



# Índice general

<b>Prefacio</b>	<b>III</b>
<b>1. Preliminares</b>	<b>1</b>
1.1. Buen orden . . . . .	1
Tarea . . . . .	2
1.2. Inducción . . . . .	2
Tarea . . . . .	3
1.3. Principio de las pichoneras de Dirichlet . . . . .	3
Tarea . . . . .	3
<b>2. Divisibilidad y primos</b>	<b>4</b>
2.1. Divisibilidad y algoritmo de división . . . . .	4
Tarea . . . . .	8
2.2. Máximo común divisor . . . . .	9
Tarea . . . . .	10
2.3. Primos y factorización única . . . . .	10
Tarea . . . . .	12
2.4. Algoritmo de Euclides y ecuaciones diofánticas lineales . . . . .	13
Tarea . . . . .	15
<b>3. Funciones aritméticas</b>	<b>16</b>
3.1. Funciones multiplicativas . . . . .	16
Tarea . . . . .	21
3.2. La función parte entera . . . . .	23
Tarea . . . . .	29
<b>4. Congruencias</b>	<b>30</b>
4.1. Congruencias . . . . .	30
Tarea . . . . .	32
4.2. Sistemas residuales completos y reducidos . . . . .	33
Tarea . . . . .	35
4.3. Teoremas de Fermat, Wilson y Euler . . . . .	35
Tarea . . . . .	37
4.4. Teorema sónico de los residuos . . . . .	37
4.5. Criterios de divisibilidad . . . . .	38
Tarea . . . . .	39
<b>A. Indicaciones y respuestas</b>	<b>41</b>

# Prefacio

He aquí mi pequeña contribución a la difusión de matemáticas en castellano.

# Notación

$\mathbb{N}$	Los números naturales $\{0, 1, 2, 3, \dots\}$ .
$\mathbb{Z}$	Los enteros $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ .
$\mathbb{Q}$	Los números racionales (fracciones).
$\mathbb{R}$	Los números reales.
$\mathbb{P}$	Los números primos $\{2, 3, 5, 7, 11, \dots\}$ .
$]a; b[$	El intervalo $\{x \in \mathbb{R} : a < x < b\}$ .
$[a; b]$	El intervalo $\{x \in \mathbb{R} : a \leq x \leq b\}$ .
$]a; b]$	El intervalo $\{x \in \mathbb{R} : a < x \leq b\}$ .
$[a; b[$	El intervalo $\{x \in \mathbb{R} : a \leq x < b\}$ .
$]a; +\infty[$	El intervalo $\{x \in \mathbb{R} : x > a\}$ .
$[a; +\infty[$	El intervalo $\{x \in \mathbb{R} : x \geq a\}$ .
$] -\infty; a[$	El intervalo $\{x \in \mathbb{R} : x < a\}$ .
$] -\infty; a]$	El intervalo $\{x \in \mathbb{R} : x \leq a\}$ .
$\llbracket x \rrbracket$	El único entero que satisface $x - 1 < \llbracket x \rrbracket \leq x$
$\lceil x \rceil$	El único entero que satisface $x < \lceil x \rceil \leq x + 1$

# Capítulo 1

## Preliminares

### 1.1. Buen orden

**1 Definición** Se denotará los enteros mediante el símbolo  $\mathbb{Z}$  y los números naturales (enteros positivos, incluyendo al 0) mediante el símbolo  $\mathbb{N}$ . Un entero natural  $p > 1$  es *primo* si sus únicos divisores son  $p$  mismo y la unidad 1. Se denotará el conjunto de los primos mediante el símbolo  $\mathbb{P}$ . Si un entero diferente de 1 no es primo, entonces se dice que es *compuesto*. Obsérvese que 1 ni es primo ni compuesto.

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

**3 Ejemplo** Demuéstrese que  $\sqrt{2}$  es irracional.

**Resolución:** Presúmase al contrario que  $\sqrt{2}$  es racional, esto es, que hay enteros  $a, b$  con  $\sqrt{2} = \frac{a}{b}$ . Esto implica que el conjunto

$$\mathcal{A} = \{n\sqrt{2} : (n, n\sqrt{2}) \in (\mathbb{N} \setminus \{0\})^2\}$$

no es nulo ya que contiene a  $a$ . Por el axioma del buen orden,  $\mathcal{A}$  tiene un elemento mínimo, llámese  $j = k\sqrt{2}$ . Como  $\sqrt{2} - 1 > 0$ , se tiene que

$$j(\sqrt{2} - 1) = j\sqrt{2} - k\sqrt{2} = (j - k)\sqrt{2}$$

es un entero positivo. Como  $2 < 2\sqrt{2}$  implica que  $2 - \sqrt{2} < \sqrt{2}$  y también  $j\sqrt{2} = 2k$ , se ve entonces que

$$(j - k)\sqrt{2} = k(2 - \sqrt{2}) < k(\sqrt{2}) = j.$$

Así pues,  $(j - k)\sqrt{2}$  es un entero positivo de  $\mathcal{A}$  menor que  $j$ . Esto contradice la elección de  $j$  como el menor elemento de  $\mathcal{A}$  y termina la demostración. Contrástese este método con el del ejemplo 61.

**4 Ejemplo** Sean  $a, b, c$  enteros  $a^6 + 2b^6 = 4c^6$ . Demuéstrese que  $a = b = c = 0$ .

**Resolución:** Claramente basta considerar enteros positivos. Escójase un trío  $a, b, c$  que satisface la ecuación y con

$$\max(a, b, c) > 0$$

tan pequeño como fuere posible. Si  $a^6 + 2b^6 = 4c^6$  entonces  $a$  ha de ser par, dígase  $a = 2a_1$ . Esto conlleva a  $32a_1^6 + b^6 = 2c^6$ . Luego  $b$  es par, dígase  $b = 2b_1$  y por tanto  $16a_1^6 + 32b_1^6 = c^6$ . De esto resulta que  $c$  también es par, dígase  $c = 2c_1$ , y así  $a_1^6 + 2b_1^6 = 4c_1^6$ . Pero entonces  $\max(a_1, b_1, c_1) < \max(a, b, c)$ : contradicción. Así todas las variables deben ser cero.

**5 Ejemplo** Demuéstrese que el producto de  $n$  enteros consecutivos es divisible por  $n!$ .

**Resolución:** Obsérvese que el problema se reduce a considerar enteros estrictamente positivos, ya que si fuesen estrictamente negativos, con multiplicar por  $(-1)^n$  no se afecta la divisibilidad, y si incluyesen al 0, el producto sería 0, que es definitivamente divisible por  $n!$ .

Preúmase pues que todos los enteros en consideración son estrictamente positivos. Se utilizará el axioma del buen orden (Axioma 2) y se argüirá por contradicción. Sea  $M$  el menor entero para el cual

$$\frac{(M+1)(M+2)\cdots(M+n)}{n!}$$

no es entero. Obsérvese que  $M > 0$  ya que  $\frac{n!}{n!} = 1$  es entero. Ahora bien,

$$\begin{aligned} (M+1)\cdots(M+n) &= (M+1)\cdots(M+n-1)(M+n) \\ &= M(M+1)(M+2)\cdots(M+n-1) \\ &\quad + (M+2)\cdots(M+n-1)n. \end{aligned}$$

Por definición de  $M$ ,

$$n! \text{ divide a } (M(M+1)(M+2)\cdots(M+n-1))$$

y

$$(n-1)! \text{ divide a } ((M+2)\cdots(M+n-1)).$$

Luego  $n!$  divide a  $((M+2)\cdots(M+n-1)n)$ . Pero entonces

$$n! \text{ divide a } ((M+1)(M+2)\cdots(M+n)),$$

lo cual es una contradicción.

## Tarea

**6 Problema** Demuéstrese que no existe ningún entero en el intervalo  $]0;1[$ .

**7 Problema (IMO, 1988)** Si  $a, b$  son enteros positivos para los cuales la cantidad  $\frac{a^2 + b^2}{1 + ab}$  es entera, demuéstrese entonces  $\frac{a^2 + b^2}{1 + ab}$  es un cuadrado perfecto.

**8 Problema** Demuéstrese que la cantidad  $n^3 - n$  es siempre divisible por 6 y que  $n^5 - 5n^3 + 4n$  es siempre divisible por 120 para todo entero  $n$ .

## 1.2. Inducción

**9 Axioma (Principio (débil) de la inducción matemática)** Si  $\mathcal{S}$  es un conjunto de enteros tal que  $0 \in \mathcal{S}$  y si  $n \in \mathcal{S} \implies n+1 \in \mathcal{S}$ , entonces  $\mathcal{S} = \mathbb{N}$ .

**10 Axioma (Principio (fuerte) de la inducción matemática)** Si  $\mathcal{S}$  es un conjunto de enteros tal que  $m \in \mathcal{S}$  y si  $\{m, m+1, \dots, n\} \in \mathcal{S} \implies n+1 \in \mathcal{S}$ , entonces  $\forall k \geq m$  se tiene  $k \in \mathcal{S}$ .

**11 Ejemplo (USAMO, 1978)** Llámese *bueno* al entero  $n$  si se pudiere escribir de la forma

$$n = a_1 + a_2 + \cdots + a_k,$$

en donde  $a_1, a_2, \dots, a_k$  son enteros positivos, no necesariamente distintos y satisfaciendo

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k} = 1.$$

Dada la información de que todo entero desde el 33 hasta el 73 es bueno, demuéstrese que todo entero  $\geq 33$  es bueno.

**Resolución:** Primero se demostrará que si  $n$  es bueno entonces también  $2n + 8$  y  $2n + 9$  son buenos. Para esto presúmase que  $n = a_1 + a_2 + \dots + a_k$  y que

$$1 = \frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_k}.$$

Luego  $2n + 8 = 2a_1 + 2a_2 + \dots + 2a_k + 4 + 4$  y

$$\frac{1}{2a_1} + \frac{1}{2a_2} + \dots + \frac{1}{2a_k} + \frac{1}{4} + \frac{1}{4} = \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1.$$

Además,  $2n + 9 = 2a_1 + 2a_2 + \dots + 2a_k + 3 + 6$  y

$$\frac{1}{2a_1} + \frac{1}{2a_2} + \dots + \frac{1}{2a_k} + \frac{1}{3} + \frac{1}{6} = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1.$$

Luego si

$$\text{si } n \text{ es bueno entonces ambos } 2n + 8 \text{ y } 2n + 9 \text{ son buenos.} \quad (1.1)$$

Sea  $P(n)$  la proposición: “todos los enteros  $n, n + 1, n + 2, \dots, 2n + 7$  son buenos”. Por hipótesis  $P(33)$  es cierta. Pero (1.1) implica la veracidad de  $P(n + 1)$  cada vez que  $P(n)$  sea cierta. Luego la aserción es demostrada por inducción fuerte.

## Tarea

### 1.3. Principio de las pichoneras de Dirichlet

**12 Regla (Principio de las casillas (pichoneras) de Dirichlet)** Si  $n + 1$  palomas vuelan hacia  $n$  pichoneras deberá existir al menos una casilla que tenga dos o más palomas.

**13 Ejemplo (Putnam, 1978)** Sea  $A$  un conjunto cualquiera de 20 enteros tomados de la progresión aritmética

$$1, 4, \dots, 100.$$

Compruébese que deberá de haber dos enteros distintos en  $A$  cuya suma es 104.

**Resolución:** Fórmese una partición de los 34 elementos de la progresión en los 19 grupos

$$\{1\}, \{52\}, \{4, 100\}, \{7, 97\}, \{10, 94\} \dots \{49, 55\}.$$

Como se han de tomar 20 para formar el conjunto  $A$ , por el principio de las casillas de Dirichlet deben de haber dos enteros que pertenezcan a uno de los pares, y por tanto suman a 104.

## Tarea

**14 Problema** Póngase en evidencia que entre siete enteros cualesquiera menores o iguales que 126, siempre se podrá hallar dos, llámense  $a$  y  $b$ , los cuales satisfacen las desigualdades

$$b < a \leq 2b.$$

**15 Problema** Dados cualesquiera 10 enteros en el conjunto  $\{1, 2, \dots, 99\}$  demuéstrese que siempre habrá dos subconjuntos disjuntos cuyos elementos sumarán a la misma suma.

**16 Problema** No importa que 55 enteros se elija del conjunto

$$\{1, 2, \dots, 100\},$$

demuéstrese que siempre habrá dos que difieren por 10.

## Divisibilidad y primos

### 2.1. Divisibilidad y algoritmo de división

**17 Definición (Divisibilidad)** Se dice que un entero  $d \neq 0$  divide a otro  $a$ , denotado por  $d \mid a$ , si existe un entero  $d'$  tal que  $dd' = a$ . El caso en que  $d$  no dividiere a  $a$  se denotará por  $d \nmid a$ .

**18 Teorema (Propiedades de la divisibilidad)** Sean  $a, b, c, d, x, y$  enteros. Entonces

- ❶  $(d \mid a, d \mid b) \implies d \mid (ax + by)$ .
- ❷  $(d \mid a, a \mid b) \implies d \mid b$ .
- ❸  $(d \mid a, a \neq 0) \implies |d| \leq |a|$ .
- ❹  $(d \mid a, a \mid d) \implies d = \pm a$ .

**Demostración:** Se tiene que

- ❶ hay  $d', d''$  con  $dd' = a$ ,  $dd'' = b$ . Así

$$xa + yb = xdd' + ydd'' = (xd' + yd'')d,$$

lo que implica que  $d \mid (xa + yb)$ .

- ❷ hay  $d', a'$  con  $dd' = a$  y  $aa' = b$ , de donde

$$dd'a' = aa' = b \implies d \mid b.$$

- ❸ el número  $\frac{a}{d}$  es un entero no nulo, luego  $\left| \frac{a}{d} \right| \geq 1 \implies |a| \geq |d|$ .

- ❹ por definición  $da \neq 0$ . Existen  $d', r$  ambos diferentes de 0, tales que  $dd' = a$  y  $ar = d$ . Entonces  $dd'r = ar = d$ . Luego  $d'r = 1$  y como  $d', r$  son enteros, se tiene que  $d' = \pm 1$ ,  $r = \mp 1$ . Se colige que  $d = \pm a$ .

□

**19 Teorema (Algoritmo de división)** Sean  $b \in \mathbb{Z} \setminus \{0\}$  y  $a \in \mathbb{Z}$ . Entonces hay enteros únicos  $q$  y  $r$  tales que

$$a = bq + r, \quad 0 \leq r < |b|.$$

**Demostración:** Si  $b > 0$  tómese  $q = \lfloor \frac{a}{b} \rfloor$  y  $r = a - bq$ . En virtud de la definición de la función mayor entero,

$$q \leq \frac{a}{b} < q + 1,$$

luego  $bq \leq a < bq + b$ , de donde  $0 \leq r < b = |b|$ . Si acaso  $b < 0$  entonces póngase  $q = -\lfloor \frac{a}{|b|} \rfloor$ .

Para demostrar la unicidad, supóngase que  $a = bq' + r' = bq + r$ , con  $0 \leq r', r < |b|$ . Luego  $r' - r = b(q - q')$ , de donde  $b \mid (r' - r)$ . Pero  $|r' - r| < |b|$ , lo que requiere que  $r' = r$ , en virtud del Teorema 18. De aquí también se deduce  $q' = q$ .  $\square$

**20 Definición** En la ecuación  $a = bq + r$ ,  $a$  es el *dividendo*,  $b \neq 0$  el *divisor*,  $q$  el *cociente* y  $r$  el *residuo*.

El algoritmo de división crea particiones de los enteros según el residuo que éstos dejen al ser divididos por un entero no nulo. Por ejemplo, si  $n = 5$  el algoritmo de división dice que los enteros se pueden arreglar en las siguientes cinco columnas:

⋮	⋮	⋮	⋮	⋮
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
⋮	⋮	⋮	⋮	⋮

El arreglo aquí mostrado evidencia que los enteros vienen en uno de cinco sabores: aquellos cuyo residuo es 0 al ser divididos por 5, aquellos cuyo residuo es 1 al ser divididos por 5, etc. Dicho de otra manera, todo entero es de la forma  $5k$ ,  $5k + 1$ ,  $5k + 2$ ,  $5k + 3$  ó  $5k + 4$ . Obsérvese además que se puede decir que todo entero es de la forma  $5k$ ,  $5k \pm 1$  ó  $5k \pm 2$ . El algoritmo de división pues discrimina y crea clases entre los enteros, llamadas *clases de equivalencia*, que se denotarán (en el caso cuando el divisor es 5) por

$$\begin{aligned} 5\mathbb{Z} &= \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\} = \bar{0}, \\ 5\mathbb{Z} + 1 &= \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\} = \bar{1}, \\ 5\mathbb{Z} + 2 &= \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} = \bar{2}, \\ 5\mathbb{Z} + 3 &= \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} = \bar{3}, \\ 5\mathbb{Z} + 4 &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\} = \bar{4}, \end{aligned}$$

y se pondrá

$$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

**21 Ejemplo** Demuéstrese que el cuadrado de todo entero es de la forma  $4k$  o de la forma  $4k + 1$ . Luego demuéstrese que ningún entero en la sucesión

$$11, 111, 1111, 11111, \dots$$

es el cuadrado de un entero.

**Resolución:** Si el entero es par, es decir de la forma  $2a$ , su cuadrado es  $(2a)^2 = 4a^2$ , que es de la forma  $4k$ . Si el entero es impar, digamos  $2t + 1$ , entonces  $(2t + 1)^2 = 4(t^2 + t) + 1$ , que es de la forma  $4k + 1$ .

Ahora bien, para  $n \geq 2$ ,

$$\underbrace{11\dots1}_{n \text{ 1's}} = \underbrace{11\dots11}_{n-2 \text{ 1's}}00 + 8 + 3 = 100 \cdot \underbrace{11\dots11}_{n-2 \text{ 1's}} + 8 + 3 := 4s + 3,$$

en donde  $s = 25 \cdot \underbrace{11\dots11}_{n-2 \text{ 1's}} + 2$ . Así pues, todo número en esta sucesión es de la forma  $4k + 3$ . Pero se sabe que un cuadrado ha de tener la forma  $4k$  ó  $4k + 1$  y por lo tanto ningún miembro de esta sucesión es el cuadrado de un entero.

**22 Ejemplo** Sea  $n > 0$  entero.

❶ Sea  $a \neq 1$ . Demuéstrese la identidad

$$1 + a + a^2 + \dots + a^{n-1} = \frac{a^n - 1}{a - 1}. \quad (2.1)$$

❷ Demuéstrese la identidad

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + xy^{n-2} + y^{n-1}). \quad (2.2)$$

De esto se deduce que si  $x, y$  son enteros con  $x \neq y$  entonces  $x - y$  divide a  $x^n - y^n$ .

❸ Si  $n$  es impar, hágase patente que  $(x + y) \mid (x^n + y^n)$ .

❹ Demuéstrese que si  $k$  es un entero positivo impar

$$1^k + 2^k + \dots + n^k$$

es divisible por

$$1 + 2 + \dots + n.$$

**Resolución:** Para el primer inciso, se procederá por inducción. Para  $n = 1$  es claro que  $1 = \frac{a-1}{a-1}$ , y para  $n = 2$  es evidente que  $1 + a + a^2 = \frac{a^3 - 1}{a - 1}$ . Suponiendo la validez de 2.1 para  $n$ , habrá de demostrarse para  $n + 1$ . Ahora bien

$$\begin{aligned} (1 + a + a^2 + \dots + a^{n-1}) + a^n &= \frac{a^n - 1}{a - 1} + a^n \\ &= \frac{a^n - 1 + a^{n+1} - a^n}{a - 1} \\ &= \frac{a^{n+1} - 1}{a - 1}, \end{aligned}$$

demostrando la validez de 2.1 para  $n + 1$ . Así la primera aseveración queda demostrada por inducción.

Para demostrar 2.2 basta poner  $a = \frac{x}{y}$  en 2.1 y simplificar. Es evidente entonces que  $(x - y) \mid (x^n - y^n)$ .

Si  $n$  fuere impar, entonces  $(-y)^n = -y^n$  y con substituir  $-y$  por  $y$  en 2.2 se obtiene el resultado.

Para obtener la última aseveración obsévese primero que

$$1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

Se considerará los casos cuando  $n$  es par y cuando  $n$  es impar por separado.

Presúmase primero que  $n$  es par. Luego  $\frac{n}{2}$  es un entero y cada una de las expresiones

$$1^k + (n-1)^k; 2^k + (n-2)^k; \dots; \left(\frac{n-2}{2}\right)^k + \left(\frac{n+2}{2}\right)^k; \left(\frac{n}{2}\right)^k; n^k,$$

es divisible por  $\frac{n}{2}$  en vista del inciso anterior. Reagrupando de la manera

$$1^k + n^k; 2^k + (n-1)^k; \dots; \left(\frac{n}{2}\right)^k + \left(\frac{n+2}{2}\right)^k,$$

también se ve que la suma es divisible por  $n + 1$ . Como  $\frac{n}{2}$  y  $n + 1$  no tienen factores en común, se deduce que la suma es divisible por  $\frac{n(n+1)}{2}$ .

Presúmase ahora que  $n$  es impar, de donde  $\frac{n+1}{2}$  es un entero. Cada una de las expresiones

$$1^k + n^k; 2^k + (n-1)^k; \dots; \left(\frac{n-1}{2}\right)^k + \left(\frac{n+3}{2}\right)^k; \left(\frac{n+1}{2}\right)^k,$$

es divisible por  $\frac{n+1}{2}$  en vista del inciso anterior. De igual manera la suma es divisible por  $n$  ya que cada una de las expresiones

$$1^k + (n-1)^k; 2^k + (n-2)^k; \dots; \left(\frac{n-1}{2}\right)^k + \left(\frac{n+1}{2}\right)^k; n^k,$$

lo es. Como  $\frac{n+1}{2}$  y  $n$  no tienen factores en común, se deduce que la suma es divisible por  $\frac{n(n+1)}{2}$ .

**23 Ejemplo** Demuéstrese que si  $n$  es un entero positivo tal que  $2n+1$  es un cuadrado, entonces  $n+1$  es la suma de dos cuadrados consecutivos.

**Resolución:** Como  $2n+1$  es un cuadrado impar, tenemos  $2n+1 = (2t+1)^2$  para algún entero  $t$ . Resolviendo para  $n$ ,

$$n = \frac{(2t+1)^2 - 1}{2} = 2t^2 + 2t.$$

Luego  $n+1 = t^2 + (t+1)^2$ , la suma de dos cuadrados consecutivos.

**24 Ejemplo** Demuéstrese que el único primo de la forma  $n^4+4$  es el 5.

**Resolución:** Se puede restringir el argumento a enteros positivos. Obsérvese que

$$\begin{aligned} n^4 + 4 &= n^4 + 4n^2 + 4 - 4n^2 \\ &= (n^2 + 2)^2 - (2n)^2 \\ &= (n^2 - 2n + 2)(n^2 + 2n + 2). \end{aligned}$$

Si este producto es un número primo entonces el factor más pequeño debe ser igual a 1. Así  $n^2 - 2n + 2 = 1$ , o sea  $(n-1)^2 = 0$ , esto es  $n = 1$ . Así, el único primo de esta forma es  $1^4 + 4 = 5$ .

**25 Ejemplo** Sean  $a_1, a_2, \dots, a_{2n}$  enteros tales que la ecuación

$$(x - a_1)(x - a_2) \cdots (x - a_{2n}) - (-1)^n (n!)^2 = 0$$

posee una solución entera  $a$ . Demuéstrese que

$$a = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}.$$

**Resolución:** Evidentemente se tiene  $a \neq a_i$  para ninguna de las  $i$  y los enteros  $a - a_i$  son  $2n$  enteros diferentes. Así pues

$$\left| (a - a_1)(a - a_2) \cdots (a - a_{2n}) \right| \geq \left| (1)(2) \cdots (n)(-1)(-2) \cdots (-n) \right| = (n!)^2,$$

la igualdad ocurriendo si y sólo si

$$\{a_1, a_2, \dots, a_{2n}\} = \{1, 2, \dots, n, -1, -2, \dots, -n\}.$$

Se deberá tener entonces

$$(a - a_1) + (a - a_2) + \cdots + (a - a_{2n}) = 1 + 2 + \cdots + n - 1 - 2 - \cdots - n$$

sí y sólo si

$$2an - (a_1 + a_2 + \cdots + a_{2n}) = 0$$

sí y sólo si

$$a = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n},$$

como se quería demostrar.

## Tarea

**26 Problema** Hallése todos los enteros positivos de la forma

$$r + \frac{1}{r},$$

donde  $r$  es un número racional.

**27 Problema** Demuéstrese que el entero

$$\underbrace{11 \dots 11}_{221 \text{ 1's}}$$

es compuesto.

**28 Problema** Demuéstrese que 100 divide a  $11^{10} - 1$ .

**29 Problema** Demuéstrese que entre tres enteros siempre se pueden escoger dos tales que  $a^3b - ab^3$  sea divisible por 10.

**30 Problema** Demuéstrese, vía inducción, que la expresión

$$3^{3n+3} - 26n - 27$$

es un múltiplo de 169 para todos los números naturales  $n$ .

**31 Problema** Demuéstrese que si  $3n + 1$  es un cuadrado, entonces  $n + 1$  es la suma de tres cuadrados.

**32 Problema** Demuéstrese que si  $n > 11$  entonces  $n$  se puede escribir como la suma de dos números compuestos.

**33 Problema (AHSME, 1976)** Sea  $r$  el residuo cuando 1059, 1417 y 2312 se dividen por  $d > 1$ . Halle el valor de  $d - r$ .

**34 Problema** Demuéstrese que  $n^2 + 23$  es divisible por 24 para un número infinito de números  $n$ .

**35 Problema** La suma de enteros positivos es 1996. ¿Cuál es el valor máximo de su producto?

**36 Problema (Eötvös, 1899)** Compruébese que para todo entero positivo  $n$ , la expresión

$$2903^n - 803^n - 464^n + 261^n$$

es siempre divisible por 1897.

**37 Problema** Demuéstrese que todo entero  $n > 6$  puede ser escrito como la suma de dos enteros ambos mayores que 1 tales que cada sumando sea relativamente primo.

**38 Problema** Demuéstrese que si ambos  $p$  es primo, o bien  $8p - 1$  es primo y  $8p + 1$  compuesto o viceversa.

**39 Problema** Demuéstrese que 7 divide a  $2222^{5555} + 5555^{2222}$ .

**40 Problema** Demuéstrese que si  $2^n - 1$  es un número primo, entonces  $n$  es un número primo. Primos de esta forma se llaman *primos de Mersenne*.

**41 Problema** Demuéstrese que si  $2^n + 1$  es un número primo, entonces  $n$  es una potencia de 2. Primos de esta forma se llaman *primos de Fermat*.

**42 Problema ((UM)<sup>2</sup>C<sup>4</sup>, 1987)** Dado que 1002004008016032 tiene un factor primo  $p > 250000$ , encuéntrese.

**43 Problema** Demuéstrese que

$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca).$$

Luego demuéstrese que

$$6 \mid (a + b + c) \implies 6 \mid (a^3 + b^3 + c^3).$$

Demuéstrese además que si  $n$  es la suma de tres cubos consecutivos, entonces  $9 \mid n$ .

**44 Problema** Compruébese que el producto de cuatro enteros consecutivos, diferentes de 0, jamás es un cuadrado.

**45 Problema** Demuéstrese que si  $k$  es impar entonces  $2^{n+2}$  divide a

$$k^{2^n} - 1$$

para todos los enteros naturales  $n \geq 1$ .

## 2.2. Máximo común divisor

**46 Definición (Máximo común divisor)** Sea  $(a, b) \in \mathbb{Z}^2$ ,  $(a, b) \neq (0, 0)$ . Si  $r \mid a$  y  $r \mid b$  entonces  $r$  es un *divisor común* de  $a$  y  $b$ . Si  $d$  es un divisor común de  $a$  y  $b$  tal que cualquier otro divisor común de  $a$  y  $b$  divide a  $d$ , entonces  $d$  es el *máximo común divisor* de  $a$  y  $b$ , denotado por  $\text{MCD}(a, b)$ . Obsérvese que esto requiere que  $d$  sea  $> 0$ .

**47 Definición** Dícese que dos enteros  $a$  y  $b$  son *relativamente primos* si  $\text{MCD}(a, b) = 1$ .

**48 Teorema (Teorema de Bachet-Bézout)** Sea  $(a, b) \in \mathbb{Z}^2$ ,  $(a, b) \neq (0, 0)$ . Si  $d = \text{MCD}(a, b)$  entonces hay enteros  $x, y$  tales que

$$ax + by = d.$$

**Demostración:** *Considérese el conjunto*

$$\mathcal{S} = \{n \in \mathbb{Z} : n > 0, n = as + bt, (s, t) \in \mathbb{Z}^2\}.$$

$\mathcal{S} \neq \emptyset$  ya que o bien  $\pm a \in \mathcal{S}$  o bien  $\pm b \in \mathcal{S}$ . Luego por el buen orden de los enteros,  $\mathcal{S}$  tiene un elemento mínimo estrictamente positivo al que se llamará  $n_0 = ax_0 + by_0$ . Obsérvese que  $d \mid n_0$  en virtud del Teorema 18 ya que  $d \mid a$  y  $d \mid b$ . Ahora bien, por el algoritmo de división existen enteros  $q, r$  con  $a = qn_0 + r$ ,  $0 \leq r < n_0$ . Si  $r \neq 0$  entonces

$$r = a - qn_0 = a - q(ax_0 + by_0) = a(1 - qx_0) - qby_0 \in \mathcal{S}$$

que es menor que  $n_0$ , contradiciendo la definición de  $n_0$ , de donde se concluye que  $r = 0$ . De la misma manera se puede demostrar que  $n_0 \mid b$ . Luego  $n_0$  es un divisor común de  $a$  y  $b$ , por lo tanto divide a  $d$ . Ya que  $d \mid n_0$  y  $n_0 \mid d$  se tiene, en virtud del Teorema 18, se tiene que  $d = \pm n_0$ . Como ambos  $d > 0$ ,  $n_0 > 0$  se colige que  $d = n_0$ .  $\square$

**49 Ejemplo** Si  $\text{MCD}(a, b) = 1$  entonces  $\text{MCD}(a + b, a^2 - ab + b^2) = 1$  ó  $3$ .

**Resolución:** Sea  $d = \text{MCD}(a + b, a^2 - ab + b^2)$ . Ahora bien,  $d$  divide a

$$(a + b)^2 - a^2 + ab - b^2 = 3ab.$$

Así,  $d$  divide a  $3b(a+b) - 3ab = 3b^2$ . De manera semejante se deduce que  $d \mid 3a^2$ . Pero entonces  $d \mid \text{MCD}(3a^2, 3b^2) = 3\text{MCD}(a^2, b^2) = 3\text{MCD}(a, b)^2 = 3$ .

**50 Ejemplo** Sean  $m, n, a \neq 1$  enteros positivos. Demuéstrese que

$$\text{MCD}(a^m - 1, a^n - 1) = a^{\text{MCD}(m, n)} - 1.$$

**Resolución:** Póngase  $d = \text{MCD}(m, n)$ ,  $sd = m$ ,  $td = n$ . Entonces  $a^m - 1 = (a^d)^s - 1$  es divisible por  $a^d - 1$  y de manera semejante,  $a^n - 1$  es divisible por  $a^d - 1$ . Así  $(a^d - 1) \mid \text{MCD}(a^m - 1, a^n - 1)$ . Ahora bien, en virtud al Teorema de Bachet-Bezout (Teorema 48) existen enteros  $x, y$  con  $mx + ny = d$ . Nótese que  $x, y$  habrán de tener signos opuestos (no pueden ser ambos negativos, ya que  $d$  sería entonces negativo. Si ambos fuesen positivos entonces  $d \geq m + n$ , lo que contradice al hecho que  $d \leq m, d \leq n$ ). Presúmase pues, sin pérdida de generalidad, que  $x > 0, y \leq 0$ . Póngase  $t = (a^m - 1, a^n - 1)$ . Entonces  $t \mid (a^{mx} - 1)$  y  $t \mid (a^{-ny} - 1)$ . Luego  $t \mid ((a^{mx} - 1) - a^d(a^{-ny} - 1)) = a^d - 1$ , estableciendo el resultado.

## Tarea

**51 Problema (IMO, 1959)** Compruébese que la fracción  $\frac{21n+4}{14n+3}$  es irreducible para todo entero natural  $n$ .

**52 Problema (AIME, 1985)** Los números de la sucesión

$$101, 104, 109, 116, \dots$$

son de la forma  $a_n = 100 + n^2, n = 1, 2, \dots$ . Para cada  $n$  póngase  $d_n = \text{MCD}(a_n, a_{n+1})$ . Hállese  $\max_{n \geq 1} d_n$ .

**53 Problema** Tómese cualesquiera 51 enteros de entre  $1, 2, \dots, 100$ . Demuéstrese que hay al menos dos que son relativamente primos.

**54 Problema** Demuéstrese que el producto de tres enteros estrictamente positivos consecutivos jamás será una potencia perfecta.

## 2.3. Primos y factorización única

**55 Lema (Lema de Gauss)** Si  $d \mid ab$  y  $\text{MCD}(d, a) = 1$  entonces  $d \mid b$ .

**Demostración:** Por el Teorema de Bachet-Bezout (Teorema 48) existen enteros  $x, y$  tales que  $ax + dy = 1$ . Luego  $bax + bdy = b$ . Como  $d \mid ab$  se tiene que  $d \mid (bax + bdy) = b$ .  $\square$

**56 Lema (Lema de Euclides)** Si  $p$  es primo, y  $p \mid ab$  o bien  $p \mid a$  o bien  $p \mid b$ .

**Demostración:** Si  $p \nmid a$  entonces  $\text{MCD}(p, a) = 1$ . Gracias al Lema de Gauss (Lema 55) se tiene que  $p \mid b$ .  $\square$

**57 Teorema (Teorema fundamental de la aritmética)** Todo entero  $n > 1$  puede descomponerse en factores de la manera

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

en donde  $p_1 < p_2 < \cdots < p_r$  son primos. Esta representación es única, a la cual se llamará la *factorización canónica de  $n$* .

**Demostración:** Si  $n > 1$  es primo, entonces no hay nada que demostrar. Supóngase que  $n > 1$  es el menor entero no primo que no se puede descomponer de la manera dicha. Como  $n$  no es primo, existen  $n' > 1, n'' > 1$  con  $n = n'n''$ . Pero luego  $n'$  y  $n''$  son menores que  $n$  y por tanto se pueden descomponer como  $n' = q_1^{\beta_1} \cdots q_s^{\beta_s}$  y  $n'' = q_1^{\gamma_1} \cdots q_t^{\gamma_t}$  donde algunos de los exponentes pueden ser 0. Se sigue que

$$n = n'n'' = n' = q_1^{\beta_1 + \gamma_1} q_2^{\beta_2 + \gamma_2} \cdots,$$

lo que contradice la suposición de que  $n$  no se podía descomponer en primos.

Para demostrar la unicidad de la descomposición, se argüirá por inducción. Supóngase que todo entero mayor que 1 y menor que  $n$  puede descomponerse en primos de manera única. Si

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = q_1^{\eta_1} \cdots q_s^{\eta_s},$$

en donde  $p_1 < p_2 < \cdots < p_r$  y  $q_1 < q_2 < \cdots < q_r$ . Entonces por el Lema de Euclides (Lema 56)  $p_1$  debe dividir a exactamente una  $q$  y  $q_1$  debe dividir a exactamente una de las  $p$ 's. Pero esto fuerza  $p_1 = q_1$ . Luego al dividir por  $p_1$  uno y otro lado se obtiene se obtiene

$$\frac{n}{p_1} = p_1^{\alpha_1 - 1} \cdots p_r^{\alpha_r} = p_1^{\eta_1 - 1} q_2^{\eta_2} \cdots q_s^{\eta_s}.$$

Por la hipótesis de inducción  $\frac{n}{p_1}$  se descompone en primos de manera única, luego  $r = s$ ,  $p_i = q_i$  y  $\alpha_1 - 1 = \eta_1 - 1$ ,  $\alpha_2 = \eta_2, \dots, \alpha_r = \eta_r$ , de donde se colige que  $\alpha_1 = \eta_1$  y por lo tanto  $n$  también se descompone en primos de manera única.  $\square$

**58 Teorema (Euclides-Infinitud de los primos)** El conjunto  $\mathbb{P}$  de los primos es inagotable. Aún más, si  $p_1 = 2, p_2 = 3, \dots$  y en general  $p_k$  es el  $k$ -ésimo primo, entonces

$$p_{k+1} \leq p_1 \cdots p_k + 1.$$

**Demostración:** Considérese el entero  $n = p_1 \cdots p_k + 1$ . Por el Teorema fundamental de la aritmética (Teorema 57) o bien  $n = p_1 \cdots p_k + 1$  es primo, o puede descomponerse como un producto de primos, lo que demuestra la existencia de una lista de primos dividiendo a  $n$ , lista que se llamará  $\mathcal{P}$ . Ahora bien, al dividir  $n$  por los primos de la lista  $\mathcal{P}' = \{p_1, p_2, \dots, p_k\}$ ,  $n$  deja residuo 1. De aquí se infiere que  $\mathcal{P} \cap \mathcal{P}' = \emptyset$  y luego a cualquier lista finita de primos puede agregársele un primo más, de donde ninguna lista finita de primos es exhaustiva. El primo mínimo  $p$  dividiendo a  $n$  debe ser mayor que  $p_k$  y se tiene  $p \leq n$  en virtud del Teorema 18. Es claro que  $p_{k+1} \leq p$ .  $\square$

La sucesión de los primos comienza pues así

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \dots$$

**59 Definición** Un múltiplo común de dos enteros  $a, b$  es un entero no negativo que es divisible por ambos  $a$  y  $b$ . Si  $m$  es múltiplo común de  $a, b$  y si  $m$  divide a todo otro múltiplo común, entonces  $m$  es el mínimo común múltiplo, de  $a, b$ , al que se denotará por  $\text{mcm}(a, b)$ .

**60 Teorema** Sean  $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$  y  $n' = q_1^{\gamma_1} \cdots q_t^{\gamma_t}$  donde algunos de los exponentes pueden ser 0. Entonces

$$\text{MCD}(n, n') = q_1^{\min(\beta_1, \gamma_1)} q_2^{\min(\beta_2, \gamma_2)} \cdots \tag{2.3}$$

$$\text{mcm}(n, n') = q_1^{\max(\beta_1, \gamma_1)} q_2^{\max(\beta_2, \gamma_2)} \cdots \tag{2.4}$$

Aún más:

$$nn' = \text{MCD}(n, n') \text{mcm}(n, n'). \tag{2.5}$$

y si  $k$  es un entero positivo entonces

$$\text{MCD}(a, b)^k = \text{MCD}(a^k, b^k), \quad \text{mcm}(a, b)^k = \text{mcm}(a^k, b^k). \tag{2.6}$$

**Demostración:** Las dos primeras aseercciones son evidentes gracias al Teorema fundamental de la aritmética (Teorema 57). Para la tercera aseercción basta notar que

$$\text{mín}(\beta, \eta) + \text{máx}(\beta, \eta) = \beta + \eta.$$

La cuarta se deriva de las primeras dos.  $\square$

**61 Ejemplo** Demuéstrese que  $\sqrt{2}$  es irracional.

**Resolución:** Supóngase a miras de contradicción que  $\sqrt{2} = \alpha/\mathbf{b}$  con enteros positivos  $\alpha, \mathbf{b}$  relativamente primos. Entonces  $2\mathbf{b}^2 = \alpha^2$ . El lado siniestro de esta ecuación tiene un número impar de factores primos mientras que el diestro tiene un número par. Esto contradice el Teorema fundamental de la aritmética (Teorema 57). Contrástese este método con el del ejemplo 3.

**62 Ejemplo** Demuéstrese que dados cualesquiera 33 enteros diferentes con todos sus factores primos en el conjunto  $\{5, 7, 11, 13, 23\}$ , siempre hay dos distintos cuyo producto es un cuadrado.

**Resolución:** Cada uno de los 33 enteros es de la forma

$$5^a 7^b 11^c 13^d 23^f.$$

Así, a cada uno de los 33 enteros se les puede asociar un vector de la forma  $(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{f})$ . Dependiendo la paridad de los componentes del vector, hay  $32 = 2^5$  tipos de estos vectores. Por ejemplo, uno de los tipos es (par, par, impar, impar, par). Piénsese de estas 32 clases de vectores como en 32 casillas. A los 33 enteros se les distribuirá en las 32 casillas y por tanto, una de las casillas tendrá al menos dos enteros diferentes. En esta casilla los exponentes de los números son de la misma paridad, así que al multiplicarse, todos los exponentes serán pares. Luego este producto será un cuadrado.

## Tarea

**63 Problema (IMO 1985)** Dado un conjunto  $\mathcal{M}$  de 1985 enteros positivos distintos, ninguno de cuyos factores primos es mayor que 26, demuéstrese que  $\mathcal{M}$  siempre tendrá cuatro elementos distintos cuyo producto es una cuarta potencia.

**64 Problema** Tómese 51 enteros cualesquiera del conjunto

$$\{1, 2, \dots, 100\}.$$

Demuéstrese que siempre habrá dos, uno dividiendo al otro.

**65 Problema** Demuéstrese que si el polinomio

$$p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$$

con coeficientes íntegros alcanza el valor de 7 para cuatro valores íntegros de  $x$  entonces no puede tomar el valor de 14 para ningún valor íntegro de la variable  $x$ .

**66 Problema** Compruébese que  $m^5 + 3m^4 n - 5m^3 n^2 - 15m^2 n^3 + 4mn^4 + 12n^5$  nunca será igual a 33.

**67 Problema** Demuéstrese que la suma

$$S = 1/2 + 1/3 + 1/4 + \dots + 1/n$$

jamás es íntegra.

**68 Problema** Demuéstrese que existe un entero único  $n$  para el cual  $2^8 + 2^{11} + 2^n$  es un cuadrado perfecto.

## 2.4. Algoritmo de Euclides y ecuaciones diofánticas lineales

Se dará ahora un procedimiento eficaz para hallar soluciones  $x, y$  a la ecuación  $\text{MCD}(a, b) = ax + by$ . Este procedimiento se llama el *algoritmo de Euclides* y opera como sigue. Sean  $a, b$  enteros positivos. Luego de aplicar el algoritmo de división repetidamente, se ve que

$$\begin{aligned} a &= bq_1 + r_2, & 0 < r_2 < b, \\ b &= r_2q_2 + r_3, & 0 < r_3 < r_2, \\ r_2 &= r_3q_3 + r_4, & 0 < r_4 < r_3, \\ \vdots & \vdots \quad \vdots & \vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_n. \end{aligned} \tag{2.7}$$

La sucesión de residuos eventualmente llegará a un  $r_{n+1}$  que será 0 ya que la sucesión  $b, r_2, r_3, \dots$  es una sucesión de enteros monótona decreciente la cual no puede tener más de  $b$  términos estrictamente positivos.

**69 Lema** Si  $b \neq 0, a = qb + r$  entonces  $\text{MCD}(a, b) = \text{MCD}(b, r)$ .

**Demostración:** Póngase  $d = \text{MCD}(a, b), c = \text{MCD}(b, r)$ . Como  $d \mid a$  y  $d \mid b$ , se sigue que  $d \mid (a - qb) = r$ . Así pues  $d$  es un divisor común de  $r$  y  $b$ . Esto implica que  $d \mid c$ . Por otra parte,  $c \mid r$  y  $c \mid b$  implican que  $c \mid (qb + r) = a$ . Luego  $c$  es un divisor común de  $a$  y  $b$  de donde  $c \mid d$ , lo que acaba la demostración.  $\square$

**70 Teorema** Si  $r_n$  es el último residuo diferente de 0 encontrado en el algoritmo de Euclides, entonces

$$r_n = \text{MCD}(a, b).$$

**Demostración:** Aplicando el Lema 69 varias veces se ve que

$$\begin{aligned} \text{MCD}(a, b) &= \text{MCD}(b, r_2) \\ &= \text{MCD}(r_2, r_3) \\ &= \vdots \\ &= \text{MCD}(r_{n-1}, r_n) \\ &= r_n. \end{aligned}$$

$\square$



De las ecuaciones en 2.7 se ve que

$$\begin{aligned} r_2 &= a - bq_1 \\ r_3 &= b - r_2q_2 \\ r_4 &= r_2 - r_3q_3 \\ \vdots & \quad \vdots \\ r_n &= r_{n-2} - r_{n-1}q_{n-1}, \end{aligned}$$

luego es posible expresar  $\text{MCD}(a, b)$  como una combinación lineal de  $a$  y  $b$  trazando estas igualdades en reversa.

**71 Teorema** Sean  $a, b, c$  son enteros tales que  $(a, b) \mid c$ . Dada una solución  $(x_0, y_0)$  de la ecuación diofántica lineal

$$ax + by = c,$$

cualquier otra solución es de la forma

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

en donde  $d = (a, b)$  y  $t \in \mathbb{Z}$ .

**Demostración:** Es inmediato que si  $(x_0, y_0)$  es una solución de  $ax + by = c$ , entonces  $x = x_0 + tb/d, y = y_0 - ta/d$  es también una solución. Demostrárase ahora que toda otra solución es de la forma deseada.

Supóngase que  $(x', y')$  satisface  $ax' + by' = c$ . Si además  $ax_0 + by_0 = c$  entonces

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

Dividiendo por  $d = (a, b)$ ,

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y').$$

Como  $(a/d, b/d) = 1$ , se sigue que  $\frac{a}{d} | (y_0 - y')$ , por virtud del Lema de Euclides. Así pues existe un entero  $t$  tal que  $t \frac{a}{d} = y_0 - y'$ , ésto es,  $y = y_0 - ta/d$ . Se colige entonces que

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}t \frac{a}{d},$$

which is to say  $x' = x_0 + tb/d$ , demostrando el teorema.  $\square$

**72 Ejemplo** Hállese  $\text{MCD}(23, 29)$  mediante el algoritmo de Euclides y Encuéntrase soluciones enteras para la ecuación  $23x + 29y = 1$ .

**Resolución:** Se tiene

$$29 = 1 \cdot 23 + 6,$$

$$23 = 3 \cdot 6 + 5,$$

$$6 = 1 \cdot 5 + 1,$$

$$5 = 5 \cdot 1.$$

El último residuo no nulo es el 1 de donde  $\text{MCD}(23, 29) = 1$ .

Ahora bien,

$$1 = 6 - 1 \cdot 5,$$

$$5 = 23 - 3 \cdot 6,$$

$$6 = 29 \cdot 1 - 23.$$

Luego,

$$\begin{aligned} 1 &= 6 - 1 \cdot 5 \\ &= 6 - 1 \cdot (23 - 3 \cdot 6) \\ &= 4 \cdot 6 - 1 \cdot 23 \\ &= 4(29 \cdot 1 - 23) - 1 \cdot 23 \\ &= 4 \cdot 29 - 5 \cdot 23. \end{aligned}$$

Esto resuelve la ecuación con  $x = -5, y = 4$ .

**73 Ejemplo** Encuéntrase un número infinito de soluciones para  $23x + 29y = 1$ .

**Resolución:** Gracias al ejemplo 72 se tiene que el par  $x_0 = -5, y_0 = 4$  es una solución. Se puede encontrar una familia infinita de soluciones en poniendo

$$x = -5 + 29t, y = 4 - 23t, t \in \mathbb{Z}.$$

**74 Ejemplo** Hállese soluciones enteras para la ecuación  $23x + 29y = 7$ .

**Resolución:** Del ejemplo 72 se tiene  $23(-5) + 29(4) = 1$ . Multiplicando uno y otro lado por 7,

$$23(-35) + 29(28) = 7,$$

lo que resuelve el problema.

**Tarea**


---

# Capítulo 3

## Funciones aritméticas

### 3.1. Funciones multiplicativas

**75 Definición (Función aritmética)** Llámase *función aritmética* a una función  $f: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{C}$ .  $f$  es *multiplicativa* si  $\text{MCD}(m, n) = 1 \implies f(mn) = f(m)f(n)$ .  $f$  es *completamente multiplicativa* si  $f(mn) = f(n)f(n)$  para todos los enteros positivos  $m$  y  $n$ .

 Toda función completamente multiplicativa es, a fortiori, multiplicativa. Una función multiplicativa está completamente determinada por sus valores en las potencias de los primos. Así, si  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  entonces  $f(n) = f(p_1^{\alpha_1}) \cdots f(p_r^{\alpha_r})$ . Además  $f(1 \cdot 1) = f(1)f(1) = (f(1))^2$ . Luego, o bien  $f(1) = 1$  o bien  $f(1) = 0$ . Este último caso hace que la función sea idénticamente 0 por lo cual no se considerará. Por tanto, se tendrá por convención que para toda función multiplicativa  $f$ ,  $f(1) = 1$ .

**76 Teorema** Sea  $n > 0$  un entero y  $f, g$  funciones con

$$g(n) = \sum_{d|n} f(d).$$

Si  $f$  es multiplicativa, también lo es  $g$ .

**Demostración:** Tómese además  $n' > 0$  entero, con  $\text{MCD}(n, n') = 1$ . Todo  $d|nn'$  puede descomponerse en  $d = d_1 d_2$ ,  $d_1|n$ ,  $d_2|n'$ , de donde  $\text{MCD}(d_1, d_2) = 1$ . Luego

$$\begin{aligned} g(nn') &= \sum_{d|nn'} f(d) \\ &= \sum_{d_1|n, d_2|n'} f(d_1 d_2) \\ &= \sum_{d_1|n, d_2|n'} f(d_1) f(d_2) \\ &= \left( \sum_{d_1|n} f(d_1) \right) \left( \sum_{d_2|n'} f(d_2) \right), \end{aligned}$$

demostrando la aserción.

□

**77 Definición (Función número de divisores)** La función

$$d: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\} \\ \mathbf{n} \mapsto \sum_{d|\mathbf{n}} 1$$

cuenta el número de divisores positivos de un entero positivo  $\mathbf{n}$ .

**78 Teorema** La función

$$d: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\} \\ \mathbf{n} \mapsto \sum_{d|\mathbf{n}} 1$$

es multiplicativa, y si  $\mathbf{n} = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  es la descomposición canónica en primos de  $\mathbf{n}$ , entonces

$$d(\mathbf{n}) = (\alpha_1 + 1) \cdots (\alpha_r + 1).$$

**Demostración:** Ya que la función  $d \mapsto 1$  es completamente multiplicativa es, a fortiori, multiplicativa. Luego

$d(\mathbf{n}) = \sum_{d|\mathbf{n}} 1$  es multiplicativa en virtud del Teorema 76. Si  $\mathbf{p}$  es primo,  $\mathbf{p}^\alpha$  tiene  $\alpha + 1$  divisores:  $1, \mathbf{p}, \mathbf{p}^2, \dots, \mathbf{p}^\alpha$ .

Así  $d(\mathbf{p}^\alpha) = \alpha + 1$  y

$$d(\mathbf{n}) = d(\mathbf{p}_1^{\alpha_1}) \cdots d(\mathbf{p}_r^{\alpha_r}) = (\alpha_1 + 1) \cdots (\alpha_r + 1).$$

□

**79 Ejemplo (El problema de los casilleros)** La guardarropiá de un gimnasio tiene 100 casilleros y 100 usuarios. Al principio, todos los casilleros están abiertos. Entra el usuario número 1 y cierra todos los casilleros. Entra el usuario número 2, y cierra todos los casilleros con número par. Entra el usuario número 3 y cambia de estado (de cerrado a abierto o vice versa) todos los casilleros cuyo número es un múltiplo de 3. Entra el usuario número 4 y cambia de estado (de cerrado a abierto o vice versa) todos los casilleros cuyo número es un múltiplo de 4. Sucede así sucesivamente hasta que entra el usuario número 100 y cambia de estado el casillero número 100. ¿Qué casilleros permanecen cerrados?

**Resolución:** Se verá que los casilleros cuyo número es un cuadrado perfecto permanecen cerrados. Así los casilleros número 1, 4, 9, 16, 25, 36, 49, 64, 81 y 100 son los que permanecen cerrados. Obsérvese que el casillero número  $\mathbf{n}$  es afectado por el usuario  $\mathbf{d}$  si y sólo si  $\mathbf{d}$  divide a  $\mathbf{n}$ . Así sólo aquellas  $\mathbf{n}$  que tengan un número impar de divisores permanecerán cerradas. Ahora bien, cada factor  $\mathbf{d}$  de  $\mathbf{n}$  se puede aparear con  $\frac{\mathbf{n}}{\mathbf{d}}$ , y así,  $\mathbf{n}$  tendrá un número impar de factores si y sólo si se tiene  $\mathbf{d} = \frac{\mathbf{n}}{\mathbf{d}}$ , esto es, si  $\mathbf{n}$  es un cuadrado perfecto.

**80 Definición (Función suma de divisores)** La función

$$\sigma: \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\} \\ \mathbf{n} \mapsto \sum_{d|\mathbf{n}} d$$

suma los divisores positivos de un entero positivo  $\mathbf{n}$ .

**81 Teorema** La función

$$\sigma : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$$

$$\mathbf{n} \mapsto \sum_{\mathbf{d} | \mathbf{n}} \mathbf{d}$$

es multiplicativa y si  $\mathbf{n} = \mathbf{p}_1^{\alpha_1} \cdots \mathbf{p}_r^{\alpha_r}$  es la descomposición canónica en primos de  $\mathbf{n}$ , entonces

$$\sigma(\mathbf{n}) = \frac{\mathbf{p}_1^{\alpha_1+1} - 1}{\mathbf{p}_1 - 1} \cdots \frac{\mathbf{p}_r^{\alpha_r+1} - 1}{\mathbf{p}_r - 1}.$$

**Demostración:** Ya que la función  $\mathbf{d} \mapsto \mathbf{d}$  es completamente multiplicativa es, a fortiori, multiplicativa. Luego  $\sigma(\mathbf{n}) = \sum_{\mathbf{d} | \mathbf{n}} \mathbf{d}$  es multiplicativa en virtud del Teorema 76. Si  $\mathbf{p}$  es primo,  $\mathbf{p}^\alpha$  tiene por suma de divisores la suma geométrica

$$\sigma(\mathbf{p}^\alpha) = 1 + \mathbf{p} + \mathbf{p}^2 + \cdots + \mathbf{p}^\alpha = \frac{\mathbf{p}^{\alpha+1} - 1}{\mathbf{p} - 1}.$$

Luego

$$\sigma(\mathbf{n}) = \sigma(\mathbf{p}_1^{\alpha_1}) \cdots \sigma(\mathbf{p}_r^{\alpha_r}) = \frac{\mathbf{p}_1^{\alpha_1+1} - 1}{\mathbf{p}_1 - 1} \cdots \frac{\mathbf{p}_r^{\alpha_r+1} - 1}{\mathbf{p}_r - 1}.$$

□

**82 Definición** Dado  $\mathbf{n} = \mathbf{p}_1^{\alpha_1} \cdots \mathbf{p}_r^{\alpha_r}$ , la función  $\omega : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$  cuenta cuántos primos distintos  $\mathbf{n}$  tiene sin contar factores repetidos, esto es  $\omega(\mathbf{n}) = r$ . La función  $\Omega : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$  cuenta cuántos primos distintos  $\mathbf{n}$  tiene incluyendo factores repetidos, esto es  $\Omega(\mathbf{n}) = \alpha_1 + \alpha_2 + \cdots + \alpha_r$ .



Es evidente que tanto  $\omega$  como  $\Omega$  son multiplicativas, aún más,  $\Omega$  es totalmente multiplicativa. También es evidente que  $\Omega(\mathbf{n}) \geq \omega(\mathbf{n})$  siempre y que  $\Omega(\mathbf{n}) = \omega(\mathbf{n})$  si y sólo si  $\mathbf{n}$  no tiene ningún factor cuadrado mayor que 1.

**83 Definición (Función de Möbius)** Sean  $\mathbf{p}, \mathbf{p}_1, \dots, \mathbf{p}_r$  primos distintos y  $\mathbf{n} > 0$  entero. La función

$$\mu : \mathbb{N} \setminus \{0\} \rightarrow \{-1, 0, 1\}$$

$$\mathbf{n} \mapsto \mu(\mathbf{n})$$

se define como sigue:

$$\mu(\mathbf{n}) = \begin{cases} 1 & \text{si } \mathbf{n} = 1 \\ (-1)^{\omega(\mathbf{n})} & \text{si } \omega(\mathbf{n}) = \Omega(\mathbf{n}) \\ 0 & \text{si } \Omega(\mathbf{n}) > \omega(\mathbf{n}) \end{cases}$$

**84 Teorema** La función de Möbius es multiplicativa.

**Demostración:** Sea  $\mathbf{n} = \mathbf{a}\mathbf{b}$ , con  $\text{MCD}(\mathbf{a}, \mathbf{b}) = 1$ . Si  $\mathbf{p} \in \mathbb{P}$  y  $\mathbf{p}^2 | \mathbf{n}$  entonces  $\mathbf{p}^2$  debe dividir o bien a  $\mathbf{a}$  o bien a  $\mathbf{b}$ . En todo caso  $\mu(\mathbf{n}) = \mu(\mathbf{a})\mu(\mathbf{b}) = 0$ . Si  $\mathbf{a} = \mathbf{p}_1 \cdots \mathbf{p}_r$ ,  $\mathbf{b} = \mathbf{q}_1 \cdots \mathbf{q}_s$  donde todas las  $\mathbf{p}$ 's y  $\mathbf{q}$ 's son diferentes, entonces

$$\mu(\mathbf{n}) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(\mathbf{a})\mu(\mathbf{b}),$$

de donde  $\mu$  es multiplicativa. □

**85 Teorema** Si  $n > 0$  es un entero,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{si } n>1 \end{cases}$$

**Demostración:** Póngase

$$A = \left( d|n : \omega(d) = k, p^2 \nmid d, p \in \mathbb{P} \right).$$

Entonces  $\#(A) = \binom{n}{k}$  y si  $d \in A$  se tiene  $\mu(d) = (-1)^k$ . La suma requerida es

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{\omega(n)} \binom{\omega(n)}{k} (-1)^k.$$

En virtud del Teorema del binomio,  $(1 - 1)^{\omega(n)} = 0$ .  $\square$

**86 Teorema (Fórmula de inversión de Möbius)** Sean  $f$  y  $F$  funciones aritméticas, en donde  $F(n) = \sum_{d|n} f(d)$ . Luego

$$f(n) = \sum_{d|n} \mu(d)F(n/d) = \sum_{d|n} \mu(n/d)F(d).$$

Recíprocamente, si  $f(n) = \sum_{d|n} \mu(d)F(n/d)$  para todo entero  $n > 0$ , entonces  $F(n) = \sum_{d|n} f(d)$ .

**Demostración:** Se tiene

$$\begin{aligned} \sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n} \sum_{d|n} \sum_{s|\frac{n}{d}} f(s) \\ &= \sum_{ds|n} \mu(d)f(s) \\ &= \sum_{s|n} f(s) \sum_{d|\frac{n}{s}} \mu(d). \end{aligned}$$

Gracias al Teorema 85, la suma interna es diferente de 0 sólo cuando  $\frac{n}{s} = 1$ . Así, el único término que sobrevive en la suma externa el de  $s = n$ , que simplifica a  $f(n)$ .

Recíprocamente, si

$$\begin{aligned}
 \sum_{\mathbf{d}|\mathbf{n}} \mathbf{f}(\mathbf{d}) &= \sum_{\mathbf{d}|\mathbf{n}} \sum_{\mathbf{s}|\mathbf{d}} \mu(\mathbf{s}) \mathbf{F}(\mathbf{d}/\mathbf{s}) \\
 &= \sum_{\mathbf{d}|\mathbf{n}} \sum_{\mathbf{s}|\mathbf{d}} \mu(\mathbf{d}/\mathbf{s}) \mathbf{F}(\mathbf{s}) \\
 &= \sum_{\mathbf{s}|\mathbf{n}} \sum_{\mathbf{r}|\frac{\mathbf{n}}{\mathbf{s}}} \mu(\mathbf{r}) \mathbf{F}(\mathbf{s}) \\
 &= \sum_{\mathbf{s}|\mathbf{n}} \mathbf{F}(\mathbf{s}) \sum_{\mathbf{r}|\frac{\mathbf{n}}{\mathbf{s}}} \mu(\mathbf{r}).
 \end{aligned}$$

Utilizando el Teorema 85, la suma interna será 0 a menos que  $\mathbf{s} = \mathbf{n}$ , en cuyo caso la suma simplifica a  $\mathbf{F}(\mathbf{n})$ .  $\square$

**87 Definición (Función indicatriz de Euler)** La función

$$\begin{aligned}
 \phi: \mathbb{N} \setminus \{0\} &\rightarrow \mathbb{N} \setminus \{0\} \\
 \mathbf{n} &\mapsto \phi(\mathbf{n})
 \end{aligned}$$

cuenta el número de enteros entre 1 y  $\mathbf{n}$  que son relativamente primos a  $\mathbf{n}$ :

$$\phi(\mathbf{n}) = \#\{\mathbf{k} : 1 \leq \mathbf{k} \leq \mathbf{n}, \text{MCD}(\mathbf{k}, \mathbf{n}) = 1\}.$$

**88 Teorema** Sea  $\mathbf{n} \geq 1$  entero. Entonces  $\sum_{\mathbf{d}|\mathbf{n}} \phi(\mathbf{d}) = \mathbf{n}$ .

**Demostración:** Para cada divisor  $\mathbf{d}$  de  $\mathbf{n}$ , sea  $\mathbf{T}_{\mathbf{d}}(\mathbf{n})$  el conjunto de enteros positivos  $\leq \mathbf{n}$  cuyo máximo común divisor con  $\mathbf{n}$  es  $\mathbf{d}$ . Tanto  $\mathbf{d}$  varía sobre los divisores de  $\mathbf{n}$ , los conjuntos  $\mathbf{T}_{\mathbf{d}}(\mathbf{n})$  forman una partición de  $\{1, 2, \dots, \mathbf{n}\}$  y por lo tanto

$$\sum_{\mathbf{d}|\mathbf{n}} \mathbf{T}_{\mathbf{d}}(\mathbf{n}) = \mathbf{n}.$$

Se demostrará de inmediato que  $\mathbf{T}_{\mathbf{d}}(\mathbf{n})$  posee  $\phi(\mathbf{n}/\mathbf{d})$  elementos. Obsérvese que los elementos de  $\mathbf{T}_{\mathbf{d}}(\mathbf{n})$  yacen en el conjunto  $\mathbf{d}, 2\mathbf{d}, \dots, \frac{\mathbf{n}}{\mathbf{d}}\mathbf{d}$ . Si  $\mathbf{k} \in \mathbf{T}_{\mathbf{d}}(\mathbf{n})$ , entonces  $\mathbf{k} = \mathbf{a}\mathbf{d}$ ,  $1 \leq \mathbf{a} \leq \mathbf{n}/\mathbf{d}$  y  $\text{MCD}(\mathbf{k}, \mathbf{n}) = \mathbf{d}$ . Pero entonces  $\text{MCD}\left(\frac{\mathbf{k}}{\mathbf{d}}, \frac{\mathbf{n}}{\mathbf{d}}\right) = 1$ , lo que implica que  $\text{MCD}\left(\mathbf{a}, \frac{\mathbf{n}}{\mathbf{d}}\right) = 1$ . Se deduce que contar los elementos de  $\mathbf{T}_{\mathbf{d}}(\mathbf{n})$  es equivalente a contar el número de enteros  $\mathbf{a}$  que satisface  $1 \leq \mathbf{a} \leq \mathbf{n}/\mathbf{d}$ ,  $\text{MCD}\left(\mathbf{a}, \frac{\mathbf{n}}{\mathbf{d}}\right) = 1$ . Pero el número de estos enteros es precisamente  $\phi(\mathbf{n}/\mathbf{d})$ . Colegimos que

$$\mathbf{n} = \sum_{\mathbf{d}|\mathbf{n}} \phi(\mathbf{n}/\mathbf{d}).$$

Pero en tanto  $\mathbf{d}$  varía sobre los divisores de  $\mathbf{n}$ ,  $\frac{\mathbf{n}}{\mathbf{d}}$  varía en reverso. Así pues  $\mathbf{n} = \sum_{\mathbf{d}|\mathbf{n}} \phi(\mathbf{n}/\mathbf{d}) = \sum_{\mathbf{d}|\mathbf{n}} \phi(\mathbf{d})$ , lo que

demuestra el teorema.  $\square$

**89 Corolario** Si  $n \geq 1$  es un entero,

$$\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

**Demostración:** Esto se deduce de inmediato en combinando el Teorema de inversión de Möbius (Teorema 86) y el Teorema 88.  $\square$

**90 Corolario** La función

$$\phi : \begin{array}{ccc} \mathbb{N} \setminus \{0\} & \rightarrow & \mathbb{N} \setminus \{0\} \\ n & \mapsto & \phi(n) \end{array}$$

es multiplicativa y si  $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$  es la descomposición canónica en primos de  $n$ , entonces

$$\phi(n) = \prod_{p|n} (p^\alpha - p^{\alpha-1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

**Demostración:** Combínese el Corolario 89 con el Teorema 76 para demostrar que  $\phi$  es multiplicativa. Por otra parte, si  $p$  es primo, hay  $p^{\alpha-1}$  enteros positivos  $\leq p^\alpha$  que tienen un factor común con  $p$ :  $1p, 2p, 3p, \dots, p^{\alpha-1}p$ . Por lo tanto  $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$  de donde resulta la segunda aseveración.  $\square$

## Tarea

**91 Problema** Demuéstrese que si  $n$  es compuesto entonces  $\phi(n) \leq n - \sqrt{n}$ . ¿Cuándo se verificará la igualdad?

**92 Problema (AIME, 1992)** Encuétrase la suma de todos los números racionales positivos que sean menores que 10 y tengan denominador 30 cuando se escriban en términos mínimos..

**93 Problema** Demuéstrese que  $\phi(n) \geq n2^{-\omega(n)}$ .

**94 Problema** Demuéstrese que  $\phi(n) > \sqrt{n}$  para  $n > 6$ .

**95 Problema** Demuéstrese que si  $\phi(n) \mid n$ , entonces  $n$  debe de ser de la forma  $2^a 3^b$  para enteros no negativos  $a, b$ .

**96 Problema** Demuéstrese que si  $\phi(n) \mid n - 1$ , entonces  $n$  no es divisible por ningún cuadrado mayor que 1.

**97 Problema (Mandelbrot 1994)** Cuatrocientas personas se colocan alrededor de un círculo. Se marca a una persona, se perdona a las próximas  $k$  personas, luego se marca a otra, se perdona a las próximas  $k$ , etcétera, continuando hasta que se marque a una persona por segunda vez. ¿Para cuántos valores de  $k$  menores que 400 se marcarán a todas las personas en el círculo al menos una vez?

**98 Problema** Demuéstrese que si  $\phi(n) \mid n - 1$  y  $n$  es compuesto, entonces  $n$  tiene al menos tres factores primos distintos.

**99 Problema** Demuéstrese que si  $\phi(n) \mid n - 1$  y  $n$  es compuesto, entonces  $n$  tiene al menos cuatro factores primos distintos.

**100 Problema** Describese todos los enteros positivos  $n$  para los cuales  $d(n) = 10$ .

**101 Problema** Demuéstrese que

$$d(2^n - 1) \geq d(n).$$

**102 Problema** Demuéstrese que  $d(n) \leq \sqrt{3n}$  verificándose la igualdad si y sólo si  $n = 12$ .

**103 Problema** Demuéstrese que se cumple la expansión

$$\sum_{n=1}^{\infty} d(n)t^n = \sum_{n=1}^{\infty} \frac{t^n}{1-t^n},$$

llamada *expansión de Lambert*.

**104 Problema** Póngase  $d_1(n) = d(n)$ ,  $d_k(n) = d(d_{k-1}(n))$ ,  $k = 2, 3, \dots$ . Descríbase  $d_k(n)$  para  $k$  lo suficientemente grande.

**105 Problema** Dado  $m \in \mathbb{N}$ , demuéstrese que el conjunto

$$\mathcal{A} = \{n \in \mathbb{N} : m \mid d(n)\}$$

posee una progresión aritmética infinita.

**106 Problema** Sea  $n$  un número perfecto. Demuéstrese que

$$\sum_{d \mid n} \frac{1}{d} = 2.$$

**107 Problema** Demuéstrese que

$$\prod_{d \mid n} d = n^{d(n)/2}.$$

**108 Problema (AIME 1995)** Sea  $n = 2^{31} 3^{19}$ . ¿Cuántos divisores positivos de  $n^2$  son menores que  $n$  pero no dividen a  $n$ ?

**109 Problema** Demuéstrese que si  $n$  es compuesto, entonces  $\sigma(n) > n + \sqrt{n}$ .

**110 Problema** Demuéstrese que la ecuación  $\sigma(n) = n + k$ , donde  $k > 1$  es un número natural fijo, posee un número finito de soluciones.

**111 Problema** Caracterícese todos los enteros positivos  $n$  para los cuales  $\sigma(n)$  es impar.

**112 Problema** Demuéstrese que  $p$  es primo si y solamente si  $\sigma(p) = 1 + p$ .

**113 Problema** Demuéstrese que

$$\frac{\sigma(n!)}{n!} \geq 1 + \frac{1}{2} + \dots + \frac{1}{n}.$$

**114 Problema** Demuéstrese que ninguna potencia de un primo no puede ser un número perfecto. Luego, demuéstrese que de existir un número perfecto impar, éste debe tener al menos dos factores primos distintos.

**115 Problema** Demuéstrese que si  $n$  es un número perfecto impar, entonces solamente uno de sus factores primos ocurre con potencia par.

**116 Problema** Demuéstrese que

$$\sum_{k=1}^n \sigma(k) = \sum_{j=1}^n j \left\lfloor \frac{n}{j} \right\rfloor.$$

**117 Problema** Hállese todos los conjuntos de enteros positivos  $\{a, b, c\}$  tales que  $a \times b \times c = 462$ .

### 3.2. La función parte entera

**118 Definición** Sea  $x \in \mathbb{R}$ . Llámase *suelo* de  $x$  (o *función mayor entero de  $x$* ) al único entero  $\lfloor x \rfloor$  que satisface

$$x - 1 < \lfloor x \rfloor \leq x.$$

Nótese que cada  $x \in \mathbb{R}$  puede escribirse como  $x = \lfloor x \rfloor + \{x\}$ , en donde  $0 \leq \{x\} < 1$  es la *parte fraccionaria* de  $x$ .

Análogamente, llámase *techo* de  $x$  (o *función menor entero de  $x$* ) al único entero  $\lceil x \rceil$  que satisface

$$x \leq \lceil x \rceil < x + 1$$

**119 Teorema** Sean  $(\alpha, \beta) \in \mathbb{R}^2$ ,  $a \in \mathbb{Z}$ ,  $n \in \mathbb{N} \setminus \{0\}$ . Entonces

1.  $\lfloor \alpha + a \rfloor = \lfloor \alpha \rfloor + a$
2.  $\left\lfloor \frac{\alpha}{n} \right\rfloor = \left\lfloor \frac{\lfloor \alpha \rfloor}{n} \right\rfloor$
3.  $\lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \lfloor \alpha + \beta \rfloor \leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 1$

**Demostración:** Se demostrará cada inciso individualmente.

1. Sea  $m = \lfloor \alpha + a \rfloor$ . Entonces  $m \leq \alpha + a < m + 1$ . De aquí  $m - a \leq \alpha < m - a + 1$ . Esto significa que  $m - a = \lfloor \alpha \rfloor$ , completando la demostración de este inciso.
2. Póngase  $\alpha/n = \lfloor \alpha/n \rfloor + \theta$ ,  $0 \leq \theta < 1$ . Como  $n\lfloor \alpha/n \rfloor$  es un entero, se deduce del inciso 1 que

$$\lfloor \alpha \rfloor = \lfloor n\lfloor \alpha/n \rfloor + n\theta \rfloor = n\lfloor \alpha/n \rfloor + \lfloor n\theta \rfloor.$$

Ahora bien,  $0 \leq \lfloor n\theta \rfloor \leq n\theta < n$ , y por lo tanto,  $0 \leq \lfloor n\theta \rfloor/n < 1$ . Si  $\Theta = \lfloor n\theta \rfloor/n$ , entonces se obtiene

$$\frac{\lfloor \alpha \rfloor}{n} = \left\lfloor \frac{\alpha}{n} \right\rfloor + \Theta, \quad 0 \leq \Theta < 1,$$

demostrando este inciso.

3. De las desigualdades

$$\alpha - 1 < \lfloor \alpha \rfloor \leq \alpha, \quad \beta - 1 < \lfloor \beta \rfloor \leq \beta$$

se obtiene  $\alpha + \beta - 2 < \lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \alpha + \beta$ . Ya que  $\lfloor \alpha \rfloor + \lfloor \beta \rfloor$  es un entero  $\leq \alpha + \beta$ , entonces será  $\leq \lfloor \alpha + \beta \rfloor$ . De aquí se colige que  $\lfloor \alpha \rfloor + \lfloor \beta \rfloor \leq \lfloor \alpha + \beta \rfloor$ . Además  $\alpha + \beta$  es  $\leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 2$ , de donde su parte íntegra  $\lfloor \alpha + \beta \rfloor$  deberá ser  $\leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 2$ , pero como  $\lfloor \alpha + \beta \rfloor < \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 2$  entonces se tiene  $\lfloor \alpha + \beta \rfloor \leq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + 1$ , demostrando las desigualdades.

□

**120 Teorema (Formula de De Polignac)** La máxima potencia del primo  $p$  que divide a  $n!$  está dada por

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

**Demostración:** El número de factores contribuyendo un factor de  $p$  es  $\lfloor n/p \rfloor$ , el número de factores contribuyendo un segundo factor de  $p$  es  $\lfloor n/p^2 \rfloor$ , etc.  $\square$

**121 Teorema** Si  $a, b$  son relativamente primos, entonces

$$\sum_{k=1}^{a-1} \left\lfloor \frac{kb}{a} \right\rfloor = \sum_{k=1}^{b-1} \left\lfloor \frac{ka}{b} \right\rfloor = \frac{(a-1)(b-1)}{2}.$$

**Demostración:** Considérese el rectángulo con vértices en  $(0,0), (0,b), (a,0), (a,b)$ . Este rectángulo contiene  $(a-1)(b-1)$  puntos cuyas coordenadas son ambas enteras. El rectángulo se divide en dos partes gracias a la recta  $y = \frac{xb}{a}$ . Se demostrará que no hay puntos de coordenadas ambas enteras sobre esta recta, a excepción de los extremos. Si hubiese puntos de coordenadas enteras  $(m,n), 0 < m < a, 0 < n < b$ , entonces  $\frac{n}{m} = \frac{b}{a}$ . Luego  $n/m$  es una fracción reducida de la fracción irreducible  $b/a$ , contradicción. Los puntos  $L_k = (k, \frac{kb}{a}), 1 \leq k \leq a-1$  están sobre esta recta. Ahora bien,  $\lfloor \frac{kb}{a} \rfloor$  es el número de puntos de coordenadas enteras sobre la recta vertical que va desde  $(k,0)$  hasta  $(k, \frac{kb}{a})$ , esto es,  $\sum_{k=1}^{a-1} \lfloor \frac{kb}{a} \rfloor$ , que es el número de puntos con coordenadas enteras en la parte inferior del rectángulo. De igual manera,  $\sum_{k=1}^{b-1} \lfloor \frac{ka}{b} \rfloor$  cuenta el número de puntos con coordenadas enteras en la parte superior del rectángulo. Como hay  $(a-1)(b-1)$  puntos de coordenadas enteras en total, y su número es compartido de manera igual por ambas partes, queda demostrado el teorema.  $\square$

**122 Definición** Llámase *espectro* de un número real  $\alpha$  a la sucesión infinita

$$\mathbf{Esp}(\alpha) = \{\lfloor \alpha \rfloor, \lfloor 2\alpha \rfloor, \lfloor 3\alpha \rfloor, \dots\}.$$

Dos sucesiones  $\mathbf{Esp}(\alpha)$  y  $\mathbf{Esp}(\beta)$  se dicen *complementarias* si hacen una partición de los números naturales no nulos, esto es,  $\mathbf{Esp}(\alpha) \cap \mathbf{Esp}(\beta) = \emptyset$  y  $\mathbf{Esp}(\alpha) \cup \mathbf{Esp}(\beta) = \mathbb{N}$ .

Demostrarase más adelante que las sucesiones

$$\mathbf{Esp}(\sqrt{2}) = \{1, 2, 4, 5, 7, 8, 9, 11, 12, 14, 15, 16, 18, 19, 21, 22, 24, 25, \dots\},$$

y

$$\mathbf{Esp}(2 + \sqrt{2}) = \{3, 6, 10, 13, 17, 20, 23, 27, 30, 34, 37, 40, 44, 47, 51, \dots\}$$

son complementarias.

**123 Teorema (Teorema de Beatty, 1926)** Si  $\alpha > 1$  es irracional y

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1,$$

entonces las sucesiones

$$\mathbf{Esp}(\alpha) \text{ y } \mathbf{Esp}(\beta)$$

son complementarias.

**Demostración:** Ya que  $\alpha > 1, \beta > 1$ ,  $\text{Esp}(\alpha)$  y  $\text{Esp}(\beta)$  son ambas sucesiones de términos distintos y el total de términos no excediendo  $N$  en una y otra sucesión es  $\lfloor N/\alpha \rfloor + \lfloor N/\beta \rfloor$ . Pero

$$N/\alpha - 1 + N/\beta - 1 < \lfloor N/\alpha \rfloor + \lfloor N/\beta \rfloor < N/\alpha + N/\beta,$$

siendo la última desigualdad estricta ya que ambos  $\alpha, \beta$  son irracionales. Como  $1/\alpha + 1/\beta = 1$ , se deduce que  $N - 2 < \lfloor N/\alpha \rfloor + \lfloor N/\beta \rfloor < N$ . Como la cantidad emparedada es entera, se deduce que

$$\lfloor N/\alpha \rfloor + \lfloor N/\beta \rfloor = N - 1.$$

Así, la cantidad total de términos que no exceden a  $N$  en  $\text{Esp}(\alpha)$  y  $\text{Esp}(\beta)$  es  $N - 1$ . Como esto es cierto para cada  $N \geq 1$ , cada intervalo  $(n, n + 1)$  contiene exactamente uno de los términos de  $\text{Esp}(\alpha)$  y  $\text{Esp}(\beta)$ . Se sigue que  $\text{Esp}(\alpha) \cup \text{Esp}(\beta) = \mathbb{N}, \text{Esp}(\alpha) \cap \text{Esp}(\beta) = \emptyset$ .

□

Se observa también un resultado en la dirección opuesta.

**124 Teorema (Teorema de Bang, 1957)** Si las sucesiones

$$\text{Spec}(\alpha) \text{ y } \text{Spec}(\beta)$$

son complementarias, entonces  $\alpha, \beta$  son números irracionales positivos que satisfacen

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1.$$

**Demostración:** Si ambos  $\alpha, \beta$  fueren números racionales, entonces eventualmente  $\text{Spec}(\alpha), \text{Spec}(\beta)$  contendrían los mismos enteros, y por lo tanto no serían disjuntas. Así pues,  $\alpha$  y  $\beta$  son irracionales. Si  $0 < \alpha \leq 1$ , dado  $n$  entonces existe  $m$  para el cual  $m\alpha - 1 < n \leq m\alpha$ ; luego  $n = \lfloor m\alpha \rfloor$ , lo que implica que  $\text{Spec}(\alpha) = \mathbb{N}$ , de donde  $\alpha > 1$  (y con esto también  $\beta > 1$ ). Si la intersección  $\text{Spec}(\alpha) \cap \text{Spec}(\beta)$  fuese finita, entonces

$$\lim_{n \rightarrow \infty} \frac{\lfloor n/\alpha \rfloor + \lfloor n/\beta \rfloor}{n} = 1,$$

pero entonces  $(\lfloor n/\alpha \rfloor + \lfloor n/\beta \rfloor) \frac{1}{n} \rightarrow 1/\alpha + 1/\beta$  ya que  $n \rightarrow \infty$ , se colige que  $1/\alpha + 1/\beta = 1$ . □

**125 Ejemplo** Hállese un polinomio no idénticamente nulo  $P(x, y)$  tal que para todo número real  $t$  se tenga  $P(\lfloor 2t \rfloor, \lfloor 3t \rfloor) = 0$ .

**Resolución:** Comprobarse que  $3\lfloor 2t \rfloor - 2\lfloor 3t \rfloor = 0, \pm 1$  o  $-2$ . Luego entonces se podrá elegir

$$P(x, y) = (3x - 2y)(3x - 2y - 1)(3x - 2y + 1)(3x - 2y + 2).$$

Para verificar la aserción, obsérvese que como  $\lfloor x \rfloor$  tiene período unitario, es suficiente comprobar la aserción para  $t \in [0; 1[$ . Divídase  $[0; 1[$  así

$$[0; 1[ = [0; 1/3[ \cup [1/3; 1/2[ \cup [1/2; 2/3[ \cup [2/3; 1[.$$

Si  $t \in [0; 1/3[$ , entonces tanto  $\lfloor 2t \rfloor$  como  $\lfloor 3t \rfloor$  son  $= 0$ , y así  $3\lfloor 2t \rfloor - 2\lfloor 3t \rfloor = 0$ . Si  $t \in [1/3; 1/2[$  entonces  $\lfloor 3t \rfloor = 1$  y  $\lfloor 2t \rfloor = 0$ , y así  $3\lfloor 2t \rfloor - 2\lfloor 3t \rfloor = -2$ . Si  $t \in [1/2; 2/3[$ , luego  $\lfloor 2t \rfloor = 1, \lfloor 3t \rfloor = 1$ , dando  $3\lfloor 2t \rfloor - 2\lfloor 3t \rfloor = 1$ . Si  $t \in [2/3; 1[$ , se tendrá  $\lfloor 2t \rfloor = 1, \lfloor 3t \rfloor = 2$ , y  $3\lfloor 2t \rfloor - 2\lfloor 3t \rfloor = -1$ .

**126 Ejemplo** Descríbase todos los enteros positivos  $n$  para los cuales  $1 + \lfloor \sqrt{2n} \rfloor \mid 2n$ .

**Resolución:** Sea  $2n = m(1 + \lfloor \sqrt{2n} \rfloor)$ . Si  $m \leq \lfloor \sqrt{2n} \rfloor - 1$  entonces  $2n \leq (\lfloor \sqrt{2n} \rfloor - 1)(\lfloor \sqrt{2n} \rfloor + 1) = \lfloor \sqrt{2n} \rfloor^2 - 1 \leq 2n - 1 < 2n$ , contradicción. Si  $m \geq \lfloor \sqrt{2n} \rfloor + 1$ , entonces  $2n \geq (\lfloor \sqrt{2n} \rfloor + 1)^2 \geq 2n + 1$ , otra contradicción. Por lo tanto se debe tener  $m = \lfloor \sqrt{2n} \rfloor$ .

Recíprocamente, sea  $n = \frac{l(l+1)}{2}$ . Ya que  $l < \sqrt{2n} < l+1$ , se tiene  $l = \lfloor \sqrt{2n} \rfloor$ . Luego todos los enteros con la propiedad deseada son números triangulares.

**127 Ejemplo** Demuéstrese que la sucesión de enteros

$$\lfloor (1 + \sqrt{2})^n \rfloor$$

donde  $n$  es un entero no negativo, es alternadamente par e impar.

**Resolución:** En virtud del teorema del binomio,

$$(1 + \sqrt{2})^n + (1 - \sqrt{2})^n = 2 \sum_{0 \leq k \leq n/2} (2)^k \binom{n}{2k} := 2N,$$

un número par. Como  $-1 < 1 - \sqrt{2} < 0$ , entonces  $(1 - \sqrt{2})^n$  es la parte fraccionaria de  $(1 + \sqrt{2})^n$  o de  $(1 + \sqrt{2})^n + 1$  dependiendo de la paridad de  $n$ . Para  $n$  impar,

$$(1 + \sqrt{2})^n - 1 < (1 + \sqrt{2})^n + (1 - \sqrt{2})^n < (1 + \sqrt{2})^n,$$

de donde  $(1 + \sqrt{2})^n + (1 - \sqrt{2})^n = \lfloor (1 + \sqrt{2})^n \rfloor$ , que es siempre par, y para  $n$  par  $2N := (1 + \sqrt{2})^n + (1 - \sqrt{2})^n = \lfloor (1 + \sqrt{2})^n \rfloor + 1$ , y así  $\lfloor (1 + \sqrt{2})^n \rfloor = 2N - 1$ , es siempre impar para  $n$  par.

**128 Ejemplo** Demuéstrese que los primeros mil dígitos de

$$(6 + \sqrt{35})^{1980}$$

luego del punto decimal son todos 9's.

**Resolución:** Gracias al ejemplo 127,

$$(6 + \sqrt{35})^{1980} + (6 - \sqrt{35})^{1980} = 2k,$$

es un entero par. Ahora bien,  $0 < 6 - \sqrt{35} < 1/10$  (si no  $\frac{1}{10} < 6 - \sqrt{35}$ , y al cuadrar  $3500 < 3481$ , contradicción) y luego  $0 < (6 - \sqrt{35})^{1980} < 10^{-1980}$ . Se deduce que

$$2k - 1 + \underbrace{0,9\dots9}_{1979 \text{ nines}} = 2k - \frac{1}{10^{1980}} < (6 + \sqrt{35})^{1980} < 2k,$$

demonstrando la aserción.

**129 Ejemplo (Putnam 1948)** Si  $n$  es un entero positivo, demuéstrese que

$$\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor.$$

**Resolución:** Elevando al cuadrado se ve que

$$\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+3}.$$

Ni  $4n+2$  ni  $4n+3$  son cuadrados, ya que todo cuadrado es congruente a 0 o 1 módulo 4, luego

$$\lfloor \sqrt{4n+2} \rfloor = \lfloor \sqrt{4n+3} \rfloor,$$

de donde se colige el resultado.

**130 Ejemplo** Hállese una fórmula para el  $n$ -ésimo entero positivo no cuadrado.

**Resolución:** Sea  $T_n$  el  $n$ -ésimo entero positivo no cuadrado. Luego, existe un número entero positivo  $m$  tal que  $m^2 < T_n < (m+1)^2$ . Ya que hay  $m$  cuadrados menores que  $T_n$  se tiene que  $T_n = n + m$ . Entonces se ve que

$$m^2 < n + m < (m+1)^2$$

o sea

$$m^2 - m < n < m^2 + m + 1.$$

Como  $n, m^2 - m, m^2 + m + 1$  son todos enteros, las desigualdades anteriores implican que

$$m^2 - m + \frac{1}{4} < n < m^2 + m + \frac{1}{4},$$

esto es,  $(m - 1/2)^2 < n < (m + 1/2)^2$ . Pero entonces  $m = \lfloor \sqrt{n} + 1/2 \rfloor$ . Luego el  $n$ -ésimo entero positivo no cuadrado es  $T_n = n + \lfloor \sqrt{n} + 1/2 \rfloor$ .

**131 Ejemplo (Putnam 1983)** Sea  $f(n) = n + \lfloor \sqrt{n} \rfloor$ . Demuéstrese que para cada entero positivo  $m$ , la sucesión

$$m, f(m), f(f(m)), f(f(f(m))), \dots$$

tiene al menos el cuadrado de un entero.

**Resolución:** Sea  $m = k^2 + j, 0 \leq j \leq 2k$ . Divídase las  $m$ 's en dos grupos: aquéllas (grupo **A**) para las que  $j, 0 \leq j \leq k$  y éstas (grupo **B**) para las que  $j, k < j \leq 2k + 1$ .

Obsérvese que  $k^2 \leq m < (k+1)^2 = k^2 + 2k + 1$ . Si  $j = 0$ , no hay nada que demostrar. Supóngase primero que  $m \in \mathbf{B}$ . Como  $\lfloor \sqrt{m} \rfloor = k$ , se tiene  $f(m) = k^2 + j + k = (k+1)^2 + j - k - 1$ , con  $0 \leq j - k - 1 \leq k - 1 < k + 1$ . Esto quiere decir que  $f(m)$  o bien es un cuadrado, o bien  $f(m) \in \mathbf{A}$ . Así pues, es sólo necesario considerar la alternativa  $m \in \mathbf{A}$ , en cuyo caso  $\lfloor \sqrt{m+k} \rfloor = k$  y

$$f(f(m)) = f(m+k) = m + 2k = (k+1)^2 + j - 1.$$

Esto significa que o bien  $f(f(m))$  es un cuadrado, o bien  $f(f(m)) \in \mathbf{A}$  con un exceso  $j - 1$  menor que el exceso  $j$  de  $m$ . Luego de cada iteración el exceso se reduce, y eventualmente será cero, en cuyo caso se obtendrá un cuadrado.

**132 Ejemplo** Resuélvase la ecuación

$$\lfloor x^2 - x - 2 \rfloor = \lfloor x \rfloor,$$

para  $x \in \mathbb{R}$ .

**Resolución:** Obsérvese que  $\lfloor a \rfloor = \lfloor b \rfloor$  si y sólo si  $\exists k \in \mathbb{Z}$  with  $a, b \in [k, k+1)$ , lo que sucede si y sólo si  $|a - b| < 1$ . Luego, la ecuación dada tendrá solución si y solamente si  $|x^2 - 2x - 2| < 1$ , de donde el conjunto solución es

$$\left\{ x \in \mathbb{R} : x \in ]-1 : \frac{1}{2}(1 - \sqrt{5})] \cup \left[ \frac{1}{2}(1 + \sqrt{17}), \frac{1}{2}(1 + \sqrt{21})[ \right\}.$$

**133 Ejemplo** Encuéntrese la parte entera

$$\sum_{k=1}^{10^6} \frac{1}{\sqrt{k}}.$$

**Resolución:** La función  $x \mapsto x^{-1/2}$  es decreciente. Luego, para todo entero positivo  $k$ ,

$$\frac{1}{\sqrt{k+1}} < \int_k^{k+1} \frac{dx}{\sqrt{x}} < \frac{1}{\sqrt{k}}.$$

Sumando de  $k = 1$  hasta  $k = 10^6 - 1$  se deduce que

$$\sum_{k=2}^{10^6} \frac{1}{\sqrt{k}} < \int_1^{10^6} \frac{dx}{\sqrt{x}} < \sum_{k=1}^{10^6-1} \frac{1}{\sqrt{k}}.$$

Se verifica fácilmente que la integral es 1998. Luego

$$1998 + 1/10^3 < \sum_{k=1}^{10^6} \frac{1}{\sqrt{k}} < 1999.$$

La parte entera es así 1998.

**134 Ejemplo** ¿En cuántos ceros termina  $300!$ ?

**Resolución:** El número de ceros queda determinado por la potencia mayor de 10 que divida a  $300!$ . Ya que abundan más los múltiplos de 2 en  $300!$  que los múltiplos de 5, el número de ceros queda determinado por la potencia mayor de 5 que divida a  $300!$ . En virtud de la fórmula de De Polignac, la buscada potencia es

$$\sum_{k=1}^{\infty} \ll 300/5^k \rrbracket = 60 + 12 + 2 = 74.$$

**135 Ejemplo** ¿Divide 7 a  $\binom{1000}{500}$ ?

**Resolución:** La potencia mayor de 7 que divide a  $1000!$  es  $\ll 1000/7 \rrbracket + \ll 1000/7^2 \rrbracket + \ll 1000/7^3 \rrbracket = 142 + 20 + 2 = 164$ , gracias a la fórmula de De Polignac (teorema 120). De manera semejante, la potencia mayor de 7 que divide a  $500!$  es  $71 + 10 + 1 = 82$ . Ya que  $\binom{1000}{500} = \frac{1000!}{(500!)^2}$ , la potencia mayor de 7 que divide a  $\binom{1000}{500}$  es  $164 - 2 \cdot 82 = 0$ , de donde se colige que el 7 no divide a  $\binom{1000}{500}$ .

**136 Ejemplo** Sea  $n = n_1 + n_2 + \dots + n_k$  donde los  $n_i$  son enteros no negativos. Demuéstrese que la cantidad

$$\frac{n!}{n_1! n_2! \dots n_k!}$$

es entera.

**Resolución:** Por 3 del teorema 119 se deduce mediante inducción que

$$\ll \mathbf{a}_1 \rrbracket + \ll \mathbf{a}_2 \rrbracket + \dots + \ll \mathbf{a}_k \rrbracket \leq \ll \mathbf{a}_1 + \mathbf{a}_2 + \dots + \mathbf{a}_k \rrbracket.$$

Por la fórmula de De Polignac (teorema 120) la potencia de un primo  $p$  que divide a  $n!$

$$\sum_{j \geq 1} \ll n/p^j \rrbracket = \sum_{j \geq 1} \ll (n_1 + n_2 + \dots + n_k)/p^j \rrbracket.$$

Luego la potencia de  $p$  que divide a  $n_1! n_2! \dots n_k!$  es

$$\sum_{j \geq 1} \ll n_1/p^j \rrbracket + \ll n_2/p^j \rrbracket + \dots + \ll n_k/p^j \rrbracket.$$

Ya que

$$\ll n_1/p^j \rrbracket + \ll n_2/p^j \rrbracket + \dots + \ll n_k/p^j \rrbracket \leq \ll (n_1 + n_2 + \dots + n_k)/p^j \rrbracket,$$

se colige que la potencia de cualquier primo que divida al numerador de

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

es al menos tan grande como la potencia del mismo primo que divida al denominador. Esto demuestra la aserción.

**137 Ejemplo** Dado un entero  $n > 3$ , demuéstrese que el mínimo común múltiplo de los productos,  $x_1x_2\cdots x_k$  ( $k \geq 1$ ), cuyos factores  $x_i$  son enteros positivos satisfaciendo

$$x_1 + x_2 + \cdots + x_k \leq n,$$

es menor que  $n!$ .

**Resolución:** Se demostrará que el mínimo común múltiplo en cuestión es

$$\prod_{\substack{p \\ p \text{ primo}}} p^{\lfloor n/p \rfloor}.$$

Considérese un producto arbitrario  $x_1x_2\cdots x_k$ , y un primo arbitrario  $p$ . Supóngase que  $p^{\alpha_j}$  divide a  $x_j$  pero que  $p^{\alpha_j+1}$  no divide a  $x_j$ . Claramente,  $p^{\alpha_1} + \cdots + p^{\alpha_k} \leq n$  y como  $p^\alpha \geq \alpha p$ , se tiene

$$p(\alpha_1 + \cdots + \alpha_k) \leq n \text{ o } \alpha_1 + \cdots + \alpha_k \leq \left\lfloor \frac{n}{p} \right\rfloor.$$

Luego, se sigue que el exponente de un primo arbitrario dividiendo el mínimo común múltiplo  $p$  es a lo sumo  $\lfloor n/p \rfloor$ . Pero en tomando  $x_1 = \cdots = x_k = p$ ,  $k = \lfloor n/p \rfloor$ , se observa que para al menos un producto se consigue la igualdad. Esto demuestra la aserción.

**138 Ejemplo** Supóngase que se criba los enteros positivos de la manera siguiente: se toma  $a_1 = 1$  y se deja  $a_1 + 1 = 2$ . El próximo término es 3, al que se llamará  $a_2$  y tomará, y luego se dejará  $a_2 + 2 = 5$ . El próximo entero disponible es 4 =  $a_3$ , y luego se dejará  $a_3 + 3 = 7$ , etc. Así se tomará los enteros 1, 3, 4, 6, 8, 9, 11, 12, 14, 16, 17, ... Encuéntrese una fórmula para  $a_n$ .

**Resolución:** Se pide una sucesión  $\{S_n\}$  complementaria a  $\{S_n + n\}$ . Por el teorema de Beatty (teorema 123),  $\lfloor n\tau \rfloor$  y  $\lfloor n\tau \rfloor + n = \lfloor n(\tau + 1) \rfloor$  son complementarias si  $1/\tau + 1/(\tau + 1) = 1$ . Pero luego  $\tau = (1 + \sqrt{5})/2$ , la razón dorada. El enésimo término es pues  $a_n = \lfloor n\tau \rfloor$ .

## Tarea

# Capítulo 4

## Congruencias

### 4.1. Congruencias

**139 Definición (Congruencias)** Sean  $n \geq 1$ ,  $a, b$  enteros. Dícese que  $a \equiv b \pmod{n}$  (léase “ $a$  es congruente a  $b$  módulo  $n$ ”) si  $a$  y  $b$  dejan el mismo residuo al ser divididos por  $n$ , o, equivalentemente, si  $n \mid (a - b)$ .

**140 Teorema (Propiedades de las congruencias)** Sean  $n \geq 1$ ,  $a, b, c, d$  enteros. Si  $a \equiv b \pmod{n}$  y si  $c \equiv d \pmod{n}$  entonces

❶  $a + c \equiv b + d \pmod{n}$ ,

❷  $ac \equiv bd \pmod{n}$ .

**Demostración:** Se tiene  $n \mid (a - b)$  y  $n \mid (c - d)$ . Luego hay enteros  $u, v$  con  $nu = a - b$  y  $nv = c - d$ . Así

$$\begin{aligned} (a + c) - (b + d) &= n(u + v) \implies n \mid ((a + c) - (b + d)) \\ &\implies a + c \equiv b + d \pmod{n}, \end{aligned}$$

y además

$$\begin{aligned} ac - bd &= a(d + nv) \\ -d(a - nu) &= n(av + du) \implies n \mid (ac - bd) \\ &\implies ac \equiv bd \pmod{n}, \end{aligned}$$

de donde se obtiene el teorema.  $\square$

**141 Corolario** Si  $j \geq 1$  es entero y si  $a \equiv b \pmod{n}$  entonces  $a^j \equiv b^j \pmod{n}$ .

**Demostración:** Basta utilizar inducción en el segundo inciso del Teorema 140, poniendo  $c = a^{j-1}$  y  $d = b^{j-1}$ .  $\square$

**142 Corolario** Si

$$p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

es polinomio cuyos coeficientes son todos enteros y si  $a \equiv b \pmod{n}$  entonces  $p(a) \equiv p(b) \pmod{n}$ .

**Demostración:** Utilícese el Corolario 141 para demostrar que  $\alpha_i a^i \equiv \alpha_i b^i \pmod{n}$  y súmese cada término.  $\square$

**143 Teorema** Sean  $a, b, n$  enteros. Si la congruencia  $ax \equiv b \pmod n$  posee al menos una solución, entonces tiene exactamente  $(a, n)$  soluciones incongruentes  $\pmod n$ .

**Demostración:** Del teorema 71, todas las soluciones de la ecuación diofántica  $ax + ny = b$  son de la forma  $x = x_0 + nt/d, y = y_0 - at/d, d = (a, n), t \in \mathbb{Z}$ , en donde  $x_0, y_0$  satisfacen  $ax_0 + ny_0 = b$ . Dejando que  $t$  corra por los valores  $t = 0, 1, \dots, (a, n) - 1$ , se obtiene  $(a, n)$  soluciones que son mutuamente incongruentes, ya que el valor absoluto de la diferencia de cualesquiera dos de ellas es menor que  $n$ . Si  $x = x_0 + nt'/d$  es cualquier otra solución, se escribe  $t'$  como  $t' = qd + r, 0 \leq r < d$ . Entonces

$$\begin{aligned} x &= x_0 + n(qd + r)/d \\ &= x_0 + nq + nr/d \\ &\equiv x_0 + nr/d \pmod n. \end{aligned}$$

Luego, toda solución de la congruencia  $ax \equiv b \pmod n$  es congruente  $\pmod n$  a uno y solamente uno de los  $d$  valores  $x_0 + nt/d, 0 \leq t \leq d - 1$ . Quiérese decir que si existiese una solución de la congruencia, entonces existirán  $d$  soluciones incongruentes  $\pmod n$ .  $\square$

**144 Teorema** Sean  $x, y$  enteros y sean  $a, n$  enteros diferentes de cero. Entonces

$$ax \equiv ay \pmod n$$

si y sólo si

$$x \equiv y \pmod{\frac{n}{(a, n)}}.$$

**Demostración:** Si  $ax \equiv ay \pmod n$  entonces  $a(x - y) = sn$  para algún entero  $s$ . Esto implica que

$$(x - y) \frac{a}{(a, n)} = s \frac{n}{(a, n)}.$$

Ya que  $(a/(a, n), n/(a, n)) = 1$ , se deduce que

$$\frac{n}{(a, n)} | (x - y),$$

gracias al lema de Euclides (lema 56). Esto implica que

$$x \equiv y \pmod{\frac{n}{(a, n)}}.$$

Recíprocamente, si se tiene  $x \equiv y \pmod{\frac{n}{(a, n)}}$  entonces se tendrá

$$ax \equiv ay \pmod{\frac{an}{(a, n)}},$$

en multiplicando por  $a$ . Como  $(a, n)$  divide a  $a$ , la congruencia anterior implica, a fortiori que  $ax - ay = tn$  para algún entero  $t$ . Esto termina la demostración.  $\square$

**145 Corolario** Si  $ax \equiv ay \pmod n$  y  $(a, n) = 1$ , entonces  $x \equiv y \pmod n$ .

**146 Ejemplo** Demuéstrese que 7 divide a  $2222^{5555} + 5555^{2222}$  utilizando congruencias. Esta pregunta se vió ya en el problema 39.

**Resolución:**  $2222 \equiv 3 \pmod 7, 5555 \equiv 4 \pmod 7$  y  $3^5 \equiv 5 \pmod 7$ . Ahora bien,  $2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv (3^5)^{1111} + (4^2)^{1111} \equiv 5^{1111} - 5^{1111} \equiv 0 \pmod 7$ , lo que demuestra la aserción.

**147 Ejemplo** Hallése el residuo cuando  $6^{1987}$  es dividido por 37.

**Resolución:**  $6^2 \equiv -1 \pmod{37}$ . Así pues,  $6^{1987} \equiv 6 \cdot 6^{1986} \equiv 6(6^2)^{993} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \pmod{37}$ .

**148 Ejemplo** Encuéntrese todas las soluciones de  $5x \equiv 3 \pmod{7}$

**Resolución:** De acuerdo al teorema 143 existe una solución única a la congruencia  $\pmod{7}$  por ser  $(5, 7) = 1$ . Gracias al algoritmo de Euclides,

$$\begin{aligned} 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Así,

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ 2 &= 7 - 5 \cdot 1, \end{aligned}$$

dando

$$1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5 \cdot 1) = 5 \cdot 3 - 7 \cdot 2.$$

De aquí,  $3 = 5(9) - 7(6)$ . De ésto resulta que  $5 \cdot 9 \equiv 3 \pmod{7}$ , o sea,  $5 \cdot 2 \equiv 3 \pmod{7}$ . Así pues  $x \equiv 2 \pmod{7}$ .

**149 Ejemplo** Resuélvase la congruencia

$$3x \equiv 6 \pmod{12}.$$

**Resolución:** Como  $(3, 12) = 3$  y  $3|6$ , la congruencia tiene tres soluciones incongruentes. Por inspección  $x = 2$  es na solución. En virtud del teorema 71, todas las soluciones son de la forma  $x = 2 + 4t$ ,  $t \in \mathbb{Z}$ . Poniendo  $t = 0, 1, 2$ , se obtienen las tres soluciones incongruentes  $t = 2, 6, 10$  módulo 12.

**150 Ejemplo (USAMO, 1979)** Determinése todas las soluciones no negativas

$$(n_1, n_2, \dots, n_{14})$$

de la ecuación diofántica

$$n_1^4 + n_2^4 + \dots + n_{14}^4 = 1599$$

de haberlas.

**Resolución:** No hay tales soluciones. Todas las cuartas potencias  $\pmod{16}$  son o bien  $\equiv 0$  o bien  $\equiv 1 \pmod{16}$ . Esto significa que

$$n_1^4 + \dots + n_{14}^4$$

es a lo sumo  $14 \pmod{16}$ . Pero  $1599 \equiv 15 \pmod{16}$ .

## Tarea

**151 Problema** Hallése el último dígito de  $3^{100}$ .

**152 Problema** Hallése el dígito de las unidades de  $7^{7^7}$ .

**153 Problema** Compruébese que 7 divide a  $3^{2n+1} + 2^{n+2}$  para todo número entero  $n > 0$ .

**154 Problema (Olimpiada polaca)** ¿Qué dígitos debe substituirse por  $a$  y  $b$  en  $30a0b03$  de tal manera que el entero resultante sea divisible por 13 ?

**155 Problema** Compruébese que la ecuación  $x^2 - 5y^2 = 2$  no tiene soluciones enteras.

**156 Problema** Compruébese la siguiente observación de Euler:  $2^{32} + 1$  es divisible por 641.

**157 Problema** Hallése un número infinito de enteros  $n$  tal que  $2^n + 27$  sea divisible por 7.

**158 Problema** ¿Existe acaso enteros positivos  $x, y$  tal que  $x^3 = 2y + 15$ ?

**159 Problema** Compruébese que  $2^k - 5, k = 0, 1, 2, \dots$  nunca deja residuo 1 cuando es dividido por 7.

## 4.2. Sistemas residuales completos y reducidos

**160 Definición** Si  $a \equiv b \pmod{n}$  entonces  $b$  es llamado un *residuo* de  $a$  módulo  $n$ . Un conjunto

$$\{a_1, a_2, \dots, a_n\}$$

es llamado un *sistema completo de residuos* módulo  $n$  si para cada entero  $b$  existe exactamente uno índice  $j$  para el cual  $b \equiv a_j \pmod{n}$ . En particular, al conjunto  $\{0, 1, \dots, n-1\}$  se le llama *conjunto canónico de residuos* módulo  $n$ .

**161 Definición** Sea  $n > 1$ . Los  $\phi(n)$  enteros

$$1 = a_1 < a_2 < \dots < a_{\phi(n)} = n-1$$

menores que  $n$  y relativamente primos a  $n$  reciben el nombre de *residuos canónicos reducidos* módulo  $n$ .

**162 Definición** Sea  $n > 1$  un entero. Un entero  $b$  es llamado *inverso multiplicativo* de un entero  $a$  módulo  $n$  si  $ab \equiv 1 \pmod{n}$ .

**163 Teorema** Si existiese, el inverso multiplicativo  $x$  de un entero  $a$  módulo el entero  $n > 1$ , es único.

**Demostración:** Si  $x, y$  fuesen inversos de  $a \pmod{n}$  entonces  $ax \equiv 1 \pmod{n}$  y también  $ay \equiv 1 \pmod{n}$ . Multiplicando por  $y$  la primera congruencia, se ve que  $(ya)x \equiv y \pmod{n}$ . Así,  $x \equiv y \pmod{n}$ .  $\square$

**164 Teorema** Sean  $n > 1, a$  enteros. Entonces  $a$  posee un inverso módulo  $n$  si y sólo si  $a$  es relativamente primo a  $n$ .

**Demostración:** Presúmase que  $b$  es un inverso de  $a \pmod{n}$ . Luego  $ab \equiv 1 \pmod{n}$  que conlleva la existencia de un entero  $s$  tal que  $ab - 1 = sn$ , esto es,  $ab - sn = 1$ . Ésta es una combinación lineal de  $a$  y  $n$ , luego será divisible por  $(a, n)$ , dando  $(a, n) = 1$ .

Recíprocamente, si  $(a, n) = 1$ , por el teorema de Bachet-Bezout existe enteros  $x, y$  tales que  $ax + ny = 1$ . Esto da de inmediato  $ax \equiv 1 \pmod{n}$ , lo cual quiere decir que  $a$  tiene como inverso a  $x, \pmod{n}$ .

$\square$

**165 Corolario** Si  $n > 1$  es entero, entonces existe solamente  $\phi(n)$  enteros invertibles, módulo  $n$ .

**166 Teorema** Si  $a$  es relativamente primo al entero positivo integer  $n$ , entonces existe un entero positivo  $k \leq n$  tal que  $a^k \equiv 1 \pmod{n}$ .

**Demostración:** Ya que  $(a, n) = 1$  se tiene  $(a^j, n) = 1$  para toda  $j \geq 1$ . Considérese la sucesión  $a, a^2, a^3, \dots, a^{n+1} \pmod{n}$ . Como ésta posee  $n+1$  términos y hay sólo  $n$  residuos diferentes módulo  $n$ , el principio de las pichoneras

de Dirichlet implica que dos de estas potencias están en la misma clase residual  $\pmod n$ . Ésto es, se puede hallar  $s, t$  con  $1 \leq s < t \leq n+1$  tal que  $a^s \equiv a^t \pmod n$ . Ahora bien,  $1 \leq t-s \leq n$ . Luego  $a^s \equiv a^t \pmod n$  resulta en  $a^{t-s} a^s \equiv a^{t-s} a^t \pmod n$ , lo que quiere decir que  $a^t \equiv a^{t-s} a^t \pmod n$ . Utilizando el corolario 145 se deduce que  $a^{t-s} \equiv 1 \pmod n$ , lo que demuestra el resultado.  $\square$

Si  $(a, n) = 1$ , el teorema anterior dice que existe un entero positivo  $k$  con  $a^k \equiv 1 \pmod n$ . Por el axioma del buen orden, existe un entero mínimo satisfaciendo esta congruencia, lo que sugiere la próxima definición.

**167 Definición** Si  $m$  es el entero positivo mínimo con  $a^m \equiv 1 \pmod n$ , entonces se dice que  $a$  tiene orden  $m \pmod n$ .

**168 Teorema** Sea  $n > 1$  un entero. Entonces  $a \in \mathbb{Z}$  tiene un orden  $\pmod n$  si y solamente si  $(a, n) = 1$ .

**Demostración:** Si  $(a, n) = 1$ , entonces  $a$  tiene un orden en virtud del teorema 166 y el axioma del buen orden. Presúmase pues que  $a$  has an order  $\pmod n$ . Evidentemente  $a \neq 0$ . La existencia de un orden conlleva la existencia de un entero positivo  $m$  tal que  $a^m \equiv 1 \pmod n$ . Luego, existe un entero  $s$  con  $a^m + sn = 1$ , o sea,  $a \cdot a^{m-1} + sn = 1$ . Esta es una combinación lineal de  $a$  y de  $n$  por lo cual es divisible por  $(a, n)$ . De aquí se deduce que  $(a, n) = 1$ .  $\square$

**169 Teorema** Sea  $(a, n) = 1$  y sea  $t$  un entero. Entonces  $a^t \equiv 1 \pmod n$  si y sólo si  $\text{ord}_n a | t$ .

**Demostración:** Presúmase que  $\text{ord}_n a | t$ . Luego existe un entero  $s$  con  $s \text{ord}_n a = t$ , de donde se deduce

$$a^t \equiv a^{s \text{ord}_n a} \equiv (a^{\text{ord}_n a})^s \equiv 1^s \equiv 1 \pmod n.$$

Recíprocamente, presúmase que  $a^t \equiv 1 \pmod n$  y que  $t = x \cdot \text{ord}_n a + y$ ,  $0 \leq y < \text{ord}_n a$ . Entonces

$$a^y \equiv a^{t - x \text{ord}_n a} \equiv a^t \cdot (a^{\text{ord}_n a})^{-x} \equiv 1 \cdot 1^{-x} \equiv 1 \pmod n.$$

Si  $y > 0$  entonces se tendría un entero positivo menor que  $\text{ord}_n a$  poseyendo la propiedad  $a^y \equiv 1 \pmod n$ , lo que contradice la definición de  $\text{ord}_n a$  como el menor entero positivo con esta propiedad. Así pues  $y = 0$  y entonces  $t = x \cdot \text{ord}_n a$ , esto es,  $\text{ord}_n a | t$ .

$\square$

**170 Teorema** Sea  $n > 1$ ,  $a \in \mathbb{Z}$ ,  $(a, n) = 1$ . Si  $r_1, r_2, \dots, r_{\phi(n)}$  es un sistema de residuos reducidos módulo  $n$ , entonces también  $ar_1, ar_2, \dots, ar_{\phi(n)}$  es un sistema de residuos reducidos módulo  $n$ .

**Demostración:** Se necesita demostrar que los  $\phi(n)$  enteros  $ar_1, ar_2, \dots, ar_{\phi(n)}$  son mutuamente incongruentes  $\pmod n$ . Supóngase que  $ar_i \equiv ar_j \pmod n$  para algún  $i \neq j$ . Como  $(a, n) = 1$ , se deduce del corolario 145 que  $r_i \equiv r_j \pmod n$ . Ésto contradice el hecho que las  $r$ 's son incongruentes, con lo que queda demostrado el teorema.  $\square$

**171 Corolario** Sea  $n > 1$ ,  $a, b \in \mathbb{Z}$ ,  $(a, n) = 1$ . Si  $r_1, r_2, \dots, r_{\phi(n)}$  es un sistema de residuos reducidos módulo  $n$ , entonces  $ar_1 + b, ar_2 + b, \dots, ar_{\phi(n)} + b$  es también un sistema de residuos reducido módulo  $n$ .

**172 Ejemplo** Encuéntrese el inverso de  $5 \pmod 7$ .

**Resolución:** Búscase una solución a  $5x \equiv 1 \pmod 7$ . Por inspección se ve que la solución buscada es  $x \equiv 3 \pmod 7$ .

**173 Ejemplo** Hállese el orden de  $8 \pmod 11$ .

**Resolución:** Por el corolario ??  $\text{ord}_{11} 8$  es uno de entre 1, 2, 5 o 10. Ahora  $8^2 \equiv -2 \pmod{11}$ ,  $8^4 \equiv 4 \pmod{11}$  y  $8^5 \equiv -1 \pmod{11}$ . El orden es pues  $\text{ord}_{11} 8 = 10$ .

**174 Ejemplo (Putnam, 1956)** Demuéstrese que todo entero positivo posee un múltiplo cuya expansión decimal involucra todos los 10 dígitos.

**Resolución:** Se  $n$  un entero positivo arbitrario con  $k$  dígitos, y sea  $m = 123456780 \cdot 10^{k+1}$ . Entonces los  $n$  consecutivos  $m+1, m+2, \dots, m+n$  comienzan en 1234567890, forman un sistema completo de residuos módulo  $n$  y luego uno de ellos es divisible por  $n$ .

## Tarea

### 4.3. Teoremas de Fermat, Wilson y Euler

**175 Teorema (Pequeño teorema de Fermat)** Sea  $p$  un primo y  $a$  un entero tal que  $p \nmid a$ . Entonces

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Demostración:** Ya que  $(a, p) = 1$ , los enteros  $a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)$  también forman un sistema de residuos reducido módulo  $p$  en vista del corolario 171. Luego pues

$$(a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

o sea,

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

Como  $((p-1)!, p) = 1$ , se puede cancelar las  $(p-1)!$ 's gracias al corolario 145.  $\square$

**176 Corolario** Para todo primo  $p$  y para todo entero  $a$ ,

$$a^p \equiv a \pmod{p}.$$

**Demostración:** O bien  $p|a$  o  $p \nmid a$ . Si  $p|a$ , entonces  $a \equiv 0 \equiv a^p \pmod{p}$  y no hay nada que demostrar. Si  $p \nmid a$ , el pequeño teorema de Fermat dice que  $p|a^{p-1} - 1$ . Así pues  $p|(a^{p-1} - 1) = a^p - a$ , que da el resultado.  $\square$

**177 Corolario** Sea  $p$  un primo y  $a$  un entero. Si  $p \nmid a$  entonces  $\text{ord}_p a | p-1$ .

**Demostración:** El resultado se consigue de inmediato por el teorema 169 y el pequeño teorema de Fermat.  $\square$

**178 Lema** Si  $a^2 \equiv 1 \pmod{p}$ , o bien  $a \equiv 1 \pmod{p}$  o bien  $a \equiv -1 \pmod{p}$ .

**Demostración:** Se tiene  $p|a^2 - 1 = (a-1)(a+1)$ . Como  $p$  es primo,  $p$  debe dividir a al menos uno de estos dos factores, lo que demuestra el lema.  $\square$

**179 Teorema (Teorema de Wilson)** Si  $p$  es primo, entonces  $(p-1)! \equiv -1 \pmod{p}$ .

**Demostración:** Si  $p = 2$  o  $p = 3$ , el resultado se deduce por verificación directa. Presúmase que  $p > 3$ . Considérese  $a, 2 \leq a \leq p-2$ . A cada  $a$  se le asocia su inverso único  $\bar{a} \pmod{p}$ , i.e.  $a\bar{a} \equiv 1 \pmod{p}$ . Obsérvese que  $a \neq \bar{a}$  porque si no,  $a^2 \equiv 1 \pmod{p}$  violando el lema anterior, ya que  $a \neq 1, a \neq p-1$ . En multiplicando las  $a$ 's con  $2 \leq a \leq p-2$ , se aparean éstas con sus inversos, y la contribución neta de este producto es por lo tanto 1. En símbolos,

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

En otras palabras,

$$(p-1)! \equiv 1 \cdot \left( \prod_{2 \leq a \leq p-2} j \right) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

Esto conlleva al resultado.  $\square$

**180 Teorema (Teorema de Euler)** Si  $(a, n) = 1$ , entonces  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**Demostración:** Sean  $a_1, a_2, \dots, a_{\phi(n)}$  los residuos canónicos reducidos  $\pmod{n}$ . Como  $(a, n) = 1$ ,  $aa_1, aa_2, \dots, aa_{\phi(n)}$ , también forman un sistema de residuos reducidos, gracias al corolario 171. Así pues,

$$aa_1 \cdot aa_2 \cdots aa_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n},$$

o

$$a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Como  $(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$ , se puede cancelar el producto  $a_1 a_2 \cdots a_{\phi(n)}$  en uno y otro lado, de donde se deduce el teorema.  $\square$

**181 Corolario** Si  $(a, n) = 1$ , entonces  $\text{ord}_n a \mid \phi(n)$ .

**182 Ejemplo** Sea  $a_1 = 4, a_n = 4^{a_n-1}, n > 1$ . Hállese el residuo cuando  $a_{100}$  se divide por 7.

**Resolución:** Por el pequeño teorema de Fermat,  $4^6 \equiv 1 \pmod{7}$ . Como  $4^n \equiv 4 \pmod{6}$  para todos los enteros positivos  $n$ , se tiene  $4^n = 4 + 6t$  para algún entero  $t$ . Así

$$a_{100} \equiv 4^{a_{99}} \equiv 4^{4+6t} \equiv 4^4 \cdot (4^6)^t \equiv 4 \pmod{7}.$$

**183 Ejemplo** Demuéstrese que  $m, n \in \mathbb{Z}$ ,  $mn(m^{60} - n^{60})$  es siempre divisible por 56786730.

**Resolución:** Obsérvese que  $a = 56786730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$ . Sea  $Q(x, y) = xy(x^{60} - y^{60})$ . Obsérvese que  $(x-y) \mid Q(x, y)$ ,  $(x^2 - y^2) \mid Q(x, y)$ ,  $(x^3 - y^3) \mid Q(x, y)$ ,  $(x^4 - y^4) \mid Q(x, y)$ ,  $(x^6 - y^6) \mid Q(x, y)$ ,  $(x^{10} - y^{10}) \mid Q(x, y)$ ,  $(x^{12} - y^{12}) \mid Q(x, y)$ , y  $(x^{30} - y^{30}) \mid Q(x, y)$ .

Si  $p$  es cualquiera de los primos dividiendo a  $a$ , se tiene entonces que  $m^p - m \equiv 0 \pmod{p}$  y que  $n^p - n \equiv 0 \pmod{p}$ . Así  $n(m^p - m) - m(n^p - n) \equiv 0 \pmod{p}$ , ésto es,  $mn(m^{p-1} - n^{p-1}) \equiv 0 \pmod{p}$ . Luego se tiene que

$$2 \mid mn(m-n) \mid Q(m, n), 3 \mid mn(m^2 - n^2) \mid Q(m, n), 5 \mid mn(m^4 - n^4) \mid Q(m, n),$$

$$7 \mid mn(m^6 - n^6) \mid Q(m, n), 11 \mid mn(m^{10} - n^{10}) \mid Q(m, n),$$

$$13 \mid mn(m^{12} - n^{12}) \mid Q(m, n), 31 \mid mn(m^{30} - n^{30}) \mid Q(m, n)$$

y  $61 \mid mn(m^{60} - n^{60}) \mid Q(m, n)$ . Como todos estos son primos distintos, se deduce que  $a \mid mnQ(m, n)$ , como se quería demostrar.

**184 Ejemplo** Si  $p \equiv 1 \pmod{4}$ , demuéstrese que

$$\left( \frac{p-1}{2} \right)! \equiv -1 \pmod{p}.$$

**Resolución:** En el producto  $(p-1)!$ , se apareja  $j, 1 \leq j \leq (p-1)/2$  con  $p-j$ . Obsérvese que  $j(p-j) \equiv -j^2 \pmod p$ . Luego

$$-1 \equiv (p-1)! \equiv \prod_{1 \leq j \leq (p-1)/2} -j^2 \equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)! \pmod p.$$

El resultado se consigue al observar que  $(-1)^{(p-1)/2} = 1$ .

**185 Ejemplo (IMO 1970)** Demuéstrese que para todo entero  $n$  es imposible partir el conjunto

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

en dos subconjuntos tales que el producto de los miembros del uno sea igual al producto de los miembros del otro.

**Resolución:** Supóngase en miras de contradicción que existiese tal  $n$  con tal partición, el primer subconjunto teniendo producto de miembros  $A$  y el otro teniendo producto de miembros  $B$ . O bien, uno de los enteros en  $\{n, n+1, n+2, n+3, n+4, n+5\}$  es divisible por 7, en cuyo caso exactamente uno de entre  $A$  o  $B$  es divisible por 7, y por lo tanto,  $A \cdot B$  no es divisible por  $7^2$  y así  $A \cdot B$  no es un cuadrado. En la segunda posibilidad, todos los miembros del conjunto son relativamente primos a 7. Esto quiere decir que, gracias al teorema de Wilson,

$$n(n+1) \cdots (n+6) \equiv 1 \cdot 2 \cdots 6 \equiv A \cdot B \equiv -1 \pmod 7.$$

Pero si  $A = B$  entonces  $A^2 \equiv -1 \pmod 7$ , lo que es imposible ya que  $-1$  no es cuadrado  $\pmod 7$ .

## Tarea

**186 Problema** Sea  $n \in \mathbb{N}, n \geq 2$ . Demuéstrese que si  $N$  es la suma de  $n$  números impares consecutivos, entonces  $N$  no puede ser primo.

## 4.4. Teorema sónico de los residuos

**187 Teorema (Teorema sónico de los residuos o Teorema de Sun Tsu)** Sean  $m_1, m_2, \dots, m_k$  enteros relativamente primos por pares, todos mayores que 1, y sean  $a_1, a_2, \dots, a_k$  enteros arbitrarios. Luego el sistema de congruencias

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

posee una solución única módulo  $m_1 m_2 \cdots m_k$ .

**Demostración:** Póngase  $P_j = \frac{m_1 m_2 \cdots m_k}{m_j}, 1 \leq j \leq k$  y sea  $Q_j$  el inverso de  $P_j \pmod{m_j}$ , i.e.,  $P_j Q_j \equiv 1 \pmod{m_j}$ , que sabemos que existe, ya que las  $m_i$  son relativamente primas por pares. Póngase

$$x = a_1 P_1 Q_1 + a_2 P_2 Q_2 + \cdots + a_k P_k Q_k.$$

Este número claramente satisface las condiciones descritas en el teorema. La unicidad de esta solución es fácil de establecer módulo  $m_1 m_2 \cdots m_k$ .  $\square$

**188 Ejemplo** ¿Puede encontrarse un millón de enteros positivos que sean divisibles por al menos un cuadrado?

**Resolución:** La respuesta es afirmativa. Sean  $p_1, p_2, \dots, p_{1000000}$  un millón de primos diferentes. Por el teorema sónico de los residuos existe una solución del siguiente sistema de congruencias:

$$\begin{array}{rcll} x & \equiv & -1 & \text{mód } p_1^2, \\ x & \equiv & -2 & \text{mód } p_2^2, \\ \vdots & \vdots & \vdots & \vdots \\ x & \equiv & -1000000 & \text{mód } p_{1000000}^2. \end{array}$$

Los números  $x+1, x+2, \dots, x+1000000$  son un millón de enteros consecutivos, cada uno divisible por el cuadrado de un primo.

## 4.5. Criterios de divisibilidad

**189 Teorema** Un entero  $n$  es divisible por 5 si y solamente si su último dígito es o un 0 o un 5.

**Demostración:** Se derivará el resultado para  $n > 0$ , ya que para  $n < 0$  sólo basta aplicar el teorema a  $-n > 0$ . Como  $10^k \equiv 0 \pmod{5}$  para enteros  $k \geq 1$ , se tiene

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0 \equiv a_0 \pmod{5},$$

Así pues, la divisibilidad de  $n$  por 5 depende en si  $a_0$  es divisible por 5, lo que sólo pasa cuando  $a_0 = 0$  o  $a_0 = 5$ .  
□

**190 Teorema** Sea  $k$  un entero positivo. Un entero  $n$  es divisible por  $2^k$  si y solamente si el número formado por los últimos  $k$  dígitos de  $n$  es divisible por  $2^k$ .

**Demostración:** Si  $n = 0$ , no hay nada que demostrar. Si se demuestra el resultado para  $n > 0$  entonces el resultado para  $n < 0$  se deduce al aplicar lo ya obtenido a  $-n = (-1)n > 0$ . Presúmase pues que  $n \in \mathbb{Z}$ ,  $n > 0$  y sea su expansión decimal

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0,$$

donde  $0 \leq a_i \leq 9$ ,  $a_s \neq 0$ . Ahora bien,  $10^t = 2^t 5^t \equiv 0 \pmod{2^t}$  para  $t \geq k$ . Luego pues,

$$\begin{aligned} n &= a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0 \\ &\equiv a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + \dots + a_1 10 + a_0 \pmod{2^k}, \end{aligned}$$

de donde  $n$  es divisible por  $2^k$  si y solamente si el número formado por los últimos  $k$  dígitos de  $n$  es divisible por  $2^k$ . □

**191 Teorema (Regla de los 9's)** Un entero  $n$  es divisible por 9 si y solamente si la suma de sus dígitos es divisible por 9.


**Demostración:** Si  $n = 0$  no hay nada que demostrar. Si se demuestra el resultado para  $n > 0$  entonces se puede deducir el resultado para  $n < 0$  en aplicando lo ya obtenido al número  $-n = (-1)n > 0$ . Presúmase pues que  $n \in \mathbb{Z}$ ,  $n > 0$  y que su expansión decimal es

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0,$$

donde  $0 \leq a_i \leq 9$ ,  $a_s \neq 0$ . Observése que  $10 \equiv 1 \pmod{9}$  y que  $10^t \equiv 1^t \equiv 1 \pmod{9}$ . Ahora bien,

$$\begin{aligned} n &= a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0 \\ &\equiv a_s + \dots + a_1 + a_0 \pmod{9}, \end{aligned}$$

de donde se colige el resultado. □

 Como  $10 \equiv 1 \pmod{3}$  se puede también ver que  $n$  es divisible por 3 si y solamente si la suma de sus dígitos es divisible por 3.

**192 Definición** Si el entero  $n$  tiene expansión decimal

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0,$$

entonces su *suma alternante de dígitos* es

$$a_s - a_{s-1} + a_{s-2} - a_{s-3} + \dots + (-1)^{s-1} a_0$$

**193 Teorema** Un entero  $n$  es divisible por 11 si y solamente si su suma de dígitos alternante es divisible por 11.

**Demostración:** Presúmase que  $n > 0$ . Sea

$$n = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0,$$

donde  $0 \leq a_i \leq 9$ ,  $a_s \neq 0$ . Obsérvese que  $10 \equiv -1 \pmod{11}$  y así  $10^t \equiv (-1)^t \pmod{11}$ . Luego

$$\begin{aligned} n &= a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0 \\ &\equiv a_s (-1)^s + a_{s-1} (-1)^{s-1} + a_{s-2} (-1)^{s-2} + \dots + a_1 + a_0 \pmod{11} \end{aligned}$$

y se colige el resultado.  $\square$

## Tarea

**194 Ejemplo** ¿Para cuántos enteros  $n$  en  $\{1, 2, 3, \dots, 100\}$  es el dígito de las decenas de  $n^2$  impar?

**Resolución:** En el subconjunto  $\{1, 2, \dots, 10\}$  hay sólo dos valores de  $n$  (4 y 6) para los cuales el dígito de las decenas de  $n^2$  es impar. Ahora bien,  $(n+10)^2 = n^2 + 20n + 100$  tiene la misma paridad en su dígito de las decenas que el dígito de las decenas de  $n^2$ . Luego, hay  $2 \times 10 = 20$  enteros  $n$  para los cuales se verifica la condición prescrita.

**195 Ejemplo** Hallar todos los enteros con dígito inicial 6 tales que si se les suprime este dígito inicial, el número resultante es  $1/25$  del número original.

**Resolución:** Sea  $x$  el entero buscado. Entonces  $x = 6 \cdot 10^n + y$  donde  $y$  es un entero positivo. La condición del problema estipula que

$$y = \frac{1}{25} (6 \cdot 10^n + y),$$

o sea,

$$y = \frac{10^n}{4} = 25 \cdot 10^{n-2}.$$

Esto requiere  $n \geq 2$  y por lo tanto  $y = 25, 250, 2500, 25000, \dots$ . Luego  $x = 625, 6250, 62500, 625000, \dots$ .

**196 Ejemplo** Sea  $A$  un entero positivo y  $A'$  sea el entero positivo resultante de alguna permutación específica de los dígitos de  $A$ . Demuéstrese que si  $A + A' = 10^{10}$  entonces  $A$  es divisible por 10.

**Resolución:** Claramente,  $A$  y  $A'$  deberán tener 10 dígitos cada uno. Pongasé pues

$$A = \overline{a_{10} a_9 a_8 \dots a_1}$$

y

$$A' = \overline{b_{10} b_9 b_8 \dots b_1},$$

donde  $a_k, b_k, k = 1, 2, \dots, 10$  son los dígitos de  $A$  y  $A'$  respectivamente. Ahora, como  $A + A' = 10000000000$ , deberemos tener que  $a_1 + b_1 = a_2 + b_2 = \dots = a_i + b_i = 0$  y

$$a_{i+1} + b_{i+1} = 10, a_{i+2} + b_{i+2} = \dots = a_{10} + b_{10} = 9,$$

para algún subíndice  $i, 0 \leq i \leq 9$ . Note que si  $i = 9$  no hay ninguna suma de las  $a_{i+2} + b_{i+2}, a_{i+3} + b_{i+3}, \dots$  y si  $i = 0$  no hay ninguna suma de las  $a_1 + b_1, \dots, a_i + b_i$ .

Sumando,

$$a_1 + b_1 + a_2 + b_2 + \dots + a_i + b_i + a_{i+1} + b_{i+1} + \dots + a_{10} + b_{10} = 10 + 9(9 - i).$$

Ahora bien, si  $i$  es par,  $10 + 9(9 - i)$  es impar y si  $i$  es impar  $10 + 9(9 - i)$  es par. Pero como

$$a_1 + a_2 + \dots + a_{10} = b_1 + b_2 + \dots + b_{10},$$

tenemos

$$a_1 + b_1 + a_2 + b_2 + \dots + a_i + b_i + a_{i+1} + b_{i+1} + \dots + a_{10} + b_{10} = 2(a_1 + a_2 + \dots + a_{10}),$$

un entero par. Colegimos que  $i$  es impar, lo que necesariamente implica  $a_1 = b_1 = 0$ , esto es,  $A$  y  $A'$  son ambos divisibles por 10.

**197 Ejemplo** Demuéstrese que todos los enteros en la sucesión

$$49, 4489, 444889, 44448889, \underbrace{44 \dots 44}_{n \text{ 4's}} \underbrace{88 \dots 88}_{n-1 \text{ 8's}} 9$$

son cuadrados.

**Resolución:** Obsérvese que

$$\begin{aligned} \underbrace{44 \dots 44}_{n \text{ 4's}} \underbrace{88 \dots 88}_{n-1 \text{ 8's}} 9 &= \underbrace{44 \dots 44}_{n \text{ 4's}} \cdot 10^n + \underbrace{88 \dots 88}_{n-1 \text{ 8's}} \cdot 10 + 9 \\ &= \frac{4}{9} \cdot (10^n - 1) \cdot 10^n + \frac{8}{9} \cdot (10^{n-1} - 1) \cdot 10 + 9 \\ &= \frac{4}{9} \cdot 10^{2n} + \frac{4}{9} \cdot 10^n + \frac{1}{9} \\ &= \frac{1}{9} (2 \cdot 10^n + 1)^2 \\ &= \left( \frac{2 \cdot 10^n + 1}{3} \right)^2 \end{aligned}$$

Falta ahora demostrar que esta última cantidad es entera, esto es, que 3 divide a  $2 \cdot 10^n + 1 = \underbrace{200 \dots 001}_{n-1 \text{ 0's}}$ . Pero la suma de los dígitos de esta última cantidad es 3, y por lo tanto este entero es divisible por 3.

## Indicaciones y respuestas

**6** Presúmase a la contraria que el conjunto  $\mathcal{S}$  de enteros en  $]0; 1[$  es no nulo. Siendo un conjunto de enteros positivos, gracias al axioma del buen orden, este debe tener un elemento mínimo al que se llamará  $m$ . Ahora bien,  $0 < m^2 < m < 1$ , y por lo tanto  $m^2 \in \mathcal{S}$ . Pero esto declara que  $\mathcal{S}$  tiene un entero positivo,  $m^2$ , ¡que es menor que su elemento mínimo! Esta contradicción establece que  $\mathcal{S} = \emptyset$ .

**7** Supóngase que  $\frac{a^2 + b^2}{1 + ab} = k$  fuere un contraejemplo de un entero que no es un cuadrado perfecto con  $\mathbf{m\acute{a}x}(a, b)$  tan pequeño como fuere posible. Puede presumirse, sin perder generalidad, que  $a < b$ , ya que si  $a = b$  entonces

$$0 < k = \frac{2a^2}{a^2 + 1} < 2,$$

lo que fuerza  $k = 1$ , un cuadrado perfecto.

Ahora bien,  $a^2 + b^2 - k(ab + 1) = 0$  es una ecuación cuadrática en  $b$  cuya suma de raíces es  $ka$  y cuyo producto de raíces es  $a^2 - k$ . Si  $b_1, b$  son sus raíces se tiene que  $b_1 + b = ka$  y  $b_1 b = a^2 - k$ .

Como  $a, k$  son enteros positivos, el suponer  $b_1 < 0$  es incompatible con  $a^2 + b_1^2 = k(ab_1 + 1)$ . Como  $k$  se supone no ser un cuadrado perfecto, el suponer  $b_1 = 0$  es incompatible con  $a^2 + 0^2 = k(0 \cdot a + 1)$ . Además

$$b_1 = \frac{a^2 - k}{b} < \frac{b^2 - k}{b} < b.$$

Así pues, se ha encontrado otro entero positivo,  $b_1$  para el cual  $\frac{a^2 + b_1^2}{1 + ab_1} = k$  y el cual es menor que  $\mathbf{m\acute{a}x}(a, b)$ : contradicción. Por lo tanto  $k$  debe ser un cuadrado perfecto.

**8** Obsérvese que  $n^3 - n = (n - 1)n(n + 1)$  y que  $n^5 - 5n^3 + 4n = (n - 2)(n - 1)n(n + 1)(n + 2)$  y utilícese el ejemplo 5.

**14** Dividánse los números  $\{1, 2, 3, \dots, 126\}$  en los seis conjuntos

$$\{1, 2\}, \{3, 4, 5, 6\}, \{7, 8, \dots, 13, 14\}, \{15, 16, \dots, 29, 30\}, \\ \{31, 32, \dots, 61, 62\} \text{ y } \{63, 64, \dots, 126\}.$$

Por el principio de las casillas de Dirichlet, dos de los siete números yacerán en el mismo conjunto, donde obviamente, satisfacen las desigualdades estipuladas.

**15** Hay  $2^{10} - 1 = 1023$  subconjuntos no nulos posibles en un conjunto de 10 elementos. A cada uno de estos conjuntos no vacíos asóciase la suma de estos 10 elementos. El valor máximo que estas sumas pueden tener es  $90 + 91 + \dots + 99 = 945 < 1023$ . Luego, deben de haber al menos dos subconjuntos, llámense  $\mathbf{A}$  y  $\mathbf{B}$  con la misma suma, ya que hay más subconjuntos que sumas. Si los subconjuntos tuviesen una intersección no nula, basta considerar  $\mathbf{A} \setminus (\mathbf{A} \cap \mathbf{B})$  y  $\mathbf{B} \setminus (\mathbf{A} \cap \mathbf{B})$ , que también tienen la propiedad deseada.

**16** Obsérvese primeramente que al elegir  $n + 1$  enteros de cualquier conjunto de  $2n$  enteros consecutivos, siempre habrá dos que diferirán por  $n$ . En efecto, al parear los  $2n$  enteros consecutivos

$$\{a + 1, a + 2, a + 3, \dots, a + 2n\}$$

en los  $n$  pares

$$\{a + 1, a + n + 1\}, \{a + 2, a + n + 2\}, \dots, \{a + n, a + 2n\},$$

se ve que al elegir  $n + 1$  siempre habrá dos que pertenecen al mismo grupo.

Agrupéese pues los 100 enteros como sigue:

$$\{1, 2, \dots, 20\}, \{21, 22, \dots, 40\},$$

$$\{41, 42, \dots, 60\}, \{61, 62, \dots, 80\}$$

y

$$\{81, 82, \dots, 100\}.$$

Si se eligieren 55 siempre habrá once proviniendo del mismo grupo. Y en ese grupo en particular siempre habrá dos difiriendo por 10.

**26** Se demostrará que la expresión  $r + 1/r$  es entera sólo cuando  $r = 1$ , en cuyo caso  $r + 1/r = 2$ . Sea pues

$$r + \frac{1}{r} = k,$$

$k$  un entero positivo. Luego

$$r = \frac{k \pm \sqrt{k^2 - 4}}{2}.$$

Como  $k$  es un entero,  $r$  puede ser entero si y sólo si  $k^2 - 4$  es un cuadrado de la misma paridad que  $k$ . Ahora, si  $k \geq 3$ ,

$$(k - 1)^2 < k^2 - 4 < k^2,$$

esto es,  $k^2 - 4$  está entre dos cuadrados consecutivos y por lo tanto no puede ser un cuadrado. Si  $k = 1$ ,  $\sqrt{k^2 - 4}$  no es real. Si  $k = 2$ ,  $k^2 - 4 = 0$ . Luego,  $r + 1/r = 2$ , esto es,  $r = 1$ . Esto termina la demostración.

**27** Exprésese  $\underbrace{11 \dots 11}_{221 \text{ 1's}}$  de la forma  $\frac{10^a - 1}{10^b - 1} \cdot \frac{10^b - 1}{10 - 1}$ , para ciertos enteros  $a, b$ .

**28**  $11^{10} - 1 = (11^5 - 1)a = (11 - 1)(11^4 + 11^3 + 11^2 + 11 + 1)a$ .

**29** Obsérvese que  $a^3b - ab^3 = ab(a - b)(a + b)$  es siempre par, no importa que enteros sean substituidos. Si uno de los enteros es de la forma  $5k$ , entonces no hay más que demostrar. Si no, entonces se escogen tres enteros de entre enteros de la forma  $5k \pm 1$  (casilla I) ó  $5k \pm 2$  (casilla II). Por el principio de las casillas de Dirichlet, dos de estos tres enteros deberán caer en la misma casilla así que hay dos que o bien su suma o bien su diferencia es divisible por 5, lo que establece el resultado.

**30** Para  $n = 0$  se declara que  $3^3 - 27 = 169 \cdot 0$  es un múltiplo de 169, lo cual es evidente. Presúmase que la aserción es cierta para  $n - 1, n > 1$ , esto es, presúmase que

$$3^{3n} - 26n - 1 = 169N$$

para algún entero  $N$ . Entonces

$$3^{3n+3} - 26n - 27 = 27 \cdot 3^{3n} - 26n - 27 = 27(3^{3n} - 26n - 1) + 676n$$

lo cual se reduce a

$$27 \cdot 169N + 169 \cdot 4n,$$

que es evidentemente un múltiplo de 169. Queda demostrada la aserción por inducción.

31 Es claro que  $3n + 1$  no es un múltiplo de 3, luego  $3n + 1 = (3k \pm 1)^2$ . De aquí

$$n + 1 = \frac{(3k \pm 1)^2 - 1}{3} + 1 = 3k^2 \pm 2k + 1 = k^2 + k^2 + (k \pm 1)^2,$$

como queríamos demostrar.

32 Si  $n$  es par, escríbase  $n = n - 6 + 6$ . Como  $n > 11$ ,  $n - 6$  es par y mayor que 2, por tanto compuesto. Si  $n$  es impar,  $n = n - 9 + 9$ . Como  $n > 11$ ,  $n - 9$  es par y mayor que 2, por lo tanto compuesto.

33 Por el algoritmo de división, hay enteros  $q_1, q_2, q_3$  con  $1059 = dq_1 + r$ ,  $1417 = dq_2 + r$  y  $2312 = dq_3 + r$ . Restando se obtiene  $1253 = d(q_3 - q_1)$ ,  $895 = d(q_3 - q_2)$  y  $358 = d(q_2 - q_1)$ . Como  $7 \cdot 179$ ,  $895 = 5 \cdot 179$ ,  $358 = 2 \cdot 179$ , se ve que  $d = 179$ . Como  $1059 = 5 \cdot 179 + 164$ ,  $r = 164$ . Finalmente,  $d - r = 15$ .

34 Se tiene que  $n^2 + 23 = n^2 - 1 + 24 = (n - 1)(n + 1) + 24$ . Luego, las familias  $n = 24m \pm 1$ ,  $m = 0, \pm 1, \pm 2, \pm 3, \dots$  producen infinitos valores de  $n^2 + 23$  que son divisibles por 24.

35 Se consideran enteros positivos  $a_1, a_2, \dots, a_n$  con  $a_1 + a_2 + \dots + a_n = 1996$ . Es claro que para maximizar  $a_1 a_2 \dots a_n$ , ninguna de las  $a_k$ 's puede ser igual a 1. Se demostrará que para obtener un producto máximo se deberá tener la mayoría de las  $a_k = 3$  y a lo sumo dos  $a_j = 2$ . Supongáse que  $a_j > 4$ . Al substituir  $a_j$  por los dos términos  $a_j - 3$  y 3 la suma no se afecta, pero el producto incrementa pues  $a_j < 3(a_j - 3)$ . Así pues las  $a_k$ 's son iguales a 2, 3 ó 4. Pero como  $2 + 2 + 2 = 3 + 3$  y  $2 \times 2 \times 2 < 3 \times 3$ , si hay tres o más 2's, se pueden substituir con 3's. Como  $1996 = 3(665) + 1 = 3(664) + 4$ , el producto máximo es pues  $3^{664} \times 4$ .

36 Gracias a 2.2,  $2903^n - 803^n$  es divisible por  $2903 - 803 = 2100 = 7 \cdot 300$  y  $261^n - 464^n$  es divisible por  $-203 = (-29) \cdot 7$ . Por lo tanto, la expresión es divisible por 7. Además  $2903^n - 464^n$  es divisible por  $2903 - 464 = 2439 = 9 \cdot 271$  y  $-803^n + 261^n$  es divisible por  $-803 + 261 = -542 = -2 \cdot 271$ . Así pues, como la expresión es divisible por 7 y por 271 y como estos son relativamente primos, la expresión es pues divisible por  $7 \cdot 271 = 1897$ .

37 Si  $n$  es impar escríbase  $a = 2, b = n - 2, n = a + b$  y como  $n - 2$  es impar se tiene  $\text{MCD}(n - 2, 2) = 1$ . Si  $n$  es par, entonces o bien  $n = 4k$  o bien  $n = 4k + 2$ . Si  $n = 4k$ , escríbase  $a = 2k + 1, b = 2k - 1, n = a + b$ , los cuales son relativamente primos al ser dos enteros impares consecutivos. Si  $n = 4k + 2, k > 1$  escríbase  $a = 2k + 3, b = 2k - 1, n = a + b$ , los que de la misma manera son relativamente primos (si  $d = \text{MCD}(2k + 3, 2k - 1)$  entonces  $d$  divide a  $2k + 3 - (2k - 1) = 4$ . Luego  $d$  es 1, 2 ó 4 pero como  $d$  es impar es por fuerza  $= 1$ ).

38 Si  $p = 3$ , entonces  $8p - 1 = 23$  y  $8p + 1 = 25$ , luego la aseveración se cumple para  $p = 3$ . Si  $p > 3$ ,  $p$  es de la forma  $3k + 1$  o de la forma  $3k + 2$ . Si  $p = 3k + 1$  entonces  $8p - 1 = 24k - 7$  y  $8p + 1 = 24k - 6$ , que es divisible por 6 y por lo tanto no es primo. Si  $p = 3k + 2$  entonces  $8p - 1 = 24k - 15$  no es primo al ser divisible por 3.

39

$$2222^{5555} + 5555^{2222} = (2222^{5555} + 4^{5555}) + (5555^{2222} - 4^{2222}) - (4^{5555} - 4^{2222}).$$

Para otro punto de vista, véase el ejemplo 146.

40 Póngase  $n = pm$ , donde  $p$  es primo y  $m > 1$ . Utilícese la identidad 2.2 para factorizar  $(2^p)^m - 1$ .

41 Póngase  $n = 2^k m$ , donde  $m > 1$  es impar. Factorice  $(2^{2^k})^m + 1$ .

42 Si  $a = 10^3, b = 2$  entonces

$$1002004008016032 = a^5 + a^4 b + a^3 b^2 + a^2 b^3 + a b^4 + b^5 = \frac{a^6 - b^6}{a - b}.$$

Esta última expresión factoriza como

$$\begin{aligned} \frac{a^6 - b^6}{a - b} &= (a + b)(a^2 + ab + b^2)(a^2 - ab + b^2) \\ &= 1002 \cdot 1002004 \cdot 998004 \\ &= 4 \cdot 4 \cdot 1002 \cdot 250501 \cdot k, \end{aligned}$$

en donde  $k < 250000$ . Por lo tanto  $p = 250501$ .

44 Sean  $n-1, n, n+1, n+2$  cuatro enteros consecutivos. Entonces su producto  $P$  es

$$P = (n-1)n(n+1)(n+2) = (n^3 - n)(n+2) = n^4 + 2n^3 - n^2 - 2n.$$

Ahora bien,

$$(n^2 + n - 1)^2 = n^4 + 2n^3 - n^2 - 2n + 1 = P + 1 > P.$$

Como  $P \neq 0$  y  $P$  es 1 más que un cuadrado,  $P$  no puede ser un cuadrado.

45 La aserción es evidente para  $n = 1$ , ya que  $k^2 - 1 = (k-1)(k+1)$  es producto de dos números pares consecutivos, y por tanto uno es divisible por 2 y el otro por 4 así que el producto es divisible por 8. Presúmase que  $2^{n+2} \mid k^{2^n} - 1$ . Como  $k^{2^{n+1}} - 1 = (k^{2^n} - 1)(k^{2^n} + 1)$ , se puede notar que  $2^{n+2}$  divide a  $(k^{2^n} - 1)$ , así que el problema se reduce a demostrar que  $2 \mid (k^{2^n} + 1)$ . Pero esto es obvio, ya que como  $k^{2^n}$  es impar  $k^{2^n} + 1$  es par.

51 Nótese que  $2(21n+4) - 3(14n+3) = -1$ , de donde el máximo común divisor divide a  $-1$ . Así pues, el numerador y el denominador no pueden compartir a un factor mayor que 1.

52 Se tiene que

$$\begin{aligned} d_n &= \text{MCD}(100 + n^2, 100 + (n+1)^2) \\ &= \text{MCD}(100 + n^2, 100 + n^2 + 2n + 1) \\ &= \text{MCD}(100 + n^2, 2n + 1). \end{aligned}$$

Así pues

$$d_n \mid (2(100 + n^2) - n(2n + 1)) = 200 - n.$$

Por lo tanto,  $d_n \mid (2(200 - n) + (2n + 1)) = 401$ , de donde se colige que  $d_n \mid 401$  para toda  $n$ . ¿Alcanzará  $d_n$  un valor tan grande como 401? ¡Efectivamente! Para  $n = 200$  se tiene que  $a_{200} = 100 + 200^2 = 100(401)$  y que  $a_{201} = 100 + 201^2 = 40501 = 101(401)$ . Luego se deduce que  $\max_{n \geq 1} d_n = 401$ .

53 Póngase los 100 enteros en los 50 pares

$$\{1, 2\}, \{3, 4\}, \{5, 6\}, \dots, \{99, 100\}.$$

Como se elegirá 51 enteros, deberá de haber dos de entre ellos que yazgan en el mismo par. Éstos son relativamente primos.

54 Sea el producto  $(n-1)n(n+1) = (n^2-1)n$ ,  $n > 1$ . Como  $n^2-1$  y  $n$  son relativamente primos, por el Teorema fundamental de la aritmética (Teorema 57)  $n^2-1$  es una potencia  $k$ -ésima perfecta ( $k \geq 2$ ) y también lo es  $n$ . Esto implica que tanto  $n^2-1$  y  $n^2$  son potencias  $k$ -ésimas perfectas consecutivas, lo que es imposible. Obsérvese que ni  $n^2-1$  ni  $n^2$  son ni 0 ni 1.

63 Los números de  $\mathcal{M}$  son de la forma

$$2^a 3^b 5^c 7^d 11^f 13^g 17^h 19^i 23^k.$$

Los diez exponentes dan  $512 = 2^{10}$  vectores de paridad. Luego entre cualesquiera 513 elementos de  $\mathcal{M}$  siempre se hallará dos cuyo producto es un cuadrado.

Se “poda” ahora los cuadrados. Como  $1985 > 513$  se puede hallar un par de números distintos  $a_1, b_1$  tales que  $a_1 b_1 = c_1^2$ . Quítese este par, dejando 1983 enteros. De estos 1983 enteros, se puede hallar un par  $a_2, b_2$  tales que  $a_2 b_2 = c_2^2$ . Remuévase este par, dejando 1981 enteros. De estos 1981 enteros, se puede encontrar un par  $a_3, b_3$  tales que  $a_3 b_3 = c_3^2$ . Esta operación de remover se puede continuar  $n+1$  veces, en donde  $n$  es el mayor entero positivo que satisface  $1985 - 2n \geq 513$ , esto es,  $n = 736$ . Luego se puede recoger 737 pares  $a_k, b_k$  tales que  $a_k b_k = c_k^2$  sea un cuadrado. Como  $737 > 513$ , se puede encontrar un par de las  $c_m$  tales que su producto  $c_i c_j$  sea un cuadrado. Pero como cada una de las  $c_m$  es un cuadrado a su vez, el producto  $c_i c_j = \alpha^2$  será una cuarta potencia.

**64** Cualquier entero puede escribirse de la manera  $2^a m$ , en donde  $m$  es impar. Tan sólo hay 50 enteros impares en el conjunto dado, luego hay sólo  $m$  posibilidades para  $m$ . Luego dos de los 51 enteros elegidos deben de ser de la forma  $2^a m$  y otro de la forma  $2^a m$ . Luego el menor de estos dos dividirá al mayor.

**65** Nótese primeramente que 7 puede descomponerse en a lo sumo tres factores diferentes:  $7 = -7(1)(-1)$ . Si  $p(a_k) - 7 = 0$  para cuatro valores distintos  $a_k, 1 \leq k \leq 4$  entonces

$$p(x) - 7 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)q(x)$$

para algún polinomio  $q$  con coeficientes enteros. Presúmase ahora que existe un entero  $m$  con  $p(m) = 14$ . Entonces

$$7 = p(m) - 7 = (m - a_1)(m - a_2)(m - a_3)(m - a_4)q(m).$$

Como los factores  $m - a_k$ , la igualdad anterior descompone a 7 en cuatro o más valores distintos, lo que es una contradicción.

**66** Obsérvese que

$$\begin{aligned} m^5 + 3m^4n - 5m^3n^2 - 15m^2n^3 + 4mn^4 + 12n^5 \\ = (m - 2n)(m - n)(m + n)(m + 2n)(m + 3n), \end{aligned}$$

un producto de cinco factores. Ahora bien, 33 se puede descomponer a lo sumo en cuatro factores distintos:  $33 = (-11)(3)(1)(-1)$ . Si  $n \neq 0$ , todos los factores de arriba son distintos y no pueden dar 33 en virtud del Teorema fundamental de la aritmética (Teorema 57) porque un producto de cinco factores diferentes no puede igualar a un producto de cuatro factores diferentes. Si  $n = 0$ , el producto de los factores es  $m^5$  pero 33 no es una quinta potencia.

**67** Sea  $k$  el máximo entero que satisface  $2^k \leq n$  y sea  $P$  el producto de todos los enteros impares menores o iguales a  $n$ . El número  $2^{k-1}PS$  es una suma cuyos términos, excepto el  $2^{k-1}PS \frac{1}{2^k}$ , son enteros.

**68** Si  $k^2 = 2^8 + 2^{11} + 2^n = 2304 + 2^n = 48^2 + 2^n$ , entonces  $k^2 - 48^2 = (k - 48)(k + 48) = 2^n$ . Gracias a la propiedad de factorización única,  $k - 48 = 2^s, k + 48 = 2^t, s + t = n$ . Luego  $2^t - 2^s = 96 = 3 \cdot 2^5$  o  $2^s(2^{t-s} - 1) = 3 \cdot 2^5$ . Por factorización única,  $s = 5, t - s = 2$ , dando  $s + t = n = 12$ .

**92** 400

**151** Quiérese hallar  $3^{100} \pmod{10}$ . Obsérvese que  $3^2 \equiv -1 \pmod{10}$ . Luego,  $3^{100} = (3^2)^{50} \equiv (-1)^{50} \equiv 1 \pmod{10}$ . Así, el último dígito es el 1.

**152** Se tiene que hallar  $7^{7^7} \pmod{10}$ . Ahora bien, como  $7^2 \equiv -1 \pmod{10}$ , entonces tenemos  $7^3 \equiv 7^2 \cdot 7 \equiv -7 \equiv 3 \pmod{10}$  y  $7^4 \equiv (7^2)^2 \equiv 1 \pmod{10}$ . Además,  $7^2 \equiv 1 \pmod{4}$  y por lo tanto  $7^7 \equiv (7^2)^3 \cdot 7 \equiv 3 \pmod{4}$ , lo que quiere decir que hay un entero  $t$  tal que  $7^7 = 3 + 4t$ . Ensamblando todo esto,

$$7^{7^7} \equiv 7^{4t+3} \equiv (7^4)^t \cdot 7^3 \equiv 1^t \cdot 3 \equiv 3 \pmod{10}.$$

Así el último dígito es un 3.

**153** Obsérvese que  $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \pmod{7}$  y  $2^{n+2} \equiv 4 \cdot 2^n \pmod{7}$ . Luego

$$3^{2n+1} + 2^{n+2} \equiv 7 \cdot 2^n \equiv 0 \pmod{7},$$

para todo número natural  $n$ .

**154** Como  $30a0b03 = 3 + 100b + 10000a + 3000000$ , observamos que  $30a0b03 \equiv 3 + 9b + 3a + 3 \equiv 6 + 9b + 3a \pmod{13}$ . Para que  $30a0b03$  sea divisible por 13 necesitamos  $9b + 3a \equiv 7 \pmod{13}$ . Aquí claro está, se tendrá  $0 \leq a, b \leq 9$ . Por inspección se ve que  $a = 8, b = 1; a = 5, b = 2; a = 2, b = 3; a = 9, b = 5; a = 6, b = 6; a = 3, b = 7; a = 0, b = 8$ . Luego 3080103, 3050203, 3020303, 3090503, 3060603, 3030703, 3000803 son todos divisibles por 13.

**155** Si  $x^2 = 2 - 5y^2$ , entonces  $x^2 \equiv 2 \pmod{5}$ . Pero 2 no es un cuadrado  $\pmod{5}$ .

**156** Obsérvese que  $641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$ . Luego  $2^7 \cdot 5 \equiv -1 \pmod{641}$  y  $5^4 \equiv -2^4 \pmod{641}$ . Ahora bien,  $2^7 \cdot 5 \equiv -1 \pmod{641}$  nos da  $5^4 \cdot 2^{28} = (5 \cdot 2^7)^4 \equiv (-1)^4 \equiv 1 \pmod{641}$ . Esta última congruencia y  $5^4 \equiv -2^4 \pmod{641}$  nos da  $-2^4 \cdot 2^{28} \equiv 1 \pmod{641}$ , lo que significa que  $641 \mid (2^{32} + 1)$ .

**157** Obsérvese que  $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1 \pmod{7}$  y así  $2^{3k} \equiv 1 \pmod{7}$  para todos los enteros positivos  $k$ . Luego  $2^{3k} + 27 \equiv 1 + 27 \equiv 0 \pmod{7}$  para todos los enteros positivos  $k$ . Esto produce una familia infinita de enteros  $n = 3k, k = 1, 2, \dots$  tal que  $2^n + 27$  es divisible por 7.

**158** No. Los cubos  $\pmod{7}$  son 0, 1, y 6. Ahora bien, cada potencia de 2 es congruente con 1, 2, ó 4  $\pmod{7}$ . Así pues,  $2^y + 15 \equiv 2, 3, \text{ ó } 5 \pmod{7}$ . Esto es imposible.

**159**  $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \pmod{7}$  y este ciclo de tres se repite. Así pues,  $2^k - 5$  deja residuos 3, 4, ó 6 al ser dividido por 7.