como  $\Phi(4) = 2$  y los números primos relativos con 4 y menores que 4 son 1 y 3 entonces los enteros incongruentes módulo 17, de orden 4 módulo 17 son  $4^1$  y  $4^3$ , es decir 4 y 13 puesto que  $4^3 \equiv 13 \pmod{17}$ .

**5.32 Teorema.** Si  $p$  es un número primo y  $h \mid p - 1$ , entonces hay exactamente  $\Phi(h)$  enteros incongruentes módulo  $p$  que tienen orden  $h$  módulo  $p$ .

*Demostración.* Representemos por  $N(h)$  el número de enteros positivos  $a \leq p - 1$  tales que  $\text{ord}_p a = h$ . Por el teorema anterior  $N(h) = 0$  o  $N(h) = \Phi(h)$ , y este último caso se presenta únicamente cuando  $h \mid \Phi(p) = p - 1$ . Por lo tanto

$$\sum_{h \mid p-1} N(h) \leq \sum_{h \mid p-1} \Phi(h). \quad (5.9)$$

Como cada entero positivo  $a$  con  $a \leq p - 1$  tiene algún orden  $h \leq p - 1$ , entonces  $\sum_{h \mid p-1} N(h) = p - 1$ .

También por el Teorema 3.23,  $\sum_{h|p-1} \Phi(h) = p - 1$ , luego

$$\sum_{h|p-1} N(h) = \sum_{h|p-1} \Phi(h) = p - 1.$$

Deducimos de la última ecuación que  $N(h) = \Phi(h)$ , para cada  $h$  tal que  $h \mid p - 1$ , ya que de otra forma la desigualdad (5.9) sería estricta lo que es imposible. Por lo tanto si  $h \mid p - 1$  hay exactamente  $N(h) = \Phi(h)$  enteros incongruentes módulo  $p$ , que tienen orden  $h$  módulo  $p$ .  $\square$

Por el Corolario 5.26, sabemos que si  $a$  es un entero primo relativo con  $n$  entonces  $\text{ord}_n a$  divide a  $\Phi(n)$ . Para algunos valores de  $n$  hay enteros  $a$  tales que  $\text{ord}_n a = \Phi(n)$ . Estos casos son importantes y en consecuencia les damos un nombre especial.

**5.33 Definición.** Si  $\text{ord}_n a = \Phi(n)$ , decimos que  $a$  es una *raíz primitiva* módulo  $n$ .

**5.34 Ejemplo.** 1. Las raíces primitivas módulo 10 son 3 y 7.

2. No hay raíces primitivas módulo 12 pues  $\Phi(12) = 4$  y la tabla de potencias para los números  $a < 12$  y primos relativos con 12 es

$a$	$a^2$
1	
5	1
7	1
11	1

Como consecuencia directa del último teorema tenemos

**5.35 Corolario (de 5.32).** Si  $p$  es un número primo, hay exactamente  $\Phi(p - 1)$  raíces primitivas módulo  $p$ .

A partir de una raíz primitiva módulo  $n$ , podemos construir un sistema reducido de residuos módulo  $n$ , de acuerdo al resultado siguiente.

**5.36 Teorema.** Si  $a$  es una raíz primitiva módulo  $n$ , entonces los números  $a, a^2, \dots, a^{\Phi(n)}$  forman un sistema reducido de residuos módulo  $n$ .

*Demostración.* Como tenemos  $\Phi(n)$  números y cada uno de ellos es primo relativo con  $n$ , únicamente hay que demostrar que ellos son incongruentes módulo  $n$ . Supongamos lo contrario, es decir supongamos que existen  $i$  y  $j$  con  $1 \leq i < j \leq \Phi(n)$  tales que  $a^i \equiv a^j \pmod{n}$ . Por el corolario 5.27 tenemos que  $i \equiv j \pmod{\Phi(n)}$ . Luego  $\Phi(n) \mid (j - i)$  pero esto es contradictorio pues  $0 < j - i < \Phi(n)$ . Por lo tanto los números  $a, a^2, \dots, a^{\Phi(n)}$  son incongruentes módulo  $n$ .  $\square$

Estamos preparados para demostrar un resultado similar al criterio de Euler para potencias  $m$ -ésimas módulo  $p$ , con  $p$  un primo impar.

**5.37 Lema.** *Sea  $p$  un primo impar,  $a$  un entero tal que  $(a, p) = 1$  y  $b$  una raíz primitiva módulo  $p$ . Entonces la congruencia  $x^m \equiv a \pmod{p}$  tiene solución si y solo si  $a \equiv b^{kd} \pmod{p}$ , donde  $k$  es un entero y  $d = (m, p - 1)$ .*

*Demostración.* Como  $b$  es una raíz primitiva módulo  $p$ , por el teorema 5.36 los números  $b, b^2, \dots, b^{p-1}$  forman un sistema reducido de residuos módulo  $p$ . Como  $(a, p) = 1$ , existe  $t$  con  $1 \leq t \leq p - 1$  tal que  $a \equiv b^t \pmod{p}$ .

También, si  $u$  es una solución de  $x^m \equiv a \pmod{p}$ , a partir de  $(a, p) = 1$  se deduce que  $(u, p) = 1$  y en consecuencia existe  $s$  con  $1 \leq s \leq p - 1$  tal que  $u \equiv b^s \pmod{p}$ . Por lo tanto la congruencia  $x^m \equiv a \pmod{p}$  tiene solución si y solo si existe  $s$  tal que

$$b^{ms} \equiv b^t \pmod{p}.$$

Por el Corolario 5.27 esto ocurre si y solo si la congruencia en  $s$ ,  $ms \equiv t \pmod{p - 1}$  tiene solución, y por el Teorema 4.47 esta congruencia tiene solución si y solo si  $d \mid t$  donde  $d = (m, p - 1)$ . Como  $a \equiv b^t \pmod{p}$  y  $t$  es de la forma  $t = kd$ , vemos que  $x^m \equiv a \pmod{p}$  tiene solución si y solo si  $a \equiv b^{kd} \pmod{p}$ , donde  $k$  es un entero y  $d = (m, p - 1)$ , como queríamos demostrar.  $\square$

**5.38 Teorema (Criterio de Euler generalizado).** *Sean  $p$  un primo impar,  $a$  un entero tal que  $(a, p) = 1$ ,  $m$  un entero positivo y  $d = (m, p - 1)$ . Entonces la congruencia  $x^m \equiv a \pmod{p}$  tiene solución si y solo si*

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

*Además, si la congruencia tiene solución, entonces tiene exactamente  $d$  soluciones incongruentes módulo  $p$ .*

*Demostración.* Si  $x^m \equiv a \pmod{p}$  tiene una solución  $u$ , entonces

$$a^{\frac{p-1}{d}} \equiv u^{\frac{m(p-1)}{d}} \equiv u^{(p-1)\frac{m}{d}} \equiv 1 \pmod{p},$$

por el Teorema de Fermat, puesto que  $(u, p) = 1$  y  $\frac{m}{d}$  es entero.

Recíprocamente, supongamos que  $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$ . Como en la demostración del lema 5.37, tenemos que  $a \equiv b^t \pmod{p}$  donde  $b$  es una raíz primitiva módulo  $p$ . Por lo tanto

$$b^{\frac{t(p-1)}{d}} \equiv a^{\frac{(p-1)}{d}} \equiv 1 \pmod{p}$$

y por el Teorema 5.25,  $p-1 \mid \frac{t(p-1)}{d}$ . Luego  $\frac{t}{d} = k$  resulta entero y  $a \equiv b^{kd} \pmod{p}$ . Por el Lema 5.37 concluimos que la congruencia  $x^m \equiv a \pmod{p}$  tiene solución. Además, una revisión cuidadosa de la demostración del lema anterior, nos indica que hay exactamente  $d$  soluciones incongruentes módulo  $p$  de esta congruencia.  $\square$

También, de los resultados anteriores se deduce que hay exactamente  $\frac{(p-1)}{d}$  potencias  $m$ -ésimas módulo  $p$ , donde  $p$  es un primo impar. Concretamente tenemos:

**5.39 Teorema.** Sean  $p$  un primo impar,  $m$  un entero positivo y  $d = (m, p-1)$ . Si  $b$  es una raíz primitiva módulo  $p$ , entonces las potencias  $m$ -ésimas módulo  $p$ , incongruentes módulo  $p$  son precisamente  $b^d, b^{2d}, \dots, b^{\frac{p-1}{d}d}$ .

*Demostración.* Por el Lema 5.37, los números  $b^d, b^{2d}, \dots, b^{\frac{p-1}{d}d}$  son potencias  $m$ -ésimas módulo  $p$ . También se verifica inmediatamente que estos números son incongruentes módulo  $p$ .

Finalmente, si  $a$  es cualquier potencia  $m$ -ésima módulo  $p$ , por el lema mencionado,  $a \equiv b^{kd} \pmod{p}$  para algún entero  $k$ . Si tomamos  $t = \frac{p-1}{d}$  y modificamos ligeramente el algoritmo de la división, podemos escribir  $k$  en la forma  $k = qt + r$  con  $0 < r \leq t$ . Por lo tanto tenemos

$$\begin{aligned} a &\equiv b^{kd} = b^{(qt+r)d} \\ &= b^{(p-1)q} b^{rd} \\ &\equiv b^{rd} \pmod{p}, \end{aligned}$$

puesto que  $b$  es una raíz primitiva módulo  $p$ . Luego  $a$  es congruente con uno de los números de la colección  $b^d, b^{2d}, \dots, b^{\frac{p-1}{d}d}$  lo que completa la demostración.  $\square$

**5.40 Ejemplo.** Determinemos las potencias octavas módulo 13.

Por verificación directa vemos que 2 es una raíz primitiva módulo 13. Como  $m = 8$  y  $p - 1 = 12$  entonces  $d = (m, p - 1) = (8, 12) = 4$ .

Luego, por el teorema anterior las potencias octavas módulo 13, incongruentes módulo 13, son  $2^4, 2^8$  y  $2^{12}$  es decir 3, 9 y 1 ya que  $2^4 \equiv 3 \pmod{13}$ ,  $2^8 \equiv 9 \pmod{13}$  y  $2^{12} \equiv 1 \pmod{13}$ .

---

## Ejercicios 5.3

---

1. Hallar los órdenes de 1, 2, 3, 4, 5, 6, 8 y 11 módulo 13.
2. Probar que si  $\text{ord}_n a = t$ ,  $\text{ord}_n b = s$  y  $(t, s) = 1$ , entonces  $\text{ord}_n ab = ts$ .
3. Probar que si  $\text{ord}_n a = t$  entonces los números  $a, a^2, \dots, a^t$  son incongruentes módulo  $n$ .
4. Sea  $p$  un número primo. Probar que si  $\text{ord}_p a = t$  y  $t$  es par entonces  $a^{\frac{t}{2}} \equiv -1 \pmod{p}$ .
5. Hallar la menor raíz primitiva positiva de cada uno de los números primos menores que 30.
6. Hallar todas las raíces primitivas módulo 11 y todas las raíces primitivas módulo 13.
7. Sea  $p$  un número primo. Probar que si  $a$  es una raíz primitiva módulo  $p$  entonces  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .
8. Sea  $p$  un número primo. Probar que  $a$  es una raíz primitiva módulo  $p$  si y solo si  $(a, p) = 1$  y  $a$  no satisface ninguna de las congruencias  $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ , donde  $q$  recorre los divisores primos de  $p - 1$ .

9. Demostrar el Teorema de Wilson usando el resultado del Teorema 5.36.
10. Hallar las potencias sextas módulo 11.
11. Hallar las potencias undécimas módulo 23.
12. Cuántas soluciones incongruentes tiene cada una de las congruencias
- $x^{18} \equiv 15 \pmod{17}$ .
  - $x^{54} \equiv 8 \pmod{13}$ .
  - $x^{25} \equiv 10 \pmod{11}$ .
13. Sea  $q$  un número que tiene raíces primitivas y sea  $a$  una de ellas. Si  $a^r \equiv n \pmod{q}$ , decimos que  $r$  es un índice de  $n$  en base  $a$  con respecto al módulo  $q$  y escribimos  $r = \text{ind}_a n$ . Los índices se comportan en forma similar a los logaritmos y son de interés práctico y teórico. Demostrar las siguientes propiedades:
- Si  $(n, q) = 1$ , existe  $\text{ind}_a n$  con respecto al módulo  $q$ .
  - El  $\text{ind}_a n$  con respecto al módulo  $q$  es único módulo  $\Phi(q)$ .
  - $n \equiv m \pmod{q}$  si y solo si  $\text{ind}_a n \equiv \text{ind}_a m \pmod{\Phi(q)}$ .
  - $\text{ind}_a 1 \equiv 0 \pmod{\Phi(q)}$ ,  $\text{ind}_a a \equiv 1 \pmod{\Phi(q)}$ .
  - $\text{ind}_a(mn) \equiv \text{ind}_a m + \text{ind}_a n \pmod{\Phi(q)}$ .
  - $\text{ind}_a n^t \equiv t \text{ind}_a n \pmod{\Phi(q)}$ .
14. Construir una tabla de índice en base 2 con respecto al módulo 11.  
*Sugerencia:* Calcular las potencias  $2, 2^2, \dots, 2^{10}$  módulo 11.
15. Usando las propiedades de los índices resolver las congruencias  $3x^3 \equiv 7 \pmod{11}$  y  $7x \equiv 9 \pmod{11}$ .
16. Sea  $p$  un primo impar y  $a$  un entero tal que  $(a, p) = 1$ . Probar que  $a$  es un residuo cuadrático si  $\text{ind}_g a$  es par, donde  $g$  es una raíz primitiva módulo  $p$ .

## 5.5 Álgebra y teoría de números

En el capítulo 4 mencionamos brevemente los conceptos de grupo y de anillo, y los utilizamos para presentar demostraciones algebraicas de los teoremas

de Fermat y Euler. En esta sección vamos a desarrollar otros conceptos algebraicos que nos llevarán a obtener demostraciones más sencillas de algunos teoremas importantes en Teoría de Números y nos permitirán completar nuestro estudio de las raíces primitivas módulo un entero positivo.

Supongamos que  $(G, *)$  es un grupo con identidad  $e$  y que  $a \in G$ . Definimos las *potencias enteras* del elemento  $a$  mediante

$$\begin{aligned} a^n &= a * a * \cdots * a, & (n \text{ veces}) \\ a^0 &= e, \\ a^{-n} &= (a^{-1})^n = a^{-1} * a^{-1} * \cdots * a^{-1}, & (n \text{ veces}) \end{aligned}$$

donde  $n > 0$  y  $a^{-1}$  representa el inverso del elemento  $a$ .

Si el grupo se nota aditivamente, el producto abstracto  $a * a * \cdots * a$  ( $n$  veces) es sencillamente la suma  $a + a + \cdots + a$  ( $n$  veces). Se acostumbra a representar esta suma por la notación  $na$ . Por lo tanto en este caso, las *potencias* de  $a$  son precisamente,

$$\begin{aligned} na &= a + a + \cdots + a, & (n \text{ veces}) \\ 0a &= 0, \\ (-n)a &= n(-a) = (-a) + (-a) + \cdots + (-a), & (n \text{ veces}) \end{aligned}$$

donde  $n > 0$  y  $-a$  representa el inverso de  $a$ .

**5.41 Definición.** Un subconjunto  $H$  de un grupo  $G$  se llama un *subgrupo* de  $G$  si  $H$  es a la vez un grupo, con la misma operación que hay en  $G$ .

**5.42 Ejemplo.** 1. Si consideramos el grupo  $(\mathbb{Z}, +)$  de los números enteros con la adición y llamamos  $\mathbb{P}$  al conjunto de los enteros pares e  $\mathbb{I}$  al conjunto de los enteros impares, entonces  $(\mathbb{P}, +)$  es un subgrupo de  $(\mathbb{Z}, +)$  pero  $(\mathbb{I}, +)$  no es subgrupo de  $(\mathbb{Z}, +)$ .

2. Consideremos el grupo aditivo  $\mathbb{Z}_9$  de los enteros módulo 9. Si  $H = \{0, 3, 6\}$  entonces  $H$  es un subgrupo de  $\mathbb{Z}_9$ .

**5.43 Definición.** Sea  $G$  un grupo y  $a \in G$ . Definimos el subgrupo de  $G$  *generado* por  $a$  como el conjunto formado por todas las potencias enteras de  $a$ .

Se acostumbra a representar este subgrupo por la notación  $\langle a \rangle$ . Por lo tanto tenemos

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

Decimos que un grupo  $G$  es *cíclico con generador*  $a$  si  $G = \langle a \rangle$  para algún  $a \in G$ .

**5.44 Ejemplo.** En el grupo aditivo  $\mathbb{Z}_{12}$  de los enteros módulo 12 tenemos

$$\langle 3 \rangle = \{0, 3, 6, 9\},$$

$$\langle 4 \rangle = \{0, 4, 8\},$$

$$\langle 8 \rangle = \langle 4 \rangle,$$

$$\langle 1 \rangle = \mathbb{Z}_{12}.$$

Vemos que  $\mathbb{Z}_{12}$  es un grupo cíclico generado por 1. En general, para todo entero positivo  $n$  el grupo  $\mathbb{Z}_n$  es un grupo cíclico con generador 1.

En el capítulo 4 vimos que el grupo multiplicativo de las unidades del anillo  $\mathbb{Z}_n$  está formado por todas las clases  $\bar{a}$  tales que  $(a, n) = 1$  y que su orden es  $\Phi(n)$ . En adelante vamos a representar este grupo por  $U_n$  y como es usual, eliminaremos las barras en la representación de sus elementos.

**5.45 Ejemplo.** 1. En el grupo  $U_{11}$  de las unidades del anillo  $\mathbb{Z}_{11}$  tenemos

$$\langle 1 \rangle = \{1\},$$

$$\langle 3 \rangle = \{3, 9, 5, 4, 1\},$$

$$\langle 2 \rangle = U_{11}.$$

Vemos que  $U_{11}$  es cíclico y que un generador es 2.

2. En el grupo  $U_{12} = \{1, 5, 7, 11\}$  tenemos

$$\langle 1 \rangle = \{1\},$$

$$\langle 5 \rangle = \{5, 1\},$$

$$\langle 7 \rangle = \{7, 1\},$$

$$\langle 11 \rangle = \{11, 1\}.$$

Por lo tanto  $U_{12}$  no es un grupo cíclico.

Si  $a$  es un elemento de un grupo  $G$ , se llama *orden de*  $a$  al menor entero positivo  $k$  tal que  $a^k = e$ . Si no existe tal entero positivo, decimos que  $a$  es de *orden infinito*.

Representamos el orden de  $a$  por la notación  $o(a)$ . Si  $n$  es un entero positivo y  $a$  un entero tal que  $(a, n) = 1$ , el orden de  $a$  módulo  $n$  que

estudiamos en la sección anterior es precisamente el orden de  $a$  considerado como elemento del grupo  $U_n$ . Además un entero  $a$  es una raíz primitiva módulo  $n$  si y solo si  $a$  es un generador del grupo  $U_n$ .

El Teorema 5.25 es un caso particular del resultado más general siguiente.

**5.46 Teorema.** *Sea  $G$  un grupo y  $a \in G$  con  $o(a) = k$ . Entonces  $a^t = e$  si y solo si  $k \mid t$ .*

*Demostración.* Si  $k \mid t$  entonces  $t = kq$  y por lo tanto

$$a^t = a^{kq} = (a^k)^q = e^q = e.$$

Recíprocamente, si  $a^t = e$  podemos escribir  $t$  en la forma  $t = qk + r$  con  $0 \leq r < k$ , luego

$$e = a^t = a^{qk+r} = a^{qk}a^r = a^r,$$

y  $r = 0$  por la minimalidad de  $k$ . Por lo tanto  $t = qk$  y  $k \mid t$ .  $\square$

Recordamos que si  $G$  es un grupo finito, se llama *orden de  $G$*  al número de elementos de  $G$ . Representamos el orden del grupo  $G$  por la notación  $o(G)$ .

**5.47 Teorema.** *Sea  $G$  un grupo y  $a \in G$  con  $o(a) = k$ . Entonces  $o(a) = o(\langle a \rangle)$ . Es decir el orden de un elemento  $a$  es igual al orden del subgrupo generado por  $a$ .*

*Demostración.* Veamos primero que los elementos  $e, a, \dots, a^{k-1}$  son todos diferentes. En efecto, si  $a^r = a^s$  con  $0 \leq r < s \leq k-1$  entonces  $a^{s-r} = e$  con  $0 < s-r \leq k-1$  lo que contradice que  $o(a) = k$ . Veamos ahora que todo elemento de  $\langle a \rangle$  se encuentra en la lista  $e, a, \dots, a^{k-1}$ . Si  $a^t \in \langle a \rangle$ , por el algoritmo de la división podemos escribir  $t$  en la forma  $t = qk + r$  con  $0 \leq r < k$ . Por lo tanto

$$a^t = a^{qk+r} = (a^k)^q a^r = ea^r = a^r,$$

y en consecuencia  $\langle a \rangle = \{e, a, \dots, a^{k-1}\}$ . Luego  $o(\langle a \rangle) = k = o(a)$ .  $\square$

**5.48 Corolario.** *Sea  $G = \langle a \rangle$  un grupo cíclico de orden  $k$  con generador  $a$ . Entonces*

$$G = \{e, a, \dots, a^{k-1}\}.$$

Sean  $G$  el grupo multiplicativo  $U_3 = \{1, 2\}$  de las unidades del anillo  $\mathbb{Z}_3$  y  $H = \mathbb{Z}_2$  el grupo aditivo de los enteros módulo 2. Las tablas de multiplicación de estos grupos son:

·	1	2
1	1	2
2	2	1

+	0	1
0	0	1
1	1	0

Aunque  $G$  y  $H$  son grupos diferentes, no hay ninguna diferencia significativa entre ellos, ya que si reemplazamos 1 por 0 y 2 por 1 en la primera tabla obtenemos la segunda. Es decir estos grupos se diferencian únicamente por el nombre de sus elementos.

Formalizamos esta idea mediante la definición siguiente.

**5.49 Definición.** Decimos que los grupos  $(G, *)$  y  $(H, \circ)$  son *isomorfos* si existe una función  $f : G \rightarrow H$  tal que:

1.  $f$  es uno a uno,
2.  $f$  es sobre,
3.  $f(a * b) = f(a) \circ f(b)$ , para todo  $a, b \in G$ .

La función  $f$  se llama un *isomorfismo* de  $G$  sobre  $H$ . Para indicar que los grupos son isomorfos escribimos  $G \simeq H$ .

Un isomorfismo entre los grupos  $G$  y  $H$  anteriormente mencionados es la función  $f : G \rightarrow H$  definida por  $f(1) = 0$  y  $f(2) = 1$ .

**5.50 Ejemplo.** Consideremos los grupos  $U_8$  y  $U_{12}$  de las unidades de los anillos  $\mathbb{Z}_8$  y  $\mathbb{Z}_{12}$ . Sus tablas de multiplicación son:

·	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Si estudiamos por un momento estas tablas, nos damos cuenta que estos grupos son isomorfos y que un isomorfo de  $U_8$  sobre  $U_{12}$  es la función

$f : U_8 \rightarrow U_{12}$  definida por

$$f(1) = 1$$

$$f(3) = 5$$

$$f(5) = 7$$

$$f(7) = 11.$$

Es claro que la función  $f$  es uno a uno y sobre. Para verificar que  $f$  cumple la condición 3 de la definición de isomorfismo hay que comprobar los 16 casos posibles. Verifiquemos algunos de ellos

$$f(5 \cdot 7) = f(3) = 5 = 7 \cdot 11 = f(5) \cdot f(7),$$

$$f(3 \cdot 5) = f(7) = 11 = 5 \cdot 7 = f(3) \cdot f(5),$$

$$f(1 \cdot 3) = f(3) = 5 = 1 \cdot 5 = f(1) \cdot f(3).$$

**5.51 Teorema.** Si  $G$  es un grupo cíclico de orden  $n$ , entonces  $G$  es isomorfo al grupo aditivo  $\mathbb{Z}_n$ .

*Demostración.* Supongamos que  $G = \langle a \rangle$  y que  $o(G) = n$ . Por el corolario del Teorema 5.47,  $G = \{e, a, \dots, a^{n-1}\}$ . Consideremos la función  $f : G \rightarrow \mathbb{Z}_n$  definida por  $f(a^k) = \bar{k}$ . Veamos que  $f$  es un isomorfismo.

1.  $f$  es uno a uno. En efecto, si  $f(a^k) = f(a^j)$  entonces  $\bar{k} = \bar{j}$ , luego  $k \equiv j \pmod{n}$ , o sea  $k - j = qn$  y por lo tanto

$$a^k = a^{j+qn} = a^j(a^n)^q = a^j e = a^j,$$

ya que  $a^n = e$ .

2.  $f$  es sobre. Esto es evidente pues si  $\bar{k} \in \mathbb{Z}_n$ ,  $\bar{k}$  es imagen de  $a^k$  por  $f$ .
3.  $f(a^k a^j) = f(a^{k+j}) = \overline{k+j} = \bar{k} + \bar{j} = f(a^k) + f(a^j)$ , para todo  $a^k, a^j \in G$ .  $\square$

**5.52 Corolario.** Dos grupos cíclicos del mismo orden son isomorfos.

*Demostración.* Este resultado se sigue del hecho de que la relación *ser isomorfo a* es una relación de equivalencia entre grupos, en particular es transitiva.  $\square$

Sean  $G$  y  $H$  dos grupos que por comodidad notamos multiplicativamente. Sobre el *producto cartesiano*  $G \times H = \{(g, h) \mid g \in G \text{ y } h \in H\}$  definimos una operación que es una multiplicación por componentes, mediante la fórmula siguiente,

$$(g, h)(g', h') = (gg', hh').$$

Es fácil de verificar que  $G \times H$  con esta operación es un grupo cuya identidad es  $(e_G, e_H)$  donde  $e_G$  y  $e_H$  son las identidades de  $G$  y  $H$  respectivamente. Además si  $G$  y  $H$  son grupos finitos se tiene que  $o(G \times H) = o(G)o(H)$ . El grupo que acabamos de definir se llama el *producto directo* de  $G$  y  $H$ .

**5.53 Ejemplo.** El producto directo de los grupos aditivos  $\mathbb{Z}_2 = \{0, 1\}$  y  $\mathbb{Z}_3 = \{0, 1, 2\}$  es el conjunto

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\},$$

con la operación, notada aditivamente, definida por  $(a, b) + (c, d) = (a + c, b + d)$ . Algunas muestras de la adición en  $\mathbb{Z}_2 \times \mathbb{Z}_3$  son

$$(0, 1) + (0, 2) = (0 + 0, 1 + 2) = (0, 0),$$

$$(1, 1) + (1, 2) = (1 + 1, 1 + 2) = (0, 0),$$

$$(1, 0) + (1, 1) = (1 + 1, 0 + 1) = (0, 1).$$

**5.54 Ejemplo.** El producto directo de los grupos  $U_3 = \{1, 2\}$  y  $\mathbb{Z}_2 = \{0, 1\}$  es  $U_3 \times \mathbb{Z}_2 = \{(1, 0), (1, 1), (2, 0), (2, 1)\}$  con la operación definida por  $(a, b)(c, d) = (a \cdot c, b + d)$ . Algunos productos son

$$(1, 1)(2, 0) = (1 \cdot 2, 1 + 0) = (2, 1),$$

$$(2, 1)(2, 1) = (2 \cdot 2, 1 + 1) = (1, 0),$$

$$(1, 0)(1, 1) = (1 \cdot 1, 0 + 1) = (1, 1).$$

La noción de producto directo se puede extender en forma natural a más de dos grupos. Dejamos los detalles al lector. El teorema siguiente nos conduce a una demostración sencilla del Teorema Chino del residuo.

**5.55 Teorema.** Sea  $n = m_1 m_2$  con  $m_1$  y  $m_2$  enteros positivos tales que  $(m_1, m_2) = 1$ . Entonces la función  $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  definida por

$$f(\bar{x}) = (\bar{x}^1, \bar{x}^2)$$

donde  $\bar{x}$ ,  $\bar{x}^1$  y  $\bar{x}^2$  representan las clases residuales de  $x$  módulos  $n, m_1$  y  $m_2$  respectivamente, es un isomorfismo de grupos.

*Demostración.* Tenemos que verificar primero que la función está *bien definida*, es decir que distintas elecciones del representante de una clase en  $\mathbb{Z}_n$  conducen al mismo valor de  $f$ . Supongamos que  $\bar{x} = \bar{y}$ . Entonces  $x \equiv y \pmod{n}$  y  $n \mid (x - y)$ . Luego  $m_1 \mid (x - y)$  y  $m_2 \mid (x - y)$ , o sea  $x \equiv y \pmod{m_1}$  y  $x \equiv y \pmod{m_2}$ . Por lo tanto  $\bar{x}^1 = \bar{y}^1$  y  $\bar{x}^2 = \bar{y}^2$  y en consecuencia  $f(\bar{x}) = f(\bar{y})$ .

Veamos ahora que  $f$  es uno a uno. En efecto, si  $f(\bar{x}) = f(\bar{y})$  entonces  $(\bar{x}^1, \bar{x}^2) = (\bar{y}^1, \bar{y}^2)$  o sea  $\bar{x}^1 = \bar{y}^1$  y  $\bar{x}^2 = \bar{y}^2$ . Luego  $x \equiv y \pmod{m_1}$  y  $x \equiv y \pmod{m_2}$  y por el Corolario 4.11,  $x \equiv y \pmod{n}$ . Por lo tanto  $\bar{x} = \bar{y}$ .

Como  $\mathbb{Z}_n$  y  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  tienen igual número de elementos y  $f$  es uno a uno, entonces necesariamente es sobre.

Finalmente tenemos

$$\begin{aligned} f(\bar{x} + \bar{y}) &= f(\overline{x + y}) = (\overline{x + y}^1, \overline{x + y}^2) \\ &= (\bar{x}^1 + \bar{y}^1, \bar{x}^2 + \bar{y}^2) \\ &= (\bar{x}^1, \bar{x}^2) + (\bar{y}^1, \bar{y}^2) = f(\bar{x}) + f(\bar{y}). \quad \square \end{aligned}$$

Por inducción matemática o mediante una demostración similar a la del teorema, tenemos:

**5.56 Corolario.** Sea  $n = m_1 m_2 \cdots m_r$  donde los  $m_i$  son enteros positivos primos relativos dos a dos. Entonces la función

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$$

definida por

$$f(\bar{x}) = (\bar{x}^1, \bar{x}^2, \dots, \bar{x}^r),$$

donde  $\bar{x}, \bar{x}^1, \bar{x}^2, \dots, \bar{x}^r$  representan las clases residuales de  $x$  módulo  $n, m_1, m_2, \dots, m_r$  respectivamente, es un isomorfismo de grupos.

**5.57 Teorema (Chino del residuo).** Sean  $m_1, m_2, \dots, m_r$  enteros positivos primos relativos dos a dos, y sean  $a_1, a_2, \dots, a_r$  enteros arbitrarios. Entonces el sistema de congruencia lineales

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdot \\ &\cdot \\ &\cdot \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

tiene solución única módulo  $n = \prod_{i=1}^r m_i$ .

*Demostración.* Consideremos el elemento  $(\bar{a}_1^1, \bar{a}_2^2, \dots, \bar{a}_r^r)$  de  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r}$ . Como la función  $f$  del corolario anterior es un isomorfismo, existe un único  $\bar{x} \in \mathbb{Z}_n$  tal que  $\bar{x}^1 = \bar{a}_1^1, \bar{x}^2 = \bar{a}_2^2, \dots, \bar{x}^r = \bar{a}_r^r$ , es decir un entero  $x$ , único módulo  $n$ , tal que  $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_r \pmod{m_r}$ .  $\square$

Los conceptos de isomorfismo y de producto directo de grupos pueden extenderse inmediatamente a conceptos similares para anillos. Concretamente tenemos las definiciones siguientes.

**5.58 Definición.** Decimos que los anillos  $(A_1, +, \cdot)$  y  $(A_2, +, \cdot)$  son *isomorfos* si existe un isomorfismo de grupos  $f$  entre el grupo aditivo de  $A_1$  y el grupo aditivo de  $A_2$ , con la propiedad adicional

$$f(ab) = f(a)f(b) \text{ para todo } a, b \in A_1.$$

**5.59 Definición.** El *producto directo de los anillos*  $A_1$  y  $A_2$  es el producto cartesiano  $A_1 \times A_2$  con las operaciones definidas por

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$

y

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2).$$

Es fácil verificar que efectivamente  $(A_1 \times A_2, +, \cdot)$  con las operaciones que acabamos de definir es un anillo. Además, la noción de producto directo de anillos, se puede extender en forma natural a más de dos anillos.

**5.60 Ejemplo.** El producto directo de los anillos  $\mathbb{Z}_4$  y  $\mathbb{Z}_3$  es el producto cartesiano  $\mathbb{Z}_4 \times \mathbb{Z}_3$  con la suma y la multiplicación definidas por  $(a, b) + (c, d) = (a + c, b + d)$  y  $(a, b)(c, d) = (ac, bd)$ . Algunos ejemplos de la suma y la multiplicación son

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

**5.61 Teorema.** *Los isomorfismos construidos en el Teorema 5.55 y su corolario son isomorfismo de anillos.*

*Demostración.* Para ver que el isomorfismo de grupos

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \text{ definido por } f(\bar{x}) = (\bar{x}^1, \bar{x}^2),$$

es un isomorfismo de anillos, solo falta por comprobar que se cumple la condición adicional  $f(\overline{xy}) = f(\bar{x})f(\bar{y})$  para todo  $\bar{x}, \bar{y} \in \mathbb{Z}_n$ ; pero esto se tiene porque,

$$\begin{aligned} f(\overline{xy}) &= (\overline{xy}^1, \overline{xy}^2) = (\bar{x}^1\bar{y}^1, \bar{x}^2\bar{y}^2) \\ &= (\bar{x}^1, \bar{x}^2)(\bar{y}^1, \bar{y}^2) \\ &= f(\bar{x})f(\bar{y}). \end{aligned}$$

En forma similar se demuestra que el isomorfismo del corolario, es un isomorfismo de anillos.  $\square$

**5.62 Teorema.** Si  $A_1$  y  $A_2$  son anillos isomorfos, sus grupos de unidades también son isomorfos.

*Demostración.* Sea  $f : A_1 \longrightarrow A_2$  un isomorfismo de anillos y sean  $A_1^*$  y  $A_2^*$  los grupos de las unidades de  $A_1$  y  $A_2$  respectivamente. La demostración del teorema consiste en verificar que la restricción  $f|_{A_1^*}$  de  $f$  a  $A_1^*$  es un isomorfismo de grupos de  $A_1^*$  sobre  $A_2^*$ . Dejamos los detalles como ejercicio.  $\square$

**5.63 Teorema.** Sea  $n = m_1m_2$  con  $m_1$  y  $m_2$  enteros positivos tales que  $(m_1, m_2) = 1$ . Entonces  $U_n \simeq U_{m_1} \times U_{m_2}$ . En forma más general si  $n = m_1m_2 \dots m_r$  donde los  $m_i$  son enteros positivos primos relativos dos a dos, entonces  $U_n \simeq U_{m_1} \times U_{m_2} \times \dots \times U_{m_r}$ .

*Demostración.* Por el Teorema 5.61 sabemos que los anillos  $\mathbb{Z}_n$  y  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  son isomorfos. Por lo tanto sus grupos de unidades son isomorfos. Luego  $U_n$  es isomorfo al grupo de las unidades de  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ .

Pero el grupo de las unidades de  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  es precisamente el producto directo  $U_{m_1} \times U_{m_2}$  de los grupos de las unidades de  $\mathbb{Z}_{m_1}$  y  $\mathbb{Z}_{m_2}$ , puesto que  $(a, b)$  es una unidad de  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  si y solo si existe  $(a', b')$  en  $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$  tal que  $(a, b)(a', b') = (1, 1)$ , es decir si y solo si  $aa' = 1$  y  $bb' = 1$ , o en otras palabras si y solo si  $a \in U_{m_1}$  y  $b \in U_{m_2}$ .

Usando un razonamiento similar, se demuestra la afirmación más general.  $\square$

Para terminar esta sección vamos a estudiar la existencia de raíces primitivas módulo  $n$ . Como mencionamos anteriormente, un entero  $a$  es una raíz primitiva módulo  $n$  si y solo si  $a$  es un generador del grupo  $U_n$ . Por lo tanto solo existen raíces primitivas módulo  $n$  para aquellos enteros positivos  $n$  tales que  $U_n$  es un grupo cíclico.

**5.64 Teorema.** *Si  $U_n$  es cíclico entonces  $n$  es alguno de los números  $2, 4, p^k$  o  $2p^k$  con  $p$  un primo impar,  $k \in \mathbb{N}$ .*

*Demostración.* Supongamos que  $n$  no es de ninguna de las formas mencionadas. Podemos considerar dos casos:

1.  $n = 2^r \prod_{i=1}^k p_i^{s_i}$  con  $k \geq 2$  o con  $k = 1$  y  $r \geq 2$ .
2.  $n = 2^k$  con  $k \geq 3$ .

Veamos que en ninguno de estos casos  $U_n$  es cíclico.

En el primer caso los números  $p_1^{s_1}$  y  $\frac{n}{p_1^{s_1}}$  son mayores que 2 y por el ejercicio 4 de la sección 3.4 sabemos que  $\Phi(p_1^{s_1})$  y  $\Phi(n|p_1^{s_1})$  son pares.

Además si  $(a, n) = 1$  por el Teorema de Euler  $a^{\Phi(p_1^{s_1})=1} \equiv 1 \pmod{p_1^{s_1}}$  y  $a^{\Phi(n|p_1^{s_1})} \equiv 1 \pmod{n|p_1^{s_1}}$ .

Luego  $a^{\frac{1}{2}\Phi(p_1^{s_1})\Phi\left(\frac{n}{p_1^{s_1}}\right)}$  es congruente con 1 módulo  $p_1^{s_1}$  y módulo  $\frac{n}{p_1^{s_1}}$  y por lo tanto módulo  $n$  en virtud del Corolario 4.11. Luego si  $a \in U_n$ ,

$$o(a) \leq (1|2)\Phi(p_1^{s_1})\Phi(n|p_1^{s_1}) = \Phi(n)/2 < \Phi(n),$$

y  $U_n$  no puede ser cíclico.

En el segundo caso, si  $(a, n) = 1$  donde  $n = 2^k$  entonces  $a$  es impar de la forma  $a = 1 + 2b$  y tenemos

$$\begin{aligned} a^2 &= 1 + 4b + 4b^2 = 1 + 4b(1 + b) = 1 + 8c = 1 + 2^3c, \\ a^4 &= (1 + 8c)^2 = 1 + 16c + 64c^2 = 1 + 16d = 1 + 2^4d, \\ a^8 &= (1 + 2^4d)^2 = 1 + 2^5d + 2^8d^2 = 1 + 2^5e, \end{aligned}$$

y en general por un argumento inductivo, si  $j \geq 3$

$$a^{2^{j-2}} = 1 + 2^j g \equiv 1 \pmod{2^j}.$$

Por lo tanto,  $a^{2^{k-2}} \equiv 1 \pmod{2^k}$  y si  $a \in U_{2^k}$ , entonces

$$o(a) \leq 2^{k-2} < 2^{k-1} = \Phi(2^k),$$

lo que implica que  $U_{2^k}$  no es cíclico.  $\square$

Veamos ahora que el recíproco del teorema anterior también es cierto. Necesitamos un lema previo.

**5.65 Lema.** *Si  $p$  es un primo impar y  $n$  un entero positivo, el orden de  $1 + p$  en  $U_{p^{n+1}}$  es  $p^n$ .*

*Demostración.* Si probamos que:

1.  $(1 + p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}}$  y
2.  $(1 + p)^{p^n} \equiv 1 \pmod{p^{n+1}}$ ,

por el Teorema 5.46 podemos concluir que  $o(1 + p) = p^n$  en  $U_{p^{n+1}}$ . La prueba de 1 es por inducción sobre  $n$ . Si  $n = 1$  la congruencia es evidente. Supongamos que la congruencia es válida para  $n$  y veamos que es válida para  $n + 1$ . Por hipótesis de inducción

$$(1 + p)^{p^{n-1}} = 1 + p^n + tp^{n+1} = 1 + (1 + tp)p^n,$$

luego

$$(1 + p)^{p^n} = \left( (1 + p)^{p^{n-1}} \right)^p = (1 + (1 + tp)p^n)^p$$

y por el Teorema del binomio tenemos

$$\begin{aligned} (1 + p)^{p^n} &= 1 + \binom{p}{1}(1 + tp)p^n + \binom{p}{2}((1 + tp)p^n)^2 + \\ &\quad + \cdots + \binom{p}{p}((1 + tp)p^n)^p, \\ &= 1 + (1 + tp)p^{n+1} + sp^{n+2}, \\ &= 1 + p^{n+1} + hp^{n+2}, \\ &\equiv 1 + p^{n+1} \pmod{p^{n+2}}. \end{aligned}$$

Por lo tanto por el principio de inducción matemática, 1 es cierta para todo entero positivo  $n$ .

Como la congruencia en 1 es cierta para todo entero positivo, en particular tenemos

$$(1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}},$$

luego

$$(1+p)^{p^n} = 1 + p^{n+1} + kp^{n+2} \equiv 1 \pmod{p^{n+1}}$$

que es precisamente la condición 2.  $\square$

**5.66 Teorema.** *Si  $n$  es alguno de los números  $2, 4, p^k$  o  $2p^k$  con  $p$  primo impar, entonces  $U_n$  es cíclico.*

*Demostración.* Claramente  $U_2 = \{1\}$  y  $U_4 = \{1, 3\}$  son grupos cíclicos. También, por el corolario 5.35,  $U_p$  es cíclico. Veamos ahora que  $U_{p^k}$  es cíclico si  $k > 1$ . Por comodidad representamos  $k$  en la forma  $k = n + 1$ . Debemos encontrar en  $U_{p^{n+1}}$  un elemento de orden  $o(U_{p^{n+1}}) = \Phi(p^{n+1})$ . Nuestro candidato es  $a^p(1+p)$  donde  $a$  es un generador de  $U_p$ . Sea  $t = o(a^p(1+p))$  en  $U_{p^{n+1}}$ .

Por el corolario 5.26,  $t \mid \Phi(p^{n+1}) = p^n(p-1)$ .

Como  $a^p(1+p) \equiv a^p \equiv a \pmod{p}$ , entonces  $a^p(1+p)$  y  $a$  tienen el mismo orden módulo  $p$ , que de acuerdo a la elección de  $a$  es  $p-1$ .

Teniendo en cuenta que  $(a^p(1+p))^t \equiv 1 \pmod{p^{n+1}} \equiv 1 \pmod{p}$ , de la observación anterior y el Teorema 5.25 deducimos que  $p-1 \mid t$ .

Puesto que  $t \mid p^n(p-1)$  y  $p-1 \mid t$ , entonces  $t = p^k(p-1)$  para algún  $k = 1, 2, \dots, n$ . Nuestro objetivo es probar que  $k = n$ , es decir que  $t = p^n(p-1)$ .

Como

$$\begin{aligned} (a^p(1+p))^{p^{n-1}(p-1)} &= a^{p^n(p-1)}(1+p)^{p^{n-1}(p-1)} \\ &\equiv (1+p)^{p^{n-1}(p-1)} \pmod{p^{n+1}}, \end{aligned}$$

entonces

$$(a^p(1+p))^{p^{n-1}(p-1)} \not\equiv 1 \pmod{p^{n+1}}$$

ya que por el lema,  $1+p$  tiene orden  $p^n$  en  $U_{p^{n+1}}$ .

Por lo tanto  $t \nmid p^{n-1}(p-1)$  y necesariamente  $t = p^n(p-1)$  como queríamos probar.

Finalmente, si  $p$  es un primo impar, por el Teorema 5.63,

$$U_{2p^k} \simeq U_2 \times U_{p^k} \simeq U_{p^k}$$

y también  $U_{2p^k}$  resulta cíclico si  $k \geq 1$ .  $\square$

Podemos resumir los dos últimos teoremas en uno solo estableciendo lo siguiente.

**5.67 Teorema.** *El grupo  $U_n$  es cíclico si y solo si  $n$  es alguno de los números  $2, 4, p^k$  o  $2p^k$  con  $p$  primo impar.*

Usando el concepto de raíces primitivas tenemos:

**5.68 Corolario.** *Un entero  $n$  tiene raíces primitivas si y solo si  $n$  es alguno de los números  $2, 4, p^k$  o  $2p^k$  con  $p$  primo impar.*

---

## Ejercicios 5.4

---

1. Construir un isomorfismo de  $U_9$  sobre  $U_{18}$ .
2. Si  $g = (a, b)$  es un elemento del producto directo  $G \times H$ , probar que el orden de  $g$  es el mínimo común múltiplo de los ordenes de  $a$  y  $b$ .
3. Hallar generadores para  $U_{25}$ ,  $U_{125}$ , y  $U_{625}$ .
4. Hallar una raíz primitiva módulo 19.683.
5. Si  $a$  es una raíz primitiva módulo  $p$ , probar que el número que sea impar entre  $a$  y  $a + p^k$  es una raíz primitiva módulo  $2p^k$ .
6. Hallar raíces primitivas módulos 250 y 162.

## 6.1 Nociones básicas

Los orígenes de la criptografía se remontan al comienzo de nuestra civilización. En la antigüedad se usó principalmente para el intercambio de información secreta en los campos político y militar, hoy en día su aplicación es fundamental en la transmisión segura de información confidencial a través de las redes de computadores.

La **criptografía** es la parte de la **criptología** (del griego *kripto* y *logos*, estudio de lo oculto) que trata del diseño e implementación de los sistemas secretos. La otra parte de la criptología es el **criptoanálisis** que consiste en el estudio de los métodos para descifrar estos sistemas.

Los mensajes que un emisor quiere enviar a un determinado receptor son llamados **textos planos** y los mensajes secretos que son enviados son llamados **textos cifrados**. Los textos planos y los textos cifrados se escriben utilizando un *alfabeto* que consiste de letras, números, signos de puntuación o cualquier otro símbolo. El proceso de convertir textos planos en textos

cifrados se llama *cifrado* o *encriptación*, y el proceso inverso de convertir textos cifrados en textos planos, se llama *desciframiento* o *desencriptación*.

Usualmente los textos planos y los textos cifrados se dividen en *unidades de mensaje*. Una unidad de mensajes puede estar formada por un único elemento del alfabeto o por bloques de dos o mas símbolos del mismo. Las transformaciones que se aplican a las unidades de mensaje para convertir textos planos en textos cifrados se conocen con el nombre de *transformaciones o funciones de cifrado* y las transformaciones utilizadas para recuperar los textos planos a partir de los textos cifrados se llaman las *transformaciones o funciones de desciframiento*.

Se conoce con el nombre de *claves* a ciertas informaciones que permiten determinar las funciones de cifrado y descifrado.

Un sistema criptográfico o *criptosistema* esta formado por un alfabeto, un conjunto de transformaciones de cifrado, un conjunto de transformaciones de desciframiento y un conjunto de claves. Un buen sistema criptográfico es aquél en el que los algoritmos de cifrado y descifrado son sencillos de aplicar conocidas las claves, pero que resulte imposible o muy difícil de desencriptar sin conocer las mismas.

## 6.2 Cifrados monográficos

Los *cifrados monográficos* o de caracteres son aquellos que están basados en la sustitución de cada símbolo del alfabeto por otro símbolo. Los criptosistemas más sencillos de esta clase están basados en la aritmética módulo  $n$ .

La historia afirma que el emperador Julio Cesar utilizó un sistema de estos que consistía en reemplazar cada letra del alfabeto por la letra que se encontraba tres posiciones adelante. Usando como alfabeto, el alfabeto español usual, formado por las 27 letras de la A a la Z, donde hemos excluidos las letras CH y LL, vamos a describir como funciona este sistema.

Empezamos asignando a cada letra un número que llamaremos su *equivalente numérico*, como se indica en la tabla (6.1).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Q	R	S	T	U	V	W	X	Y	Z							
17	18	19	20	21	22	23	24	25	26							

TABLA 6.1. Equivalente numérico

Si representamos por  $P$  el equivalente numérico de una letra en el texto plano y por  $C$  el equivalente numérico de la correspondiente letra en el texto cifrado, para el sistema del Cesar, tenemos la transformación de cifrado,

$$C \equiv P + 3 \pmod{27}.$$

Para facilidad reunamos los textos planos y los textos cifrados en la siguiente tabla:

Texto Plano	A	B	C	D	E	F	G	H	I	J	K	L	M
Texto Cifrado	3	4	5	6	7	8	9	10	11	12	13	14	15
	D	E	F	G	H	I	J	K	L	M	N	Ñ	O

Texto Plano	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Texto Cifrado	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	16	17	18	19	20	21	22	23	24	25	26	0	1	2
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

TABLA 6.2. Cifrado  $C \equiv P + 3 \pmod{27}$ .

Para cifrar un mensaje usando esta transformación, primero cambiamos cada letra por su equivalente numérico, luego cambiamos cada uno de estos números sumándole 3 y tomando el resultado módulo 27, y por último transformamos nuevamente los números así obtenidos a letras, para obtener el mensaje cifrado que será enviado.

**6.1 Ejemplo.** Cifremos la palabra YACIMIENTO usando la transformación de Cesar.

Primero, utilizando los equivalentes numéricos, convertimos la palabra en números, obteniendo

25 0 2 8 12 8 4 13 20 15

luego cambiamos cada número sumándole 3 y tomando el resultado módulo 27. Este trabajo ya está resumido en la tabla anterior. Como resultado obtenemos

1 3 5 11 15 11 7 16 23 18

Finalmente el texto cifrado es, BDFLOLHPWR.

Para evitar que un *criptoanalista* descifre fácilmente los mensajes al reconocer ciertas palabras de uso frecuente, es aconsejable agrupar las letras en bloques de un tamaño determinado.

**6.2 Ejemplo.** Cifremos el mensaje NOS VEMOS MAÑANA EN EL PUERTO usando bloques de tamaño 4.

Si escribimos el mensaje usando bloques de cuatro letras, obtenemos,

NOSV EMOS MAÑA NAEN ELPU ERT0

Convirtiendo las letras en su equivalente numérico tenemos,

13 15 19 22 4 12 15 19 12 0 14 0 13 0 4 13 4 11 16 21 4 18 20 15

Aplicando la transformación  $C \equiv P + 3 \pmod{27}$ , obtenemos

16 18 22 25 7 15 18 22 15 3 17 3 16 3 7 16 7 14 19 24 7 21 23 18

Usando la Tabla 6.2 de textos planos y textos cifrados, convertimos los bloques anteriores en letras para obtener el mensaje cifrado que se envía

PRVY HORV ODQD PDHP HÑSX HUWR

Si el número de letras en el mensaje que se quiere enviar no es múltiplo de 4, se añade, cuantas veces se necesite, una letra arbitraria por ejemplo X para completar el último bloque, o algunos prefieren dejar el último bloque con menos letras que los restantes.

**6.3 Ejemplo.** Ilustremos ahora como se descifra un mensaje recibido si sabemos que el cifrado utilizado es el de Julio Cesar.

Supongamos que el mensaje recibido es

KRBH VHÑG LDHV FRJL GRAA

Primero convertimos las letras en números usando el equivalente numérico, el resultado es

10 18 1 7      22 7 14 6      11 3 7 22      5 18 9 11      6 18 0 0

Luego aplicamos a cada uno de estos números la transformación  $P \equiv C - 3 \pmod{27}$  que es la inversa de la transformación del Cesar. Obtenemos,

7 15 25 4      19 4 11 3      8 0 4 19      2 15 6 8      3 15 24 24.

Finalmente escribiendo las letras correspondientes encontramos el mensaje  
HOYE SELD IAES COGI DOXX

que leído adecuadamente se convierte en HOY ES EL DIA ESCOGIDO.

Hacemos notar que todo el trabajo anterior se puede leer directamente de la tabla de textos planos y textos cifrados.

El cifrado de Julio Cesar es un caso especial de una transformación de la forma

$$C \equiv P + k \pmod{27},$$

con  $0 \leq k \leq 26$ . Estas transformaciones se llaman *translaciones*. La correspondiente transformación para descifrar los mensajes cifrados es  $P \equiv C - k \pmod{27}$ . Hay 27 posibles translaciones.

Las translaciones son un caso especial de las *transformaciones afines* que son de la forma

$$C \equiv aP + b \pmod{27},$$

donde  $0 \leq a, b \leq 26$  y  $(a, 27) = 1$ . Se escoge  $a$  primo relativo con 27 para que cuando  $P$  recorra un sistema completo de residuos módulo 27,  $C$  también lo recorra.

Hay  $\phi(27) = 18$  elecciones para  $a$  y 27 elecciones para  $b$ , luego hay 486 posibles transformaciones afines. La transformación de desciframiento para una transformación afín es

$$P \equiv a^{-1}(C - b) \pmod{27},$$

donde  $0 \leq P \leq 26$  y  $aa^{-1} \equiv 1 \pmod{27}$ .

La tabla 6.3 da los inversos módulo 27 de los números positivos menores que 27 y primos relativos con 27.

**6.4 Ejemplo.** Cifremos el texto plano NO TENGO DINERO usando la transformación afín  $C \equiv 4P + 9 \pmod{27}$ .

$a$	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23
$a^{-1}$	1	14	7	11	4	17	19	5	25	2	22	8	10	23	16	20

$a$	25	26
$a^{-1}$	13	26

TABLA 6.3. Los inversos módulo 27 de los números positivos menores que 27 y primos relativos con 27

Utilizando aritmética módulo 27, construimos la tabla correspondiente de textos planos y textos cifrados para esta transformación. Por ejemplo, el equivalente numérico de la letra M es 12 en el texto plano, y aplicando a este número la transformación  $C \equiv 4P + 9 \pmod{27}$ , obtenemos el número  $4 \cdot 12 + 9 = 57 \equiv 3 \pmod{27}$ , que corresponde a la letra D, como se aprecia en la columna encabezada por M de la tabla resultante siguiente.

Texto Plano	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Texto Cifrado	9	13	17	21	25	2	6	10	14	18	22	26	3	7	11
	J	N	Q	U	Y	C	G	K	Ñ	R	V	Z	D	H	L

Texto Plano	O	P	Q	R	S	T	U	V	W	X	Y	Z
	15	16	17	18	19	20	21	22	23	24	25	26
Texto Cifrado	15	19	23	0	4	8	12	16	20	24	1	5
	O	S	W	A	E	I	M	P	T	X	B	F

TABLA 6.4. Usando la transformación afín  $C \equiv 4P + 9 \pmod{27}$ .

Dividiendo el mensaje en bloques de longitud 4 y procediendo como en el ejemplo 2, encontramos usando la tabla anterior, que el criptograma o texto cifrado que debemos enviar es

HOIY HGOU ÑHYA OXXX

La gran desventaja de los sistemas de cifrado que usan transformaciones afines, es la facilidad con que se pueden descifrar analizando la frecuencia con que aparecen las letras en el texto. La tabla 6.5 muestra en porcentaje la frecuencia de ocurrencia de las letras más usadas en Español, en orden descendente.

**6.5 Ejemplo.** Supongamos que deseamos descifrar el siguiente texto, suponiendo que fue cifrado usando una transformación afín

RPGNR HPGTG NHZGH EJDOD XQRHT IHPJG PDE

E	A	O	L	S	N	D	R	U	I	T	C
16,78	11,96	8,69	8,37	7,88	7,01	6,87	4,94	4,80	4,15	3,31	2,92
P	M	Y	Q	B	H	G	F				
2,78	2,12	1,54	1,53	0,92	0,89	0,73	0,52				

TABLA 6.5. Frecuencia de ocurrencia de las letras más usadas en Español, en orden descendente

Las letras que aparecen con más frecuencia en el mensaje son la H que aparece 6 veces y la G que aparece 5 veces. Por lo tanto podemos pensar que la E se transforma en H y la A se transforma en G. Como el equivalente numérico de la E es 4 y esta letra se transforma en H cuyo equivalente numérico es 7, tenemos la relación

$$7 \equiv 4a + b \pmod{27}.$$

Similarmente, tenemos la relación  $6 \equiv 0a + b \pmod{27}$ .

Resolviendo las congruencias anteriores tenemos

$$b \equiv 6 \pmod{27} \quad \text{y} \quad 4a \equiv 1 \pmod{27}.$$

Multiplicando la última congruencia por 7, que es el inverso de 4 módulo 27, obtenemos finalmente

$$a \equiv 7 \pmod{27} \quad \text{y} \quad b \equiv 6 \pmod{27}.$$

Concluimos que la transformación afín usada fue  $C \equiv 7P + 6 \pmod{27}$ . Procediendo como en los ejemplos anteriores, encontramos que el mensaje cifrado es

UNA BUENA CABEZA ES MEJOR QUE CIEN MANOS.

Es conveniente anotar que dependiendo del módulo  $n$ , no siempre las congruencias anteriores tienen solución única. En este caso se escogen las soluciones que proporcionan mensajes ininteligibles, o se utiliza alguna información adicional.

Hay otros métodos de cifrado por sustitución más eficaces. Por ejemplo, algunos sistemas usan la *sustitución polialfabética*, en la cual se usan varios alfabetos para cifrar los mensajes. El sistema polialfabético más conocido es el de Vigenère, creado por el criptógrafo francés Blaise de Vigenère en 1586. El principal elemento de este sistema es la tabla 6.6, llamada *Tabla de Vigenère*.

Tabla 6.6. Tabla de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

En este sistema los distintos alfabetos están formados por las columnas. Para cifrar un mensaje se usa repetidamente una palabra clave, como ilustraremos en el siguiente ejemplo.

**6.6 Ejemplo.** Cifremos el siguiente texto

MEDIOCRE ES EL DISCIPULO QUE NO SUPERA A SU MAESTRO

usando la palabra clave EXITO.

Como la clave tiene cinco letras descomponemos el texto plano en bloques de longitud cinco y lo escribimos debajo de la palabra clave, que se repite tantas veces como sea necesario. Para este caso tenemos,

EXITO EXITO EXITO EXITO EXITO EXITO EXITO EXITO EX

MEDIO CREES ELDIS CIPUL OQUEN OSUPE RAASU MAEST RO

Enseguida codificamos cada letra del texto plano con el alfabeto de la tabla marcado por la letra de la clave situada en su parte superior. Por ejemplo, en el primer bloque la M se codifica como Q usando el alfabeto que empieza por E (la letra Q está en la intersección de la columna E y la fila M), la E se codifica como B usando el alfabeto que empieza por X y así sucesivamente. El texto cifrado completo es

QBLBC GOMXG IILBG GFXNZ SNCXB SPCIS VXILI QXMLH VL.

Vigenère desarrolló otras clases de cifrado basadas en su tabla, dos de ellos merecen mencionarse. En el primero de ellos la clave es el texto plano y en el otro la clave es el texto cifrado. Además en ambos casos se conoce la primera letra de la clave.

**6.7 Ejemplo.** Descifremos el mensaje GBDDRUMZ si sabemos que se utilizó el texto plano como clave, y que la primera letra de la clave es T.

Con la información suministrada, usando la matriz de Vigenère vemos que la primera letra del texto plano es N. Puesto que la clave es el texto plano, N es la segunda letra de la clave y utilizando la matriz de Vigenère, encontramos que O es la segunda letra del texto plano y por lo tanto la tercera letra de la clave, P es la tercera letra del texto plano y en consecuencia la cuarta letra de la clave, etc. Continuando este proceso completamos la tabla 6.7 donde vemos que el mensaje es NO PODRE IR.

Clave	T	N	O	P	O	D	R	E	I
Texto plano	N	O	P	O	D	R	E	I	R
Texto cifrado	G	B	D	D	R	U	V	M	Z

TABLA 6.7. Ejemplo 6.7

**6.8 Ejemplo.** Supongamos que conocemos el texto cifrado UIYSAEVJEIZSW y sabemos que H es la primera letra de la clave y el texto cifrado se ha utilizado como clave.

Para descifrar el mensaje, usamos la matriz de Vigenère para construir la tabla siguiente que nos revela el mensaje

Clave	H	U	I	Y	S	A	E	V	J	E	I	Z	S
Texto plano	N	O	Q	U	I	E	R	O	V	E	R	T	E
Texto cifrado	U	I	Y	S	A	E	V	J	E	I	Z	S	W

TABLA 6.8. Ejemplo 6.8

Con el fin de evitar el criptoanálisis basado en la frecuencia de las letras, se utiliza el **cifrado por transposición** que consiste en la alteración del orden de las letras del texto original, usualmente de acuerdo a una clave o convención determinados.

**6.9 Ejemplo.** El caso más sencillo es el de la transposición simple de las letras. Por ejemplo, el mensaje ESTE JUEGO ES DIVERTIDO lo podemos dividir en la siguiente forma

E T J E O S I E T D  
S E U G E D V R I O

y enviar como texto cifrado el mensaje

ETJE OSIE TDSE UGED VRIO

**6.10 Ejemplo.** Si utilizamos como clave la palabra TEATRO, podemos cifrar el mensaje del ejemplo anterior utilizando una matriz, que construimos de la siguiente forma:

Primero construimos una matriz cuya primera fila esta formada por las letras no repetidas de la palabra clave, y cuyas filas siguientes se obtienen escribiendo de izquierda a derecha las letras que forman el texto plano. Luego construimos una nueva matriz permutando las columnas de la matriz

anterior de tal forma que las letras de la palabra clave queden ordenadas en orden alfabético. Finalmente el texto cifrado que enviamos se forma con las letras de las columnas de esta última matriz, léidas de abajo hacia arriba.

En este caso la primera matriz que obtenemos es

T	E	A	R	O
E	S	T	E	J
U	E	G	O	E
S	D	I	V	E
R	T	I	D	O

Después de ordenar las columnas obtenemos

A	E	O	R	T
T	S	J	E	E
G	E	E	O	U
I	D	E	V	S
I	T	O	D	R

El texto cifrado que enviamos es

IIGT TDES OEEJ DVOE RSUE.

---

## Ejercicios 6.1

---

- Usar el cifrado del Cesar para encriptar los siguientes mensajes:
  - NOS VEREMOS EN ROMA.
  - DE POCO SIRVE LA CIENCIA DONDE FALTA LA PRUDENCIA.
- Descifrar los siguientes mensajes si se sabe que fueron encriptados usando la transformación  $C \equiv P + 13 \pmod{27}$ :
  - NXDH QTNF PQON FGUS NEOB ZBÑE NFZB GENG QFYN  
XOBZ CNXN ÑENF.

- (b) FQNY BPQE NPBG HFHQ ABDH QQXD HQZB YNPE HSNQ  
BZQX FBXZ BSBM NPQX PUNK.
3. Mediante un análisis de frecuencia descifrar el siguiente texto que fue cifrado usando una translación de la forma  $C \equiv P + k \pmod{27}$ .  
SIBMW ZPILM UCTMZ WAMAP TXWZB IUBMM UMSMA BCLPW  
LMSIK ZPXBW SWÑPI.
  4. Usar la transformación afín  $C \equiv 10P + 20 \pmod{27}$  para cifrar el mensaje NO DEJES PARA MAÑANA LO QUE PUEDES HACER HOY.
  5. Descifrar el mensaje EDK BFL EQV DLB LPL FZQ EKZ ZQZ KBB QFQ que fue encriptado usando la transformación afín  $C \equiv 5P + 17 \pmod{27}$ .
  6. Mediante un análisis de frecuencia desencriptar el siguiente texto que fue encriptado usando una transformación afín TFVS FMKK BUKB CKÑL BFSK MFGL KTFM CKUO ÑMFV DOBO KNMF VIII.
  7. Usando la tabla de Vigenère y la palabra clave SISTEMA, cifrar el texto NO BEBAS AGUA QUE NO VEAS.
  8. Descifrar el mensaje VZZOX SFWSP EGSTZ CCZAN VHGDZ TCFRP WZWXT FB que fue encriptado usando la tabla de Vigenère y la palabra clave ROSAL.
  9. Descifrar el texto BLRVYHVWBRWWRPCRKTGKRN, si se sabe que fue cifrado usando como clave el texto plano, que la primera letra de la clave es Q y la primera letra del texto plano es L.
  10. Descifrar el texto RVILLWOOQSAOBFXVV, si se sabe que fue cifrado usando como clave el texto cifrado y que la primera letra de la clave es W.
  11. Encriptar los siguientes mensajes usando una transposición simple
    - (a) ESTAS APLICACIONES SON MUY IMPORTANTES.
    - (b) EL DEL OIDO ES EL SENTIDO MAS FACIL DE ENGAÑAR.
  12. Cifrar el mensaje UN BUEN SUEÑO VALE MAS QUE CUALQUIER REMEDIO usando una matriz y la palabra clave CARRETA.

13. Descifrar el mensaje AOAAUHRZNEUVHRHYNOIOTNEO si se sabe que fue cifrado usando una transposición simple.
14. Descifrar el texto cifrado ITRESOR AEACUR ADITSSE DOMSESE ADDMÑÑ VOUOOLC LNROEE si se sabe que fue cifrado usando una matriz y la palabra clave PELIGRO.
15. ¿Qué transformación de cifrado se obtiene si se aplica la transformación  $C \equiv 4P + 11 \pmod{27}$  seguida de la transformación  $C \equiv 10P + 20 \pmod{27}$ ?

### 6.3 Cifrado en Bloques

Como los cifrados monográficos o de carácter son relativamente fáciles de descifrar mediante análisis estadísticos, en 1929 el matemático Lister Hill, desarrolló el cifrado en bloques. Este cifrado opera sobre bloques de  $n$  letras transformándolos en bloques del mismo tamaño.

Para empezar, supongamos que nuestras unidades de mensajes, tanto de texto plano como de texto cifrado, están formadas por bloques de dos letras que llamamos *dígrafos*. A cada dígrafo le asignamos un vector  $\begin{pmatrix} x \\ y \end{pmatrix}$  donde  $x$  y  $y$  son enteros módulo 27 cuando usamos el alfabeto español, o más generalmente, son enteros módulo  $n$  si el alfabeto en consideración tiene  $n$  letras. Por ejemplo si usamos el alfabeto español, al dígrafo ES le corresponde el vector  $\begin{pmatrix} 4 \\ 19 \end{pmatrix}$ .

Antes de dar un ejemplo, recordemos algunas nociones básicas de álgebra lineal. Si  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  es una matriz de tamaño  $2 \times 2$  y  $P = \begin{pmatrix} x \\ y \end{pmatrix}$  es un vector con componentes en un anillo conmutativo con identidad  $R$ , definimos el producto  $AP$  mediante

$$AP = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

El producto de dos matrices de tamaño  $2 \times 2$  lo definimos como

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}.$$

Decimos que una matriz  $A$  es *invertible* si existe otra matriz  $B$  tal que  $AB = BA = I$ , donde  $I$  es la matriz identidad  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . No todas las matrices son invertibles. Se puede demostrar fácilmente que la matriz  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  es invertible si y solo si su *determinante*  $\det A = D = ad - bc$  es una unidad del anillo  $R$ , es decir  $D$  es un elemento invertible para la multiplicación en  $R$ . En tal caso la inversa de  $A$ , que se nota  $A^{-1}$ , está dada por

$$A^{-1} = D^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix},$$

donde  $D^{-1}$  es el inverso del determinante  $D$  en el anillo  $R$ .

Para cifrar un texto plano usando el sistema de Hill, lo dividimos en bloques de dos letras, añadiendo si es necesario al final una letra X para que todos los bloques tengan el mismo tamaño. Luego hallamos los vectores correspondientes a cada bloque, les aplicamos a estos vectores una transformación de la forma

$$C \equiv AP \pmod{n}$$

tomando los resultados módulo  $n$ , donde  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  es una matriz de tamaño  $2 \times 2$  con componentes en  $\mathbb{Z}_n$  y tal que  $(\det A, n) = 1$ . Finalmente con los nuevos vectores así obtenidos formamos el texto cifrado.

**6.11 Ejemplo.** Usando el alfabeto español, cifremos el mensaje YA ENTENDI, aplicando una transformación de la forma  $C \equiv AP \pmod{27}$  con  $A = \begin{pmatrix} 2 & 1 \\ 6 & 7 \end{pmatrix}$ .

Dividimos el mensaje en bloques de longitud dos, obteniendo

YA EN TE ND IX

donde la X al final se añadió para que todos los bloques tengan el mismo tamaño.

Hallamos los vectores correspondiente a cada bloque, estos son

$$\begin{pmatrix} 25 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 4 \\ 13 \end{pmatrix} \quad \begin{pmatrix} 20 \\ 4 \end{pmatrix} \quad \begin{pmatrix} 13 \\ 3 \end{pmatrix} \quad \begin{pmatrix} 8 \\ 24 \end{pmatrix}.$$

Aplicamos la transformación  $C \equiv AP \pmod{27}$  a estos vectores, obteniendo

$$\begin{pmatrix} 2 & 1 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 25 \\ 0 \end{pmatrix} = \begin{pmatrix} 23 \\ 15 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 2 & 1 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 4 \\ 13 \end{pmatrix} = \begin{pmatrix} 21 \\ 7 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 2 & 1 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 20 \\ 4 \end{pmatrix} = \begin{pmatrix} 17 \\ 13 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 2 & 1 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 18 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 2 & 1 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 8 \\ 24 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \pmod{27}.$$

Escribiendo los dígrafos correspondientes a los vectores encontrados, obtenemos el texto cifrado

WO UH QN CR NA.

Si llamamos  $C = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$  y  $P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$  observamos que la ecuación matricial  $C \equiv AP \pmod{n}$  es equivalente al sistema de congruencias

$$C_1 \equiv aP_1 + bP_2 \pmod{n},$$

$$C_2 \equiv cP_1 + dP_2 \pmod{n}.$$

Para descifrar un mensaje cifrado mediante una transformación de la forma  $C \equiv AP \pmod{n}$ , hallamos la matriz inversa  $A^{-1}$  y multiplicamos la transformación anterior a la izquierda por  $A^{-1}$  obteniendo la transformación de desciframiento  $P \equiv A^{-1}C \pmod{n}$ . La matriz  $A^{-1}$  existe puesto que estamos suponiendo que  $(\det A, n) = 1$ .

**6.12 Ejemplo.** Descifremos el texto **SÑ RT BÑ IS TJ** si sabemos que fue encriptado usando una transformación de la forma  $C \equiv AP \pmod{27}$

con  $A = \begin{pmatrix} 4 & 5 \\ 3 & 2 \end{pmatrix}$ .

Primero encontramos la inversa de  $A$  módulo 27. Sabemos que  $\det A = 4 \times 2 - 3 \times 5 = -7 = 20 \pmod{27}$ ; de la tabla de inversos módulo 27, y de la fórmula para calcular la inversa de una matriz tenemos

$$A^{-1} = 23 \begin{pmatrix} 2 & -5 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} 46 & -115 \\ -69 & 92 \end{pmatrix} = \begin{pmatrix} 19 & 20 \\ 12 & 11 \end{pmatrix} \pmod{27}.$$

Enseguida aplicamos la transformación  $P \equiv A^{-1}C \pmod{n}$  a cada uno de los vectores que representan los dígrafos que forman el texto cifrado, obteniendo:

$$\begin{pmatrix} 19 & 20 \\ 12 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 14 \end{pmatrix} = \begin{pmatrix} 20 \\ 4 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 19 & 20 \\ 12 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 20 \end{pmatrix} = \begin{pmatrix} 13 \\ 4 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 19 & 20 \\ 12 & 11 \end{pmatrix} \begin{pmatrix} 1 \\ 14 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 19 & 20 \\ 12 & 11 \end{pmatrix} \begin{pmatrix} 8 \\ 19 \end{pmatrix} = \begin{pmatrix} 19 \\ 8 \end{pmatrix} \pmod{27}$$

$$\begin{pmatrix} 19 & 20 \\ 12 & 11 \end{pmatrix} \begin{pmatrix} 20 \\ 9 \end{pmatrix} = \begin{pmatrix} 20 \\ 15 \end{pmatrix} \pmod{27}.$$

Finalmente interpretando los vectores encontrados como dígrafos, vemos que el texto cifrado corresponde al texto plano: TE NECESITO.

Los cifrados por bloques de tamaño dos de la forma  $C \equiv AP \pmod{n}$  son vulnerables al criptoanálisis basado en la frecuencia con que se presentan los dígrafos en un alfabeto, como veremos en el siguiente ejemplo.

**6.13 Ejemplo.** Descifremos el siguiente mensaje si sabemos que los dígrafos que se presentan con mayor frecuencia en Español son ES y LA.

MN RX MN XV OU PN BL EH VJ EH DE QF AM EH ND BC KÑ FF RG.

Los dígrafos que se presentan en el texto cifrado con mayor frecuencia son EH, que aparece tres veces y MN que aparece dos veces. Por lo tanto EH corresponde a ES y MN corresponde a LA.

Si suponemos que  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , dado que los vectores asociados a EH, ES, MN y LA son respectivamente  $\begin{pmatrix} 4 \\ 7 \end{pmatrix}$ ,  $\begin{pmatrix} 4 \\ 19 \end{pmatrix}$ ,  $\begin{pmatrix} 12 \\ 13 \end{pmatrix}$  y  $\begin{pmatrix} 11 \\ 0 \end{pmatrix}$ , tenemos

$$\begin{pmatrix} 4 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix} \pmod{27} \quad \text{y} \quad \begin{pmatrix} 12 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 11 \\ 0 \end{pmatrix} \pmod{27}.$$

Desarrollando, obtenemos las cuatro congruencias

$$4 \equiv 4a + 19b \pmod{27}$$

$$7 \equiv 4c + 19d \pmod{27}$$

$$12 \equiv 11a \pmod{27}$$

$$13 \equiv 11c \pmod{27}.$$

Resolviendo la tercera congruencia tenemos  $a = 6$  y reemplazando este valor en la primera encontramos que  $b = 16$ . Similarmente de la cuarta y la segunda congruencias encontramos que  $c = 11$  y  $d = 8$ .

Por lo tanto  $A = \begin{pmatrix} 6 & 16 \\ 11 & 8 \end{pmatrix}$ , y procediendo como en el ejemplo anterior, vemos que el mensaje original es

LA MALA IMAGEN DE ESTE ESCRITOR ES INMEREIDA.

Como en el caso de cifrado de caracteres, una forma más general de cifrar por bloques, es aplicando a los vectores una *transformación afín* de la forma

$$C \equiv AP + B \pmod{n},$$

donde  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  es una matriz de tamaño  $2 \times 2$  tal que  $(\det A, n) = 1$  y  $B = \begin{pmatrix} e \\ f \end{pmatrix}$  es un vector fijo, ambos con componentes en  $\mathbb{Z}_n$ . Puesto que  $A$  resulta inversible, podemos descifrar los mensajes cifrados mediante una transformación afín, aplicando la transformación inversa

$$P \equiv A^{-1}C - A^{-1}B \pmod{n}.$$

**6.14 Ejemplo.** Cifremos el texto,

LA DESCONFIANZA ES LA MADRE DE LA SEGURIDAD,

usando la transformación afín  $C \equiv \begin{pmatrix} 8 & 9 \\ 5 & 14 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 21 \\ 12 \end{pmatrix} \pmod{27}$ .

Dividimos el texto en unidades de tamaño dos, encontramos los vectores correspondientes a cada dígrafo, les aplicamos la transformación afín y con los vectores obtenidos construimos el texto cifrado. Los resultados son los siguientes:

Los vectores originales son

$$\begin{pmatrix} 11 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 2 \end{pmatrix}, \begin{pmatrix} 15 \\ 13 \end{pmatrix}, \begin{pmatrix} 5 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 13 \end{pmatrix}, \begin{pmatrix} 26 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 19 \end{pmatrix}, \begin{pmatrix} 11 \\ 0 \end{pmatrix}, \begin{pmatrix} 12 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 18 \end{pmatrix}, \\ \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 11 \end{pmatrix}, \begin{pmatrix} 0 \\ 19 \end{pmatrix}, \begin{pmatrix} 4 \\ 6 \end{pmatrix}, \begin{pmatrix} 21 \\ 18 \end{pmatrix}, \begin{pmatrix} 8 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix}.$$

Aplicando la transformación afín a estos vectores obtenemos:

$$\begin{pmatrix} 1 \\ 13 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 15 \\ 26 \end{pmatrix}, \begin{pmatrix} 25 \\ 14 \end{pmatrix}, \begin{pmatrix} 3 \\ 5 \end{pmatrix}, \begin{pmatrix} 13 \\ 7 \end{pmatrix}, \begin{pmatrix} 8 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 13 \end{pmatrix}, \begin{pmatrix} 9 \\ 18 \end{pmatrix}, \begin{pmatrix} 18 \\ 9 \end{pmatrix}, \\ \begin{pmatrix} 26 \\ 20 \end{pmatrix}, \begin{pmatrix} 17 \\ 24 \end{pmatrix}, \begin{pmatrix} 3 \\ 8 \end{pmatrix}, \begin{pmatrix} 26 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 18 \end{pmatrix}, \begin{pmatrix} 4 \\ 13 \end{pmatrix}, \begin{pmatrix} 21 \\ 0 \end{pmatrix}.$$

Luego el texto cifrado es

BN AC CA OZ YÑ DF NH IB BN JR RJ ZT QX DI ZI AR EN UA

Ilustremos como se encontraron los dos primeros vectores del último grupo.

Aplicando la transformación afín al vector  $\begin{pmatrix} 11 \\ 0 \end{pmatrix}$  obtenemos

$$\begin{pmatrix} 8 & 9 \\ 5 & 14 \end{pmatrix} \begin{pmatrix} 11 \\ 0 \end{pmatrix} + \begin{pmatrix} 21 \\ 12 \end{pmatrix} \pmod{27} = \begin{pmatrix} 88 \\ 55 \end{pmatrix} + \begin{pmatrix} 21 \\ 12 \end{pmatrix} = \begin{pmatrix} 1 \\ 13 \end{pmatrix} \pmod{27}.$$

Aplicando la transformación afín al vector  $\begin{pmatrix} 3 \\ 4 \end{pmatrix}$  obtenemos

$$\begin{pmatrix} 8 & 9 \\ 5 & 14 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 21 \\ 12 \end{pmatrix} \pmod{27} = \begin{pmatrix} 60 \\ 71 \end{pmatrix} + \begin{pmatrix} 21 \\ 12 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix} \pmod{27}.$$

Continuando de esta forma se obtuvieron los demás vectores.

Para dar más seguridad a los cifrados en bloques, podemos aumentar el tamaño de éstos. La teoría desarrollada para dígrafos y vectores de dos componentes, puede extenderse de manera natural para el caso de unidades de mensaje de tamaño mayor de dos, trabajando con vectores de  $n$  componentes y matrices de tamaño  $n \times n$  que tengan un determinante primo relativo con el módulo  $n$ .

## Ejercicios 6.2

1. Usando el cifrado  $C \equiv \begin{pmatrix} 9 & 13 \\ 8 & 20 \end{pmatrix} P \pmod{27}$  encriptar el mensaje MIENTRAS VAMOS EN POS DE LO INCIERTO PERDEMOS LO SEGURO.
2. Hallar la inversa módulo 30 de la matriz  $\begin{pmatrix} 8 & 9 \\ 5 & 14 \end{pmatrix}$ .
3. Descifrar el texto ÑR EN AM JM BO JH AE ÑK XB DP ES EN JG VL AW ÑA si se sabe que fue cifrado usando el cifrado de Hill,

$$C_1 \equiv 7P_1 + 3P_2 \pmod{27}$$

$$C_2 \equiv 6P_1 + 4P_2 \pmod{27}.$$

4. Mediante un cifrado de la forma  $C \equiv AP \pmod{27}$ , los dígrafos en español EN y LO se transformaron en NR y KH respectivamente. Encontrar la transformación de cifrado.
5. Mediante un análisis de frecuencia, descifrar el siguiente texto que fue encriptado usando un cifrado digráfico de Hill usando el alfabeto español, QP QF QP IW ZW AN ZT DR QP YQ UD MU SE RR IW JI TY KG LL ES.
6. Cifrar el texto LA FRASE ES NUEVA PERO LA IDEA NO, usando una transformación afín de la forma  $C \equiv AP + B \pmod{27}$  con  $A = \begin{pmatrix} 2 & 3 \\ 7 & 5 \end{pmatrix}$  y  $B = \begin{pmatrix} 6 \\ 11 \end{pmatrix}$ .

7. Descifrar el mensaje GE QY HJ OE EI GE SN AM FQ GH ÑÑ GV ZÑ NN UH GH IV XA NF GE CQ ÑF XJ KV, si se sabe que fue encriptado usando una transformación afín donde los dígrafos EL, OD y TI se transformaron en GE, EI y XJ respectivamente.
8. Hallar las transformaciones de cifrado y de desciframiento que se utilizan en un sistema donde los textos se cifran aplicando primero la transformación  $C \equiv \begin{pmatrix} 4 & 1 \\ 3 & 7 \end{pmatrix} P \pmod{27}$  y luego la transformación  $C \equiv \begin{pmatrix} 2 & 11 \\ 10 & 9 \end{pmatrix} P \pmod{27}$ .
9. Cifrar el mensaje RETIRATE PRONTO usando una transformación de la forma  $C \equiv AP \pmod{27}$  donde  $A = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 4 & 10 \\ 8 & 4 & 0 \end{pmatrix}$ .

## 6.4 Cifrados Exponenciales

Los cifrados exponenciales, que son relativamente resistentes al criptoanálisis, fueron desarrollados en 1978 por Martin Hellman. Expliquemos como funcionan estos sistemas. Primero hallamos el equivalente numérico de las letras que forman el mensaje de acuerdo con la siguiente tabla para el idioma Español.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
O	P	Q	R	S	T	U	V	W	X	Y	Z			
15	16	17	18	19	20	21	22	23	24	25	26			

TABLA 6.9. Equivalente numérico para el idioma Español.

Luego agrupamos los números resultantes en bloques de tamaño  $2n$  y escogemos un número primo  $p$  de tal forma que el mayor entero que se obtiene escribiendo los equivalentes numéricos correspondientes a una palabra de  $n$  letras sea menor que el primo  $p$ . Por ejemplo, en el caso más frecuente, que es el que vamos a considerar, usamos  $n = 2$ , obtenemos bloques de tamaño 4 y escogemos el número primo  $p$  tal que  $2626 < p < 262626$ .

Enseguida escogemos un entero positivo  $e$ , llamado la *clave de ciframiento*, tal que  $(e, p-1) = 1$ , y a cada bloque  $P$  de texto plano le aplicamos la transformación

$$C \equiv P^e \pmod{p}, \quad 0 \leq C < p$$

para obtener los correspondientes bloques cifrados, que son enteros menores que  $p$  y constituyen el texto cifrado que enviamos.

Antes de dar un ejemplo, presentamos un algoritmo para calcular potencias de la forma  $P^e$  módulo  $p$ .

#### 6.4.1 Algoritmo para calcular $P^e$ módulo $p$ .

1. Encontramos la representación de  $e$  en base 2, supongamos que esta representación es  $e = (r_k r_{k-1} \cdots r_0)_2$ .
2. Calculamos los menores residuos positivos de  $P, P^2, P^4, P^8, \dots, P^{2^k}$  módulo  $p$ . Esto lo hacemos elevando al cuadrado y reduciendo módulo  $p$  en forma sucesiva.
3. Por último multiplicamos los menores residuos positivos de  $P^{2^i}$  módulo  $p$  para aquellos  $i$  tales que  $r_i \neq 0$ , reduciendo cada vez el resultado módulo  $p$ , para obtener el valor de  $P^e$  módulo  $p$ .

**6.15 Ejemplo.** Calculemos  $2743^{21} \pmod{2897}$ .

La representación de 21 en base 2 es  $21 = (1, 0, 1, 0, 1)_2$ . Luego tenemos

$$2743 \equiv 2743 \pmod{2897}$$

$$2743^2 \equiv 540 \pmod{2897}$$

$$2743^4 \equiv 1900 \pmod{2897}$$

$$2743^8 \equiv 338 \pmod{2897}$$

$$2743^{16} \equiv 1261 \pmod{2897}.$$

Por último tenemos

$$2743^{21} \equiv 2743^{2^4+2^2+2^0} \equiv 2743^{16} \cdot 2743^4 \cdot 2743 \equiv 1261 \cdot 1900 \cdot 2743 \equiv 81 \cdot 2743 \equiv 2011 \pmod{2897}.$$

**6.16 Ejemplo.** Cifremos exponencialmente el texto

GENERALIZAR ES SIEMPRE EQUIVOCARSE

usando como número primo  $p = 2707$  y como clave de enciframiento  $e = 17$ .

Convertimos las letras del texto en su equivalente numérico y formamos bloques de longitud cuatro obteniendo

0604	1304	1800	1108	2600	1804	1919	0804
1216	1804	0417	2108	2215	0200	1819	0424

donde adicionamos al final los dos dígitos 24, correspondientes a la letra X, para que todos los bloques tengan cuatro dígitos.

Enseguida aplicamos a cada bloque P la transformación

$$C \equiv P^{17} \pmod{2707}.$$

Después de algún trabajo obtenemos, usando el algoritmo anterior, el texto cifrado que es

0185	2343	1853	0912	1316	2524	2645	1781
2653	2524	1325	2111	1615	0084	1543	0504

Para descifrar un mensaje cifrado exponencialmente, observamos que, como  $(e, p - 1) = 1$ , existe un entero  $d$  talque  $ed \equiv 1 \pmod{p - 1}$ ; por lo tanto para algún entero  $k$  tenemos que  $ed = k(p - 1) + 1$  y aplicando el Teorema de Fermat 4.39, tenemos

$$C^d \equiv (P^e)^d = P^{ed} = P^{k(p-1)+1} = P(P^{p-1})^k \equiv P \pmod{p}.$$

En consecuencia, la función de desciframiento para este cifrado exponencial esta dada por

$$P \equiv C^d \pmod{p},$$

donde  $d$  es el inverso de  $e$  módulo  $p - 1$ .

En general el proceso de cifrar y descifrar mensajes usando exponenciación modular puede efectuarse rápidamente utilizando el algoritmo mencionado. Sin embargo para que un criptoanalista descifre un mensaje necesita una gran cantidad de tiempo de computación para determinar el número primo y la clave utilizados. Aún conociendo el primo  $p$ , se pueden necesitar muchos años para determinar la clave de enciframiento, cuando  $p$  tiene más de 100 dígitos y  $p$  es de la forma  $p = 2q + 1$  con  $q$  primo.

Diffie y Hellman desarrollaron un mecanismo para que dos individuos que utilizan cifrados exponenciales puedan compartir la misma clave. Supongamos que para realizar el cifrado se está utilizando el primo  $p$ . Se elige un entero  $a$  menor que  $p$  tal que  $(a, p - 1) = 1$ , y cada individuo elige su clave  $k_i$  donde  $k_i$  es un número primo relativo con  $p - 1$ . Luego, el primer individuo comunica al segundo individuo el entero

$$y_1 \equiv a^{k_1} \pmod{p},$$

y el segundo individuo comunica al primer individuo el número

$$y_2 \equiv a^{k_2} \pmod{p},$$

Para encontrar la clave común el primer individuo calcula

$$K \equiv y_2^{k_1} \equiv a^{k_1 k_2} \pmod{p},$$

y el segundo individuo calcula

$$K \equiv y_1^{k_2} \equiv a^{k_1 k_2} \pmod{p}.$$

Aunque una tercera persona conozca  $a^{k_1}$  y  $a^{k_2}$  no puede conocer  $a^{k_1 k_2}$  sin tener que utilizar un tiempo de computador muy considerable.

En forma similar, con un poco de trabajo se puede probar que un grupo de  $n$  individuos pueden utilizar como clave común el número

$$K \equiv a^{k_1 k_2 \cdots k_n} \pmod{p}.$$

---

## Ejercicios 6.3

---

1. Usando un cifrado exponencial con  $p = 3253$ ,  $e = 35$  y  $n = 2$ , cifrar el mensaje NECESITO AYUDA.
2. Usando un cifrado exponencial con  $p = 5209$ ,  $e = 5$  y  $n = 2$ , cifrar el mensaje ES MEJOR VOLVER ATRAS QUE PERDERSE EN EL CAMINO.
3. Descifrar el mensaje 1359 2666 1617 2169 1212 2303 2846 2137 2336 2183 2164 1391 0791, si sabemos que fue encriptado usando un cifrado exponencial con  $p = 2897$ ,  $e = 21$  y  $n = 2$ .
4. Descifrar el texto cifrado 2147 4620 3987 0775 4346 3888 1538 4620, que fue encriptado digráficamente usando un cifrado exponencial con  $p = 7321$  y  $e = 19$ .
5. ¿Cuál es la clave común que deben usar dos individuos que han escogido como claves los números  $k_1 = 21$  y  $k_2 = 38$ , si el módulo es  $p = 719$  y  $a = 5$ ?
6. Si  $p = 6833$ ,  $a = 15$  y tres individuos escogen como claves  $k_1 = 3$ ,  $k_2 = 25$  y  $k_3 = 45$ , ¿qué número pueden usar como clave común?

## 6.5 Sistemas de Clave Pública

Supongamos que un grupo de personas tienen que comunicarse entre sí en forma secreta y que para hacerlo todos utilizan un mismo tipo de funciones de cifrado. Cada par de personas que desean comunicarse deben utilizar claves de enciframiento que se mantienen secretas para el resto de los individuos del grupo. Desafortunadamente en la mayoría de los sistemas criptográficos conocidos, con poco trabajo de computador, se pueden encontrar las claves de enciframiento, lo que hace imperativo cambiarlas frecuentemente. Estos

cifrados donde la seguridad depende de claves secretas compartidas exclusivamente por el emisor y el receptor, se llaman *cifrados de clave secreta*.

Para evitar los problemas de seguridad que se presentan con los cifrados de clave secreta, se han desarrollado los llamados *cifrados de clave pública*. En estos cifrados es prácticamente imposible calcular las claves de desciframiento a partir de las claves de ciframiento. Estos sistemas han adquirido una gran importancia ante las necesidades modernas de transmisión de datos confidenciales, transacciones electrónicas y otras aplicaciones.

En un sistema de clave pública, las funciones de cifrado deben ser fáciles de calcular, pero sus inversas deben ser computacionalmente imposibles de calcular sin la información adicional proporcionada por las claves de desciframiento, que se mantienen secretas. En estos sistemas las claves de ciframiento se publican en un libro de claves, lo que permite que cualquier usuario pueda cifrar mensajes usando las claves públicas, pero solo aquellos que conozcan las claves secretas puedan descifrarlos.

Supongamos que un grupo de individuos se comunican entre sí usando un sistema de cifrado de clave pública. Cada persona tiene una clave de ciframiento  $E$  que es pública y una clave de desciframiento  $D$  que es secreta. Sean  $A$  y  $B$  dos individuos del grupo que se quieren comunicar. Puesto que las claves  $E_A$  y  $E_B$  son conocidas por todos los usuarios, si  $A$  quiere enviarle un mensaje  $M$  a  $B$ , le envía  $E_B(M)$ . El individuo  $B$ , que es el único que conoce la clave de desciframiento  $D_B$ , recupera el mensaje aplicando  $D_B$  a  $E_B(M)$ , ya que

$$D_B(E_B(M)) = M.$$

Los sistemas de clave pública pueden usarse también para enviar *mensajes firmados*. Cuando se usan mensajes firmados, el receptor no solo está seguro de que el mensaje fue enviado por el emisor, sino que además debe ser capaz de demostrar ante un juez que este mensaje procede efectivamente del mencionado emisor. Si el individuo  $A$  desea enviar un mensaje firmado  $M$ , al individuo  $B$ , le envía  $E_B(D_A(M))$ . Para descifrar el mensaje  $B$  calcula primero  $D_B(E_B(D_A(M))) = D_A(M)$  y luego  $E_A(D_A(M)) = M$ . Como  $B$  obtiene un mensaje legible, él sabe que solo puede proceder de una persona que conoce la clave de desciframiento  $D_A$ , es decir el mensaje ha sido enviado por el usuario  $A$ . Este proceso no afecta la seguridad del sistema puesto que solo  $A$  conoce  $D_A$  y solo  $B$  conoce  $D_B$ .

### 6.5.1 Sistema RSA

En 1976 Ronald Rivest, Adi Shamir y Leonard Adleman desarrollaron un sistema de clave pública basado en la exponenciación modular y cuya seguridad depende del hecho de que no existen algoritmos eficientes que permitan factorizar un número que es producto de dos grandes primos. El nombre del sistema RSA proviene de las iniciales de los apellidos de quienes lo desarrollaron. Los autores de este sistema fueron galardonados con el premio A. M. Turing en el año 2002. Este premio que se considera equivalente al premio Nobel en computación, fue creado en honor del matemático Británico Alan. M. Turing, por la Association for Computing Machinery (A. C. M.).

Veamos como trabaja el sistema *RSA*. Cada usuario escoge dos números primos muy grandes  $p$  y  $q$ , de aproximadamente 100 dígitos cada uno y calcula el número  $n = pq$ . Luego escoge un entero  $e$  tal que  $(e, \varphi(n)) = 1$ , y calcula el inverso  $d$  de  $e$  módulo  $\varphi(n)$ . Se publica la clave de ciframiento que esta formada por la pareja de números  $(n, e)$  y se guarda en secreto la clave de desciframiento que es el número  $d$ .

Para cifrar un mensaje, transformamos las letras en su equivalente numérico, formamos bloques  $P$  de longitud par como en el cifrado exponencial y aplicamos la transformación

$$C \equiv P^e \pmod{n}, 0 \leq C < n.$$

Para descifrar un mensaje utilizamos la congruencia  $de \equiv 1 \pmod{\varphi(n)}$  que nos permite escribir  $ed = k\varphi(n) + 1$  para algún entero  $k$  y por lo tanto

$$C^d \equiv (P^e)^d = P^{ed} = P^{k\varphi(n)+1} = P(P^{\varphi(n)})^k \equiv P \pmod{n},$$

ya que según el Teorema de Euler,  $P^{\varphi(n)} \equiv 1 \pmod{\varphi(n)}$ , cuando  $(P, n) = 1$ . ( se puede ver que la probabilidad de que  $(P, n) > 1$  es prácticamente cero.)

En la elección del número  $e$  tal que  $(e, \varphi(n)) = 1$  se acostumbra a escoger  $e$  tal que  $2^e > n = pq$ , para que sea imposible recuperar el texto plano  $P$  calculando la raíz  $e$ -ésima de  $C \equiv P^e \pmod{n}$ . La seguridad del sistema se basa en que el conocimiento de la clave de ciframiento  $(e, n)$  no permite calcular la clave de desciframiento  $d$ , pues para encontrar  $d$  tal que  $de \equiv 1 \pmod{\varphi(n)}$ , hay necesidad de calcular  $\varphi(n) = (p-1)(q-1)$ , para lo cual se

requiere conocer la factorización de  $n$  lo que es virtualmente imposible sin conocer  $p$  y  $q$ . Se sabe que usando el algoritmo de factorización más rápido conocido, cuando  $p$  y  $q$  tienen 100 dígitos, se requieren  $3.8 \times 10^9$  años de computador para factorizar el entero  $n = pq$ .

Sin embargo al escoger  $p$  y  $q$  debe tenerse cierto cuidado para que no se puedan aplicar algunas técnicas rápidas que se conocen para factorizar un entero positivo  $n$ . Las precauciones más importantes son: que los dos números primos no sean muy próximos, uno de ellos debe tener unos cuantos dígitos más que el otro; y que el máximo común divisor  $(p - 1, q - 1)$  sea pequeño.

Observamos que tratar de encontrar  $\varphi(n)$  es tan difícil como factorizar  $n$ , puesto que si conocemos  $\varphi(n)$  entonces las identidades

1.  $p + q = n - \varphi(n) + 1$
2.  $p - q = \sqrt{(p + q)^2 - 4n}$
3.  $p = \frac{(p + q) + (p - q)}{2}$
4.  $q = \frac{(p + q) - (p - q)}{2},$

nos indican que a partir del conocimiento de  $n$  y  $\varphi(n)$  conocemos la factorización de  $n = pq$ .

En cuanto a la seguridad de este sistema es conveniente señalar que esta basado en la suposición que no hay un procedimiento computacionalmente eficiente para factorizar el entero  $n$ , si este se escoge adecuadamente. No obstante, con el desarrollo acelerado de la computación, es posible que algún día existan estos procedimientos y el sistema RSA sea vulnerable al criptoanálisis.

**6.17 Ejemplo.** Usemos el sistema RSA con  $n = 47 \times 61 = 2867$  y  $e = 7$  para cifrar el mensaje

LA SABIDURIA NO LLEGA POR LA EDAD SINO POR LA EXPERIENCIA.

Primero convertimos las letras en sus equivalentes numéricos y formamos grupos de longitud cuatro, obteniendo

1100 1900 0108 0321 1808 0013 1511 1104 0600 1615 1811 0004  
 0300 0319 0813 1516 1518 1100 0424 1604 1808 0413 0208 0024

donde al final como de costumbre añadimos el número 24 correspondiente a la letra X para igualar el tamaño de los bloques. Luego, aplicamos a cada bloque  $P$  la transformación

$$C \equiv P^7 \pmod{2867}$$

para obtener el mensaje cifrado que es

2568 2094 2609 2150 2323 1355 0291 0922 0157 0520 1155 2049  
 0382 1600 0400 2298 2092 2568 2022 2072 2323 1694 0073 2509

### 6.5.2 Sistema de Rabin

En esta sección presentaremos un criptosistema inventado por el matemático Michael Rabin, cuya seguridad también está basada en la dificultad para factorizar grandes números. La función de cifrado es muy sencilla y está dada por la congruencia

$$C \equiv P(P + b) \pmod{n}$$

donde  $n = pq$  es el producto de dos números primos impares  $p$  y  $q$  muy grandes tales que  $p \equiv q \equiv 3 \pmod{4}$ , y  $b$  es un entero positivo menor que  $n$ .

Como tenemos la siguiente cadena de congruencias equivalentes

$$C \equiv P(P + b) \pmod{n}$$

$$C \equiv P^2 + Pb \pmod{n}$$

$$C \equiv P^2 + 22^{-1}Pb \pmod{n}, \text{ donde } 2^{-1} \text{ es el inverso de 2 módulo } n.$$

$$C \equiv (P + 2^{-1}b)^2 - (2^{-1}b)^2 \pmod{n}$$

$$C + (2^{-1}b)^2 \equiv (P + 2^{-1}b)^2 \pmod{n}$$

$$C + a \equiv (P + d)^2 \pmod{n}, \text{ con } a = (2^{-1}b)^2 \text{ y } d = 2^{-1}b$$

$$C_1 \equiv P_1^2 \pmod{n}, \text{ donde } C_1 = C + a \text{ y } P_1 = P + d,$$

nos podemos limitar a estudiar solo el caso donde la transformación de cifrado es de la forma

$$C \equiv P^2 \pmod{n} \tag{6.1}$$

Para descifrar un mensaje encriptado usando la transformación anterior, tenemos que resolver la congruencia, considerando a  $P$  como la incognita. Puesto que  $n = pq$  con  $p$  y  $q$  primos impares, según el Teorema 4.59 resolver la congruencia es equivalente a resolver el sistema

$$C \equiv P^2 \pmod{p}$$

$$C \equiv P^2 \pmod{q}$$

lo que hace necesario conocer la factorización del número  $n$ .

Consideremos la primera de las congruencias del sistema. Supongamos que  $P$  es una solución de ella, como  $p \equiv 3 \pmod{4}$  tenemos

$$\begin{aligned} \left(C^{\frac{p+1}{4}}\right)^2 &\equiv \left((P^2)^{\frac{p+1}{4}}\right)^2 \\ &\equiv P^{p+1} \\ &\equiv P^p P \\ &\equiv P P \\ &\equiv P^2 \\ &\equiv C \pmod{p}, \end{aligned}$$

ya que por el Teorema de Fermat  $P^p \equiv P \pmod{p}$ .

El cálculo anterior nos muestra que una solución de la primera congruencia es precisamente  $C^{\frac{p+1}{4}} \pmod{p}$ . Obviamente otra solución de la primera congruencia es  $-C^{\frac{p+1}{4}} \pmod{p}$ . En virtud del Teorema de Lagrange, la congruencia no tiene más soluciones. Similarmente, las soluciones de la segunda congruencia del sistema son  $C^{\frac{q+1}{4}} \pmod{q}$  y  $-C^{\frac{q+1}{4}} \pmod{q}$ .

Por lo tanto, si suponemos que las soluciones de la primera congruencia son  $a$  y  $b$ , y las de la segunda son  $c$  y  $d$  entonces las soluciones de la congruencia (6.1) son las que resultan de resolver los siguientes cuatro sistemas de congruencias

1.  $x \equiv a \pmod{p}$   
 $x \equiv c \pmod{q}$ ,
2.  $x \equiv a \pmod{p}$   
 $x \equiv d \pmod{q}$ ,
3.  $x \equiv b \pmod{p}$   
 $x \equiv c \pmod{q}$ ,
4.  $x \equiv b \pmod{p}$   
 $x \equiv d \pmod{q}$ ,

La solución de esta clase de sistemas se estudió en la sección 4.8.

Desafortunadamente encontramos cuatro valores posibles de  $P$  para cada texto cifrado usando una transformación de Rabin, esto complica bastante la tarea de desciframiento de un mensaje y se considera una de las debilidades de este sistema.

**6.18 Ejemplo.** Descifremos el mensaje 0553 1178 que nos fue enviado usando una transformación de la forma  $C \equiv P^2 \pmod{n}$  con  $n = 47 \cdot 59 = 2773$ .

Para descifrar el primer bloque 0553, tenemos que resolver el sistema de congruencias

$$\begin{aligned} 553 &\equiv P^2 \pmod{47} \\ 553 &\equiv P^2 \pmod{59} \end{aligned}$$

De acuerdo con la teoría desarrollada, las soluciones de la primera congruencia del sistema son  $553^{12} \pmod{47}$  y  $-553^{12} \pmod{47}$ , y las soluciones de la segunda congruencia son  $553^{15} \pmod{59}$  y  $-553^{15} \pmod{59}$ . Usando el algoritmo estudiado en la sección 6.4 para calcular potencias de un número módulo  $p$ , obtenemos que las soluciones de la primera congruencia son 6  $\pmod{47}$  y 41  $\pmod{47}$ , y las soluciones de la segunda congruencia son 9  $\pmod{59}$  y 50  $\pmod{59}$ .

Enseguida, tenemos que resolver los cuatro sistemas de congruencias

1.  $x \equiv 6 \pmod{47}$   
 $x \equiv 9 \pmod{59}$ ,

2.  $x \equiv 6 \pmod{47}$   
 $x \equiv 50 \pmod{59}$ ,
3.  $x \equiv 41 \pmod{47}$   
 $x \equiv 9 \pmod{59}$ ,
4.  $x \equiv 41 \pmod{47}$   
 $x \equiv 50 \pmod{59}$ .

Utilizando los métodos estudiados en la sección 4.8, las soluciones menores que  $n = 2773$  de estos sistemas son respectivamente 2074, 0758, 2015 y 0699. De acuerdo a la tabla 6.9, la única solución que tiene sentido es 2015 que corresponde al dígrafo TO.

En forma similar para descifrar el bloque 1178, tenemos que resolver el sistema de congruencias

$$1178 \equiv P^2 \pmod{47}$$

$$1178 \equiv P^2 \pmod{59}.$$

Las soluciones de la primera congruencia son  $1178^{12} \pmod{47}$  y  $-1178^{12} \pmod{47}$ , y las soluciones de la segunda congruencia son  $1178^{15} \pmod{59}$  y  $-1178^{15} \pmod{59}$ . Usando el algoritmo estudiado en la sección 6.4 para calcular potencias de un número módulo  $p$ , obtenemos que las soluciones de la primera congruencia son  $12 \pmod{47}$  y  $35 \pmod{47}$ , y las soluciones de la segunda congruencia son  $36 \pmod{59}$  y  $23 \pmod{59}$ .

Resolviendo los cuatro sistemas de congruencias

1.  $x \equiv 12 \pmod{47}$   
 $x \equiv 36 \pmod{59}$ ,
2.  $x \equiv 12 \pmod{47}$   
 $x \equiv 23 \pmod{59}$ ,
3.  $x \equiv 35 \pmod{47}$   
 $x \equiv 36 \pmod{59}$ ,
4.  $x \equiv 35 \pmod{47}$   
 $x \equiv 23 \pmod{59}$ ,

obtenemos, las soluciones menores que  $n = 2773$  de estos sistemas, que son respectivamente 2691, 0200, 2573 y 0082. De acuerdo a la tabla 6.9, la única solución que tiene sentido es 0200 que corresponde al dígrafo CA.

Por lo tanto el mensaje que nos enviaron esta formado por la palabra  
TOCA.

### 6.5.3 Sistema de la mochila

Este es un criptosistema de clave pública que esta basado en el llamado “Problema de la mochila”. Se trata de un antiguo problema que consiste en llenar una gran mochila con cierto número de artículos de tal forma que escogiendo en cada caso, uno o ninguno de los artículos, se cubra exactamente el volumen de la mochila. Matemáticamente podemos describir el problema de la siguiente forma: Dado un número positivo  $V$  y un conjunto de enteros positivos  $a_1, a_2, \dots, a_n$  buscamos todos los valores  $x_1, x_2, \dots, x_n$  con  $x_i = 0$  o  $x_i = 1$  que satisfagan la ecuación

$$V = a_1x_1 + a_2x_2 + \dots + a_nx_n.$$

Observamos que el problema puede no tener solución, tener solución única o tener varias soluciones. Como conjunto de números  $a_1, a_2, \dots, a_n$  se acostumbra a escoger una *sucesión supercreciente*, es decir una sucesión que satisface la relación  $a_{k+1} > \sum_{i=1}^k a_i$  para todo  $k = 1, 2, \dots, n-1$ . Por ejemplo, la sucesión 4, 7, 15, 32, 68 es una sucesión supercreciente pues  $7 > 4$ ,  $15 > 4 + 7$ ,  $32 > 4 + 7 + 15$  y  $68 > 4 + 7 + 15 + 32$ .

Si elegimos a  $V$  como la suma de algunos o todos los números de una sucesión supercreciente  $a_1, a_2, \dots, a_n$ , el problema de la mochila tiene solución única que puede encontrarse utilizando el siguiente algoritmo:

Primero elegimos  $x_n$  como

$$x_n = \begin{cases} 1 & \text{si } V \geq a_n \\ 0 & \text{si } V < a_n \end{cases}$$

y luego para  $i = n-1, n-2, \dots, 1$  elegimos

$$x_i = \begin{cases} 1 & \text{si } V - \sum_{k=i+1}^n a_k x_k \geq a_i \\ 0 & \text{si } V - \sum_{k=i+1}^n a_k x_k < a_i \end{cases}$$

**6.19 Ejemplo.** Consideremos la sucesión supercreciente 4, 7, 15, 32, 68 y resolvamos el problema de la mochila con  $V = 90$ , es decir resolvamos la ecuación  $90 = 4x_1 + 7x_2 + 15x_3 + 32x_4 + 68x_5$ , donde los  $x_i$  deben ser 0 o 1.

Siguiendo el algoritmo, como  $90 \geq 68$ , tomamos  $x_5 = 1$ . Como  $90 - 68 \cdot 1 = 22 < 32$ , tomamos  $x_4 = 0$ . Como  $90 - 68 \cdot 1 - 32 \cdot 0 = 22 \geq 15$ , tomamos  $x_3 = 1$ . Como  $90 - 68 \cdot 1 - 32 \cdot 0 - 15 \cdot 1 = 7 \geq 7$ , tomamos  $x_2 = 1$  y finalmente como  $90 - 68 \cdot 1 - 32 \cdot 0 - 15 \cdot 1 - 7 \cdot 1 = 0 < 4$ , tomamos  $x_1 = 0$ . Por lo tanto la solución del problema es  $90 = 7 + 15 + 68$ .

Explicuemos como funciona el sistema de cifrado de la mochila. Primero, cada usuario escoge una sucesión supercreciente de enteros positivos  $(a_1, a_2, \dots, a_n)$  de una longitud previamente acordada, usualmente la longitud es un múltiplo de 5. Luego escoge un entero  $m$  tal que  $m > 2a_n$  y un entero  $w$  tal que  $(w, m) = 1$ , y forma la sucesión  $(w_1, w_2, \dots, w_n)$  de menores residuos positivos módulo  $m$ , donde  $w_1 \equiv wa_1 \pmod{m}$ ,  $w_2 \equiv wa_2 \pmod{m}$ ,  $\dots$ ,  $w_n \equiv wa_n \pmod{m}$ . Esta sucesión, que ya no es una sucesión supercreciente, se comunica como la clave pública, en tanto que se guarda secreta la clave de desciframiento que es la pareja de números  $(m, w^{-1})$  donde  $w^{-1}$  es el inverso de  $w$  módulo  $m$ .

Para cifrar un mensaje agrupamos las letras consecutivas en parejas, ternas etc. de acuerdo con la longitud de las sucesiones supercrecientes y usamos la tabla 6.10 la cual se obtiene al escribir los equivalentes numéricos de las letras en base dos, para así dividir el mensaje en bloques de longitud 5, 10, 15, etc, según el caso.

Luego efectuamos el producto punto de los vectores cuyas componentes son estas sucesiones de ceros y unos, y el vector  $(w_1, w_2, \dots, w_n)$ . El mensaje que enviamos es el conjunto de los productos así definidos. Recordamos que el *producto punto* de dos vectores  $a = (a_1, a_2, \dots, a_n)$  y  $b = (b_1, b_2, \dots, b_n)$ , se define como el número

$$a \cdot b = a_1b_1 + a_2b_2 + \dots + a_nb_n.$$

**6.20 Ejemplo.** Cifremos el mensaje SIEMPRE HAY ESPERANZA, usando la sucesión supercreciente (3, 8, 15, 29, 58, 117, 240, 475, 952, 1901), y escogiendo  $m = 3852 > 2 \cdot 1901$  y  $w = 875$ , donde  $(3852, 875) = 1$ .

A	00000	J	01001	R	10010
B	00001	K	01010	S	10011
C	00010	L	01011	T	10100
D	00011	M	01100	U	10101
E	00100	N	01101	V	10110
F	00101	N	01110	W	10111
G	00110	O	01111	X	11000
H	00111	P	10000	Y	11001
I	01000	Q	10001	Z	11010

TABLA 6.10. Equivalentes numéricos en base 2

Multiplicando cada número de la sucesión supercreciente por  $w$  y tomando el resultado módulo  $m$ , obtenemos la sucesión

$$(2625, 3148, 1569, 2263, 674, 2223, 1992, 3461, 968, 3163).$$

Dividiendo el mensaje en bloques de dos letras y tomando los equivalentes numéricos de acuerdo con la tabla 6.10, tenemos los siguientes bloques de diez dígitos de unos y ceros, cada uno

$$\begin{array}{ccccc} 1001101000 & 0010001100 & 1000010010 & 0010000111 & 0000011001 \\ 0010010011 & 1000000100 & 1001000000 & 0110111010 & 0000011000 \end{array}$$

Efectuando los productos punto de cada uno de los vectores que tienen como componentes los bloques anteriores, con el vector cuyas componentes son la sucesión antes obtenida, encontramos el conjunto de números que enviamos como mensaje cifrado. El resultado es

$$7554, 7022, 5816, 9161, 7378, 7923, 6086, 4888, 9606, 4215.$$

Para ilustrar como se obtuvo el primero de los números anteriores, evaluamos el producto punto

$$\begin{aligned} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \cdot (2625, 3148, 1569, 2263, 674, 2223, 1992, 3461, 968, 1561) &= \\ &= 2625 + 2263 + 674 + 1992 = 7554 \end{aligned}$$

Los demás números se calculan en forma similar.

Para descifrar un mensaje, primero hallamos el inverso de  $w = 875$  módulo 3852, este es  $w^{-1} = 383$ . Luego, multiplicamos cada número del

mensaje recibido por  $w^{-1} = 383$ , tomando el resultado módulo 3852, y resolvemos los problemas de la mochila resultantes con respecto a la sucesión supercreciente original (3, 8, 15, 29, 58, 117, 240, 475, 952, 1901). Por ejemplo para el primer número tenemos  $7554 \cdot 383 \equiv 330 \pmod{3852}$  y resolviendo el problema de la mochila para  $V = 330$ , con respecto a la sucesión original obtenemos  $330 = 3 + 29 + 58 + 240$ . Esto nos indica que el primer número corresponde al bloque 1001101000, que representa el diagrama SI.

Dado que en 1982 Shamir encontró un algoritmo para resolver el problema de la mochila en tiempo relativamente corto, estos sistemas, aunque se han modificado para mejorar su seguridad, no son confiables como sistemas de clave pública.

Para finalizar este capítulo, queremos señalar que el objetivo que nos propusimos fue interesar al estudiante en el conocimiento básico de estos temas, ya que el estudio de la Criptología es hoy en día una de las ramas de mayor desarrollo, con métodos basados en matemáticas avanzadas y en teoría de la computación.

---

## Ejercicios 6.4

---

1. Cifrar el mensaje EL FINAL ESTA PROXIMO usando el sistema RSA con  $n = 37 \cdot 73$  y  $e = 17$ .
2. Un texto cifrado usando el sistema RSA con  $(e, n) = (5, 7663)$  es 5033 6283 5033 1458 5927 2550 6616. Hallar el texto plano correspondiente.
3. Hallar los primos  $p$  y  $q$  utilizados en un cifrado RSA, si se conoce que  $n = 31621$  y  $\phi(n) = 31212$ .
4. En un sistema RSA se sabe que  $n = 153863$ ,  $\phi(n) = 153000$  y que la clave de enciframiento es  $e = 19$ . Hallar la clave de desciframiento.
5. Probar que si un criptoanalista descubre un mensaje  $P$  que no es primo relativo con el módulo  $n = pq$ , usado en un cifrado RSA, entonces puede factorizar  $n$ .

6. Probar que la probabilidad de que un mensaje  $P$  cifrado con un sistema RSA, no sea primo relativo con el módulo  $n$  es  $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$ .
7. Usando un cifrado de Rabin de la forma  $C \equiv P(P + 9) \pmod{9379}$ , cifrar el mensaje TODO SE PAGA MENOS LA SALUD.
8. Descifrar el siguiente mensaje 0009 1460 3224, que fue encriptado usando una transformación de la forma  $C \equiv P^2 \pmod{3233}$ .
9. Determinar cuáles de las siguientes sucesiones son supercrecientes:
  - (a) (2, 7, 20, 35, 62)
  - (b) (5, 12, 25, 43, 90, 178)
  - (c) (4, 9, 16, 32, 61, 160)
10. Usando la sucesión supercreciente (2, 3, 7, 14, 30, 57, 115, 230, 472, 940) con  $m = 2112$  y  $w = 595$  encriptar el mensaje EL PRECIO SE OLVIDA LA CALIDAD PERMANECE.
11. Descifrar el mensaje 561 168 220 613 573 348 168 170 220 052 495 000 393 613, que fue encriptado usando la sucesión supercreciente (12, 20, 36, 74, 163) con  $m = 372$  y  $w = 77$ .

---

## Fracciones continuas

---

En este capítulo vamos a estudiar las *fracciones simples*, sus propiedades más importantes y algunas de sus aplicaciones.

Una *fracción continua* es una expresión de la forma,

$$a_1 + \frac{b_1}{a_2 + \frac{b_2}{a_3 + \frac{b_3}{a_4 + \cdots}}}$$

donde los  $a_i$  y  $b_i$  son números reales o complejos. Si todos los  $b_i$  son 1,  $a_1$  es un entero arbitrario y todos los  $a_i$  con  $i \geq 2$  son enteros positivos, decimos que la fracción es una *fracción continua simple*. Por lo tanto una fracción continua simple tiene la forma,

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \cdots}}}$$

donde los  $a_i$  son enteros y  $a_i > 0$  para  $i \geq 2$ .

Los números  $a_i$  en una fracción simple se llaman los términos de la fracción. Si el número de términos de una fracción continua simple es finito, decimos que la fracción es una *fracción continua simple finita* y claramente representa un número racional.

Si el número de términos es infinito, decimos que la fracción es una *fracción continua simple infinita* y en este caso, hay que precisar su significado matemático.

Únicamente vamos a estudiar fracciones continuas simples, por lo tanto cuando hablemos de fracciones continuas, asumiremos que ellas son simples aunque no lo mencionemos explícitamente.

## 7.1 Fracciones continuas finitas

La fracción continua finita,

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots + \frac{1}{a_n}}}}}$$

se representa por la notación  $[a_1, a_2, \dots, a_n]$  y es simplemente un número racional que se obtiene efectuando las operaciones indicadas. El recíproco de esta afirmación también es cierto es decir tenemos el siguiente resultado.

**7.1 Teorema.** *Todo número racional puede expresarse como una fracción continua simple finita.*

*Demostración.* Sea  $r = \frac{p}{q}$  un número racional con  $q > 0$ . Aplicando repeti-

damente el algoritmo de la división tenemos

$$\begin{array}{ll}
 p = qa_1 + r_1, & 0 < r_1 < q \\
 q = r_1a_2 + r_2, & 0 < r_2 < r_1 \\
 r_1 = r_2a_3 + r_3, & 0 < r_3 < r_2 \\
 \vdots & \vdots \\
 r_{n-3} = r_{n-2}a_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2} \\
 r_{n-2} = r_{n-1}a_n + r_n & \text{con } r_n = 0.
 \end{array}$$

Como los residuos  $r_1, r_2, \dots$  forman una sucesión decreciente de enteros positivos menores que  $q$ , el proceso debe terminarse en un número finito de pasos con un residuo  $r_n = 0$  como se ha indicado.

Las ecuaciones anteriores pueden escribirse en la forma

$$\begin{aligned}
 \frac{p}{q} &= a_1 + \frac{r_1}{q} = a_1 + \frac{1}{\frac{q}{r_1}} \\
 \frac{q}{r_1} &= a_2 + \frac{r_2}{r_1} = a_2 + \frac{1}{\frac{r_1}{r_2}} \\
 \frac{r_1}{r_2} &= a_3 + \frac{r_3}{r_2} = a_3 + \frac{1}{\frac{r_2}{r_3}} \\
 &\vdots \\
 \frac{r_{n-3}}{r_{n-2}} &= a_{n-1} + \frac{r_{n-1}}{r_{n-2}} = a_{n-1} + \frac{1}{\frac{r_{n-2}}{r_{n-1}}} \\
 \frac{r_{n-2}}{r_{n-1}} &= a_n
 \end{aligned}$$

y por sustituciones sucesivas obtenemos

$$\begin{aligned}
 \frac{p}{q} &= a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots + \frac{1}{a_n}}}}} \\
 &= [a_1, a_2, \dots, a_n].
 \end{aligned}$$

□

**7.2 Ejemplo.** Expresemos  $\frac{-63}{11}$  como fracción continua simple.

Tenemos,

$$-63 = 11 \cdot (-6) + 3$$

$$11 = 3 \cdot 3 + 2$$

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

$$2 = 1 \cdot 2 + 0,$$

luego

$$\frac{-63}{11} = -6 + \frac{3}{11} = -6 + \frac{1}{\frac{11}{3}}$$

$$= -6 + \frac{1}{3 + \frac{2}{3}}$$

$$= -6 + \frac{1}{3 + \frac{1}{\frac{3}{2}}}$$

$$= -6 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}$$

$$= [-6, 3, 1, 2].$$

Escribiendo el último término en la forma  $2 = 1 + 1$ , observamos también que,

$$\begin{aligned} \frac{-63}{11} &= -6 + \frac{1}{3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}} \\ &= [-6, 3, 1, 1, 1]. \end{aligned}$$

En general, todo número racional puede expresarse como una fracción continua simple finita de dos formas diferentes. En efecto, si  $\frac{p}{q} = [a_1, a_2, \dots, a_n]$

con  $a_n > 1$ , escribiendo el último término  $a_n$  en la forma  $a_n = (a_n - 1) + 1$  tenemos

$$\frac{p}{q} = [a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_{n-1}, a_n - 1, 1],$$

y si  $a_n = 1$ , podemos escribir

$$a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{1} = a_{n-1} + 1$$

y por lo tanto

$$\frac{p}{q} = [a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_{n-2}, a_{n-1} + 1].$$

El razonamiento anterior también nos muestra que si una representación de un número racional como fracción continua finita tiene un número par de términos, su otra representación tiene un número impar de términos.

---

## Ejercicios 7.1

---

Expresar cada uno de los siguientes números racionales como una fracción continua simple finita.

1.  $128/43$ .
2.  $112/253$ .
3.  $302/53$ .
4.  $-72/23$ .
5.  $-100/37$ .
6.  $-426/107$ .
7. Expresar como fracción continua simple los números racionales  $3,14159$  y  $3.1416$ . ¿Qué se puede conjeturar sobre la representación de  $\pi$  como una fracción continua simple?

En los ejercicios 8 al 11 determinar el número racional representado por cada fracción continua simple.

8.  $[1, 3, 1, 2]$ .
9.  $[-4, 2, 3, 5]$ .
10.  $[0, 3, 2, 1]$ .
11.  $[-1, 2, 1, 2, 1, 2]$ .
12. A partir del Teorema 7.1 deducir un método rápido para expresar un número racional positivo como fracción continua simple.
13. Para  $2 \leq k \leq n$ , probar que  $[a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_{k-1}, x_k]$  donde  $x_k = [a_k, a_{k+1}, \dots, a_n]$ .
14. Si  $p > q > 0$  y  $\frac{p}{q} = [a_1, a_2, \dots, a_n]$ , encontrar una representación de  $\frac{q}{p}$  como fracción continua simple finita.

## 7.2 Convergentes

Dada una fracción continua simple  $[a_1, a_2, \dots]$ , que puede ser finita o infinita, definimos sus *convergentes o reducidas* como los números racionales  $C_i = [a_1, a_2, \dots, a_{i-1}, a_i]$  donde  $i = 1, 2, 3, \dots$

**7.3 Ejemplo.** Consideremos la fracción continua finita  $[2, 4, 1, 6]$ . Sus convergentes son

$$\begin{aligned}
 C_1 &= [2] = 2 \\
 C_2 &= [2, 4] = 2 + \frac{1}{4} = \frac{9}{4} \\
 C_3 &= [2, 4, 1] = 2 + \frac{1}{4 + \frac{1}{1}} = \frac{11}{5} \\
 C_4 &= [2, 4, 1, 6] = 2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{6}}} \\
 &= \frac{75}{34}.
 \end{aligned}$$

Observamos que en el caso de una fracción continua simple finita  $[a_1, a_2, \dots, a_n]$  su última convergente  $C_n$  es simplemente el número racional representado por dicha fracción.

**7.4 Ejemplo.** Consideremos la fracción continua simple infinita  $[3, \overline{2, 6}]$  donde la barra sobre los enteros 2 y 6 indica que ellos se repiten indefinidamente. Una fracción de esta clase se llama *periódica*, los términos 2, 6 forman el periodo. Las convergentes quinta y sexta de esta fracción son

$$C_5 = [3, 2, 6, 2, 6] = 3 + \frac{1}{2 + \frac{1}{6 + \frac{1}{2 + \frac{1}{6}}}} = \frac{627}{181}$$

$$C_6 = [3, 2, 6, 2, 6, 2] = 3 + \frac{1}{2 + \frac{1}{6 + \frac{1}{2 + \frac{1}{6 + \frac{1}{2}}}}} = \frac{1351}{390}.$$

El teorema siguiente nos permite calcular fácilmente el valor de las convergentes de una fracción continua.

**7.5 Teorema.** Sea  $C_n = \frac{p_n}{q_n}$  la convergente  $n$ -ésima de una fracción continua simple  $[a_1, a_2, \dots]$ . Definamos además  $p_0 = 1$ ,  $q_0 = 0$ ,  $p_{-1} = 0$  y  $q_{-1} = 1$ . Entonces se tienen las fórmulas de recurrencia

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}, \end{aligned} \tag{7.1}$$

válidas para todo  $n \geq 1$ .

*Demostración.* La demostración es por inducción sobre  $n$ . Si  $n = 1$  las fórmulas (7.1) se transforman en

$$\begin{aligned} p_1 &= a_1 \cdot 1 + 0 = a_1 \\ q_1 &= a_1 \cdot 0 + 1 = 1, \end{aligned}$$

luego  $C_1 = \frac{p_1}{q_1} = a_1 = [a_1]$  como se requiere.

Supongamos ahora que el resultado es cierto para  $n = k$  y cualquier fracción continua. Tenemos

$$C_{k+1} = [a_1, a_2, \dots, a_k, a_{k+1}] = \left[ a_1, a_2, \dots, a_{k-1}, a_k + \frac{1}{a_{k+1}} \right]$$

y por la hipótesis de inducción

$$\begin{aligned} C_{k+1} &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}}. \end{aligned}$$

En consecuencia

$$p_{k+1} = a_{k+1} p_k + p_{k-1},$$

$$q_{k+1} = a_{k+1} q_k + q_{k-1}.$$

Por lo tanto, las fórmulas (7.1) son válidas para todo entero  $n \geq 1$ .  $\square$

Para calcular las convergentes de una fracción continua usamos las fórmulas de recurrencia, elaborando una tabla como en el ejemplo siguiente.

**7.6 Ejemplo.** Evaluemos las convergentes de la fracción continua  $[3, 4, 1, 2, 2]$ .

Elaboramos la tabla siguiente:

$i$	-1	0	1	2	3	4	5
$a_i$			3	4	1	2	2
$p_i$	0	1	3	13	16	45	106
$q_i$	1	0	1	4	5	14	33
$C_i$			3	13/4	16/5	45/14	106/33

En particular, el valor de la fracción continua es la última convergente  $C_5$ , es decir  $[3, 4, 1, 2, 2] = 106/33$ .

Vamos a deducir algunas propiedades de las convergentes que nos permitan precisar el significado de una fracción continua infinita y nos mostraran como se pueden usar las convergentes de una fracción para encontrar aproximaciones de un número irracional.

**7.7 Teorema.** Sea  $C_n = \frac{p_n}{q_n}$  la convergente  $n$ -ésima de la fracción continua simple  $[a_1, a_2, \dots]$ , entonces

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n \quad (7.2)$$

para todo  $n \geq 1$ .

*Demostración.* La demostración es por inducción sobre  $n$ . Si  $n = 1$  tenemos

$$p_1 q_0 - p_0 q_1 = a_1 \cdot 0 - 1 \cdot 1 = (-1) = (-1)^1$$

puesto que  $p_1 = a_1$  y por definición  $p_0 = 1$  y  $q_0 = 0$ .

Supongamos que el resultado es cierto para  $n = k$ . Por las fórmulas (7.1) tenemos

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= -(p_k q_{k-1} - p_{k-1} q_k) \\ &= -(-1)^k = (-1)^{k+1} \end{aligned}$$

y por el principio de inducción matemática, (7.2) es cierta para todo  $n \geq 1$ .  $\square$

**7.8 Corolario.** Para todo  $n \geq 2$

$$C_n - C_{n-1} = \frac{(-1)^n}{q_n q_{n-1}}. \quad (7.3)$$

*Demostración.* Dividiendo (7.2) por  $q_n q_{n-1}$  tenemos el resultado deseado.  $\square$

**7.9 Corolario.** Para todo  $n \geq 1$ ,  $(p_n, q_n) = 1$ .

*Demostración.* De (7.2) se sigue que

$$p_n \frac{q_{n-1}}{(-1)^n} + q_n \frac{p_{n-1}}{(-1)^{n+1}} = 1$$

y por el Teorema 2.11  $(p_n, q_n) = 1$ .  $\square$

**7.10 Teorema.** Sea  $C_n = \frac{p_n}{q_n}$  la convergente  $n$ -ésima de la fracción continua simple  $[a_1, a_2, \dots]$ , entonces

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^{n-1} a_n$$

para todo  $n \geq 1$ .

*Demostración.* Para  $n \geq 1$ , por las fórmulas de recurrencia y el Teorema 7.7 tenemos

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2} (a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= a_n (-1)^{n-1}. \quad \square \end{aligned}$$

Dividiendo por  $q_n q_{n-2}$  tenemos el siguiente corolario.

**7.11 Corolario.** Para todo  $n \geq 3$ ,

$$C_n - C_{n-2} = \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}. \quad (7.4)$$

**7.12 Teorema.** Si  $C_n = \frac{p_n}{q_n}$  es la convergente  $n$ -ésima de la fracción continua simple  $[a_1, a_2, \dots]$ , entonces para todo  $n \geq 1$

$$q_n \geq q_{n-1}$$

y la desigualdad es estricta para  $n > 1$ .

*Demostración.* La demostración es por inducción sobre  $n$ . Si  $n = 1$  la desigualdad se reduce a  $q_1 \geq q_0 = 1$  que es verdadera puesto que  $q_1$  es un entero positivo. Supongamos que la desigualdad es cierta para  $n = k$ . Usando el Teorema 7.5 y observando que  $a_{k+1} \geq 1$ , tenemos

$$q_{k+1} = a_{k+1} q_k + q_{k-1} \geq q_k + q_{k-1} > q_k.$$

Por lo tanto el resultado es cierto para todo entero positivo  $n \geq 1$ .  $\square$

**7.13 Corolario.** Para todo  $n \geq 1$ ,  $q_n \geq n$ .

*Demostración.* Como  $q_0 = 1$ , el resultado es consecuencia de la desigualdad estricta.  $\square$

**7.14 Teorema.** *Las convergentes  $C_n$  de una fracción continua simple satisfacen las desigualdades*

$$\begin{aligned} C_1 &< C_3 < C_5 < \dots, \\ C_2 &> C_4 > C_6 > \dots. \end{aligned}$$

*Además toda convergente impar es menor que toda convergente par.*

*Demostración.* Si  $n \geq 3$  y  $n$  es un entero impar, el lado derecho de la ecuación (7.4) es positivo y por lo tanto las convergentes impares forman una sucesión creciente. En forma similar se ve que las convergentes pares forman una sucesión decreciente.

Por el Corolario 7.8 tenemos que

$$C_n - C_{n-1} = \frac{(-1)^n}{q_n q_{n-1}}, \text{ para } n \geq 2.$$

Tomando  $n = 2k$  tenemos

$$C_{2k} - C_{2k-1} = \frac{1}{q_{2k} q_{2k-1}} > 0,$$

luego

$$C_{2k} \geq C_{2k-1} \text{ para todo } k \geq 1. \quad (7.5)$$

Sean ahora  $r$  y  $s$  dos enteros positivos arbitrarios. Se pueden presentar 3 casos:  $r > s$ ,  $r = s$  o  $r < s$ .

1. Si  $r > s$  entonces

$$C_{2s-1} < C_{2r-1}$$

pues las convergentes impares forman una sucesión creciente.

Además por (7.5)

$$C_{2r-1} < C_{2r},$$

por lo tanto

$$C_{2s-1} < C_{2r}.$$

2. Si  $r = s$  por (7.5)

$$C_{2s-1} < C_{2r}.$$

3. Si  $r < s$  entonces

$$C_{2s} < C_{2r}$$

pues las convergentes pares forman una sucesión decreciente. Además por (7.5)

$$C_{2s-1} < C_{2s},$$

por lo tanto

$$C_{2s-1} < C_{2r}.$$

De (1), (2) y (3) concluimos que toda convergente impar es menor que toda convergente par.  $\square$

## Ejercicios 7.2

Encontrar las convergentes de cada una de las siguientes fracciones continuas y verificar que satisfacen el Teorema 7.14.

1.  $[1, 3, 2, 1, 2]$
2.  $[3, 1, 4, 5, 6, 2]$
3.  $[-2, 3, 1, 1, 3]$

Elaborando una tabla apropiada encontrar las primera 7 convergentes de cada una de las siguientes fracciones continuas:

4.  $[3, 7, 15, 1, 292, 1, 1]$
5.  $[3, \overline{8}]$
6.  $[4, \overline{1, 1, 1, 6}]$
7. Si  $a_1 > 0$  y  $p_n/q_n = [a_1, \dots, a_n]$  probar que para  $n \geq 1$ ,  $p_n/p_{n-1} = [a_n, \dots, a_1]$
8. Si  $p_n/q_n = [a_1, \dots, a_n]$  probar que para  $n \geq 2$ ,  $q_n/q_{n-1} = [a_n, \dots, a_2]$
9. Probar que las convergentes de la fracción continua periódica  $[1, \overline{1}]$  son  $C_n = F_{n+1}/F_n$  donde las  $F_n$  son los números de Fibonacci.

### 7.3 Fracciones continuas infinitas

El teorema siguiente nos permite darle significado preciso a una fracción continua simple infinita.

**7.15 Teorema.** Si  $[a_1, a_2, a_3, \dots]$  es una fracción continua simple infinita y  $C_n = \frac{p_n}{q_n}$  es su  $n$ -ésima convergente, entonces existe un número real  $x$  tal que

$$x = \lim_{n \rightarrow \infty} C_n.$$

*Demostración.* Por el Teorema 7.14 las convergentes impares forman una sucesión creciente y acotada superiormente de números reales, por lo tanto forman una sucesión convergente. Similarmente las convergentes pares son una sucesión convergente ya que forman una sucesión decreciente y acotada inferiormente. Supongamos que

$$\lim_{n \rightarrow \infty} C_{2n-1} = L$$

y

$$\lim_{n \rightarrow \infty} C_{2n} = M.$$

Veamos que  $L = M$ , lo cual implica que

$$\lim_{n \rightarrow \infty} C_n = L.$$

En efecto, por los Corolarios 7.8 y 7.13 tenemos

$$0 \leq C_{2n} - C_{2n-1} = \frac{(-1)^{2n}}{q_{2n}q_{2n-1}} < \frac{1}{2n(2n-1)},$$

luego

$$\lim_{n \rightarrow \infty} (C_{2n} - C_{2n-1}) = 0,$$

y por lo tanto

$$\lim_{n \rightarrow \infty} C_{2n} - \lim_{n \rightarrow \infty} C_{2n-1} = 0,$$

es decir

$$M = L,$$

como queríamos probar. □

El teorema anterior nos sugiere que definamos la fracción continua simple infinita  $[a_1, a_2, a_3, \dots]$  como el número real  $x$ . Por lo tanto definimos

$$[a_1, a_2, a_3, \dots] = x = \lim_{n \rightarrow \infty} C_n$$

donde  $C_n = q_n/q_n$  es la  $n$ -ésima convergente.

**7.16 Teorema.** *El número real  $x$  del teorema anterior es un número irracional.*

*Demostración.* Por los teoremas anteriores tenemos que

$$C_1 < C_3 < C_5 < \dots < x < \dots < C_6 < C_4 < C_2,$$

luego para cualquier valor de  $n$ ,  $x$  siempre esta entre  $C_n$  y  $C_{n+1}$ , por lo tanto

$$0 < |x - C_n| < |C_{n+1} - C_n| = \frac{1}{q_{n+1}q_n}.$$

Supongamos que  $x$  fuera un número racional  $x = \frac{a}{b}$  con  $b > 0$ . de la desigualdad anterior tenemos,

$$0 < \left| \frac{a}{b} - \frac{p_n}{q_n} \right| < \frac{1}{q_{n+1}q_n},$$

y por lo tanto

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}.$$

Escogiendo  $n$  suficientemente grande para que  $b < q_{n+1}$ , lo cual es posible porque los enteros  $q_n$  crecen con  $n$ , tendríamos que el entero  $|aq_n - bp_n|$  estaría entre 0 y 1 lo cual es imposible. Luego necesariamente  $x$  es un número irracional.

Veamos ahora que todo número irracional se puede expresar como una fracción continua simple infinita.  $\square$

**7.17 Teorema.** *Sea  $x$  un número irracional entonces  $x$  puede expresarse de manera única como una fracción continua simple infinita.*

*Demostración.* Sea  $x$  un número irracional, podemos expresar el número  $x$  en la forma

$$x = a_1 + \frac{1}{x_1},$$

con  $a_1 = [x]$  y  $0 < \frac{1}{x_1} < 1$ .

Como  $x$  es irracional se tiene que  $x_1$  es irracional y como  $0 < \frac{1}{x_1} < 1$  se tiene que  $x_1 > 1$ . Podemos expresar  $x_1$  en la forma

$$x_1 = a_2 + \frac{1}{x_2}$$

donde  $a_2 = [x_1]$  y  $0 < \frac{1}{x_2} < 1$ .

Resulta que  $a_2$  es un entero positivo y  $x_2$  es un número irracional mayor que 1. Procediendo en forma recursiva, podemos expresar el número  $x_i$  en la forma

$$x_i = a_{i+1} + \frac{1}{x_{i+1}}$$

donde  $a_{i+1} = [x_i]$  es un entero positivo y  $x_{i+1}$  es un número irracional mayor que 1. Por lo tanto tenemos la representación

$$\begin{aligned} x &= a_1 + \frac{1}{x_1} \\ &= a_1 + \frac{1}{a_2 + \frac{1}{x_2}} \\ &\vdots \\ &= [a_1, a_2, a_3, \dots]. \end{aligned}$$

Finalmente, como  $a_1 = [x]$  y para cada  $i \geq 1$  tenemos  $a_{i+1} = [x_i]$ , la representación de  $x$  como fracción continua simple infinita es única.  $\square$

**7.18 Ejemplo.** Expresemos  $\sqrt{10}$  como una fracción continua simple infini-

ta. Como  $3 < \sqrt{10} < 4$ , entonces  $[\sqrt{10}] = 3$  y por lo tanto,

$$\begin{aligned}\sqrt{10} &= 3 + (\sqrt{10} - 3) = 3 + \frac{1}{\frac{1}{\sqrt{10} - 3}} \\ &= 3 + \frac{1}{\frac{1}{\sqrt{10} + 3}} \\ &= 3 + \frac{1}{6 + (\sqrt{10} - 3)} \\ &= 3 + \frac{1}{6 + \frac{1}{\frac{1}{\sqrt{10} - 3}}}\end{aligned}$$

Puesto que la expresión  $\frac{1}{\sqrt{10} - 3}$  vuelve a aparecer tenemos,

$$\sqrt{10} = 3 + \frac{1}{6 + \frac{1}{6 + \frac{1}{\frac{1}{\sqrt{10} - 3}}}}$$

y continuando sí, obtenemos

$$\sqrt{10} = [3, 6, 6, 6, 6, \dots] = [3, \overline{6}].$$

Algunas veces se puede utilizar la técnica ilustrada en el siguiente ejemplo:

**7.19 Ejemplo.** Expresemos  $\sqrt{17}$  como una fracción continua simple infinita.

Sea  $x = \sqrt{17}$  entonces  $x^2 = 17$ ,  $x^2 - 16 = 1$  y  $(x - 4)(x + 4) = 1$ .

Por lo tanto,

$$\begin{aligned}
 x - 4 &= \frac{1}{x + 4} \\
 x &= 4 + \frac{1}{4 + x} \\
 x &= 4 + \frac{1}{4 + \left(4 + \frac{1}{4 + x}\right)} \\
 x &= 4 + \frac{1}{8 + \frac{1}{4 + x}} \\
 &= \dots
 \end{aligned}$$

Continuando este proceso obtenemos que

$$x = [4, 8, 8, 8, \dots] = [4, \overline{8}].$$

**7.20 Ejemplo.** Determinemos el número irracional representado por la fracción periódica infinita  $[3, \overline{1, 6}]$ .

Sea  $x = [3, \overline{1, 6}]$ . Entonces

$$x = 3 + \frac{1}{1 + \frac{1}{6 + \frac{1}{1 + \frac{1}{6 + \dots}}}}$$

luego,

$$\begin{aligned}
 x - 3 &= \frac{1}{1 + \frac{1}{6 + (x - 3)}} \\
 &= \frac{1}{1 + \frac{1}{x + 3}} \\
 &= \frac{1}{\frac{x + 4}{x + 3}} \\
 &= \frac{x + 3}{x + 4},
 \end{aligned}$$

de donde,

$$\begin{aligned}
 (x - 3)(x + 4) &= x + 3 \\
 x^2 + x - 12 &= x + 3 \\
 x^2 &= 15.
 \end{aligned}$$

Por lo tanto

$$x = [3, \overline{1, 6}] = \sqrt{15}$$

Observamos que  $x \neq -\sqrt{15}$  porque el primer término de la fracción continua simple es positivo.

---

## Ejercicios 7.3

---

Expresar como fracción continua simple infinita cada uno de los números irracionales siguientes:

1.  $\sqrt{5}$ .
2.  $\sqrt{8}$ .

3.  $\sqrt{14}$ .
4.  $\sqrt{21}$ .
5.  $3 + \sqrt{26}$ .
6.  $\sqrt{37}$ .

En cada uno de los ejercicios del 7 al 10, hallar el número irracional representado por la fracción continua

7.  $[1, \overline{1}]$ .
8.  $[5, \overline{5, 10}]$ .
9.  $[-7, \overline{3, 6}]$ .
10.  $[\overline{1, 2}, \overline{1}]$ .
11. Hallar los cuatro primeros términos de la fracción continua que representa al número  $\pi$ .
12. Para  $x > 1$ , probar que la convergente  $n$ -ésima de la fracción que representa a  $1/x$  es el inverso multiplicativo de la convergente  $(n-1)$ -ésima de la fracción que representa a  $x$ .

## 7.4 Fracciones continuas periódicas

Una *fracción continua periódica* es una fracción continua de la forma

$$[a_1, a_2, \dots, a_n, \overline{b_1, b_2, \dots, b_m}]$$

donde  $n$  es un entero no negativo y  $m$  es un entero positivo. El *periodo de la fracción continua* es la sucesión de términos que se repiten  $b_1, b_2, \dots, b_m$ . Vamos a demostrar que toda fracción continua periódica representa un número *irracional cuadrático*, es decir un número que es raíz de una ecuación de la forma  $ax^2 + bx + c = 0$  con coeficientes enteros  $a, b, c$ . De acuerdo a la fórmula para resolver ecuaciones de segundo grado, los irracionales cuadráticos son números de la forma  $r + s\sqrt{d}$  donde  $r$  y  $s$  son números racionales con  $s \neq 0$  y  $d$  es un número entero positivo que no es un cuadrado perfecto.

**7.21 Teorema.** Si  $x = [a_1, a_2, \dots, a_n, \overline{b_1, b_2, \dots, b_m}]$ , entonces  $x$  es un número irracional cuadrático.

*Demostración.* Sea  $y = \overline{[b_1, b_2, \dots, b_m]}$ . Por el Teorema 7.16  $y$  es un número irracional, y tenemos

$$\begin{aligned} y &= [b_1, b_2, \dots, b_m, y] \\ &= \frac{yp'_m + p'_{m-1}}{yq'_m + q'_{m-1}} \end{aligned}$$

donde  $p'_m/q'_m$  y  $p'_{m-1}/q'_{m-1}$  son las dos últimas convergentes de  $[b_1, b_2, \dots, b_m]$ . De la ecuación anterior tenemos que

$$q'_m y^2 + (q'_{m-1} - p'_m)y - p'_{m-1} = 0,$$

luego  $y$  es un número irracional cuadrático. Supongamos que  $y = r + s\sqrt{d}$  con  $r$  y  $s$  números racionales,  $s \neq 0$  y  $d$  un entero positivo que no es un cuadrado perfecto. Si  $p_n/q_n$  y  $p_{n-1}/q_{n-1}$  son las últimas convergentes de la fracción  $[a_1, a_2, \dots, a_n]$  tenemos

$$\begin{aligned} x &= [a_1, a_2, \dots, a_n, y] \\ &= \frac{yp_n + p_{n-1}}{yq_n + q_{n-1}} \\ &= \frac{(r + s\sqrt{d})p_n + p_{n-1}}{(r + s\sqrt{d})q_n + q_{n-1}} \\ &= \frac{A + B\sqrt{d}}{C + D\sqrt{d}} \end{aligned}$$

donde  $A, B, C$  y  $D$  son números racionales. Por lo tanto

$$\begin{aligned} x &= \frac{(A + B\sqrt{d})(C - D\sqrt{d})}{(C + D\sqrt{d})(C - D\sqrt{d})} \\ &= \frac{AC - dBD}{C^2 - dD^2} + \frac{(BC - AD)\sqrt{d}}{C^2 - dD^2} \\ &= r' + s'\sqrt{d} \end{aligned}$$

donde  $r'$  y  $s'$  son números racionales. De esta forma queda demostrado que  $x$  es un irracional cuadrático, como queríamos probar.  $\square$

El recíproco del teorema anterior es cierto, pero su demostración es muy complicada para presentarla en un primer curso de teoría de números.

**7.22 Ejemplo.** Encontramos el número irracional cuadrático representado por la fracción periódica  $[4, 2, 5, \overline{2, 3}]$ .

Procediendo como en la demostración del teorema tenemos  $x = [4, 2, 5, y]$  donde  $y = [\overline{2, 3}]$ . Entonces  $y = [2, 3, y]$ . Las últimas convergentes de  $[2, 3]$  son  $C_1 = 2$  y  $C_2 = 7/3$ , por lo tanto

$$\begin{aligned} y &= \frac{7y + 2}{3y + 1} \\ 3y^2 - 6y - 2 &= 0 \\ y &= \frac{3 + \sqrt{15}}{3}. \end{aligned}$$

Los últimos convergentes de  $[4, 2, 5]$  son  $C_2 = 9/2$  y  $C_3 = 49/11$ . Por lo tanto

$$\begin{aligned} x &= \frac{\left(\frac{3 + \sqrt{15}}{3}\right) 49 + 9}{\left(\frac{3 + \sqrt{15}}{3}\right) 11 + 2} \\ &= \frac{174 + 49\sqrt{15}}{39 + 11\sqrt{15}} \\ &= \frac{433}{98} + \frac{\sqrt{15}}{98}. \end{aligned}$$

**7.23 Ejemplo.** Encontramos el irracional cuadrático representado por la fracción periódica  $[4, \overline{6}]$ .

Sea  $x = [4, \overline{6}]$ . Tenemos  $x = [4, y]$  con  $y = [\overline{6}]$ . Luego

$$\begin{aligned} y &= [6, y] = 6 + \frac{1}{y} = \frac{6y + 1}{y} \\ y^2 - 6y - 1 &= 0 \\ y &= 3 + \sqrt{10} \end{aligned}$$

por lo tanto

$$\begin{aligned} x = [4, y] &= 4 + \frac{1}{y} = \frac{4y + 1}{y} \\ &= \frac{4(3 + \sqrt{10}) + 1}{3 + \sqrt{10}} \\ &= \frac{13 + 4\sqrt{10}}{3 + \sqrt{10}} \\ &= 1 + \sqrt{10}. \end{aligned}$$

Usando los números  $x_i$  y  $a_i$  definidos en la prueba del Teorema 7.17 se puede demostrar, con cierta dificultad, que: “si  $x = r + s\sqrt{d}$  es un número irracional cuadrático tal que  $x > 1$  y  $-1 < \bar{x} < 0$  donde  $\bar{x} = r - s\sqrt{d}$ , entonces la fracción continua que representa a  $x$  es una *fracción continua periódica pura*, es decir una fracción de la forma  $x = [\overline{a_1, a_2, \dots, a_n}]$ ”.

Como consecuencia directa de este resultado tenemos el teorema siguiente.

**7.24 Teorema.** *Si  $d$  es un entero positivo que no es un cuadrado perfecto, entonces  $\sqrt{d}$  tiene una representación como fracción continua simple de la forma*

$$\sqrt{d} = [a_1, \overline{a_2, a_3, \dots, a_n, 2a_1}].$$

*Demostración.* Supongamos que  $\sqrt{d} = [a_1, a_2, a_3, \dots]$ . Como  $a_1 = [\sqrt{d}]$  tenemos que  $a_1 + \sqrt{d} > 1$  y  $-1 < a_1 - \sqrt{d} < 0$ . Por lo tanto  $a_1 + \sqrt{d}$  es una fracción continua periódica pura. Luego, existe un entero positivo  $n$  tal que

$$a_1 + \sqrt{d} = a_1 + [a_1, a_2, a_3, \dots] = [\overline{2a_1, a_2, a_3, \dots, a_n}],$$

y en consecuencia

$$\begin{aligned} \sqrt{d} &= -a_1 + [\overline{2a_1, a_2, a_3, \dots, a_n}] \\ &= -a_1 + [2a_1, a_2, a_3, \dots, a_n, 2a_1] \\ &= [a_1, \overline{a_2, a_3, \dots, a_n, 2a_1}]. \end{aligned} \quad \square$$

**7.25 Ejemplo.** Veamos que

$$\sqrt{a^2 - 1} = [a - 1, \overline{1, 2(a - 1)}]$$

donde  $a$  es un entero positivo mayor que 1.

En efecto,

$$\begin{aligned}
 \sqrt{a^2 - 1} &= (a - 1) + (\sqrt{a^2 - 1} - (a - 1)) \\
 &= (a - 1) + \frac{1}{\frac{1}{\sqrt{a^2 - 1} - (a - 1)}} \\
 &= (a - 1) + \frac{1}{\frac{\sqrt{a^2 - 1} + (a - 1)}{2(a - 1)}} \\
 &= (a - 1) + \frac{1}{\frac{2(a - 1) + (\sqrt{a^2 - 1} - (a - 1))}{2(a - 1)}} \\
 &= (a - 1) + \frac{1}{1 + \frac{\sqrt{a^2 - 1} - (a - 1)}{2(a - 1)}} \\
 &= (a - 1) + \frac{1}{1 + \frac{1}{\frac{2(a - 1)}{\sqrt{a^2 - 1} - (a - 1)}}} \\
 &= (a - 1) + \frac{1}{1 + \frac{1}{\frac{1}{\sqrt{a^2 - 1} + (a - 1)}}} \\
 &= (a - 1) + \frac{1}{1 + \frac{1}{2(a - 1) + (\sqrt{a^2 - 1} - (a - 1))}}
 \end{aligned}$$

Como la expresión  $\sqrt{a^2 - 1} - (a - 1)$  aparece otra vez, concluimos que

$$\sqrt{a^2 - 1} = [(a - 1), \overline{1, 2(a - 1)}].$$

## Ejercicios 7.4

Cada uno de los ejercicios del 1 al 4, hallar el número irracional cuadrático representado por la fracción continua

1.  $[1, 2, 3, \overline{3, 2, 1}]$
2.  $[5, 3, \overline{2, 1, 4}]$
3.  $[2, \overline{5}]$
4.  $[4, \overline{1, 3, 1, 8}]$
5. Hallar la fracción continua periódica que representa a  $\sqrt{d}$  cuando  $d = 5, 10, 15$  y  $20$ .
6. Si  $a$  es un entero positivo, probar que la fracción continua periódica que representa al número  $\sqrt{a^2 + 1}$  es  $[a, \overline{2a}]$ .
7. Si  $a$  es un entero positivo, probar la fracción continua periódica que representa a  $\sqrt{a^2 + 2a}$  es  $[a, \overline{1, 2a}]$
8. Si  $a$  es un entero mayor que 2, probar que

$$\sqrt{a^2 - 2} = [a - 1, \overline{1, a - 2, 1, 2(a - 1)}].$$

## 7.5 Aproximación de números irracionales

Veamos ahora como utilizar las convergentes de una fracción continua simple para encontrar aproximaciones racionales para un número irracional  $x$ .

Empezaremos probando que las convergentes de la fracción continua simple cuyo valor es  $x$  son sucesivamente más próximas al número  $x$ .

**7.26 Teorema.** Sea  $C_n = \frac{p_n}{q_n}$  la convergente  $n$ -ésima de la fracción continua simple  $[a_1, a_2, \dots]$  que representa al número  $x$ . Entonces

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p_{n-1}}{q_{n-1}} \right|.$$

*Demostración.* Escribamos  $x$  en la forma  $x = [a_1, a_2, \dots, a_n, y]$  donde  $y = [a_{n+1}, a_{n+2}, \dots]$ . Entonces

$$\begin{aligned} x &= \frac{yp_n + p_{n-1}}{yq_n + q_{n-1}} \\ y(xq_n - p_n) &= -xq_{n-1} + p_{n-1} \\ &= -q_{n-1} \left( x - \frac{p_{n-1}}{q_{n-1}} \right), \end{aligned}$$

y dividiendo por  $yq_n$

$$\begin{aligned} x - \frac{p_n}{q_n} &= -\frac{q_{n-1}}{yq_n} \left( x - \frac{p_{n-1}}{q_{n-1}} \right) \\ \left| x - \frac{p_n}{q_n} \right| &= \left| \frac{q_{n-1}}{yq_n} \right| \left| x - \frac{p_{n-1}}{q_{n-1}} \right|. \end{aligned}$$

Como  $y > 1$  y  $q_n > q_{n-1}$  para  $n > 1$ , tenemos que

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p_{n-1}}{q_{n-1}} \right|$$

como queríamos probar.  $\square$

El teorema siguiente nos proporciona una medida de la exactitud obtenida al aproximar  $x$  por su convergente  $n$ -ésima.

**7.27 Teorema.** Sea  $C_n = \frac{p_n}{q_n}$  la convergente  $n$ -ésima de la fracción continua simple que representa al número real  $x$ , entonces

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}.$$

*Demostración.* Como las convergentes de la fracción continua simple que representa al número  $x$  satisfacen las desigualdades

$$C_1 < C_3 < C_5 < \dots < x < \dots < C_6 < C_4 < C_2,$$

entonces para cualquier valor de  $n$ ,  $x$  siempre está entre  $C_n$  y  $C_{n+1}$  y por lo tanto tenemos que

$$|x - C_n| < |C_n - C_{n+1}| = \frac{1}{q_n q_{n+1}}.$$

Por el Teorema 7.12, sabemos que  $q_{n+1} \geq q_n$  para todo  $n \geq 1$ , luego  $q_n q_{n+1} \geq q_n^2$  y por lo tanto concluimos que

$$|x - C_n| < \frac{1}{q_n^2}. \quad \square$$

En el ejemplo que sigue ilustramos como se utiliza este teorema para calcular aproximaciones racionales del número real  $x$ .

**7.28 Ejemplo.** Encontramos una aproximación racional del número  $x = [2, \overline{1, 4, 2, 1}]$  que sea correcta a la milésima.

Para que la aproximación tenga el grado de exactitud requerido, necesitamos que  $1/q_n^2 < 0,0005$ . Por lo tanto  $q_n^2 > 2000$ , o sea  $q_n > 44$ . En consecuencia, toda convergente  $C_n = p_n/q_n$  con  $q_n > 44$  nos proporciona una aproximación racional de  $x$ , correcta a la milésima. Si elaboramos una tabla de convergentes obtenemos

$i$	-1	0	1	2	3	4	5	6	7
$a_i$			2	1	4	2	1	1	4
$p_i$	0	1	2	3	14	31	45	76	349
$q_i$	1	0	1	1	5	11	16	27	124

Como  $q_7 > 44$ , la séptima convergente es una de las aproximaciones buscadas. Por lo tanto

$$x \simeq 349/124 \simeq 2,814$$

Si calculamos el valor exacto de  $x = [2, \overline{1, 4, 2, 1}]$  procediendo como en la demostración del Teorema 7.21, encontramos que  $x = \frac{37 + \sqrt{621}}{22} \simeq 2,8145396$  y observamos que la aproximación encontrada es correcta a la milésima.

Para terminar, queremos mencionar que hay numerosos e importantes resultados para aproximar un número irracional que hacen uso de la teoría de las fracciones continuas, y que se pueden investigar en textos mas avanzados de Teoría de Números.

## Ejercicios 7.5

Encontrar una aproximación correcta a la diezmilésima del número irracional representado por cada una de las fracciones continuas siguientes:

1.  $[2, \overline{1}]$ .
2.  $[4, \overline{1, 3, 1, 5}]$ .
3.  $[-2, \overline{1, 1, 2}]$ .
4.  $[0, \overline{3, 1, 2, 1, 4}]$ .

En los ejercicios 5 al 8 encontrar una aproximación correcta a la milésima de los números dados.

5.  $\sqrt{48}$ .
6.  $\sqrt{15}$ .
7.  $\sqrt{23}$ .
8.  $2 + \sqrt{7}$ .
9. Hallar una aproximación correcta a la cienmilésima del número  $\pi$ , donde

$$\pi = [3, 7, 15, 1, 292, 1, \dots].$$

10. Hallar una aproximación correcta a la diezmilésima del número  $e$ , donde

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots].$$

11. Si  $C_n = p_n/q_n$  es la convergente  $n$ -ésima de la fracción continua simple que representa al número real  $x$ , probar que se tiene alguna de las desigualdades

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2}, \text{ o } \left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_{n+1}^2}.$$

GUSTAVO  
RUBIANO

---

Números primos menores que 10.000

---

2	173	401	647	919	1193	1483	1759	2081
3	179	409	653	929	1201	1487	1777	2083
5	181	419	659	937	1213	1489	1783	2087
7	191	421	661	941	1217	1493	1787	2089
11	193	431	673	947	1223	1499	1789	2099
13	197	433	677	953	1229	1511	1801	2111
17	199	439	683	967	1231	1523	1811	2113
19	211	443	691	971	1237	1531	1823	2129
23	223	449	701	977	1249	1543	1831	2131
29	227	457	709	983	1259	1549	1847	2137
31	229	461	719	991	1277	1553	1861	2141
37	233	463	727	997	1279	1559	1867	2143
41	239	467	733	1009	1283	1567	1871	2153
43	241	479	739	1013	1289	1571	1873	2161
47	251	487	743	1019	1291	1579	1877	2179
53	257	491	751	1021	1297	1583	1879	2203
59	263	499	757	1031	1301	1597	1889	2207
61	269	503	761	1033	1303	1601	1901	2213
67	271	509	769	1039	1307	1607	1907	2221
71	277	521	773	1049	1319	1609	1913	2237
73	281	523	787	1051	1321	1613	1931	2239
79	283	541	797	1061	1327	1619	1933	2243
83	293	547	809	1063	1361	1621	1949	2251
89	307	557	811	1069	1367	1627	1951	2267
97	311	563	821	1087	1373	1637	1973	2269
101	313	569	823	1091	1381	1657	1979	2273
103	317	571	827	1093	1399	1663	1987	2281
107	331	577	829	1097	1409	1667	1993	2287
109	337	587	839	1103	1423	1669	1997	2293
113	347	593	853	1109	1427	1693	1999	2297
127	349	599	857	1117	1429	1697	2003	2309
131	353	601	859	1123	1433	1699	2011	2311
137	359	607	863	1129	1439	1709	2017	2333
139	367	613	877	1151	1447	1721	2027	2339
149	373	617	881	1153	1451	1723	2029	2341
151	379	619	883	1163	1453	1733	2039	2347
157	383	631	887	1171	1459	1741	2053	2351
163	389	641	907	1181	1471	1747	2063	2357
167	397	643	911	1187	1481	1753	2069	2371

---

2377	2689	2999	3329	3631	3943	4271	4637	4967
2381	2693	3001	3331	3637	3947	4273	4639	4969
2383	2699	3011	3343	3643	3967	4283	4643	4973
2389	2707	3019	3347	3659	3989	4289	4649	4987
2393	2711	3023	3359	3671	4001	4297	4651	4993
2399	2713	3037	3361	3673	4003	4327	4657	4999
2411	2719	3041	3371	3677	4007	4337	4663	5003
2417	2729	3049	3373	3691	4013	4339	4673	5009
2423	2731	3061	3389	3697	4019	4349	4679	5011
2437	2741	3067	3391	3701	4021	4357	4691	5021
2441	2749	3079	3407	3709	4027	4363	4703	5023
2447	2753	3083	3413	3719	4049	4373	4721	5039
2459	2767	3089	3433	3727	4051	4391	4723	5051
2467	2777	3109	3449	3733	4057	4397	4729	5059
2473	2789	3119	3457	3739	4073	4409	4733	5077
2477	2791	3121	3461	3761	4079	4421	4751	5081
2503	2797	3137	3463	3767	4091	4423	4759	5087
2521	2801	3163	3467	3769	4093	4441	4783	5099
2531	2803	3167	3469	3779	4099	4447	4787	5101
2539	2819	3169	3491	3793	4111	4451	4789	5107
2543	2833	3181	3499	3797	4127	4457	4793	5113
2549	2837	3187	3511	3803	4129	4463	4799	5119
2551	2843	3191	3517	3821	4133	4481	4801	5147
2557	2851	3203	3527	3823	4139	4483	4813	5153
2579	2857	3209	3529	3833	4153	4493	4817	5167
2591	2861	3217	3533	3847	4157	4507	4831	5171
2593	2879	3221	3539	3851	4159	4513	4861	5179
2609	2887	3229	3541	3853	4177	4517	4871	5189
2617	2897	3251	3547	3863	4201	4519	4877	5197
2621	2903	3253	3557	3877	4211	4523	4889	5209
2633	2909	3257	3559	3881	4217	4547	4903	5227
2647	2917	3259	3571	3889	4219	4549	4909	5231
2657	2927	3271	3581	3907	4229	4561	4919	5233
2659	2939	3299	3583	3911	4231	4567	4931	5237
2663	2953	3301	3593	3917	4241	4583	4933	5261
2671	2957	3307	3607	3919	4243	4591	4937	5273
2677	2963	3313	3613	3923	4253	4597	4943	5279
2683	2969	3319	3617	3929	4259	4603	4951	5281
2687	2971	3323	3623	3931	4261	4621	4957	5297

---

5303	5647	5953	6301	6661	6983	7351	7691	8081
5309	5651	5981	6311	6673	6991	7369	7699	8087
5323	5653	5987	6317	6679	6997	7393	7703	8089
5333	5657	6007	6323	6689	7001	7411	7717	8093
5347	5659	6011	6329	6691	7013	7417	7723	8101
5351	5669	6029	6337	6701	7019	7433	7727	8111
5381	5683	6037	6343	6703	7027	7451	7741	8117
5387	5689	6043	6353	6709	7039	7457	7753	8123
5393	5693	6047	6359	6719	7043	7459	7757	8147
5399	5701	6053	6361	6733	7057	7477	7759	8161
5407	5711	6067	6367	6737	7069	7481	7789	8167
5413	5717	6073	6373	6761	7079	7487	7793	8171
5417	5737	6079	6379	6763	7103	7489	7817	8179
5419	5741	6089	6389	6779	7109	7499	7823	8191
5431	5743	6091	6397	6781	7121	7507	7829	8209
5437	5749	6101	6421	6791	7127	7517	7841	8219
5441	5779	6113	6427	6793	7129	7523	7853	8221
5443	5783	6121	6449	6803	7151	7529	7867	8231
5449	5791	6131	6451	6823	7159	7537	7873	8233
5471	5801	6133	6469	6827	7177	7541	7877	8237
5477	5807	6143	6473	6829	7187	7547	7879	8243
5479	5813	6151	6481	6833	7193	7549	7883	8263
5483	5821	6163	6491	6841	7207	7559	7901	8269
5501	5827	6173	6521	6857	7211	7561	7907	8273
5503	5839	6197	6529	6863	7213	7573	7919	8287
5507	5843	6199	6547	6869	7219	7577	7927	8291
5519	5849	6203	6551	6871	7229	7583	7933	8293
5521	5851	6211	6553	6883	7237	7589	7937	8297
5527	5857	6217	6563	6899	7243	7591	7949	8311
5531	5861	6221	6569	6907	7247	7603	7951	8317
5557	5867	6229	6571	6911	7253	7607	7963	8329
5563	5869	6247	6577	6917	7283	7621	7993	8353
5569	5879	6257	6581	6947	7297	7639	8009	8363
5573	5881	6263	6599	6949	7307	7643	8011	8369
5581	5897	6269	6607	6959	7309	7649	8017	8377
5591	5903	6271	6619	6961	7321	7669	8039	8387
5623	5923	6277	6637	6967	7331	7673	8053	8389
5639	5927	6287	6653	6971	7333	7681	8059	8419
5641	5939	6299	6659	6977	7349	7687	8069	8423

---

8429	8761	9133	9461	9811
8431	8779	9137	9463	9817
8443	8783	9151	9467	9829
8447	8803	9157	9473	9833
8461	8807	9161	9479	9839
8467	8819	9173	9491	9851
8501	8821	9181	9497	9857
8513	8831	9187	9511	9859
8521	8837	9199	9521	9871
8527	8839	9203	9533	9883
8537	8849	9209	9539	9887
8539	8861	9221	9547	9901
8543	8863	9227	9551	9907
8563	8867	9239	9587	9923
8573	8887	9241	9601	9929
8581	8893	9257	9613	9931
8597	8923	9277	9619	9941
8599	8929	9281	9623	9949
8609	8933	9283	9629	9967
8623	8941	9293	9631	9973
8627	8951	9311	9643	
8629	8963	9319	9649	
8641	8969	9323	9661	
8647	8971	9337	9677	
8663	8999	9341	9679	
8669	9001	9343	9689	
8677	9007	9349	9697	
8681	9011	9371	9719	
8689	9013	9377	9721	
8693	9029	9391	9733	
8699	9041	9397	9739	
8707	9043	9403	9743	
8713	9049	9413	9749	
8719	9059	9419	9767	
8731	9067	9421	9769	
8737	9091	9431	9781	
8741	9103	9433	9787	
8747	9109	9437	9791	
8753	9127	9439	9803	

---

EJERCICIOS 1.1

1. Aplique el axioma  $A - 5$  al conjunto

$$S = \{0\} \cup \{n \in \mathbb{N} \mid \text{para algún } m \in \mathbb{N}, n = m^+\}.$$

3. Suponga que  $m \neq 0$  ó  $n \neq 0$  y use el ejercicio 1.
4. Para  $m$  fijo considere los conjuntos  $S = \{n \in \mathbb{N} \mid m + n \in \mathbb{N}\}$  y  $T = \{n \in \mathbb{N} \mid mn \in \mathbb{N}\}$ .
5. Suponga que  $m \neq 0$  y  $n \neq 0$  y luego use el ejercicio 1.

EJERCICIOS 1.2

1. Use los ejercicios 1 y 2 del grupo 1.1.
2. Como  $p \neq 0$  asuma que  $p = t^+$  con  $t \in \mathbb{N}$ .
8. Use el ejercicio 5.
9. Para  $m \in \mathbb{N}$  fijo considere el conjunto

$$S = \{n \in \mathbb{N} \mid n \leq m \text{ o } m \leq n\}.$$

## EJERCICIOS 1.3

6. Expresé  $2^{2(k+1)+1} - 9(k+1)^2 + 3(k+1) - 2$  en la forma  $a(2^{2k+1} - 9k^2 + 3k - 2) + b$  con  $b$  divisible por 54.

11.

$$\begin{aligned} \sum_{j=1}^m \sum_{i=1}^n a_i b_j &= \sum_{j=1}^m \left[ \sum_{i=1}^n a_i b_j \right] \\ &= \sum_{j=1}^m \left[ b_j \sum_{i=1}^n a_i \right] \\ &= \left( \sum_{i=1}^n a_i \right) \left( \sum_{j=1}^m b_j \right). \end{aligned}$$

15. Considere cuatro casos:

- i.  $k = 0$ .
- ii.  $k = n + 1$ .
- iii.  $k < 0$  ó  $k > n + 1$ .
- iv.  $1 \leq k \leq n$ .

16. Use el ejercicio 15.

21. Analice cuidadosamente el paso de  $P_1$  a  $P_2$ .

22. Razone por contradicción.

23. Considere el conjunto  $H = \{n \in \mathbb{N} \mid n + a \in S\}$ .

25. Use PIM2 y para  $m$  fijo escriba  $U_{n+1+m+1} = U_{n+m+1} + U_{n-1+m+1}$ .

26. Para  $n$  fijo, haga inducción sobre  $m$ . Use el ejercicio anterior.

27.  $(4685)_9 (3483)_9 = (17832126)_9$ .

28.  $(400803)_9 = (30034342)_5$ .

29.  $b = 7$ .

30. Base 11.

## EJERCICIOS 2.1

5. Haga inducción sobre  $s$ .
6. Si  $n \mid m$  se ve fácilmente que  $a^n - 1 \mid a^m - 1$ . Suponga que  $a^n - 1 \mid a^m - 1$ , entonces  $n \leq m$  y escribiendo  $m = qn + r$  con  $0 \leq r < n$  y  $q \geq 0$ , si se tuviera  $r > 0$  entonces

$$a^m - 1 = a^{qn+r} - 1 = (a^{qn} - 1)a^r + (a^r - 1),$$

y como  $a^n - 1 \mid a^{qn} - 1$  entonces  $a^n - 1 \mid a^r - 1$ . Como  $0 < r < n$  y  $a > 1$  entonces  $1 < a^r < a^n$ , luego  $a^r - 1 < a^n - 1$  lo cual es una contradicción. Luego  $r = 0$  y  $n \mid m$ .

8. Use el ejercicio 7.
9. Para cada entero  $n > 1$  sea  $T = \{a \mid a > 1 \text{ y } a \mid n\}$
10.  $(382, 26) = 2 = (382)(3) + (26)(-44)$ .  
 $(-275, 726) = 11 = (-275)(29) + (726)(11)$ .  
 $(1137, 419) = 1 = (1137)(206) + (419)(-559)$   
 $(-2947, -3997) = 7 = (-2947)(-118) + (-3997)(87)$ .
11.  $3 = (1426)(324) + (343)(-1347)$   
 $12 = (630)(-18) + (132)(86)$   
 $4 = (4001)(-4468) + (2689)(6648)$ .
12. Considere primero el caso  $c = 1$ .
13. Sea  $d = (a + b, ab)$ . Pruebe que  $d \mid a^2$ ,  $d \mid b^2$  y use el ejercicio 12.
15. Sea  $d = (a, b)$ . Pruebe que  $d \mid 3a$  y  $d \mid 3b$ .
16. Sean  $d_1 = (a, b)$  y  $d_2 = (a, c)$ . Pruebe que  $(d_1, d_2) = 1$ .
18. Tome  $d_1 = (d, m)$ .
20. El máximo común divisor de dos números se puede expresar de infinitas formas como combinación lineal de los dos números.
22.  $(ab, p^4) = p^3$ ,  $(a + b, p^4) = p$ .
24. Use que  $(u_n, u_{n+1}) = 1$  para  $n \geq 1$ . Si  $d = (u_{n+3}, u_n)$  pruebe que  $d \mid 2$ .

25. Sean  $d = (u_m, u_n)$  y  $d' = (u_r, u_n)$ . Use los ejercicios 25 y 26 del grupo 1.3 para probar que  $d \mid u_r u_{qn-1}$  y  $d \mid u_r u_{qn}$ . Luego use que  $(u_{qn-1}, u_q) = 1$ .
26. Use el ejercicio anterior y el algoritmo Euclideo.
27. Razone por contradicción, en algún momento puede que necesite probar que  $(u_n, u_{qn-1}) = 1$ .

## EJERCICIOS 2.2

2. Si  $d = (a, b)$  pruebe que  $a = b = d$ .
3. Escriba  $a = Ad$  y  $b = Bd$  con  $(A, B) = 1$ .
5. Use  $|ab| (k/a, k/b) = (ab.k/a, ab.k/b) = (bk, ak)$ .
7.  $a = d$ ,  $b = g$ .
10. 96 y 120.
11. 24 y 1440, 96 y 360, 72 y 480, 120 y 288.
12. El MCD es 1.
13.  $(4410, 1404, 8712) = 18 = (-7)(4410) + (22)(1404) + (0)(8712)$ .
14.  $(112, 240, 192, 768) = 16 = (1)(112) + (-2)(240) + (2)(192) + (0)(768)$ .
15.  $x = 6$ ,  $y = -4$ ,  $z = 0$ ,  $w = 0$ . Hay otras respuestas.
16.  $(p-1)(q-1)$ .
17. Utilice  $[a, b, c] = [[a, b], c] = \frac{|[a, b]c|}{([a, b], c)}$  y el teorema 2.29 repetidamente.
18. Use el ejercicio anterior.
19.  $a = 2$ ,  $b = 4$ ,  $c = 10$ .

## EJERCICIOS 2.3

4.  $(a^2, b) = p$  o  $p^2$ ,  $(a^2, b^3) = p^2$  o  $p^3$ .
7.  $(1485, 5445, 12375) = 495$ ,  $[1485, 5445, 12375] = 408375$ .
8.  $(392, 1764, 2646, 8820) = 98$ ,  $[392, 1764, 2646, 8820] = 52920$ .
10. Use el teorema 2.43 junto con la relación

$$\min(x + y, x + z, y + z) + \max(x, y, z) = x + y + z.$$

13. *Sugerencia:* Si  $x, y, z$  son números naturales entonces  $\min(x, y, z) + \max(x, y, z) = x + y + z$  si y solo si a lo más uno de los números es diferente de cero.

## EJERCICIOS 2.4

1.  $k$  debe ser par.
2. Use el Teorema 1.16 con  $b = 6$ .
4. Todo primo impar tiene la forma  $4k + 1$  o la forma  $4k + 3$ .
5. Observe primero que todo número de la forma  $4k + 3$  se puede escribir en la forma  $4t - 1$ . Suponga que los únicos primos de esta forma son  $p_1, p_2, \dots, p_k$  y considere  $n = 4p_1p_2 \dots p_k - 1$ .
11.  $21! + 2, 21! + 3, \dots, 21! + 21$ .

## EJERCICIOS 2.5

2. Las ternas primitivas con  $x$  impar y  $1 \leq z \leq 30$  son

$$(3, 4, 5), (5, 12, 13), (15, 8, 17), (7, 24, 25) \text{ y } (21, 20, 29).$$

3. Si  $n$  no es una potencia de dos escriba  $n = kp$  con  $p$  primo impar.
4.  $(3k, 4k, 5k)$  con  $k \geq 1$ .

6. No hay.
7. Escriba la ecuación en la forma  $x^4 = y^4 + z^2$ .

## EJERCICIOS 3.1

2. Si  $n$  es el entero más próximo a  $x$ , entonces  $x = n + \theta$  con  $0 \leq |\theta| < 1/2$  y  $-x + 1/2 = -n - \theta + 1/2$  con  $0 \leq 1/2 - \theta < 1$ .
4. a) Para los números reales  $x$  que cumplen  $x - [x] < 1/2$ .  
b) Para los números reales  $x$  que cumplen  $x - [x] \geq 1/2$ .
8. 207.
9. 28.
10. 48.
12. El exponente con que 2 aparece en la representación canónica de  $(2n)!$  es  $\sum_{k=1}^{\infty} \left[ \frac{2n}{2^k} \right]$  y el exponente con que 2 aparece en la representación de  $(n!)^2$  es  $2 \left( \sum_{k=1}^{\infty} \left[ \frac{n}{2^k} \right] \right)$ . Pruebe que  $\sum_{k=1}^{\infty} \left[ \frac{2n}{2^k} \right] \geq 2 \left( \sum_{k=1}^{\infty} \left[ \frac{n}{2^k} \right] \right)$  usando el teorema 3.2(h).
13. Para cada primo  $p$  comparar el exponente con que  $p$  aparece en la representación canónica de  $(2n-2)!$  con el exponente con que  $p$  aparece en la representación de  $n!(n-1)!$
14. Es similar a los dos ejercicios anteriores.

## EJERCICIOS 3.2

1.  $\tau(4320) = 48$ ,  $\sigma(4320) = 15120$ .
3. 144.
4. 864.
5. Considere  $x = p^{n-1}$  con  $p$  primo.

7. 22.

11. Si  $n = \prod_{i=1}^k p_i^{n_i}$  entonces

$$\sum_{d|n} d^2 = \prod_{i=1}^k \frac{p_i^{2(n_i+1)} - 1}{p_i^2 - 1}.$$

### EJERCICIOS 3.3

1. Use el Teorema 3.14 y considere que  $p$  es de alguna de las formas  $4k+1$  o  $4k+3$ .
3. Use la formula  $1 + 2 + \dots + n = \frac{1}{2}n(n+1)$ .
4. Si  $n$  es un cuadrado perfecto pruebe que  $\sigma(n)$  es impar.
6. Pruebe que  $n$  no tiene factores primos impares.

### EJERCICIOS 3.4

3. Cuando  $n$  es par.
6.  $n = 2^a$  con  $a \geq 1$ .
7. 1920.
8. Si  $n$  es un número perfecto par, entonces

$$\Phi(n) = 2^{p-1}(2^{p-1} - 1).$$

12. Suponga que hay solo un número finito de primos  $p_1, p_2, \dots, p_k$  y considere el número  $N = p_1 p_2 \dots p_k$
14. Si  $\Phi(x) = 18$ ,  $x = 19, 27, 38, 54$ .  
 Si  $\Phi(x) = 24$ ,  $x = 35, 39, 45, 52, 56, 70, 72, 78, 84, 90$   
 Si  $\Phi(x) = 72$ ,  $x = 73, 91, 95, 111, 117, 135, 146, 148, 152, 182, 190, 216, 222, 228, 234, 252, 270$ .  
 Si  $\Phi(x) = 90$ , no hay soluciones.

## EJERCICIOS 3.5

6. Use el ejercicio 4.
7. Use el ejercicio 6.
9. Si  $n = \prod_{i=1}^k p_i^{n_i}$  entonces  $\tau_2(n) = \prod_{i=1}^k \binom{n_i+2}{2}$

## EJERCICIOS 3.6

2. Aplique el Teorema 3.26 a la función multiplicativa

$$f(n) = \sum_{d|n} \mu(d)\tau(d).$$

3.  $(-1)^k \prod_{i=1}^k p_i$ .
4.  $\prod_{i=1}^k (2 - p_i)$ .
6. La función  $g(n) = \sum_{d|n} |\mu(d)|$  es multiplicativa.
8.  $\frac{\Phi(n)}{n}$ .
10. Usando la fórmula de inversión de Möbius y el Teorema 3.35 se obtiene

$$g(n) = \prod_{i=1}^k p_i^{2n_i} \left(1 - \frac{1}{p_i^2}\right).$$

11.  $\frac{1}{n} \prod_{i=1}^k (1 - p_i)$ .

## EJERCICIOS 4.1

3. Use  $3^{2n+1} = 3 \cdot 9^n \equiv 3 \cdot 2^n \pmod{7}$ .
4. Use  $3^3 \equiv 1 \pmod{13}$  y  $4^3 \equiv 12 \equiv -1 \pmod{13}$ .
5. Use el Corolario 4.11.

10. 3 y 3.

11. 6 y 1.

#### EJERCICIOS 4.2

2.  $n = a_0 + a_1 10 + \cdots + a_k 10^k$  es divisible por 7 si y solo si  $(a_0 + 10a_1 + 10^2 a_2) - (a_3 + 10a_4 + 10^2 a_5) + \cdots$  es divisible por 7.

5.  $n = a_0 + a_1 100 + a_2 (100)^2 + \cdots + a_k (100)^k$  es divisible por 101 si y solo si  $a_0 - a_1 + a_2 - \cdots$  es divisible por 101.

#### EJERCICIOS 4.3

2. En  $\mathbb{Z}_7$  la solución de  $3x + 4 = 1$  es 6 y las soluciones de  $x^2 + 2x + 6 = 0$  son 2 y 3.

5.  $\overline{ta} + \overline{sb} = \overline{(t+s)a}$ . Escriba  $t+s$  en la forma  $t+s = qb+r$  con  $0 \leq r < b$ . Luego  $(t+s)a = qba + ra = qn + ra \equiv ra \pmod{n}$ . Similarmente se razona con el producto.

6. Un sistema completo de residuos módulo 8 es:  $\{0, 1, 2, 3, 4, 5, 6, 7\}$ .

7.  $\{7, 11, 13, 17, 19, 23, 29\}$ .

#### EJERCICIOS 4.4

3. Pruebe que  $a^{561} \equiv a \pmod{3}$ ,  $a^{561} \equiv a \pmod{11}$  y  $a^{561} \equiv a \pmod{17}$ .

5. a) 7, b) 01, c) 543.

10. Pruebe que  $a^{4n+1} - a$  es divisible por 2, 3 y 5.

11. Use  $a^{p-1} - b^{p-1} = (a^{p-2} + a^{p-3}b + \cdots + b^{p-2})(a - b)$ .

12. Use  $a^{p-1} = (a^{\frac{p-1}{2}})^2$ .

14. Como  $\mathbb{Z}_n$  es un anillo finito con identidad el resultado se sigue del Teorema 4.32.

## EJERCICIOS 4.5

1. 5, 11, 17.
2. 53, 108.
3. 16.
4. 2, 11, 20, 29.
5. No tiene solución.
6. No tiene solución .
7. 6188.
8. 69.
9. 55, 542, 1029.
10. No tiene solución.
11.  $x = 5 + 7k$ ,  $y = -3 - 5k$ .
12. No tiene solución.
13.  $x = 4k$ ,  $y = 5 + 3k$
14. No tiene solución.
15.  $x = 3 + 13k$ ,  $y = 55 - 64k$ .
16. \$32,65.
17. 94 ciruelas, 1 manzana y 5 pitahayas.
18. 40 adultos y 24 niños, 45 adultos y 12 niños.
19.  $x \equiv 1 \pmod{17}$ ,  $y \equiv 4 \pmod{17}$ ,
20.  $x \equiv 19 \pmod{24}$ ,  $y \equiv 16 \pmod{24}$ ,
21.  $x \equiv 1 \pmod{19}$ ,  $y \equiv 3 \pmod{19}$ ,  $z \equiv 1 \pmod{19}$ .

## EJERCICIOS 4.6

1.  $x \equiv 5 \pmod{168}$ .
2.  $x \equiv 1273 \pmod{3465}$ .
3.  $x \equiv 51 \pmod{126}$ .
4. 257.
5. 11.
6. 299.
7. y 8. Aplique el Teorema Chino del residuo a un sistema conveniente de congruencias lineales.

## EJERCICIOS 4.7

1. 4, 8, 13, 14.
2. 4, 11, 18, 25, 32, 39.
3. 8, 13, 20, 22, 43, 50, 55, 62, 83, 85, 92, 97.
4.  $x \equiv 41 \pmod{55}$ ,  $x \equiv 52 \pmod{55}$ .
5.  $x \equiv 14 \pmod{90}$ ,  $x \equiv 59 \pmod{90}$ .
6.  $x \equiv 15 \pmod{56}$ .

## EJERCICIOS 4.8

1.  $x \equiv 65 \pmod{125}$ .
2.  $x \equiv 1 \pmod{25}$ .
3. 5, 14, 21, 23.
4.  $x \equiv 23 \pmod{343}$ .

5. La congruencia tiene 24 soluciones. Algunas de ellas son 17, 27, 57, 65, 97, 107, 115, 147, 187.

## EJERCICIOS 4.9

1.  $2x^4 + 2x^2 + 4x \equiv 0 \pmod{5}$ .
2.  $4x^6 + 5x^4 + 5x^3 + 5x^2 + 5 \equiv 0 \pmod{7}$ .
3. Multiplique el polinomio por  $a$  donde  $a$  es un entero tal que  $aa_n \equiv 1 \pmod{p}$ .
8.  $x^{p-1} - 1 = (x^d - 1)q(x)$  donde  $q(x)$  es un polinomio de grado  $p - 1 - d$ . Aplique el teorema de Lagrange a  $q(x)$  y el teorema de Fermat para deducir el resultado.

## EJERCICIOS 5.1

1. (a)  $x \equiv 6 \pmod{11}$  y  $x \equiv 7 \pmod{11}$ .  
(b)  $x \equiv 2 \pmod{23}$  y  $x \equiv 16 \pmod{23}$ .  
(c) No tiene solución.  
(d)  $x \equiv 5 \pmod{13}$ .  
(e)  $x \equiv 5, 12, 13, 20 \pmod{28}$ .
2. 1, 4, 3, 9, 10, 12.
3.  $(1|11) = (3|11) = (-2|11) = 1$ .  
 $(2|11) = (-1|11) = (-3|11) = -1$ .
4.  $(a|p) = -1$ ,  $(b|p) = -1$ , luego  $(ab|p) = (a|p)(b|p) = 1$ .
8. Todo primo impar es de la forma  $4m + 1$  o de la forma  $4m - 1$ .

## EJERCICIOS 5.2

1.  $p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$ .
2.  $p \equiv 5, 11, 13, 15, 17, 23 \pmod{28}$ .

3.  $p \equiv 1 \pmod{12}$ ,  $p \equiv -5 \pmod{12}$ .
5. b) y d).
6. 327 y  $-532$  no son residuos cuadráticos módulo 977.
8. No tiene solución.
9.  $(129|283) = 1$ ,  $(640|277) = 1$ .
10.  $(226|563) = -1$ ,  $(-416|997) = -1$ .

## EJERCICIOS 5.3

1. 1, 12, 3, 6, 4, 12, 4, 12.
5. 

$p$	2	3	5	7	11	13	17	19	23	29
raíz	1	2	2	3	2	2	3	2	5	2
6. Módulo 11 son 2, 6, 7 y 8. Módulo 13 son 2, 6, 7 y 11.
10. 1, 3, 4, 5, 9.
11. 1, 22.
12. a) 2. b) No tiene. c) 5. Use propiedades de los índices y el Teorema 4.47.
14. 

$n$	1	2	3	4	5	6	7	8	9	10
ind	10	1	8	2	4	9	7	3	6	5
15. Tomando índice en base 2 con respecto al módulo 11, tenemos  $ind_2 3 + 3 ind_2 x \equiv ind_2 7 \pmod{10}$ , o sea  $3 ind_2 x = 7 - 8 \equiv 9 \pmod{10}$ . Luego  $ind_2 x \equiv 3 \pmod{10}$  y  $x \equiv 8 \pmod{11}$ .

## EJERCICIOS 5.4

1.  $f : U_9 \rightarrow U_{18}$  definida por:
 
$$f(1) = 1, f(2) = 5, f(4) = 7, f(5) = 11, f(7) = 13 \text{ y } f(8) = 17.$$
3. 17, 67, 192.

4. 32.

6. 67, 113.

### EJERCICIOS 6.1

1. (a) PRVY HUHO RVHP UROD.  
(b) GHSR FRVL UYHÑ DFLH PFLD GRPG HIDÑ NDÑD SUXG HPFL D
2. (a) Al que has de castigar con obras no trates mal con palabras.  
(b) Sea moderado tu sueño que el que no madruga con el sol no goza del día.
3. La teoría de números es importante en la criptología.
4. OIWG CGUR TSTF TYTO TVIB ÑGRÑ GWGU JTNG SJIA.
5. Siendo sabio no podrás errar en nada.
6. Más vale encender una vela que maldecir las tinieblas.
7. FWTFMS SOMTUGE FWQXEE
8. El hombre sensato lo hace todo con reflexión.
9. La reunión es en Cartagena.
10. Venda las acciones ya.
11. (a) ETSP IAIN SOMY MOTN ESAA LCCO ESNU IPRA TS.  
(b) EDLIO SLETD MSAID EGNRL EODEE SNIOA FCLEN AA.
12. OEUCAVSN EEAQZEU IRQEMONU MIUSAUB DRLUEÑE.
13. Ahora hay un horizonte nuevo.
14. Creer en los sueños es como estar durmiendo toda la vida.
15.  $C \equiv 13P + 22 \pmod{27}$ .

## EJERCICIOS 6.2

1. WN PV JH EC JÑ GR HP BS EÑ YW XK YA ÑH AÑ XB HS MO DC EÑ XK HP DJ GM.
2.  $\left( \begin{array}{cc} 2 & 3 \\ 25 & 14 \end{array} \right)$ .
3. La verdad no siempre es verosímil.
4.  $C \equiv \left( \begin{array}{cc} 8 & 11 \\ 5 & 4 \end{array} \right) P \pmod{27}$ .
5. Esta es la cantidad estimada para la inversión.
6. BH PB JY ZF CT GP WD WI GW BH EB ÑM WO.
7. El secreto del éxito está en la persistencia del objetivo.
8.  $C \equiv \left( \begin{array}{cc} 14 & 25 \\ 13 & 19 \end{array} \right) P \pmod{27}$ .
9. RAY QOB ATÑ FBO IJE.

## EJERCICIOS 6.3

1. 0694 0720 0262 1710 1016 0447 0802.
2. 4221 2858 0494 1361 2917 2544 1991 1672 1824 0218 3919 0860 3676  
4792 4231 2626 2684 4009 1581 0455.
3. Escucha pero no siempre creas.
4. te espero el martes.
5.  $k = 588$ .
6.  $k = 1765$ .

## EJERCICIOS 6.4

1. Esto es lo mejor.

2.  $p = 103, q = 307$ .
3.  $d = 88579$ .
4. Adios.
5. 6682 4087 4109 8096 5820 11415 6078 2948 4733 1994 5574 2948 3071  
4232 3838 6474 3676.
6. Hemos terminado.

## EJERCICIOS 7.1

1.  $[2, 1, 42]$ .
2.  $[0, 2, 3, 1, 6, 4]$ .
3.  $[8, 1, 1, 1, 2, 4]$ .
4.  $[-4, 1, 6, 1, 2]$ .
5.  $[-3, 3, 2, 1, 3]$ .
6.  $[-4, 53, 2]$ .
7.  $3, 14159 = [3, 7, 15, 1, 25, 1, 7, 4]$ ;  $3, 1416 = [3, 7, 16, 11]$ . Luego  $\pi = [3, 7, 15, 1, \dots]$ .
8.  $14/11$ .
9.  $-132/37$ .
10.  $3/10$ .
11.  $-19/11$ .
14.  $[0, a_1, a_2, a_3, \dots, a_n]$ .

## EJERCICIOS 7.2

1.  $c_1 = 1, c_2 = 4/3, c_3 = 9/7, c_4 = 13/10, c_5 = 35/27$ .
2.  $c_1 = 3, c_2 = 4, c_3 = 19/5, c_4 = 99/26, c_5 = 613/161, c_6 = 1325/348$ .

3.  $c_1 = -2$ ,  $c_2 = -5/3$ ,  $c_3 = -7/4 = -12/7$ ,  $c_5 = -43/25$ .
4.  $c_5 = 103993/33102$ ,  $c_6 = 104348/33215$ ,  $c_7 = 208341/66317$ .
5.  $c_5 = 13395/4289$ ,  $c_6 = 108809/34840$ ,  $c_7 = 883867/283009$ .

## EJERCICIOS 7.3

1.  $\sqrt{5} = [2, \overline{4}]$ .
2.  $\sqrt{8} = [2, \overline{1, 4}]$ .
3.  $\sqrt{14} = [3, \overline{1, 2, 1, 6}]$ .
4.  $\sqrt{21} = [4, \overline{1, 1, 2, 1, 1, 8}]$ .
5.  $3 + \sqrt{26} = [8, \overline{10}]$ .
6.  $\sqrt{37} = [6, \overline{12}]$ .
7.  $[1, \overline{1}] = (1 + \sqrt{5})/2$ .
8.  $[5, \overline{5, 10}] = \sqrt{27}$ .
9.  $[-7, \overline{3, 6}] = -10 + \sqrt{11}$ .
10.  $[\overline{1, 2, 1}] = (1 + \sqrt{10})/3$ .
11. 3, 7, 15, 1.

## EJERCICIOS 7.4

1.  $(308 + \sqrt{37})/219$ .
2.  $(165 + \sqrt{229})/34$ .
3.  $(\sqrt{29} - 1)/2$ .
4.  $\sqrt{23}$
5.  $\sqrt{5} = [2, \overline{4}]$ ,  $\sqrt{10} = [3, \overline{6}]$ ,  $\sqrt{15} = [3, \overline{1, 6}]$ ,  $\sqrt{20} = [4, \overline{2, 8}]$ .

## EJERCICIOS 7.5

1.  $[2, \overline{1}] \simeq 377/144.$
2.  $[4, \overline{1, 3, 1, 5}] \simeq 791/165.$
3.  $[-2, \overline{1, 1, 2}] \simeq -271/191.$
4.  $[0, 3, \overline{1, 2, 1, 4}] \simeq 65/243.$
5.  $\sqrt{48} \simeq 1254/181.$
6.  $\sqrt{15} \simeq 213/55.$
7.  $\sqrt{23} \simeq 235/49.$
8.  $2 + \sqrt{7} \simeq 655/141.$
9.  $\pi \simeq 103993/33102.$
10.  $e \simeq 1264/465.$

---

## Bibliografía

---

- [1] T. M. APOSTOL, *Introduction to analytic Number Theory*, Springer–Verlag, 1976.
- [2] D. M. BURTON, *Elementary Number Theory*, Allyn and Bacon, 1976.
- [3] A. DOXIADIS, *El tío Petros y la conjetura de Goldbach*, Ediciones B. Colección Tiempos Modernos, Barcelona, 2000.
- [4] D. E. KNUTH, *Art of computer programming*, Addison–Wesley, **1**, 1973, **2**, 1981.
- [5] C. T. LONG, *Elementary Introduction to Number Theory*, Heath, Lexington, 1972.
- [6] W. J. LEVEQUE, *Fundamentals of Number Theory*, Addison–Wesley, 1977.
- [7] C. J. MORENO, *Fermat’s Last Theorem: From Fermat to Wiles*, Rev. Col. de Mat. **29** (1995), 49–88
- [8] I. NIVEN AND H. S. ZUCKERMAN, *An introduction to the theory of Numbers*, Wiley, 1980.
- [9] A. J. PETTOFREZZO Y D. R. BYRKIT, *Introducción a la teoría de Números*. Prentice–Hall Internacional, 1972.

- 
- [10] P. RIBENBOIM, *My numbers, my friends: Popular Lectures on Number Theory*, Springer-Verlag, New York, 2000.
- [11] K. H. ROSEN, *Elementary Number Theory and its applications*, 2nd ed. Addison-Wesley, 1988.
- [12] B. M. STEWART, *The Theory of Numbers*, Macmillan, 1964.
- [13] M. R. SCHROEDER, *Number Theory in Science and communication with applications in Cryptography, Physics, Digital Information, Computing and Self-Similarity*, Springer-Verlag, 1986.
- [14] J. J. TATTERSALL, *Elementary Number Theory in Nine Chapters*, Cambridge, University press, 2001.
- [15] D. ZAIGER, *A short proof of the Prime Number Theorem*, Amer. Math. Monthly **104** (1967), 705–708
- [16] <http://primes.utm.edu>

- adición  
  de números enteros, 10  
  de números naturales, 2
- algoritmo  
  de Euclides, 29  
  de la división, 13  
  extendido de Euclides, 31
- anillo, 109  
  con identidad, 110  
  conmutativo, 110
- aritmética módulo  $n$ , 106
- axiomas  
  de Peano, 2
- base del sistema, 17
- Brun Viggo, 54
- cifrado en bloques, 206
- cifrado por transposición, 203
- cifrados  
  exponenciales, 213
- claves, 195
- coeficiente binomial, 22
- congruencia  
  de grado superior, 137  
  de segundo grado con módulo primo, 153  
  lineal, 121
- congruentes módulo  $n$ , 98
- conjetura  
  de Goldbach, 56  
  de Taniyama–Shimura, 58
- convergentes, 235
- criba de Eratóstenes, 51
- criptoanálisis, 194
- criptografía, 194
- criterio de Euler, 158
- criterios de divisibilidad, 104
- cuerpo, 112
- dígitos, 17
- dígrafos, 206
- desencriptación, 195
- divide a, 15
- divisibilidad, 25
- divisores de cero, 110
- dominio de integridad, 112
- ecuación  
  de Fermat, 58  
  diofántica, 58  
  diofántica lineal, 125
- encriptación, 195
- $\mathbb{Z}_n$ , 107
- enteros módulo  $n$ , 107
- equivalente numérico, 195

- Eratóstenes, 51  
Erdős, P., 57  
Euclides, 29  
Euler L., 54
- factorial, 22  
Fibonacci L., 36  
forma canónica, 47  
formula  
  de inversión de Möbius, 90  
fracción  
  continua simple infinita, 242  
  continua, 230  
  continua finita, 231  
  continua periódica, 248  
  continua simple, 230  
  periódica, 236  
función  
   $[x]$ , 64  
   $\Phi$  de Euler, 78  
   $\mu$ , 90  
   $\sigma(n)$ , 70  
   $\tau(n)$ , 70  
  aritmética multiplicativa, 72  
  de Euler, 94  
  multiplicativa, 86  
  número, 70  
  parte entera, 64  
  suma de divisores, 70  
funciones aritméticas, 70
- Gauss F., 57  
grupo, 108  
  abeliano, 108  
  cíclico, 185  
  isomorfismo, 184
- Hadamard, 57  
Hellman M., 213  
hipótesis  
  de inducción, 2
- índice de  $n$ , 180
- Jacobi, 167  
Julio Cesar, 195
- Legendre, 57  
lema de Gauss, 161  
ley de  
  la reciprocidad cuadrática, 160  
  la tricotomía, 8
- Máximo Común Divisor, 27  
método del descenso infinito, 62  
Mínimo Común Múltiplo, 39  
MCD, 27  
MCM, 40  
Mersenne M., 76  
multiplicación  
  de números enteros, 11  
  de números naturales, 5
- número  
  compuesto, 15  
  de Fermat, 21, 77  
  de Fibonacci, 36  
  de Mersenne, 76  
  perfecto, 74  
  primo, 15
- números  
  enteros, 10  
  naturales, 1
- orden  
  de  $a$  módulo  $n$ , 172  
  entre números naturales, 7
- PBO, 13  
Peano, Giuseppe, 1  
 $\pi(x)$ , 56  
PIM, 2  
potencias módulo  $n$ , 172

- primo, 15
  - de Mersenne, 76
- primos gemelos, 54
- primos relativos, 33, 42
- principio
  - de buena ordenación, 13
- producto directo, 186
- proporción áurea, 24
- raíces primitivas, 172
- Rabin M., 221
- relación de equivalencia, 99
- residuos cuadráticos, 153
- símbolo
  - de Jacobi, 167
  - de Legendre, 156, 167
- sistema
  - de clave pública, 217
  - de la mochila, 225
  - de Rabin, 221
  - hexadecimal, 17
  - RSA, 219
- subgrupo, 181
  - generado, 181
- sucesión de Fibonacci, 24
- sustitución polialfabética, 200
- teorema
  - chino del residuo, 131
  - de Euler, 114
  - de Fermat, 114
  - de Lagrange, 147, 148
  - de Wilson, 147, 150
  - del Binomio, 101
  - fundamental de la aritmética,  
46
- teorema de Dirichlet, 53
- Teorema de los números primos,  
56
- ternas Pitagóricas, 60
- TFA, 46
- transformaciones afines, 198
- translaciones, 198
- triángulo de Pascal, 23
- Vallee de la, P. , 57
- Vigenère B., 200
- Zagier D., 57