
# Teoría de Números para Olimpiadas Matemáticas

**José Heber Nieto Said**

**2015**

Teoría de Números para Olimpíadas Matemáticas

Asociación Venezolana de Competencias Matemáticas, Caracas, Mayo 2014

Hecho el depósito de Ley.

Depósito Legal: lfi6592015510497

ISBN: 978–980–6195–40–0

Formato digital: 76 páginas

Diseño general: José H. Nieto

# Índice general

# Introducción

Las *Olimpiadas Matemáticas* son concursos de resolución de problemas que se realizan en todo el mundo a nivel local, nacional, regional e internacional. La participación en estas competencias, en las que se plantean problemas novedosos e interesantes, alejados de la rutina, puede estimular el interés de muchos estudiantes por la matemática y ayudarlos a descubrir aptitudes y hasta vocaciones ocultas.

Para los maestros y profesores las olimpiadas ponen al alcance de su mano un amplio material que puede ser usado para reorientar y enriquecer la enseñanza: problemas cuidadosamente diseñados, libros y revistas sobre resolución de problemas, juegos matemáticos y muchos otros recursos. Además, en torno a estas competencias generalmente se realizan seminarios y talleres para los educadores.

¿Porqué se insiste en la resolución de problemas y no en pruebas de conocimientos? Pues sencillamente porque hay un amplio consenso en que los problemas son el corazón de la matemática, y por lo tanto deben ser el punto focal de la enseñanza de esta disciplina.

Paul Halmos (1916–2006), quien fuera uno de los más importantes matemáticos del siglo XX, escribió en su famoso artículo *El corazón de la matemática* [5]:

> "La principal razón de existir del matemático es resolver problemas, y por lo tanto en lo que *realmente* consisten las matemáticas es en problemas y soluciones."

En el mismo sentido se había pronunciado el insigne matemático y educador George Pólya (1887–1985):

> "*Entender* la matemática significa ser capaz de *hacer* matemática. ¿Y qué significa hacer matemática? En primer lugar, significa ser capaz de resolver problemas matemáticos."

Ahora bien, la mayor dificultad que confrontan nuestros estudiantes al participar en olimpiadas matemáticas tiene su origen en que, en los cursos de matemática de enseñanza media, probablemente han tenido que resolver numerosos *ejercicios*, pero rara vez un verdadero *problema*. La diferencia consiste en que un *ejercicio* se resuelve más o menos mecánicamente, si se ha comprendido el material instruccional que lo precede. En cambio, ante un verdadero *problema*, el estudiante no

tiene a mano un procedimiento que le permita resolverlo, sino que debe utilizar su imaginación, creatividad e ingenio. Y éstas son precisamente las capacidades intelectuales que le permitirán tener éxito en su vida profesional, hallando soluciones creativas a los innumerables problemas del mundo actual que carecen de soluciones prefabricadas.

Los problemas de las olimpiadas matemáticas preuniversitarias son de naturaleza muy variada, pero a grandes rasgos se pueden clasificar en cuatro categorías: Geometría, Teoría de Números, Álgebra y Combinatoria. La *Teoría de Números* o *Aritmética*, de la cual nos ocupamos en este libro, es la rama de la matemática que estudia todo lo relacionado con los números naturales y enteros. El hecho de que estos números se estudien desde los primeros años de la enseñanza escolar podría hacer pensar que se trata de un tema elemental y sin misterios. Pero no es así, por el contrario, la Aritmética encierra algunos de los problemas más difíciles de la matemática, algunos de los cuales permanecen o han permanecido abiertos durante siglos. En la teoría de números avanzada se utilizan toda clase de herramientas matemáticas, como por ejemplo la teoría de funciones de variable compleja. Sin embargo, aún limitándonos a las nociones más básicas y elementales, es posible generar una gama inagotable de problemas de todos los grados de dificultad imaginables. Esta es la razón por la cual la Teoría de Números es uno de los temas infaltables y favoritos en todas las olimpiadas matemáticas.

Este libro está dirigido a los profesores de matemática interesados en ayudar a sus alumnos a obtener mejores resultados en las Olimpiadas Matemáticas, y en particular a aquellos que eventualmente deseen convertirse en entrenadores de los equipos que participan en estas competencias. También puede ser utilizado por estudiantes con alguna experiencia en olimpiadas matemáticas que se estén entrenando para estas competencias.

El material de los dos primeros capítulos es básico y en general se cubre en los programas de enseñanza media en Venezuela. Sin embargo los problemas propuestos son de tipo olímpico, y se debe dedicar un buen tiempo a trabajar en ellos. El dominio de estos dos capítulos debería ser suficiente para enfrentar con éxito los problemas de teoría de números que se proponen en las diferentes fases de la Olimpiada Juvenil de Matemáticas (OJM) en Venezuela.

En el capítulo 3 se estudian las congruencias módulo un entero, que son una herramienta invalorable y casi imprescindible para resolver los problemas de teoría de números que se proponen en las competencias internacionales. El dominio de este capítulo será de gran utilidad para los estudiantes que aspiren a participar en una competencia como la Olimpiada Matemática de Centroamérica y el Caribe (OMCC) o la Olimpiada Iberoamericana de Matemáticas (OIM).

El capítulo 4, dedicado a las ecuaciones diofánticas, contiene una mezcla de material básico (la ecuación $ax + by = c$) y avanzado (la ecuación de Pell-Fermat).

El capítulo 5 es más avanzado y contiene material útil para estudiantes que aspiren a participar en una IMO.

Algunos temas de este libro se pueden estudiar desde un punto de vista superior,

por ejemplo los teoremas de Fermat y Euler del Capítulo 2 son casos particulares de un resultado básico sobre grupos finitos. Sin embargo nuestro tratamiento es siempre elemental y al alcance de un buen estudiante de enseñanza media.

El Capítulo 6 contiene soluciones para todos los problemas propuestos. Pero es muy importante que no mire una solución antes de haber realizado un serio intento por resolver el problema usted mismo. De lo contrario, perderá una oportunidad de aprender y no disfrutará la satisfaccón de haber resuelto el problema con su propio esfuerzo.

Finalmente se incluye una bibliografía. Algunas obras son específicas sobre Teoría de Números ([1], [2], [3], [16]), otras contienen recomendaciones generales sobre resolución de problemas ([4], [12], [13], [14], [15]), y hay varias que recogen los problemas de la OJM venezolana y los de las competencias internacionales en las que participa Venezuela ([7], [8], [9], [10], [11]).

José H. Nieto S.

# Capítulo 1

# Números naturales

Los números *naturales* son los que usamos para contar: 1, 2, 3, 4,... Los nombres (uno, dos,...) o los símbolos mismos (1, 2,...) no tienen mayor importancia y varían según las lenguas y las culturas. El hecho esencial es que forman una *sucesión*, una lista ilimitada de elementos diferentes, que tiene un primer elemento (el 1) y en la cual cada elemento $n$ tiene un único *sucesor* $s(n)$. Así $s(1) = 2$, $s(2) = 3$, etc. El 1 no es sucesor de ningún natural, pero cualquier natural $n$ diferente de 1 es sucesor de un único número natural $p(n)$, el predecesor de $n$. Así $p(2) = 1$, $p(3) = 2$, etc.

El conjunto (infinito) de todos los números naturales se denota $\mathbb{N}$, es decir

$$\boxed{\mathbb{N} = \{1, 2, 3, 4, \ldots\}.}$$

Algunos autores agregan a los números naturales el cero, pero en esta obra no haremos eso. Será útil sin embargo considerar el conjunto $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ (los números naturales ampliados con el 0).

## 1.1. El orden en $\mathbb{N}$

Si $a$ aparece antes que $b$ en la lista 1, 2, 3,... se dice que $a$ es *menor que* $b$, y se escribe $a < b$. En este caso también se dice que $b$ es *mayor que* $a$, y se escribe $b > a$.

Es obvio que las relaciones $<$ y $>$ son *transitivas*, es decir:

Si $a < b$ y $b < c$ entonces $a < c$.

Si $a > b$ y $b > c$ entonces $a > c$.

También es claro que, dados dos naturales $a$ y $b$, una y sólo una de las relaciones siguientes es verdadera:

$$a = b, \qquad a < b, \qquad a > b.$$

Esta propiedad se conoce como *tricotomía*.

Se dice que $a$ es *menor o igual que* $b$, y se escribe $a \leq b$, si $a < b$ ó $a = b$. En este caso se dice también que $b$ es *mayor o igual que* $a$, y se escribe $b \geq a$. Las relaciones $\leq$ y $\geq$ también son transitivas, es decir que:

Si $a \leq b$ y $b \leq c$ entonces $a \leq c$.

Si $a \geq b$ y $b \geq c$ entonces $a \geq c$.

Para las relaciones $\leq$ y $\geq$ no vale la tricotomía. En cambio se cumple lo siguiente (antisimetría):

$a \leq b$ y $b \leq a$ son ambas verdaderas si y sólo si $a = b$.

La prueba es sencilla y se deja al lector.

A las desigualdades del tipo $a > b$ y $a < b$ se les llama *estrictas*, para distinguirlas de $a \leq b$ y $a \geq b$.

Sea $A$ un subconjunto de $\mathbb{N}$. Un número $c \in \mathbb{N}$ es *cota superior* de $A$ si $a \leq c$ para todo $a \in A$. Por ejemplo 6 es cota superior de $\{1, 2, 4\}$.

Si $c$ es cota superior de $A$ y además $c \in A$, entonces se dice que $c$ es el *máximo* de $A$. El máximo de $A$, si existe, es único. En efecto, si $c$ y $c'$ son máximos de $A$ entonces $c \leq c'$ y $c' \leq c$, luego por antisimetría $c = c'$.

Análogamente $c \in \mathbb{N}$ es *cota inferior* de $A$ si $c \leq a$ para todo $a \in A$. Si $c$ es cota inferior de $A$ y además $c \in A$, entonces se dice que $c$ es el mínimo de $A$. El mínimo de $A$, si existe, es único.

La siguiente es un propiedad muy importante de $\mathbb{N}$.

**Principio 1.1 (Principio del buen orden).**

| Todo subconjunto no vacío de $\mathbb{N}$ tiene mínimo. |
|---|

*Demostración.* Sea $A \subset \mathbb{N}$. Si $A$ no es vacío, algún natural está en $A$. Examinemos en orden los naturales 1, 2, 3,... hasta encontrar el primero que esté en $A$. Evidentemente ese es el mínimo de $A$. □

Muchas veces se aplica este principio en la siguiente forma:

| Toda sucesión estrictamente decreciente de números naturales es finita. |
|---|

En efecto, si $a_1 > a_2 > \cdots$ y $A = \{a_1, a_2, \ldots\}$ entonces $A$ debe tener un elemento mínimo $a_k$, y la sucesión debe detenerse allí pues si hubiese un $a_{k+1}$ sería menor que el mínimo, absurdo.

No es cierto en cambio que todo subconjunto de $\mathbb{N}$ tenga máximo. Por ejemplo $\mathbb{N}$ mismo no tiene máximo, ya que para cualquier $n \in \mathbb{N}$, el sucesor de $n$ es mayor que $n$.

Sin embargo, si $A \subset \mathbb{N}$ no es vacío y tiene una cota superior, entonces sí se puede afirmar que tiene máximo. En efecto, sea $B$ el conjunto de todas las cotas

superiores de $A$. Por el principio del buen orden, $B$ tiene un elemento mínimo $b$. Si $b = 1$ entonces $A$ sólo puede ser el conjunto $\{1\}$, y $b = 1$ es su máximo. Si $b > 1$ entonces $b$ tiene un predecesor $p(b)$. Como $p(b) < b$ y $b$ es la menor cota superior de $A$, $p(b)$ bo es cota superior de $A$ y por lo tanto existe algún $a \in A$ tal que $a > p(b)$. Pero $a \leq b$, luego tenemos que $p(b) < a \leq b$. Pero entre $p(b)$ y su sucesor $b$ no puede haber ningún otro natural, luego $a$ debe ser el mismo $b$ y listo, $b \in A$ y $b$ es el máximo de $A$.

Otro principio fundamental es el siguiente:

**Principio 1.2 (Principio de inducción matemática).**

> Si $A$ es un subconjunto de $\mathbb{N}$ tal que $1 \in A$, y para todo $a \in A$ se cumple también que $p(a) \in A$, entonces $A = \mathbb{N}$.

*Demostración.* Como $1 \in A$, se tiene que $2 = p(1) \in A$. Luego $3 = p(2) \in A$, $4 = p(3) \in A$, y así sucesivamente. Pero si recordamos lo que es $\mathbb{N}$, resulta claro que $A = \mathbb{N}$.

Este principio puede deducirse también del principio del buen orden (en realidad ambos principios son equivalentes). En efecto, supongamos por absurdo que $A \neq \mathbb{N}$. Entonces el conjunto $B = \mathbb{N} \setminus A$ no es vacío y por el principio del buen orden tiene un menor elemento $b$. Como $b > 1$ (pues $1 \in A$), $b$ tiene un precedente $p(b)$. Y como $p(b) < b$, $p(b)$ debe estar en $A$. pero entonces, por la propiedad de $A$, se tendría que $s(p(b)) = b \in A$, absurdo. □

El principio de inducción matemática es el fundamento de una importante técnica de demostración que se ilustrará más adelante.

## 1.2. Operaciones aritméticas

Dado cualquier par de números naturales $a$, $b$ se puede realizar su *suma* (o adición), que da por resultado un natural $a + b$. La suma $a + b$ se puede definir así: a partir de la aparición de $a$ en la sucesión de los naturales 1, 2, 3,. . . , a,. . . , contamos $b$ puestos hacia adelante, y el número que se encuentra allí es $a+b$. Esta es la manera en que los niños pequeños hacen sus primeras sumas, mucho antes de conocer la tabla de sumar o cualquier algoritmo para sumar números de varias cifras.

En particular $a + 1$ no es más que el sucesor de $a$. De aquí se desprende que, a partir del 1, se pueden generar aditivamente todos los números naturales. O sea: $2 = 1 + 1$, $3 = 2 + 1 = (1 + 1) + 1$, $4 = 3 + 1 = ((1 + 1) + 1) + 1$, etc. En las expresiones anteriores los paréntesis no son realmente necesarios, ya que la suma tiene la propiedad asociativa:

$$a + (b + c) = (a + b) + c.$$

Por lo tanto, en vez de $a+(b+c)$ o $(a+b)+c$, que son iguales, se puede escribir simplemente $a+b+c$. Así se tiene que

$$\mathbb{N} = \{1, 1+1, 1+1+1, 1+1+1+1, \ldots\}.$$

La suma tiene también la propiedad *conmutativa*:

$$a+b = b+a.$$

La suma no tiene elemento neutro en $\mathbb{N}$, pero si se define $a+0 = 0+a = a$ para todo $a \in \mathbb{N}_0$, resulta que 0 es neutro para la suma en $\mathbb{N}_0$.

La suma se comporta bien con respecto a las desigualdades: dos desigualdades del mismo sentido se pueden sumar miembro a miembro. Por ejemplo si $a \leq b$ y $a' \leq b'$, entonces $a+a' \leq b+b'$. Si al menos una de las dos desigualdades es estricta, al sumarlas se obtiene también una desigualdad estricta.

Si $a, b \in \mathbb{N}$ y $a > b$ entonces existe un único $c \in \mathbb{N}$ tal que $a+c = b$. En efecto, $c$ es el número de lugares después de $a$ donde se encuentra $b$. A ese número $c$ se le llama *diferencia* entre $a$ y $b$ y se denota $b-a$. Si $a = b$ entonces $b-a = 0$.

Otra operación que se puede realizar con dos números naturales $a$ y $b$ es su *producto* (o multiplicación), que se denota $a \times b$, $a \cdot b$ o simplemente $ab$. A los operandos $a$ y $b$ de un producto se les llama *factores*.

El producto tiene al 1 como elemento neutro, es decir que $a \cdot 1 = 1 \cdot a = a$.

Si $b > 1$, $ab$ es simplemente la suma de $b$ sumandos iguales a $a$, es decir

$$ab = \underbrace{a+a+\cdots+a}_{b \text{ sumandos}}.$$

El producto tiene las propiedades conmutativa ($ab = ba$) y asociativa ($(ab)c = a(bc)$).

El producto también se comporta bien con respecto a las desigualdades: dos desigualdades del mismo sentido se pueden multiplicar miembro a miembro. Por ejemplo si $a \leq b$ y $a' \leq b'$, entonces $aa' \leq bb'$. Si al menos una de las dos desigualdades es estricta, el resultado también será una desigualdad estricta.

La suma y el producto están relacionadas por la propiedad distributiva

$$a(b+c) = ab + ac.$$

El producto se extiende a $\mathbb{N}_0$ definiendo $a \cdot 0 = 0 \cdot a = 0$ para todo $a \in \mathbb{N}_0$.

La *potencia* de base $a$ y exponente $b$ se define de la siguiente manera:

- Por convención, $a^0 = 1$ y $a^1 = a$.
- Si $b > 1$, entonces
$$a^b = \underbrace{a \cdot a \cdots a}_{b \text{ factores}}.$$

Así, por ejemplo, $5^0 = 1$, $12^1 = 12$, $3^2 = 3 \cdot 3 = 9$, $2^3 = 2 \cdot 2 \cdot 2 = 8$. Las conocideas reglas de los exponentes nos dicen que

$$a^b \cdot a^c = a^{b+c}, \qquad (a^b)^c = a^{bc}.$$

## Una nota sobre notación

Con frecuencia se desea expresar sumas con un número muy grande de sumandos para escribirlos todos, por ejemplo la suma de los números naturales desde 1 hasta 100. En esos casos se suelen escribir solamente los primeros y los últimos términos, y los demás se sustituyen por puntos suspensivos:

$$1 + 2 + 3 + \cdots + 98 + 99 + 100.$$

Claro que esto no es muy preciso, pues también podría representar, digamos, la suma de los números del 1 al 100 que no son múltiplos de 30.

Una notación más exacta se logra usando el símbolo de *sumatoria* $\Sigma$, que no es más que la letra griega sigma mayúscula. Si $E(i)$ es una expresión que depende del número natural $i$ (llamado *índice* de la sumatoria), y si $a \leq b$ son números naturales, la expresión

$$\sum_{i=a}^{b} E(i)$$

representa la suma de todos los valores que resultan al evaluar $E(i)$ en los números naturales que van desde $a$ hasta $b$. Por ejemplo

$$\sum_{i=1}^{100} i$$

es la suma de los números del 1 al 100, y

$$\sum_{i=1}^{100} i^2$$

es la suma de los cuadrados de los números del 1 al 100.

Además del intervalo de variación del índice se pueden especificar otras condiciones, por ejemplo

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

indica la suma de todos los divisores $d$ del número $n$.

Existe una notación similar para productos, que utiliza la lietra griega pi mayúscula $\Pi$. Así por ejemplo

$$\prod_{i=1}^{n} i$$

representa el producto de todos los números naturales desde 1 hasta $n$, que se conoce como el *factorial* de $n$ y se denota $n!$.

**Ejemplo 1.3.** Probar que $\sum_{i=1}^{n} i = n(n+1)/2$.
Solución 1: Lo probaremos por inducción. Para $n = 1$ es cierto, ya que $1 = 1(1 + 1)/2$. Supongamos que es cierto para $n$, es decir que $\sum_{i=1}^{n} i = n(n+1)/2$. Entonces

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}.$$

Esto muestra que la identidad se cumple también para $n+1$, y por el principio de inducción se cumple para todos los naturales.
Solución 2: Cuando $i$ va de 1 a $n$, $n+1-i$ va de $n$ a 1, en forma decreciente. Por lo tanto

$$\sum_{i=1}^{n} i = \sum_{i=1}^{n} (n+1-i) = \sum_{i=1}^{n} (n+1) - \sum_{i=1}^{n} i,$$

luego

$$2\sum_{i=1}^{n} i = \sum_{i=1}^{n} (n+1) = n(n+1)$$

de donde $\sum_{i=1}^{n} i = n(n+1)/2$.
Observación: Las demostraciones por inducción tienen el inconveniente de que requieren conocer de antemano, o al menos intuir de alguna manera, el resultado. La segunda solución, en cambio, nos permite *descubrir* el resultado al mismo tiempo que demostrarlo.

## 1.3. Divisibilidad

Si $a$ y $b$ son números naturales, se dice que

| $a$ *divide* a $b$ si existe $k \in \mathbb{N}$ tal que $b = ka$. |
|---|

En este caso también se dice que $a$ es un *divisor* de $b$, que $b$ es *divisible* entre $a$ y que $b$ es *múltiplo* de $a$. Si $a$ divide a $b$ se escribe $a \mid b$, si no se escribe $a \nmid b$.

Para cualquier $a \in \mathbb{N}$ se cumple que $1 \mid a$ y que $a \mid a$, ya que $a = 1 \cdot a$. Es decir que cualquier número natural $a > 1$ tiene al menos dos divisores: 1 y él mismo. El 1 es un caso especial: sólo tiene un divisor, que es el mismo 1.

La divisibilidad es una relación *transitiva*, es decir que si $a \mid b$ y $b \mid c$ entonces $a \mid c$. En efecto, como $a \mid b$ entonces $b = ka$ para algún $k \in \mathbb{N}$, y como $b \mid c$ entonces $c = hb$ para algún $h \in \mathbb{N}$. Luego $c = hb = h(ka) = (hk)a$ (la última igualdad es consecuencia de la propiedad asociativa del producto), es decir $c = (hk)a$, y por lo tanto $a \mid c$.

También es inmediato ver que si un número divide a otros dos entonces divide a su suma. En efecto, si $a \mid b$ y $a \mid c$ entonces $b = ka$ y $c = ha$ para ciertos $k, h \in \mathbb{N}$. Luego $b + c = ka + ha = (k + h)a$ (por la propiedad distributiva), y $a \mid b + c$.

Observemos que si $a \mid b$ entonces $a \leq b$, ya que si $b = ka$, como $1 \leq k$ entonces $a = 1 \cdot a \leq ka = b$.

A los números naturales divisibles entre 2 (o, lo que es lo mismo, múltiplos de 2) se les llama *pares*, y a los demás impares. Es decir que los naturales pares son 2, 4, 6, 8,... y los impares 1, 3, 5, 7,...

## 1.4. Números primos

Un número natural $p$ se dice que es *primo* si es mayor que 1 y sólo es divisible entre 1 y $p$. La sucesión de los números primos comienza así:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Los números $n > 1$ que no son primos se llaman *compuestos*.

**Nota 1.4.** El 1 es especial: no es ni primo ni compuesto, es simplemente la unidad. A veces se plantea la duda: si el 1 sólo es divisible entre 1 y sí mismo, ¿entonces porqué no es primo? Por eso en nuestra definición exige explícitamente la condición de ser mayor que 1 para ser primo. Otra manera ingeniosa de excluir al 1 es decir que *un número natural es primo si tiene exactamente dos divisores*. De esta manera queda fuera el 1, que sólo tiene un divisor. En realidad lo de incluir o no al 1 entre los primos es una cuestión de convención y de hecho a lo largo de la historia hubo períodos en los cuales muchos autores consideraron al 1 como primo, pero al menos desde comienzos del siglo XX hay consenso en excluirlo. La razón principal para ello es que los enunciados de muchos teoremas se complicarían si se cpmsoderase al 1 como primo.

**Lema 1.5.** *Todo número natural $n > 1$ tiene al menos un divisor primo.*

*Demostración.* Si $n$ es primo, como $n$ divide a $n$ ya está. Si $n$ no es primo, entonces $n$ tiene al menos un divisor $a$ tal que $1 < a < n$. Sea $p$ el menor de esos divisores. Si $p$ no fuese primo entonces $p$ tendría un divisor $b$ tal que $1 < b < p$, y por transitividad $b$ sería un divisor de $n$, absurdo. Por lo tanto $p$ es primo. □

### 1.4.1. Teorema Fundamental de la Aritmética

La importancia de los números primos consiste en que cualquier número natural $n > 1$ es primo o puede expresarse como producto de primos. De esta manera los números primos son como los bloques fundamentales que permiten generar, multiplicativamente, todos los números naturales (del mismo modo que el 1 los genera aditivamente). Este resultado se conoce como *Teorema Fundamental de la*

*Aritmética*, y fue probado por Euclides($\approx$ 325–265 a.C.), quien dedicó el Libro IX de sus famosos *Elementos* a la Teoría de Números.

**Teorema 1.6.** *Todo número natural $n > 1$ tiene una única representación (excepto por el orden de los factores) como producto de primos.*

*Demostración.* En el enunciado anterior, si $p$ es primo se considera que $p$ es un "producto" con un único factor. De modo que si $n$ es primo, ya está. Si $n > 1$ no es primo, por el Lema precedente existe un primo $p_1$ tal que $n = p_1 k_1$. Si $k_1$ es primo ya está. Si no, existe un primo $p_2$ tal que $k_1 = p_2 k_2$. Si $k_2$ es primo entonces $n = p_1 p_2 k_2$ y ya está. Si no, continuamos de la misma manera y obtenemos una secuencia decreciente $k_1 > k_2 > k_3 > \cdots \geq 1$, que debe detenerse en cierto $k_r$ primo, y hemos probado la existencia de la factorización.

La unicidad será probada en el siguiente capítulo. □

Agrupando los factores primos iguales, se puede escribir cualquier número natural $n > 1$ en la forma

$$\boxed{n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}}$$

donde $p_1 < p_2 < \cdots < p_k$ son números primos y los exponentes $a_1, a_2, \ldots, a_k$ son números naturales.

Una consecuencia del Teorema Fundamental es que un número natural es una potencia $k$-ésima si y sólo si todos sus factores primos aparecen elevados a exponentes múltiplos de $k$.

### 1.4.2. Criba de Eratóstenes

Para determinar si un número natural $n > 1$ es o no primo, basta ver si es divisible por algún natural $k$ con $1 < k < n$. En realidad basta probar con los $k$ primos, y sólo con aquellos tales que $k^2 \leq n$ (puesto que si $k \mid n$ y $k^2 > n$, entonces $n/k$ también es un divisor de $n$ y $n/k < n$). En esto se basa el método de Eratóstenes (276 a.C. – 194 a.C.) para hallar los primos menores o iguales que $n$: se escriben los números del 2 al $n$ y luego se ejecuta repetitivamente la siguiente acción:

> Tome el menor número no tachado ni marcado, márquelo como primo y tache a todos sus múltiplos.

Esto se repite hasta que se marque como primo un número cuyo cuadrado supere a $n$. En ese momento el proceso se detiene y todos los números que queden sin tachar son primos.

Por ejemplo para $n = 30$ escribimos

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Marcamos el 2 en negrillas como primo y tachemos sus múltiplos:

**2** 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~

Ahora el primer número sin marcar ni tachar es el 3, lo marquemos en negrillas como primo y tachamos sus múltiplos:

**2 3** ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

Ahora el primer número sin marcar ni tachar es el 5, lo marquemos en negrillas como primo y tachamos sus múltiplos:

**2 3** ~~4~~ **5** ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

Ahora el primer número sin marcar ni tachar es el 7, pero como $7^2 = 49 > 30$, el proceso se detiene y obtenemos la siguiente lista de primos menores que 30:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

### 1.4.3. Cantidad de números primos

Euclides probó también (Proposición 20 del Libro IX) que existen infinitos números primos o, para ser más fieles a su manera de pensar, que los números primos son *más que cualquier cantidad finita*. En efecto, dado cualquier conjunto finito de números primos diferentes

$$p_1, p_2, \ldots, p_k$$

considere el número $N = p_1 p_2 \cdots p_k + 1$. Como $N$ no es divisible por ningún $p_i$, en su descomposición en factores primos debe aparecer por lo menos un primo $q$ tal que $q \notin \{p_1, p_2, \ldots, p_k\}$. Por lo tanto, ningún conjunto finito de números primos los contiene a todos.

### 1.4.4. El conjunto de divisores de un número natural

Si $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ entonces sus divisores son todos los números de la forma $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, con $0 \leq b_i \leq a_i$. Por ejemplo los divisores de $24 = 2^3 \cdot 3^1$ son $2^0 \cdot 3^0 = 1$, $2^1 \cdot 3^0 = 2$, $2^2 \cdot 3^0 = 4$, $2^3 \cdot 3^0 = 8$, $2^0 \cdot 3^1 = 3$, $2^1 \cdot 3^1 = 6$, $2^2 \cdot 3^1 = 12$ y $2^3 \cdot 3^1 = 24$.

Una consecuencia de lo anterior es que el número de divisores de $n$ (incluyendo al 1 y al propio $n$), que se denota $\tau(n)$, es

$$\boxed{\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1).}$$

En efecto, para formar un divisor el exponente de $p_1$ puede escogerse de $a_1 + 1$ maneras, a saber $0, 1, 2, \ldots, a_1$. De la misma manera, el exponente de $p_2$ puede escogerse de $a_2 + 1$ maneras y así sucesivamente hasta el exponente de $p_k$ que puede escogerse de $a_k + 1$ maneras.

Una función $f : \mathbb{N} \to \mathbb{Z}$ se dice que es *multiplicativa* si para cualquier par de números naturales $a$ y $b$ sin factores primos comunes, se cumple la igualdad

$$f(ab) = f(a)f(b).$$

La expresión que obtuvimos para $\tau(n)$ muestra claramente que $\tau$ es multiplicativa.

Si se desarrolla el producto

$$(1+p_1+p_1^2+\cdots+p_1^{a_1})(1+p_2+p_2^2+\cdots+p_2^{a_2})\cdots(1+p_k+p_k^2+\cdots+p_k^{a_k})$$

se obtienen todos los términos de la forma $p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k}$ con $0 \le b_i \le a_i$ para $i = 1, 2, \ldots, k$, es decir todos los divisores de $p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$. Por lo tanto la suma de todos los divisores de $n$, que se denota $\sigma(n)$, es

$$\begin{aligned}\sigma(n) &= (1+p_1+p_1^2+\cdots+p_1^{a_1})\cdots(1+p_k+p_k^2+\cdots+p_k^{a_k}) \\ &= \frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_k^{a_k+1}-1}{p_k-1}.\end{aligned}$$

Esta expresión muestra claramente que $\sigma$ es multiplicativa.

**Proposición 1.7.** *El número natural $n$ es primo si y sólo si $\sigma(n) = n+1$.*

*Demostración.* Si $n$ es primo entonces tiene exactamente dos divisores, 1 y $n$, luego $\sigma(n) = n+1$. Recíprocamente, si $\sigma(n) = n+1$, como 1 y $n$ son siempre divisores, $n$ no tiene más que ellos dos. Además $\sigma(n) \ge 1+1 = 2$, luego $n > 1$ y $n$ es primo. □

El producto de todos los divisores de $n$ es

$$\prod_{d|n} d = n^{\frac{1}{2}(a_1+1)(a_2+1)\cdots(a_k+1)}.$$

Una forma rápida de verlo es la siguiente: escribamos todos los divisores de $n$ en orden creciente, digamos $1 = d_1 < d_2 < \cdots < d_r = n$, donde $r = \tau(n) = (a_1+1)(a_2+1)\cdots(a_k+1)$. Si $d \mid n$ entonces también $\frac{n}{d} \mid n$, luego es claro que

$$\frac{n}{d_1} > \frac{n}{d_2} > \cdots > \frac{n}{d_r}$$

es también la lista de todos los divisores de $n$. Por lo tanto

$$\left(\prod_{d|n} d\right)^2 = \prod_{i=1}^{r} d_i \prod_{i=1}^{r} \frac{n}{d_i} = n^r,$$

y listo.

### 1.4.5. Números primos de Mersenne

La importante identidad

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$$

y su consecuencia para $n$ impar (sustituyendo $b$ por $-b$)

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1})$$

tienen interesantes consecuencias aritméticas.

**Proposición 1.8.** *Si $n$ es un número natural y $2^n - 1$ es primo, entonces $n$ es primo.*

*Demostración.* Si $2^n - 1$ es primo entonces $n \geq 2$ (ya que $2^1 - 1 = 1$ no es primo). Supongamos por absurdo que $n$ sea compuesto, entonces $n = rs$ con $r, s > 1$ y

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1).$$

Pero entonces $2^n - 1$ sería compuesto, absurdo. □

El recíproco no es cierto, es decir que hay primos $p$ para los cuales $2^p - 1$ no es primo. El primer ejemplo es $p = 11$, ya que $2^{11} - 1 = 2047 = 23 \cdot 89$. Los primos de la forma $2^p - 1$ se llaman *números primos de Mersenne*, en honor al padre Marin Mersenne, quien mantuvo correspondencia con Fermat y otros importantes matemáticos de su época. Hasta ahora se conocen 47 primos de Mersenne, el mayor de los cuales (que es también el mayor número primo conocido) es $2^{43112609} - 1$. Los primos de Mersenne más grandes se han hallado por medio de una búsqueda colectiva organizada a través de Internet. Si desea saber más sobre esto visite la página `http://www.mersenne.org`

### 1.4.6. Números primos de Fermat

Otro resultado interesante es el siguiente:

**Proposición 1.9.** *Si $n$ es un número natural y $2^n + 1$ es primo entonces $n$ es una potencia de 2.*

*Demostración.* Si $n$ es divisible por algún primo impar $p$ entonces $n = pr$ y

$$2^n + 1 = (2^r)^p + 1 = (2^r + 1)(2^{r(p-1)} - 2^{r(p-2)} + \cdots - 2^r + 1),$$

y $2^n + 1$ sería compuesto, absurdo. Por lo tanto si $2^n + 1$ es primo $n$ tiene como único factor primo al 2, es decir que $n$ es una potencia de 2. □

Si se pone $F_n = 2^{2^n} + 1$ entonces $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ y $F_4 = 65537$ son todos primos. En base a esto Fermat conjeturó en 1650 que todos los $F_n$ eran primos, pero en 1732 Euler halló que $F_5 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417$ es compuesto. De hecho, no se conoce ningún $F_n$ primo con $n > 5$. Los primos de la forma $2^{2^n} + 1$ se llaman *números primos de Fermat*.

### 1.4.7. Números perfectos

Un número natural $n$ se dice que es *perfecto* si $\sigma(n) = 2n$, es decir si $n$ es igual a la suma de todos sus divisores, exceptuado él mismo. Por ejemplo 6 es perfecto, ya que $1+2+3=6$. El siguiente número perfecto es el 28: $1+2+4+7+14=28$. Euclides probó el siguiente resultado:

**Proposición 1.10.** *Si $2^{n+1}-1$ es primo, entonces $2^n(2^{n+1}-1)$ es perfecto.*

*Demostración.* Si $p = 2^{n+1}-1$ es primo, entonces $\sigma(p) = 1+p = 2^{n+1}$. Por otra parte $\sigma(2^n) = 1+2+2^2+\cdots 2^n = 2^{n+1}-1$. Como $\sigma$ es multiplicativa y $2^n$ y $2^{n+1}-1$ no tienen factores primos comunes, entonces

$$\sigma(2^n(2^{n+1}-1) = \sigma(2^n)\sigma(2^{n+1}-1) = (2^{n+1}-1)2^{n+1} = 2\cdot 2^n(2^{n+1}-1).$$

□

Observemos que, como $2^2-1=3$ y $2^3-1=7$ son primos, $2\cdot 3 = 6$ y $2^2\cdot 7 = 28$ son perfectos. El siguiente número perfecto de esta forma es $2^4(2^5-1) = 496$. En general, para cada primo de Mersenne $2^p-1$ hay un número perfecto $2^{p-1}(2^p-1)$. ¿Hay otros números perfectos? La siguiente proposición nos da una respuesta parcial a esta pregunta.

**Proposición 1.11.** *Si $N$ es un número perfecto par, entonces existe un natural $n$ tal que $N = 2^n(2^{n+1}-1)$ y $2^{n+1}-1$ es primo.*

*Demostración.* Si $N$ es par, tiene al menos un factor 2. Agrupando todos los factores 2 se puede escribir $N = 2^n u$, con $n \geq 1$ y $u$ impar. Como $N$ es perfecto se tiene $\sigma(N) = 2N$, pero $\sigma(N) = \sigma(2^n)\sigma(u) = (2^{n+1}-1)\sigma(u)$, por lo tanto

$$(2^{n+1}-1)\sigma(u) = 2\cdot 2^n u,$$

de donde

$$2^{n+1}(\sigma(u)-u) = \sigma(u) = (\sigma(u)-u)+u,$$

y se sique que

$$(2^{n+1}-1)(\sigma(u)-u) = u.$$

Esto significa que $\sigma(u)-u$ es un divisor de $u$ menor que $u$. Pero $\sigma(u)-u$ es también la suma de todos esos divisores, luego es el único y debe ser 1, es decir $\sigma(u)-u=1$. Esto implica que $u$ es primo y $u = 2^{n+1}-1$. □

Es decir que los números perfectos pares son los identificados por Euclides, y sólo ellos. Queda la duda de si hay números perfectos impares. Hasta el presente nadie ha encontrado ninguno, pero tampoco se ha probado que no existan.

### 1.4.8. Algunos problemas abiertos sobre números primos

Dos números primos son *gemelos* si difieren en dos unidades. Por ejemplo 3 y 5, 5 y 7, 11 y 13, 17 y 19, 101 y 103, 1997 y 1999. ¿Existen infinitos pares de primos gemelos? No se sabe.

La *conjetura de Goldbach*, mencionada por primera vez en una carta de Goldbach a Euler en 1742, afirma que todo número par mayor que 2 es suma de dos números primos. Por ejemplo $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $1000 = 3 + 997$, $10000 = 59 + 9941$. Se conocen muchos resultados parciales, pero la conjetura aún no se ha probado ni refutado, aunque en los últimos años se han hecho muchos anuncios al respecto.

¿Existen infinitos números primos de Mersenne?

¿Existen infinitos números primos de Fermat?

## 1.5. Problemas

> Resolver un problema es hacer un descubrimiento. Un gran problema significa un gran descubrimiento, pero hay una partícula de descubrimiento en la solución de cualquier problema. El suyo puede ser modesto, pero si pone a prueba la curiosidad que induce a poner en juego las facultades inventivas, y si lo resuelve por medios propios, puede experimentar la tensión y el encanto del descubrimiento y el goce del triunfo.
>
> George Pólya [15]

**Problema 1.1.** En una de sus clases el profesor Darío escribió en la pizarra el número 12345679012345679, y dijo que era mágico. —¡Profesor, olvidó el 8! — Bueno, sí, pero no importa, dejémoslo así...—Profesor, ¿y qué tiene de mágico ese número? —Pues veamos, díganme una cifra del 1 al 9. —¡El 7, el 7! — Multipliquen el número mágico por 63. Los alumnos lo hacen, y obtienen con asombro 777777777777777. ¿Qué hubiese respondido Darío si los alumnos escogen el 3, o cualquier otra cifra? ¿Qué explicación tiene todo esto?

**Problema 1.2.** El producto de dos enteros consecutivos, ¿puede terminar en 8?

**Problema 1.3.** ¿En qué dígito termina $2^{2011}$?

**Problema 1.4.** Juan tiene 5 tarjetas con el número 2, 8 tarjetas con el número 3, 10 tarjetas con el número 7 y 20 tarjetas con el número 8, y las usa para formar números de varias cifras, colocándolas en fila. ¿Puede formar un número que sea un cuadrado perfecto?

**Problema 1.5.** (TT 2001) Si en la pizarra está escrito un número natural $n$, una *operación permitida* consiste en sustituirlo por el producto $ab$, si $a$ y $b$ son naturales tales que $a + b = n$. Inicialmente está escrito el número 22. ¿Existe una secuencia de operaciones permitidas que nos conduzca al número 2001?

**Problema 1.6.** Halle un número natural tal que, si su última cifra a la derecha se mueve al primer lugar de la izquierda, se obtiene un número doble del original.

**Problema 1.7.** Pruebe que $1 + 3 + 5 + \cdots + (2n - 1) = \sum_{i=1}^{n}(2i - 1) = n^2$ por inducción matemática y de alguna otra manera.

**Problema 1.8** (OJM 2009)**.** Los números desde el l hasta el 2009 se escriben consecutivamente en la pizarra. En una primera pasada se borran el primer número escrito, el tercero, el quinto y así sucesivamente hasta borrar el 2009. En una segunda pasada se aplica el mismo procedimiento a los números que quedaron, borrando el primero de ellos, el tercero, el quinto y así sucesivamente. Esto se repite mientras queden números en la pizarra. ¿En qué pasada se elimina el 1728? ¿Cuál es el último número borrado y en qué pasada se elimina?

**Problema 1.9.** Pruebe que $n(n+1)(n+2)$ es múltiplo de 6 para cualquier entero $n$.

**Problema 1.10.** Pruebe que $n(n+1)(n+2)(n+3)$ es múltiplo de 24 para cualquier entero $n$.

**Problema 1.11.** Probar que el número $1 + k^2 + k^4$ es compuesto para cualquier número $k$ entero mayor que 1.

**Problema 1.12.** Pruebe que para cualquier número natural $n$ el número $n^3 + 2n$ es múltiplo de 3.

**Problema 1.13.** (Eötvös 1894) Pruebe que $17|2m + 3n$ si y sólo si $17|9m + 5n$ ($m$ y $n$ enteros).

**Problema 1.14.** Caracterice los números naturales que tienen una cantidad impar de divisores.

**Problema 1.15** (AIME 1988)**.** Calcule la probabilidad de que un divisor de $10^{99}$, tomado al azar, sea múltiplo de $10^{88}$.

**Problema 1.16.** Para cada entero positivo $n$ sean $s(n)$ la suma y $p(n)$ el producto de sus dígitos. Determine si la cantidad de enteros positivos que verifican $s(n)^2 = p(n)$ es finita o infinita.

**Problema 1.17** (Canguro 2007, 9º)**.** Dado un número, una extraña calculadora sólo puede hacer lo siguiente: multiplicarlo por 2 o por 3, o calcular su segunda o tercera potencia. Si comenzamos con el número 15, ¿cuál de los siguientes resultados se puede obtener al usar la calculadora cinco veces consecutivas?

(a) $2^6\,3^6\,5^4$; (b) $2^8\,3^5\,5^6$; (c) $2^8\,3^4\,5^2$; (d) $2^3\,3^3\,5^3$; (e) $2\,3^2\,5^6$.

**Problema 1.18.** (Canguro 2007, 9º) Halle el menor número natural $A$ tal que $10A$ es un cuadrado perfecto y $6A$ es un cubo perfecto.

**Problema 1.19.** (Canguro 2009, 10º) Un número primo se dice que es *extraño* si tiene un solo dígito, o si tiene dos o más dígitos pero los dos números que se obtienen omitiendo el primero o el último dígito son también primos *extraños*. ¿Cuántos primos extraños hay?

**Problema 1.20.** (Canguro 2010, 10º) En cada lado de un pentágono se escribe un número natural, de manera tal que números adyacentes nunca tienen un factor común mayor que 1, pero números no adyacentes siempre tienen un factor común mayor que 1. Hay muchas posibilidades de hacer esto, pero uno de los números siguientes no aparecerá nunca en los lados del pentágono. ¿Cuál es?

(a) 15; (b) 18; (c) 19; (d) 21; (e) 22.

**Problema 1.21.** (Canguro 2008, 9º) Todos los divisores del entero positivo $N$, diferentes de $N$ y 1, se escriben en orden creciente. ¿Cuántos números naturales $N$ son tales que el mayor de los divisores escritos es 45 veces más grande que el menor?

**Problema 1.22.** (TT 2003, 9º) Si $k$ es un número natural, sea $m(k)$ su mayor divisor impar. Para cualquier número natural $n$ calcule $\sum_{k=n+1}^{2n} m(k)$.

**Problema 1.23.** Si $56a = 65b$, pruebe que $a + b$ es compuesto.

**Problema 1.24.** Pruebe que para cualquier número natural $n$ existen $n$ números naturales consecutivos que son compuestos.

**Problema 1.25** (OJM regional 2008)**.** Halle el menor entero positivo $n$ tal que cada dígito de $15n$ sea 0 ó 2.

**Problema 1.26** (OIM 1999)**.** Halle todos los enteros positivos que son menores que 1000 y cumplen con la siguiente condición: el cubo de la suma de sus dígitos es igual al cuadrado de dicho entero.

**Problema 1.27.** (OIM 1999) Sea $B$ un entero mayor que 10 tal que cada uno de sus dígitos pertenece al conjunto $\{1, 3, 7, 9\}$. Demuestre que $B$ tiene un factor primo mayor o igual que 11.

**Problema 1.28.** (OMCC 2014/1) Un entero positivo se denomina *tico* si es el producto de tres números primos diferentes que suman 74. Verifique que 2014 es tico. ¿Cuál será el próximo año tico? ¿Cuál será el último año tico de la historia?

**Problema 1.29.** (OMCC 2002/5) Encuentre un conjunto infinito de enteros positivos $S$ tal que para cada $n \geq 1$ y cualesquiera $n$ elementos distintos $x_1, x_2, \ldots, x_n$ de $S$, el número $x_1 + x_2 + \cdots + x_n$ no es un cuadrado perfecto.

**Problema 1.30.** Pruebe que existen infinitos números primos de la forma $4n+3$.

**Problema 1.31.** (IMO 1989/5) ¿Para qué enteros positivos $n$ existe un entero positivo $N$ tal que ninguno de los números $1+N$, $2+N$,$\ldots$, $n+N$ es una potencia de un primo?

**Problema 1.32.** (IMO 2002/4) Los divisores positivos del entero $n > 1$ son $d_1 < d_2 < \cdots < d_k$, con $d_1 = 1$ y $d_k = n$. Sea $d = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$. Pruebe que $d < n^2$ y halle todos los $n$ para los cuales $d$ divide a $n^2$.

# Capítulo 2

# Números enteros

El conjunto de los *números enteros* se obtiene agregando a los números naturales el 0 y los *enteros negativos* $-1$, $-2$, $-3$, $-4$, ... El conjunto que resulta se denota $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

Cuando se consideran como subconjunto de los enteros, a los naturales se les llama *enteros positivos*. Los *enteros no negativos* son 0, 1, 2, 3, 4,...

El *valor absoluto* de un entero $z$, denotado $|z|$, se define así: $|0| = 0$, $|a| = a$ y $|-a| = a$, para todo natural $a$. Por ejemplo $|-3| = 3$ y $|5| = 5$.

En $\mathbb{Z}$ hay un orden natural que extiende el de los múmeros naturales:

$$\cdots, -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < \cdots$$

Las operaciones de suma y producto se extienden fácilmente de $\mathbb{N}$ a $\mathbb{Z}$, conservándose las propiedades asociativa, conmutativa y distributiva. El 0 actúa como elemento neutro para la suma ($x + 0 = x$). Además cada entero $x$ tiene un opuesto $-x$ y se cumple $x + (-x) = 0$.

El producto sigue teniendo al 1 como elemento neutro. Además se tiene $x \cdot 0 = 0$ para todo $x \in \mathbb{Z}$ (el 0 es *absorbente* para el producto).

Igual que para los naturales, se dice que un entero $a$ *divide* (o es un *divisor*) de otro entero $b$ si existe $k \in \mathbb{Z}$ tal que $b = ka$. En este caso también se dice que $b$ es *múltiplo* de $a$, y se escribe $a \mid b$. Observe que $a \mid 0$ para todo $a \in \mathbb{Z}$, es decir que cualquier entero divide al 0, y 0 es múltiplo de cualquier entero.

Recordemos que para los números naturales, si $a \mid b$ entonces $a \leq b$. Esto no es cierto, en general, para los enteros: por ejemplo $3 \mid -6$ pero $3 > -6$. Y $2 \mid 0$ pero $2 > 0$. Sin embargo se cumple lo siguiente:

Si $a$ y $b$ son enteros no nulos y $a \mid b$, entonces $|a| \leq |b|$.

En efecto, es obvio que si $a \mid b$ entonces también $|a| \mid |b|$, y como $|a|$ y $|b|$ son naturales, el resultado se desprende del correspondiente (ya probado) para números naturales.

Los enteros múltiplos de 2 se denominan *pares*, y son $\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots$ Observe que 0 es par.

Los enteros que no son múltiplos de 2 se denominan *impares*, y son $\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots$

## 2.1. La división entera

**Teorema 2.1.** *Si $a$ y $b$ son enteros positivos, entonces existen enteros no negativos* únicos *$q$ y $r$ tales que*

$$a = qb + r \quad y \quad 0 \leq r < b.$$

*A $q$ y $r$ se les llama respectivamente* cociente *y* resto *de la división entera de $a$ entre $b$.*

*Demostración.* Probemos primero la *existencia* de $q$ y $r$.

Si $a < b$, basta tomar $q = 0$ y $r = a$. Si Si $a = b$, basta tomar $q = 1$ y $r = 0$. Supongamos entonces $a > b$. Como $b \geq 1$, para todo $n > a$ se cumple $nb \geq n > a$. Por lo tanto hay sólo un número finito de números naturales $n$ tales que $nb \leq a$. Sea $q$ el mayor de todos ellos. Entonces $qb \leq a$ pero $(q+1)b > a$. Sea $r = a - qb$. Entonces $a = qb + r$. De $qb \leq a$ resulta $r = a - qb \geq 0$. Y de $(q+1)b > a$ resulta $b > a - qb = r$. Es decir que $0 \leq r < b$.

Probemos ahora la unicidad. Para ello supongamos que $a = qb + r = q'b + r'$, donde $q$, $r$, $q'$ y $r'$ son enteros no negativos y $0 \leq r < b$ y $0 \leq r' < b$. Entonces $(q - q')b = r' - r$, es decir que $b$ divide a $r' - r$. Supongamos por absurdo que $r' - r \neq 0$. Entonces $b \leq |r' - r|$. Pero suponiendo que $r < r'$, de $0 \leq r < r' < b$ se sigue $|r' - r| = r' - r < b - 0 = b$, absurdo. de igual modo se llega a una contradicción si $r' < r$. por lo tanto sólo puede ser $r' - r = 0$, de donde $r' = r$, $qb = q'b$ y por tanto también $q' = q$. □

El teorema anterior se puede generalizar fácilmente al siguiente:

**Teorema 2.2.** *Si $a, b \in \mathbb{Z}$ y $b \neq 0$, entonces existen enteros* únicos *$q$ y $r$ tales que*

$$a = qb + r \quad y \quad 0 \leq r < |b|.$$

Al resultado anterior se le llama a veces *algoritmo de la división*, lo cual no es muy apropiado ya que se trata de un resultado de existencia y no de un procedimiento efectivo para hallar $q$ y $r$.

Observe que al dividir entre un entero $m > 0$ los restos sólo pueden ser 0, 1, $2, \ldots, m-1$. Así todos los enteros quedan particionados en $m$ conjuntos disjuntos, según cuál sea el resto que se obtiene al dividirlos entre $m$. Esos conjuntos se llaman *clases residuales módulo $m$*. Es muy fácil ver que dos enteros están en una misma clase resdual módulo $m$ si y sólo si su diferencia es divisible entre $m$. En efecto, si $a = qm + r$ y $a' = q'm + r$ entonces $a' - a = (q' - q)m$ y $m \mid a' - a$. Recíprocamente si $a = qm + r$ y $a' - a = km$ entonces $a' = a + km = (q + k)m + r$.

Un conjunto de $m$ enteros $S = \{r_1, r_2, \ldots, r_m\}$ se dice que es un *sustema completo de residuos* (SCR) módulo $m$ si cada uno de ellos pertenece a una clase residual diferente módulo $m$, en otras palabras, si para cada $j \in \{0, 1, \ldots, m-1\}$ existe un $r_i \in S$ tal que $r_i \equiv j \pmod{m}$. Evidentemente $\{0, 1, \ldots, m-1\}$ es un SCR módulo $m$. Más en general, $\{a, a+1, a+2, \ldots, a+m-1\}$ es un SCR módulo $m$ para cualquier entero $a$.

Si $m = 2k+1$ un SCR muy usado es $\{-k, -k+1, \ldots, -1, 0, 1, \ldots, k\}$, y si $m = 2k$ entonces $\{-k+1, \ldots, -1, 0, 1, \ldots, k\}$.

**Paridad**

La división entera entre 2 sólo puede dejar resto 0 ó 1. Los enteros que dejan resto 0 son los pares, y los que dejan resto 1 son los impares. Todos los pares son de la forma $2q$, y los impares son de la forma $2q+1$.

Es claro que la suma de dos enteros pares es par, y más aun la suma de cualquier cantidad de sumandos pares es par. La suma de dos impares también es par, ya que

$$(2q+1) + (2q'+1) = 2q + 2q' + 2 = 2(q + q' + 1).$$

La suma de un par y un impar es impar, ya que

$$2q + (2q'+1) = 2(q + q') + 1.$$

La paridad de una suma de varios impares depende de la cantidad de sumandos. Ya sabemos que la suma de dos impares es par. Si se suma un tercer impar, tendremos la suma de un par y un impar, que es impar. Si se suma un cuarto impar, tendremos la suma de un impar y un impar, que es par. Y así sucesivamente es decir que la suma de impares es par o impar según que la cantidad de sumandos sea par o impar, respectivamente.

El producto de un entero par por otro entero cualquiera es obviamente par. El producto de dos impares es impar, ya que $(2q+1)(2s+1) = 2(2qs+q+s)+1$. Y por lo tanto el producto de cualquier cantidad de enteros impares es impar.

## 2.2. Sistemas de numeración

La manera más antigua de representar simbólicamente los números naturales parece haber sido la de hacer marcas en un palo: I, II, III, IIII, IIIII, ... Los griegos utilizaron letras para abreviar la notación, al igual que los romanos, que además utilizaron un complicado sistema aditivo-sustractivo: $XI = X + I = 11$, $IX = X - I = 9$. Ninguno de estos sistemas era muy apropiado para realizar cálculos complejos. Los sistemas modernos se caracterizan por la notación posicional y el uso del cero. El primer uso documentado de un sistema de este tipo data del año 36 a.C., y se debe a la civilización maya.

Si $b \in \mathbb{N}$, la representación de un número $n \in \mathbb{N}_0$ en *base* $b$ es la sucesión $a_k a_{k-1} \dots a_1 a_0$, donde cada $a_i$ pertenece al conjunto $\{0, 1, \dots, b-1\}$ y

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.$$

Nuestro sistema de numeración usual es el de base 10, con dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Así por ejemplo

$$2015 = 2 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10 + 5.$$

En computación es muy usado el sistema *binario*, de base 2, en el cual 2015 se expresa como 11111011111. También se usa el sistema *hexadecimal*, de base 16, el cual requiere cifras del 0 al 15. Para ello se usan las letras A, B, C, D, E y F para representar 10, 11, 12, 13, 14 y 15, respectivamente. Así por ejemplo el número B3F, en hexadecimal, corresponde al decimal $11 \cdot 16^2 + 3 \cdot 16 + 15 = 2879$.

El sistema de numeración maya tiene base 20. El símbolo para el cero es  . Los números del 1 al 19 se representan mediante puntos (que valen 1) y rayas (que valen 5). Las unidades se colocaban abajo, encima de éstas iban las unidades de 20, encima las unidades de $20^2$ y así sucesivamente.

Para indicar que un número está expresado en una base diferente de 10, se suele escribir el número entre paréntesis, seguido de la base $b$ como subíndice. Por ejemplo $(321)_7 = 3 \cdot 7^2 + 2 \cdot 7 + 1 = 162$.

Para escribir un número natural $n$ en una base $b$, se efectúa la división entera de $n$ entre $b$: $n = q_0 b + r_0$. Luego se divide $q_0$ entre $b$: $q_0 = q_1 b + r_1$. Luego se divide $q_1$ entre $b$, y se continúa así hasta obtener un cociente $q_k = 0$. Entonces

$$n = q_0 b + r_0 = q_1 b^2 + r_1 b + r_0 = \cdots = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0.$$

Por lo tanto la representación de $n$ en base $b$ es $r_k r_{k-1} \dots r_1 r_0$. Por ejemplo $2747 = 343 \cdot 8 + 3$, $343 = 42 \cdot 8 + 7$, $42 = 5 \cdot 8 + 2$, $5 = 0 \cdot 8 + 5$, luego $2747 = (5273)_8$.

En la escuela se dedica bastante tiempo al aprendizaje de las tablas de sumar y multiplicar y a los algoritmos para sumar y multiplicar números de varias cifras, en el sistema decimal. Si bien todo ello es importante y útil, hay que ponerlo en su justa perspectiva. Los algoritmos no son la definición de las operaciones. Además no son la única manera de efectuar los cálculos, de hecho existen varios algoritmos alternativos. Por último, son dependientes de la base 10. Si quisiéramos aplicarlos para operar con números en base 8, por ejemplo, deberíamos aprender las tablas en base 8.

## 2.3. Máximo común divisor

El *máximo común divisor* de dos números naturales $a$ y $b$ es el mayor de sus divisores comunes y se denota $\mathrm{mcd}(a, b)$. El mcd tiene las siguientes propiedades,

de muy fácil demostración:

$$\begin{aligned} & & \mathrm{mcd}(a,1) &= 1, \\ & & \mathrm{mcd}(a,b) &= \mathrm{mcd}(b,a), \\ & & \mathrm{mcd}(a,b) &= a \quad \text{si y sólo si} \quad a \mid b, \\ \text{Si } a > b, \text{ entonces} & & \mathrm{mcd}(a,b) &= \mathrm{mcd}(a-b,b), \\ \text{Si } a = qb + r, \text{ entonces} & & \mathrm{mcd}(a,b) &= \mathrm{mcd}(b,r). \end{aligned}$$

Si $\mathrm{mcd}(a,b) = d$ entonces $a = a'd$, $b = b'd$, para ciertos naturales $a'$ y $b'$. Si $c$ es un divisor común de $a'$ y $b'$ entonces $cd$ es un divisor común de $a'd$ y $b'd$ y por lo tanto $cd \leq d$. Luego $c = 1$ y se concluye que $\mathrm{mcd}(a', b') = 1$.

### 2.3.1. Algoritmo de Euclides

El $\mathrm{mcd}(a,b)$ se puede obtener aplicando el siguiente algoritmo, debido a Euclides: escribamos $a = bq + r$ con $0 \leq r < b$. Si $r = 0$ entonces $b \mid a$ y $\mathrm{mcd}(a,b) = b$. Si $r \neq 0$, entonces $\mathrm{mcd}(a,b) = \mathrm{mcd}(bq + r, b) = \mathrm{mcd}(r,b)$ y el problema se reduce a calcular $\mathrm{mcd}(b,r)$. Prosiguiendo de esta manera eventualmente se obtiene el resultado.

**Ejemplo 2.3.** Hallar $\mathrm{mcd}(3127, 2491)$ mediante el algoritmo de Euclides.

*Solución.*

$$\begin{aligned} 3127 &= 2491 + 636, \\ 2491 &= 3 \cdot 636 + 583, \\ 636 &= 583 + 53, \\ 583 &= 5 \cdot 53. \end{aligned}$$

y por lo tanto $\mathrm{mcd}(3127, 2491) = 53$. es interesante hacer los cálculos por descomposición en producto de factores primos y comparar el trabajo realizado. □

**Teorema 2.4** (Teorema de Bezout)**.** *Existen enteros $s$ y $t$ tales que* $\mathrm{mcd}(a,b) = sa + tb$.

Esto es consecuencia inmediata del algoritmo de Euclides. Por ejemplo, aprovechando los cálculos que acabamos de hacer se tiene

$$\begin{aligned} &\mathrm{mcd}(3127, 2491) = 53 = 636 - 583 = 636 - (2491 - 3 \cdot 636) \\ &= 4 \cdot 636 - 2491 = 4(3127 - 2491) - 2491 = 4 \cdot 3127 - 5 \cdot 2491. \end{aligned}$$

Una consecuencia importante de esta manera de expresar el máximo común divisor es el siguiente:

**Lema 2.5** (Lema de Euclides)**.** *Si $a \mid bc$ y* $\mathrm{mcd}(a,b) = 1$*, entonces $a \mid c$.*

*Demostración.* Para ciertos enteros $s$ y $t$ se tiene $1 = \text{mcd}(a, b) = sa + tb$. Multiplicando por $c$ resulta $c = sac + tbc$ y como $a \mid sac$ y $a \mid tbc$ se tiene que $a \mid sac + tbc = c$. □

Dos números $a$ y $b$ se dicen *coprimos*, *primos relativos* o *primos entre sí* si no tienen más divisor común que 1, es decir si $\text{mcd}(a, b) = 1$. Observe que dos primos diferentes $p$ y $q$ son siempre coprimos.

**Lema 2.6.** *Si* $\text{mcd}(a, b) = \text{mcd}(a, c) = 1$*, entonces* $\text{mcd}(a, bc) = 1$*.*

*Demostración.* En efecto, sea $d = \text{mcd}(a, bc)$. Como $d \mid a$ y $\text{mcd}(a, b) = 1$, es claro que $\text{mcd}(d, b) = 1$. Luego por el lema de Euclides $d \mid c$. Y como $\text{mcd}(a, c) = 1$, $d = 1$. □

**Corolario 2.7.** *Si* $\text{mcd}(a, b_1) = \text{mcd}(a, b_2) = \cdots = \text{mcd}(a, b_k) = 1$*, entonces* $\text{mcd}(a, b_1 b_2 \cdots b_k) = 1$*.*

*Demostración.* Por el lema 2.6, $\text{mcd}(a, b_1 b_2) = 1$. Aplicando el lema nuevamente a $b_1 b_2$ y $b_3$, resulta $\text{mcd}(a, b_1 b_2 b_3) = 1$. Continuando de esta manera, en $k - 1$ pasos se llega a $\text{mcd}(a, b_1 b_2 \cdots b_k) = 1$. □

**Lema 2.8.** *Sean* $p$*,* $q_1$*,* $q_2$*,. . . ,* $q_k$ *primos. Si* $p \mid q_1 q_2 \cdots q_k$*, entonces* $p$ *es igual a algún* $q_i$*.*

*Demostración.* Si $p$ fuese diferente a todos los $q_i$, sería coprimo con todos ellos, y por el corolario 2.7 sería coprimo con $q_1 q_2 \cdots q_k$. □

A continuación se concluye la demostración del Teorema Fubdamental de la Aritmética. La existencia de la descomposición en producto de factores primos ya se probó en el capítulo anterior, ahora probaremos la unicidad.

**Teorema 2.9** (Unicidad de la factorización en primos)**.** *Dos descomposiciones de un número natural* $n > 1$ *como producto de primos pueden diferir solamente en el orden de los factores.*

*Demostración.* Digamos que dos descomposiciones de un número natural como producto de primos son *esencialmente diferentes* si difieren en algo más que el orden de los factores, es decir si tienen un número distinto de factores o si alguna de ellas contiene un primo que no aparece en la otra. Supongamos por absurdo que exista un natural que admita dos descomposiciones esencialmente diferentes como producto de primos. Entonces, por el principio del buen orden, debe existir un menor natural $n$ con esa propiedad. Sean $p_1 p_2 \cdots p_k$ y $q_1 q_2 \cdots q_h$ dos descomposiciones esencialmente diferentes de $n$. Como $p_1 \mid q_1 q_2 \cdots q_h$, por el lema 2.8 debe ser $p_1 = q_j$ para algún $j$. Pero entonces $p_2 \cdots p_k$ sería una descomposición de $n/p_1$ esencialmente diferente de la que se obtiene al suprimir el factor $q_j$ en $q_1 q_2 \cdots q_h$. Esto es una contradicción, pues $n/p_1 < n$. □

Si se conoce la descomposición en producto de factores primos de $a$ y de $b$, entonces es muy fácil calcular $\mathrm{mcd}(a,b)$: es igual al producto de los factores primos comunes elevados al menor de los exponentes con que aparecen en las descomposiciones de $a$ y $b$. De aquí se deduce que $\mathrm{mcd}(a,b)$ no sólo es el mayor divisor común sino que además cualquier otro divisor común de $a$ y $b$ *divide* a $\mathrm{mcd}(a,b)$. Por ejemplo $406 = 2 \cdot 7 \cdot 29$ y $147 = 3 \cdot 7^2$, por lo tanto $\mathrm{mcd}(406, 147) = 7$.

Sin embargo desde el punto de vista computacional el algoritmo de Euclides es un método más eficiente para calcular el mcd. Hallar la descomposición en factores primos, salvo para números pequeños, es un problema computacionalmente intensivo.

## 2.4. Mínimo común múltiplo

El mínimo común múltiplo de $a$ y $b$ es el menor de sus múltiplos comunes y se denota $\mathrm{mcm}(a,b)$. El $\mathrm{mcm}(a,b)$ es igual al producto de los factores primos comunes y no comunes elevados al mayor de los exponentes con que aparecen en $a$ y $b$. De aquí se deduce que $\mathrm{mcm}(a,b)$ no sólo es el menor múltiplo común sino que además *divide* a cualquier otro múltiplo común de $a$ y $b$.

El $\mathrm{mcd}(a,b)$ y el $\mathrm{mcm}(a,b)$ satisfacen la relación

$$\mathrm{mcd}(a,b) \cdot \mathrm{mcm}(a,b) = ab.$$

Si un número natural es divisible entre el producto $ab$ de otros dos, entonces es divisible entre cada uno de ellos. El recíproco no es cierto: 12 es divisible entre 4 y entre 6 pero no es divisible entre $4 \cdot 6 = 24$. Lo que siempre se puede afirmar es que si $n$ es múltiplo de $a$ y de $b$ entonces $n$ es múltiplo de $\mathrm{mcm}(a,b)$.

## 2.5. Problemas

**Problema 2.1.** (Canguro 2007, 10º) Un entero positivo al ser dividido entre 4 deja resto 1 y al ser dividido entre 5 deja resto 3. ¿Qué resto deja al ser dividido entre 20?

**Problema 2.2.** (Canguro 2007, 11º) Si dividimos 336 entre el número natural $n$ el resto es 2. Entonces el resto que se obtiene al dividir 2007 entre $n$ es:

(a) 100; (b) 3; (c) 2; (d) 1; (e) 0.

**Problema 2.3.** (Canguro 2007, 8º) Cinco números enteros se escriben alrededor de un círculo de manera que la suma de dos o de tres números adyacentes no sea nunca múltiplo de 3. ¿Cuántos de los cinco números son múltiplos de 3?

**Problema 2.4.** (TT 1988) Los números enteros del 1 al 64 se escriben cada uno en una casilla de un tablero de ajedrez de $8 \times 8$, de izquierda a derecha y de arriba

hacia abajo (es decir que en la primera fila se escriben 1, 2, 3, 4, 5, 6, 7 y 8, en la segunda fila 9, 10, 11, 12, 13, 14, 15 y 16, y así sucesivamente). A cada número se le pone un signo + o −, de manera tal que en cada fila y en cada columna haya 4 signos + y 4 signos −. Calcule la suma de todos los números del tablero.

**Problema 2.5.** Halle el menor entero mayor que 1 tal que al dividirlo entre 2, 3, 4, 5, 6, 7, 8 o 9 deja resto 1.

**Problema 2.6.** Halle el menor entero positivo tal que al dividirlo entre 2 deja resto 1, al dividirlo entre 3 deja resto 2, al dividirlo entre 4 deja resto 2, al dividirlo entre 5 deja resto 4, al dividirlo entre 6 deja resto 5, al dividirlo entre 7 deja resto 6, al dividirlo entre 8 deja resto 7 y al dividirlo entre 9 deja resto 8.

**Problema 2.7.** (OMCC 2013/1) Juan escribe la lista de parejas $(n, 3^n)$, con $n = 1, 2, 3, \ldots$ en un pizarrón. A medida que va escribiendo la lista, subraya las parejas $(n, 3^n)$ cuando $n$ y $3^n$ tienen la misma cifra de las unidades. De las parejas subrayadas, ¿cuál ocupa la posición 2013?

**Problema 2.8.** ¿Cuál es el exponente de 7 en la descomposición de 2011! en producto de factores primos?

**Problema 2.9.** Considere las sumas

$$S_n = \sum_{i=2}^{n} \frac{1}{i} = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

¿Existe algún entero $n \geq 2$ para el cual $S_n$ sea entero?

**Problema 2.10.** ¿En cuántos ceros termina 2011!?

**Problema 2.11.** El cuentakilómetros de un carro tiene un defecto: en cualquiera de las posiciones, después del 5 se pasa al 7, saltando el 6. Por ejemplo si está en 00025 y recorre un 1 km, pasa a 00027. Y de 00599 pasa a 00700. Si actualmente marca 02015, ¿cuántos kilómetros recorrió desde que estaba en 00000?

**Problema 2.12.** Juan escribió lo siguiente en una tarea de matemática:

$$\begin{array}{rr} & 34 \\ \times & 57 \\ \hline & 261 \\ & 182 \\ \hline & 2181 \end{array}$$

y obtuvo 20 puntos. ¿Cuál es la explicación?

**Problema 2.13.** Se escriben en fichas todos los números naturales desde el 11111 hasta el 99999. Luego estas fichas se colocan en un orden arbitrario formando una cadena. Demuestre que el número obtenido, que tiene 444445 cifras, no puede ser potencia de 2.

**Problema 2.14.** (OMCC 2012/1) Hallar todos los enteros positivos que sean iguales a 700 veces la suma de sus dígitos.

**Problema 2.15.** Sean $a = \underbrace{999\ldots999}_{40 \text{ nueves}}$ y $b = 999999999999$. Halle $\text{mcd}(a, b)$.

**Problema 2.16.** Juan, Mario y Pedro entrenan dando vueltas en bicicleta a una pista circular. Juan tarda 8 minutos en dar una vuelta, Mario tarda 9 minutos y Pedro tarda 12 minutos. Si los tres parten del mismo punto a las 6:00 am, ¿a qué hora volverán a encontrarse?

**Problema 2.17.** Pruebe que todo número natural tiene un múltiplo cuyos dígitos son solamente unos o ceros.

**Problema 2.18.** Pruebe que todo número natural coprimo con 10 tiene un múltiplo cuyos dígitos son todos unos.

**Problema 2.19.** Se tiene una hoja rectangular de papel milimetrado de $259 \times 154$. Si se traza una diagonal, ¿cuántos cuadraditos atraviesa?

Se dice que la diagonal atraviesa un cuadradito si contiene al menos un punto interior del mismo.

**Problema 2.20** (OJM 2009)**.** Ana vende galletas, que vienen en cajas pequeñas de 5 unidades y en cajas grandes de 12 unidades. Si, por ejemplo, un cliente quiere 39 galletas, Ana puede despachar el pedido exactamente con tres cajas pequeñas y dos grandes, ya que $3 \times 5 + 2 \times 12 = 39$. Pero hay pedidos que no se pueden despachar exactamente, por ejemplo, cuando un cliente quiere 7, 16 ó 23 galletas. ¿Cuál es el pedido más grande que no se puede despachar exactamente?
Nota: Se supone que Ana tiene o puede pedir a la fábrica todas las galletas que le hagan falta.

**Problema 2.21.** Sean $a$ y $b$ naturales coprimos. Pruebe que cualquier natural suficientemente grande puede expresarse en la forma $sa + tb$ con $s$ y $t$ enteros no negativos. ¿Cuál es el mayor entero que no se puede expresar en esa forma?

**Problema 2.22.** (OBM 2009/4) Probar que existe un entero positivo $n_0$ tal que, para cualquier entero $n \geq n_0$, es posible partir un cubo en $n$ cubos más pequeños.

**Problema 2.23.** Los *Números de Fibonacci* se definen recursivamente así:
$F_0 = 0$, $F_1 = 1$ y $F_n = F_{n-1} + F_{n-2}$ para $n \geq 2$.

a) Pruebe que $\text{mcd}(F_n, F_{n+1}) = 1$ para todo $n \geq 1$.

b) Pruebe que si $0 \leq m < n$ entonces $F_n = F_{m+1}F_{n-m} + F_mF_{n-m-1}$.

c) Pruebe que $\text{mcd}(F_n, F_m) = F_{\text{mcd}(n,m)}$.

**Problema 2.24.** (OM 2005, 1$^{\text{er}}$ Nivel) Un número entero se llama *autodivi* si es divisible entre el número de dos cifras formado por sus dos últimos dígitos (decenas y unidades). Por ejemplo, 78013 es autodivi pues es divisible entre 13, 8517 es autodivi pues es divisible entre 17. Halle 6 números enteros consecutivos que sean autodivi y que tengan las cifras de las unidades, de las decenas y de las centenas distintas de 0.

**Problema 2.25.** Sea $S(n)$ la suma de los dígitos de la expresión decimal del número natural $n$ (por ejemplo $S(748) = 7 + 4 + 8 = 19$). ¿Qué relación existe entre $S(2n)$ y $2S(n)$?

**Problema 2.26** (OMCC 2008)**.** Halle el menor entero positivo $N$ tal que la suma de sus cifras sea 100, y la suma de las cifras de $2N$ sea 110.

**Problema 2.27.** (OMA 2012) Para cada número natural $n$ sea $S(n)$ la suma de sus dígitos. Hallar el menor natural $n$ tal que $9S(n) = 16S(2n)$.

**Problema 2.28.** (IMO 2011/5) Sea $f$ una función del conjunto de los enteros al conjunto de los enteros positivos. Se supone que para cualesquiera dos enteros $m$ y $n$, la diferencia $f(m) - f(n)$ es divisible por $f(m-n)$. Demostrar que para todos los enteros $m$ y $n$ con $f(m) \leq f(n)$, el número $f(n)$ es divisible por $f(m)$.

# Capítulo 3

# Congruencias

La noción de *congruencia* fue introducida por Gauss (1777–1855) en su libro *Disquisitiones Arithmeticae*. Son una herramienta fundamental en teoría de números, ya que sumplifican muchos cálculos, así como la presentación de resultados.

## 3.1. Definición y propiedades básicas

**Definición 3.1.** Se dice que dos enteros $a$ y $b$ son *congruentes* módulo $m$ si $m \mid (a-b)$. En ese caso se escribe

$$a \equiv b \pmod{m}.$$

Las congruencia módulo $m$ tiene muchas propiedades similares a las de la igualdad. En particular es reflexiva, simétrica y transitiva (es decir que es una relación de equivalencia).

La reflexividad $a \equiv a \pmod{m}$ es evidente, al igual que la simetría:

$$\text{Si } a \equiv b \pmod{m} \text{ entonces } b \equiv a \pmod{m}.$$

La transitividad:

$$\text{Si } a \equiv b \pmod{m} \text{ y } b \equiv c \pmod{m} \text{ entonces } a \equiv c \pmod{m}$$

también se prueba fácilmente: de las hipótesis se obtiene que $m \mid a-b$ y $m \mid b-c$, luego $m \mid (a-b)+(b-c) = a-c$, es decir que $a \equiv c \pmod{m}$.

Las congruencias de un mismo módulo también se pueden sumar, restar y multiplicar miembro a miembro:

Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces:

$$\begin{aligned} a+c &\equiv b+d \pmod{m}, \\ a-c &\equiv b-d \pmod{m}, \\ ac &\equiv bd \pmod{m}. \end{aligned}$$

La prueba de todas estas propiedades es inmediata. Por ejemplo la última se prueba así: como $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ se tiene, por definición, que $p \mid (a-b)$ y $p \mid (c-d)$. Pero $ac - bd = ac - ad + ad - bd = a(c-d) + (a-b)d$, por lo tanto $p \mid (ac-bd)$ y $ac \equiv bd \pmod{m}$.

De estas propiedades se sigue que si $a \equiv b \pmod{m}$ y $P(x)$ es un polinomio con coeficientes enteros, entonces $P(a) \equiv P(b) \pmod{m}$.

Si $\mcd(a,m) = 1$ entonces $a$ tiene un *inverso multiplicativo* módulo $m$, es decir un número $s$ tal que $as \equiv 1 \pmod{m}$. En efecto, como $sa + tm = 1$ para ciertos enteros $s$ y $t$, resulta $sa = 1 - tm \equiv 1 \pmod{m}$. Este inverso multiplicativo es único módulo $m$, ya que si $sa \equiv s'a \equiv 1 \pmod{m}$ entonces, como $\mcd(a,m) = 1$, se deduce $s \equiv s' \pmod{m}$. La existencia del inverso multiplicativo permite resolver ecuaciones lineales en congruencias del tipo $ax \equiv b \pmod{m}$. En efecto, basta multiplicar la congruencia por $s$ y resulta $sax \equiv sb \pmod{m}$, o sea $x \equiv sb \pmod{m}$.

Si $m \neq 0$ y $r$ es el resto de la división de $a$ entre $m$, entonces $a = mq + r$ y $m \mid (a-r)$, es decir que $a \equiv r \pmod{m}$. Como $0 \leq r < m$ podemos decir que cualquier entero es congruente módulo $m$ con uno de los números $0, 1, \ldots, m-1$. Si $a$ y $b$ dejan el mismo resto $r$ al dividirlos entre $m$, entonces $a \equiv r \equiv b \pmod{m}$ y por transitividad $a \equiv b \pmod{m}$. Recíprocamente, si $a \equiv b \pmod{m}$ y al dividir $a$ y $b$ entre $m$ se obtienen restos $r$ y $s$, respectivamente, entonces $r \equiv a \equiv b \equiv s \pmod{m}$ y por transitividad resulta $r \equiv s \pmod{m}$, es decir $m \mid (r-s)$. Pero como $0 \leq r, s < m$ se tiene que $0 \leq |r-s| < m$, y la única posibilidad para que $m$ divida a $r-s$ es $r-s=0$, es decir $r=s$. En resumen, $a \equiv b \pmod{m}$ si y sólo si al dividir $a$ y $b$ entre $m$ se obtienen restos iguales.

**Ejemplo 3.2.** Calcular el resto de la división de $2^{2011}$ entre 7.

*Solución.* Calcular $2^{2011}$ para después efectuar la división está claramente fuera de nuestro alcance (al menos con lápiz y papel). Pero como $2^3 = 8 \equiv 1 \pmod{7}$ se tiene

$$2^{2011} = 2^{3 \cdot 670 + 1} = (2^3)^{670} \cdot 2 \equiv 1^{670} \cdot 2 \equiv 2 \pmod{7}$$

□

## 3.2. Criterios de divisibilidad

Existen varios *criterios de divisibilidad* que permiten averiguar rápidamente si un número natural es divisible entre otros números naturales pequeños. Los más

conocidos afirman que un número es divisible entre:

**2** si y sólo si su última cifra es par.

**3** si y sólo si la suma de sus cifras es divisible entre 3.

**4** si y sólo si el número formado por sus dos últimas cifras es divisible entre 4.

**5** si y sólo si su última cifra es 0 ó 5.

**7** si y sólo si al quitarle la cifra $u$ de las unidades y restarle $2u$ al número resultante, se obtiene un múltiplo de 7.

**8** si y sólo si el número formado por sus 3 últimas cifras es divisible entre 8.

**9** si y sólo si la suma de sus cifras es divisible entre 9.

**10** si y sólo si su última cifra es 0.

**11** si y sólo si la suma algebraica alternada de sus cifras es múltiplo de 11.

Las pruebas son sencillas usando congruencias. Por ejemplo, como $10 \equiv 1 \pmod 9$ resulta que $10^k \equiv 1 \pmod 9$ y entonces

$$a_n 10^n + a_{n-1}10^{n-1} + \cdots a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + \cdots a_1 + a_0 \pmod 9,$$

de donde se deducen los criterios de divisibilidad entre 9 y 3.

como $10 \equiv -1 \pmod{11}$ resulta que $10^{2k} \equiv 1 \pmod{11}$ y $10^{2k+1} \equiv -1 \pmod{11}$, de donde

$$a_n 10^n + a_{n-1}10^{n-1} + \cdots a_1 \cdot 10 + a_0 \equiv (-1)^n a_n + \cdots + a_2 - a_1 + a_0 \pmod{11},$$

de donde se deduce el criterio de divisibilidad entre 11.

Tal vez el criterio menos conocido (y usado) sea el de divisibilidad entre 7. Ese criterio afirma que $n = 10a + u$ es divisible entre 7 si y sólo si $a - 2u$ lo es. Pero si $10a + u \equiv 0 \pmod 7$, multiplicando por $-2$ resulta $-20a - 2u \equiv 0 \pmod 7$, es decir $a - 2u \equiv 0 \pmod 7$ (pues $-20 \equiv 1 \pmod 7$), y recíprocamente si $a - 2u \equiv 0 \pmod 7$ multiplicando por 10 resulta $10a - 20u \equiv 0 \pmod 7$, es decir $10a + u \equiv 0 \pmod 7$.

Otro criterio de divisibilidad entre 7 se puede obtener observando que $10^0 \equiv 1 \pmod 7$,$10 \equiv 3 \pmod 7$, $10^2 \equiv 2 \pmod 7$, $10^3 \equiv -1 \pmod 7$, $10^4 \equiv -3 \pmod 7$, $10^5 \equiv -2 \pmod 7$, $10^6 \equiv 1 \pmod 7$, y los restos se repiten con período 6. Luego $a_n a_{n-1} \ldots a_2 a_1 a_0 \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \cdots$

Algunos ejemplos: 987654 es divisible entre 2 pero no entre 4. 123456 es divisible entre 3 pero no entre 9. 12345 es divisible entre 5 pero no entre 10. 123456789 es múltiplo de 9 pero no de 6. 273 es múltiplo de 7 pues $27 - 2 \cdot 3 = 21$ lo es. 917652 es divisible entre 11 pues $9 - 1 + 7 - 6 + 5 - 2 = 11$ lo es. Cualquier número con una cantidad par de cifras idénticas es divisible entre 11, ya que la suma alternada de todas ellas es 0.

## 3.3. Teorema chino de los restos

**Teorema 3.3.** *Sean $m_1$, $m_2$,..., $m_k$ enteros coprimos dos a dos. Entonces el sistema de congruencias*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ \cdots &\quad \cdots \quad \cdots\cdots\cdots\cdots \\ x &\equiv a_n \pmod{m_k} \end{aligned}$$

*tiene una solución única módulo $m_1 m_2 \cdots m_k$.*

*Demostración.* Sea $m = m_1 m_2 \cdots m_k$. Para cada $i = 1, 2, \ldots, k$ sea $M_i = m/m_i$. Entonces $\mcd(M_i, m_i) = 1$ y por lo tanto existe $x_i$ tal que de $M_i x_i \equiv 1 \pmod{m_i}$. Sea

$$x = M_1 x_1 a_1 + M_2 x_2 a_2 + \cdots + M_k x_k a_k.$$

Es inmediato verificar que $x$ es solución del sistema de congruencias. Si $x'$ es cualquier otra solución, entonces $x' \equiv x \pmod{m_i}$ para $i = 1, 2, \ldots, k$ y como los $m_i$ son coprimos dos a dos se deduce que $x' \equiv x \pmod{m}$. □

Este teorema permite reducir la solución de ecuaciones polinómicas en congruencias de un módulo $m$ cualquiera al caso en que el módulo sea una potencia de un primo. En efecto, si $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ es la descomposición en factores primos de $m$, la congruencia $P(x) \equiv 0 \pmod{m}$ es equivalente al sistema

$$\begin{aligned} P(x) &\equiv 0 \pmod{p_1^{a_1}}, \\ P(x) &\equiv 0 \pmod{p_2^{a_2}}, \\ \cdots &\quad \cdots \quad \cdots\cdots\cdots\cdots \\ P(x) &\equiv 0 \pmod{p_k^{a_k}}. \end{aligned}$$

En efecto, sea $P(x)$ un polinomio con coeficientes enteros. Si $P(x) \equiv 0 \pmod{m}$ tiene solución, evidentemente esa solución satisface también todas las congruencias del sistema. Recíprocamente, si $x_i$ es una solución de la congruencia $P(x) \equiv 0 \pmod{p_i^{a_i}}$, entonces por el teorema chino de los restos existe un $x$ tal que $x \equiv x_i \pmod{p_i^{a_i}}$ para $i = 1, 2, \ldots, k$, y por lo tanto $P(x) \equiv P(x_i) \equiv 0 \pmod{p_i^{a_i}}$ para $i = 1, 2, \ldots, k$ y $P(x) \equiv 0 \pmod{m}$.

## 3.4. Teoremas de Fermat, Euler y Wilson

### Función $\phi$ de Euler

Si $n$ es un número natural se define $\phi(n)$ como la cantidad de números del conjunto $\{1, 2, \ldots, n\}$ que son coprimos con $n$. Por ejemplo $\phi(6) = 2$ ya que de los números 1, 2, 3, 4, 5 y 6 solamente 1 y 5 son coprimos con 6.

La función $\phi$ es multiplicativa, es decir que:

**Teorema 3.4.** *Si $a$ y $b$ son números naturales coprimos, entonces*

$$\phi(ab) = \phi(a)\phi(b).$$

*Demostración.* Cada natural desde 1 hasta $ab$ se puede escribir en la forma $qa+r$, con $0 \leq q \leq b-1$ y $1 \leq r \leq a$. Para que $qa+r$ sea coprimo con $ab$, debe serlo con $a$ y con $b$. Pero $\mcd(qa+r, a) = \mcd(r, a)$, luego $r$ debe ser coprimo con $a$. Hay $\phi(a)$ de estos $r$. Para cada uno de ellos los números $r$, $a+r$, $2a+r$,..., $(b-1)a+r$ son un sistema completo de residuos módulo $b$, ya que la diferencia de dos de ellos (diferentes) es de la forma $ja$, con $1 \leq j \leq b-1$, y por lo tanto no es divisible entre $b$. Esto significa que $\phi(b)$ de ellos son coprimos con $b$, y por lo tanto con $ab$. Esto nos da un total de $\phi(a)\phi(b)$ números coprimos con $ab$, entre los naturales desde 1 hasta $ab$. □

Si $p$ es primo y $a$ natural entonces los números entre 1 y $p^a$ que no son coprimos con $p^a$ son $p$, $2p$, $3p$,..., $p^{a-1}p = p^a$, que son $p^{a-1}$. Luego

$$\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p).$$

Usando este resultado y el hecho de que $\phi$ es multiplicativa, resulta que si $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ entonces

$$\begin{aligned} \phi(n) &= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

**Teorema 3.5 (Teorema de Euler).**

Si $\mcd(a, n) = 1$ entonces

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}.}$$

*Demostración.* Sean $c_1$, $c_2$,..., $c_{\phi(n)}$ los elementos de $\{1, 2, \ldots, n\}$ que son coprimos con $n$ y pongamos $ac_i = q_i n + r_i$, para $i = 1$,..., $\phi(n)$, con $0 \leq r_i < n$. Es claro que los restos $r_i$ son todos diferentes, ya que $r_i = r_j \Longrightarrow ac_i = ac_j \pmod{n}$ $\Longrightarrow c_i = c_j \pmod{n}$ (por ser $a$ coprimo con $n$), absurdo. Además $\mcd(r_i, n) = \mcd(ac_i - q_i n, n) = \mcd(ac_i, n) = 1$. Se concluye que

$$\{c_1, c_2, \ldots, c_{\phi(n)}\} = \{r_1, r_2, \ldots, r_{\phi(n)}\}.$$

Pero $r_i \equiv ac_i \pmod{n}$, por lo tanto

$$c_1 c_2 \cdots c_{\phi(n)} = r_1 r_2 \cdots r_{\phi(n)} \equiv a^{\phi(n)} c_1 c_2 \cdots c_{\phi(n)} \pmod{n},$$

de donde resulta $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Un caso particular importante se presenta cuando $n$ es primo. Observe que si $p$ es primo entonces $\phi(p) = p - 1$, por lo tanto se tiene:

**Teorema 3.6** (**Teorema (pequeño) de Fermat**). *Si $p$ es primo y $p \nmid a$, entonces*

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

Otro resultado interesante es el siguiente:

**Teorema 3.7** (**Teorema de Wilson**). *Para cualquier primo $p$ se cumple*

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

*Demostración.* Cada entero $i$ desde 1 hasta $p-1$ tiene un (único) inverso multiplicativo en el mismo rango. Si $x^2 \equiv 1 \pmod{p}$ entonces $(x+1)(x-1) \equiv 0 \pmod{p}$, de donde los únicos que son inversos de sí mismos son 1 y $p-1$. Es decir que los enteros 2, 3,..., $p-2$ se agrupan en parejas de inversos multiplicativos y por lo tanto

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

□

## 3.5. Lema de Hensel

El *Lema de Hensel*, también conocido como *Lema de Mihail* o *Lema de levantamiento de exponentes*, es una herramienta muy çutil para resolver problemas olímpicos de teoría de números, especialmente aquellos relacionados con congruencias.

Primero algo de notación: si $p$ es un número primo, $a$ y $n$ son enteros y $n \geq 0$, escribiremos

$$p^n \parallel a$$

para indicar que $p^n \mid a$ pero $p^{n+1} \nmid a$. En otras palabras, $p^n \parallel a$ si y sólo si $p^n$ es la mayor potencia de $p$ que divide a $a$. Ejemplos: $3 \parallel 30$, $2^3 \parallel 72$, $5^4 \parallel 10000$.

**Teorema 3.8.** *Sean $p$ un primo impar, $a$, $b$, $n$, $r$ y $s$ enteros, $n, r \geq 1$. Si $p^r \parallel a-b$, $p \nmid b$ y $p^s \parallel n$, entonces $p^{r+s} \parallel a^n - b^n$.*

*Demostración.* Primero probaremos que $p^s \parallel \frac{a^n-b^n}{a-b}$ por inducción en $s$. Para $s = 0$ se tiene que $p \nmid n$. Como $a \equiv b \pmod{p}$ resulta $a^j \equiv b^j \pmod{p}$ y $a^j b^{n-j-1} \equiv b^{n-1} \pmod{p}$, y sumando se tiene

$$\frac{a^n - b^n}{a-b} = \sum_{j=0}^{n-1} a^j b^{n-j-1} \equiv n b^{n-1} \not\equiv 0 \pmod{p}.$$

Supongamos ahora que $p^s \parallel \frac{a^n-b^n}{a-b}$. Pongamos $a = b + xp$. Entonces $a^{nj} \equiv b^{nj} + njb^{n(j-1)}xp \pmod{p^2}$ y se tiene

$$\begin{aligned}\frac{a^{np}-b^{np}}{a^n-b^n} &= \sum_{j=0}^{p-1} a^{nj}b^{n(p-j-1)} \equiv \sum_{j=0}^{p-1}(b^{nj}+njb^{n(j-1)}xp)b^{n(p-j-1)} \\ &\equiv pb^{n(p-1)} + pnxb^{n(p-2)}\sum_{j=0}^{p-1} j \\ &\equiv pb^{n(p-1)} + pnxb^{n(p-2)}\frac{p(p-1)}{2} \\ &\equiv pb^{n(p-1)} \pmod{p^2}.\end{aligned}$$

Por lo tanto

$$p^{s+1} \parallel \frac{a^{np}-b^{np}}{a^n-b^n}\frac{a^n-b^n}{a-b} = \frac{a^{np}-b^{np}}{a-b},$$

completando la inducción.

Finalmente, como $a^n - b^n = \frac{a^n-b^n}{a-b}(a-b)$ es claro que $p^{r+s} \parallel a^n - b^n$. □

**Corolario 3.9.** *Sean $p$ un primo impar, $a$, $b$, $n$, $r$ y $s$ enteros, $n, r \geq 1$ y $n$ impar. Si $p^r \parallel a+b$, $p \nmid b$ y $p^s \parallel n$, entonces $p^{r+s} \parallel a^n + b^n$.*

*Demostración.* Basta observar que si $n$ es impar entonces $a + b = a - (-b)$ y $a^n + b^n = a^n - (-b)^n$. □

Para $p = 2$ el lema de Hensel como lo hemos enunciado no es cierto, por ejemplo $2 \parallel 3 - 1$ y $2 \parallel 2$, pero $2^3 \parallel 3^2 - 1^2$. Sin embargo vale un resultado similar:

**Teorema 3.10.** *Sean $a$, $b$, $n$, $r$ y $s$ enteros, $n, r, s \geq 1$. Si $2^r \parallel \frac{a^2-b^2}{2}$, $2 \nmid b$ y $2^s \parallel n$, entonces $2^{r+s} \parallel a^n - b^n$.*

*Demostración.* Primero probaremos que $2^{s-1} \parallel \frac{a^n-b^n}{a^2-b^2}$ por inducción en $s \geq 1$. Para $s = 1$ se tiene que $n = 2m$, con $m$ impar. Como $2 \mid \frac{a^2-b^2}{2}$ debe ser $a \equiv b \pmod 2$, de donde $a^{2j} \equiv b^{2j} \pmod 2$ y $a^{2j}b^{2m-2j-1} \equiv b^{2m-1} \pmod 2$, y sumando se obtiene

$$\frac{a^{2m}-b^{2m}}{a^2-b^2} = \sum_{j=0}^{m-1} a^{2j}b^{2m-2j-1} \equiv mb^{2m-1} \equiv 1 \pmod 2,$$

o sea que $2^0 \parallel \frac{a^n-b^n}{a^2-b^2}$. Supongamos ahora que $p^{s-1} \parallel \frac{a^n-b^n}{a^2-b^2}$. Como $a$ y $b$ son impares y $n$ es par se tiene $a^n \equiv b^n \equiv 1 \pmod 4$ y por tanto $a^n + b^n \equiv 2 \pmod 4$, es decir que $2 \parallel a^n + b^n$. Entonces

$$p^s \parallel \frac{a^n-b^n}{a^2-b^2}(a^n+b^n) = \frac{a^{2n}-b^{2n}}{a^2-b^2},$$

completando la inducción.

Finalmente, como $a^n - b^n = 2\frac{a^n-b^n}{a^2-b^2}\frac{a^2-b^2}{2}$ es claro que $p^{r+s} \parallel a^n - b^n$. □

## 3.6. Problemas

**Problema 3.1.** Un número se escribe con cien ceros, cien unos y cien doses, en algún orden. ¿Puede ser un cuadrado perfecto?

**Problema 3.2.** Pedro multiplicó dos enteros de dos cifras cada uno y codificó los factores y el producto con letras, usando letras iguales para dígitos iguales y letras diferentes para dígitos diferentes. Entonces le mostró al maestro su trabajo: $AB \cdot CD = EEFF$. Pero el maestro le contestó: Revisa lo que hiciste, pues cometiste un error. ¿Cómo supo eso el maestro?

**Problema 3.3.** Permutando las cifras del número

$$122333444455555666666777777777$$

¿podrá obtenerse un cuadrado perfecto?

**Problema 3.4.** Determine todos los valores de $k$ para los cuales el número $111\ldots1$, compuesto por $k$ unos, es un cuadrado perfecto.

**Problema 3.5.** ¿Alguno de los números que se pueden obtener permutando las cifras de 86420 es un cuadrado perfecto?

**Problema 3.6.** Halle todos los enteros positivos $n$ tales que $n! + 5$ sea un cubo perfecto.

**Problema 3.7.** Si $m$ y $n$ son enteros tales que $m^2 + n^2$ es múltiplo de 3, pruebe que tanto $m$ como $n$ son múltiplos de 3.

**Problema 3.8.** Hallar el menor entero positivo $x$ tal que $21x \equiv 2 \pmod{37}$.

**Problema 3.9.** Si $x$, $y$, $z$ son enteros tales que $x^2 + y^2 = z^2$, pruebe que al menos uno de ellos es múltiplo de 3.

**Problema 3.10.** Si tres números primos mayores que 3 están en progresión aritmética, pruebe que la razón (o diferencia común) de la progresión es múltiplo de 6.

**Problema 3.11.** Se tienen 7 números enteros tales que la suma de 6 cualesquiera de ellos es divisible entre 5. Pruebe que los 7 números son múltiplos de 5.

**Problema 3.12.** Resuelva el sistema de congruencias

$$\begin{aligned} 2x &\equiv 3 \pmod{5}, \\ 3x &\equiv 5 \pmod{7}, \\ 5x &\equiv 7 \pmod{11}. \end{aligned}$$

**Problema 3.13.** Si $x$, $y$, $z$ son enteros tales que $x^2+y^2+z^2$ es múltiplo de 4, pruebe que tanto $x$, $y$, $z$ son los tres pares.

**Problema 3.14.** (OMCC 2014/6) Un entero positivo $n$ es *divertido* si para todo $d$ divisor positivo de $n$, $d+2$ es un número primo. Encuentre todos los números divertidos que tengan la mayor cantidad posible de divisores.

**Problema 3.15.** Pruebe que $2222^{5555}+5555^{2222}$ es divisible entre 7.

**Problema 3.16.** Determine el valor de $d$ si el número

$$\underbrace{888\cdots888}_{50\ 8's}d\underbrace{999\cdots999}_{50\ 9's}$$

es divisible entre 7.

**Problema 3.17.** ¿Qué resto se obtiene al dividir $2^{3^{2011}}$ entre 17?

**Problema 3.18.** Pruebe que para todo natural $n$ se cumple $\sum_{d|n}\phi(d)=n$.

**Problema 3.19.** ¿Cuál es la cifra de las unidades de $\underbrace{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}_{2015\ 7's}$

**Problema 3.20.** Halle las tres últimas cifras de $2003^{2002^{2001}}$.

**Problema 3.21.** Pruebe que existe $n$ tal que $3^n$ tiene al menos 2011 ceros consecutivos.

**Problema 3.22** (IMO 2005/4)**.** Considere la sucesión $a_1$, $a_1$,... definida por

$$a_n=2^n+3^n+6^n-1$$

para todos los $n$ enteros positivos. Halle todos los enteros positivos que son coprimos con todos los términos de la sucesión.

**Problema 3.23.** Pruebe que, dado cualquier natural $N$, existe $n$ tal que $2^n$ tiene al menos $N$ ceros consecutivos.

**Problema 3.24.** (IMO 2009/1) Sea $n$ un entero positivo y sean $a_1$, $a_2$,..., $a_k$ ($k\geq 2$) enteros distintos del conjunto $\{1,2,\ldots,n\}$ tales que $n$ divide a $a_i(a_{i+1}-1)$ para $i=1,2,\ldots,k-1$. Demostrar que $n$ no divide a $a_k(a_1-1)$.

**Problema 3.25.** Halle el menor entero positivo $n$ tal que $2^{2007}\mid 17^n-1$.

**Problema 3.26.** (Rusia 1996) Supongamos que $a^n+b^n=p^k$, donde $a$, $b$, y $k$ son enteros positivos, $p$ es un primo iompar y $n>1$ es un entero impar. Pruebe que $n$ debe ser una potencia de $p$.

**Problema 3.27.** (IMO 1990/3) Halle todos los enteros positivos $n$ tales que $\frac{2^n+1}{n^2}$ es entero.

**Problema 3.28.** (ORP 2004, 2N P2) Encontrar todos los valores enteros positivos de $k$, $n$ y $p$ primo que satisfacen la ecuación $5^k - 3^n = p^2$.

**Problema 3.29.** (OMCC 2001/3) Encontrar todos los números naturales $N$ que cumplan las dos condiciones siguientes:

- Sólo dos de los dígitos de $N$ son distintos de 0 y uno de ellos es 3.
- $N$ es un cuadrado perfecto.

**Problema 3.30.** (IMO 2000/5) ¿Existe un entero positivo $n$ que tenga esactamente 2000 divisores primos y que divida a $2^n + 1$?

**Problema 3.31.** (IMO 2003/6) Sea $p$ un número primo. Demostrar que existe un primo $q$ tal que, para todo entero $n$, el número $n^p - p$ no es divisible por $q$.

# Capítulo 4

# Ecuaciones diofánticas

Una *ecuación diofántica* es una ecuación algebraica en una o más variables, con coeficientes enteros, de la cual estamos interesados en hallar las soluciones enteras. Ejemplo: $6x + 10y = 14$. Observe que en los reales esta ecuación es poco interesante, ya que si le damos cualquier valor a $x$ podemos despejar $y = (14 - 6x)/10$. Así la ecuación tiene infinitas soluciones de la forma $(x, (7 - 3x)/5)$. En cambio si buscamos las soluciones enteras, sólo nos interesan los $x$ enteros para los cuales $(7 - 3x)/5$ es también entero.

Este tipo de ecuaciones se estudian desde la antigüedad, de hecho su nombre proviene del matemático griego Diofanto de Alejandría, que vivió en el siglo III de nuestra era. Existe una abundante literatura sobre el tema (ver por ejemplo [2]). aquí sólo se tratarán algunos aspectos básicos.

## 4.1. Ecuación diofántica lineal

Veamos como tratar la ecuación diofántica

$$ax + by = c \qquad (*)$$

donde $a$, $b$, $c$ son enteros y $a, b \neq 0$. En primer lugar observemos que si $d = \text{mcd}(a, b)$ entonces $d \mid ax+by$. Por lo tanto, para que haya solución, es necesario que $d \mid c$. Esta condición es también suficiente. En efecto, si $d \mid c$ podemos dividir todos los coeficientes de la ecuación (*) entre $d$ y obtenemos una ecuación del mismo tipo pero en la cual los coeficientes de $x$ e $y$ son coprimos. Podemos suponer entonces, sin pérdida de generalidad, que $\text{mcd}(a, b) = 1$. El teorema de Bezout nos dice que existen enteros $s$, $t$ tales que $as+bt = 1$. Entonces $asc+btc = c$ y $(x_0, y_0) = (sc, tc)$ es una solución de (*). Supongamos que $(x, y)$ sea otra solución. Restando miembro a miembro las igualdades $ax+by = c$ y $ax_0+by_0 = c$ resulta $a(x-x_0)+b(y-y_0) = 0$, o bien $a(x-x_0) = -b(y-y_0)$. Como $\text{mcd}(a, b) = 1$, por el Lema de Euclides resulta

que $b \mid x - x_0$ y $a \mid y - y_0$. Pongamos $k = (x - x_0)/b = -(y - y_0)/a$. Entonces $x = x_0 + bk$, $y = y_0 - ak$. Todas las soluciones enteras son de esa forma, y todas esas son soluciones, como se verifica fácilmente. Luego el problema está resuelto.

**Ejemplo 4.1.** Hallar la solución general de $6x + 10y = 14$.

Luego de dividir entre $\mathrm{mcd}(6, 10) = 2$ nos queda $3x + 5y = 7$. Como $5 = 3 + 2$ y $3 = 2 + 1$, resulta $1 = 3 \cdot 2 - 5$, y multiplicando por 7, $3 \cdot 14 - 5 \cdot 7 = 7$. La solución general es entonces $x = 14 + 5k$, $y = -7 - 3k$.

## 4.2. Ternas pitagóricas

La ecuación diofántica

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

está relacionada con el Teorema de Pitágoras, ya que sus soluciones en enteros positivos, llamadas *ternas pitagóricas*, corresponden a los triángulos rectángulos con los tres lados enteros. Toda terna pitagórica es de la forma

$$x = (2uv)s, \quad y = (u^2 - v^2)s, \quad z = (u^2 + v^2)s,$$

para ciertos enteros positivos $s$, $u$, $v$, con $u > v$. En efecto, si $x^2 + y^2 = z^2$ y $x, y, z > 0$, sea $s = \mathrm{mcd}(x, y)$. Entonces $s \mid z$ y se puede escribir $x = sX$, $y = sY$, $z = sZ$. Se verifica de inmediato que $X^2 + Y^2 = Z^2$ y $\mathrm{mcd}(X, Y) = \mathrm{mcd}(X, Z) = \mathrm{mcd}(Y, Z) = 1$ (una terna pitagórica con estas características se denomina *primitiva*). Ahora bien, si $X$ e $Y$ fuesen ambos impares entonces sería $X^2 + Y^2 \equiv 2 \pmod 2$, lo cual es imposible pues $Z^2$ es congruente con 0 o con 1 módulo 2. Tampoco pueden ser ambos pares pues $\mathrm{mcd}(X, Y) = 1$. Supongamos que $X$ es par e $Y$ impar (y por lo tanto $Z$ es también impar). Entonces

$$\left(\frac{X}{2}\right)^2 = \frac{Z^2 - Y^2}{4} = \frac{Z + Y}{2}\,\frac{Z - Y}{2}.$$

Pero $(Z + Y)/2$ y $(Z - Y)/2$ son coprimos, pues de lo contrario su suma $Z$ y su diferencia $Y$ tampoco lo serían, por lo tanto cada uno de ellos debe ser un cuadrado perfecto, digamos

$$\frac{Z + Y}{2} = u^2, \quad \frac{Z - Y}{2} = v^2.$$

De aquí se sigue que $Z = u^2 + v^2$, $Y = u^2 - v^2$ y $(X/2)^2 = (uv)^2$, de donde $X = 2uv$.

## 4.3. Ecuación de Pell-Fermat

La ecuación diofántica

$$x^2 - Dy^2 = 1, \tag{4.1}$$

donde $D$ es un entero positivo, se llama comúnmente *ecuación de Pell* o *ecuación de Fermat*. Esta ecuación tiene la solución trivial $x = \pm 1$, $y = 0$. Si $D = d^2$ es un cuadrado perfecto no hay soluciones no triviales, ya que queda $x^2 - (dy)^2 = 1$ y la diferencia de dos cuadrados sólo puede ser 1 si el minuendo es 1 y el sustraendo es 0. Pero si $D$ no es un cuadrado perfecto entonces puede demostrarse que (4.1) tiene infinitas soluciones.

Aquí nos limitaremos a mostrar cómo, a partir de una solución particular, pueden generarse las demás. Asociemos ahora a cada solución $(x, y)$ el número $x + y\sqrt{D}$ y observemos que

$$(x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2 = 1.$$

Si $x, y > 0$ entonces se tiene

$$x + y\sqrt{D} > 1, \quad x - y\sqrt{D} < 1.$$

Si $u, v$ es otra solución entonces

$$(u + v\sqrt{D})(u - v\sqrt{D}) = u^2 - Dv^2 = 1$$

y multiplicando miembro a miembro resulta

$$(x + y\sqrt{D})(u + v\sqrt{D})(x - y\sqrt{D})(u - v\sqrt{D}) = 1,$$

o sea que

$$(x + y\sqrt{D})(u + v\sqrt{D}) = (xu + Dyv) + (xv + yu)\sqrt{D}$$

es el valor asociado a la solución $(xu + Dyv, xv + yu)$. En particular si a partir de una solución $(x_1, y_1)$ se definen $x_n$ e $y_n$ mediante la igualdad

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$$

se tendrán infinitas soluciones $(x_n, y_n)$, que pueden escribirse explícitamente como

$$x_n = \frac{1}{2}\left((x_1 + y_1\sqrt{D})^n + (x_1 - y_1\sqrt{D})^n\right),$$
$$y_n = \frac{1}{2\sqrt{D}}\left((x_1 + y_1\sqrt{D})^n - (x_1 - y_1\sqrt{D})^n\right).$$

Es claro que si $(x, y)$ es solución, entonces $(-x, y)$, $(x, -y)$ y $(-x, -y)$ también lo son, por lo tanto es suficiente buscar las soluciones $(x, y)$ con $x > 0$, $y > 0$. Entre éstas, supongamos que $(x_1, y_1)$ es aquella para la cual $x_1 + y_1\sqrt{D}$ sea mínimo. En ese caso las soluciones $(x_n, y_n)$ son *todas* las soluciones positivas de la ecuación de Pell. En efecto, como

$$1 < x_1 + y_1\sqrt{D} < (x_1 + y_1\sqrt{D})^2 < (x_1 + y_1\sqrt{D})^3 < \cdots$$

si $u, v$ es otra solución y no coincide con ninguna $(x_n, y_n)$, entonces $u+v\sqrt{D}$ debe estar comprendido entre dos términos consecutivos de la sucesión anterior, es decir

$$(x_1 + y_1\sqrt{D})^k < u + v\sqrt{D} < (x_1 + y_1\sqrt{D})^{k+1}.$$

Pero entonces multiplicando por $(x_1 - y_1\sqrt{D})^k$ resulta

$$1 < (u + v\sqrt{D})(x_1 - y_1\sqrt{D})^k < x_1 + y_1\sqrt{D}.$$

Como el término medio es mayor que 1, corresponde a una solución positiva. Pero esto es absurdo por la forma en que fue elegida $(x_1, y_1)$. La idea aplicada en esta demostración se conoce como *método del descenso*.

## 4.4. Problemas

**Problema 4.1.** (TT 1989) Resolver en enteros positivos:

$$x + \cfrac{1}{y + \cfrac{1}{z}} = \frac{10}{7}.$$

**Problema 4.2.** Hallar la solución general de $2x+5y+3z = 4$ en números enteros.

**Problema 4.3.** Halle todas las soluciones enteras de la ecuación

$$xy - 3x - 2y = 15.$$

**Problema 4.4.** (OMCC 2005/2) Demuestre que la ecuación $a^2b^2 + b^2c^2 + 3b^2 - a^2 - c^2 = 2005$ no tiene soluciones enteras.

**Problema 4.5.** (OMCC 2009/6) Encuentre todos los números primos $p$ y $q$ tales que $p^3 - q^5 = (p + q)^2$.

**Problema 4.6.** (OMCC 2010/1) Si $S(n)$ denota la suma de los dígitos de un número natural $n$, encuentre todas las soluciones de

$$n\,(S(n) - 1) = 2010$$

mostrando que son las únicas.

**Problema 4.7.** Demostrar que para cada entero $n \geq 3$ existen enteros impares $a$ y $b$ tales que $2^n = 7a^2 + b^2$.

**Problema 4.8** (OIM 2008)**.** Demuestre que no existen enteros positivos $x$ e $y$ tales que

$$x^{2008} + 2008! = 21^y.$$

**Problema 4.9** (OIM 2008)**.** Resuelva en enteros positivos la ecuación

$$x^2 + y^2 = 157^2(x - y).$$

**Problema 4.10.** (IMO 2006/4) Determine todas las parejas de enteros $(x, y)$ tales que $1 + 2^x + 2^{2x+1} = y^2$.

**Problema 4.11.** Halle todos los triángulos cuyos lados son tres enteros consecutivos y cuya área también es entera.

# Capítulo 5

# Residuos cuadráticos

SUPONGAMOS que se desea resolver la congruencia cuadrática

$$x^2 + x + 1 \equiv 0 \pmod{p}.$$

Si $m$ es pequeño, basta darle a $x$ sucesivamente los valores 0, 1, 2,..., $p-1$ y verificar si la congruencia se cumple o no. Por ejemplo para $p = 2$ no hay solución, para $p = 3$ la única solución es $x \equiv 1 \pmod{3}$, para $p = 5$ no hay solución, y para $p = 7$ hay dos soluciones, a saber $x \equiv 2 \pmod{7}$ y $x \equiv 4 \pmod{7}$.

Si $p$ es más grande, se puede ensayar la técnica que se usa para las ecuaciones algebraicas de segundo grado, es decir la de completar cuadrados. Así, si $p$ es coprimo con 2, nuestra congruencia es equivalente a

$$4x^2 + 4x + 4 \equiv 0 \pmod{p},$$

que se puede escribir como

$$(2x + 1)^2 + 3 \equiv 0 \pmod{p},$$

o bien

$$(2x + 1)^2 \equiv -3 \pmod{p}.$$

De este modo, la solución de congruencias cuadráticas puede reducirse a la solución de congruencias de la forma

$$x^2 \equiv a \pmod{p}.$$

## 5.1. El símbolo de Legendres

Sea $p$ un primo impar. A cualquier entero $a$ coprimo con $p$ para el cual tenga solución la congruencia

$$x^2 \equiv a \pmod{p}$$

se le llama *residuo cuadrático* módulo $p$. Por ejemplo 3 es un residuo cuadrático módulo 11, ya que $5^2 \equiv 3 \pmod{11}$.

Los resultados más importantes sobre residuos cuadráticos se expresan convenientemente mediante el *símbolo de Legendre*, que se define así:

Sea $p$ un primo impar y $a$ un entero cualquiera. Entonces

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ 1 & \text{si } p \nmid a \text{ y } a \text{ es residuo cuadrático módulo } p, \\ \text{-1} & \text{si } p \nmid a \text{ y } a \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Las siguientes son algunas propiedades elementales de los residuos cuadráticos expresadas en esta notación. Las demostraciones son muy sencillas y las dejamos como ejercicio al lector.

1. $\left(\frac{1}{p}\right) = 1$.

2. Si $a \equiv b \pmod{p}$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

3. Si $p \nmid n$ entonces $\left(\frac{an^2}{p}\right) = \left(\frac{a}{p}\right)$.

**Teorema 5.1** (Criterio de Euler)**.**

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

*Demostración.* Si $p \mid a$ entonces ambos miembros son 0 (mód $p$) y se verifica la igualdad. Supongamos entonces que $p \nmid a$. Si $\left(\frac{a}{p}\right) = 1$ entonces existe un $x$ tal que $x^2 \equiv a \pmod{p}$. Como claramente $p \nmid x$, por el teorema de Fermat se tiene $x^{p-1} \equiv 1 \pmod{p}$, y entonces

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Sólo nos queda por considerar el caso $\left(\frac{a}{p}\right) = -1$. En este caso, para cada $x \equiv 1, 2, \ldots, p-1 \pmod{p}$ existe un inverso multiplicativo $x'$ tal que $xx' \equiv 1 \pmod{p}$, y por tanto $x(x'a) \equiv a \pmod{p}$. Como $a$ no es residuo cuadrático módulo $p$, debe ser $x \not\equiv x'a \pmod{p}$. Es decir que las $p-1$ clases residuales módulo $p$ se pueden agrupar en $(p-1)/2$ parejas $(x, x'a)$. Multiplicándolas todas se tiene

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$$

(por el teorema de Wilson), o sea que también en este caso $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. □

El criterio de Euler permite establecer algunas propiedades adicionales del símbolo de Legendre.

4. $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

En efecto, $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$, y como los extremos sólo pueden ser 0, 1 ó $-1$ y $p > 1$, se sigue la igualdad.

5. $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

En efecto, ambos miembros son congruentes módulo $p$, pero como sólo pueden ser 1 ó $-1$ y $p > 1$, deben ser iguales.

**Teorema 5.2** (Lema de Gauss)**.** *Sean $p > 2$ primo y $m$ entero positivo coprimo con $p$. Sea $s$ el número de elementos del conjunto $A = \{m, 2m, 3m, \ldots, \frac{1}{2}(p-1)m\}$ que dejan resto $\geq \frac{1}{2}(p+1)$ al dividirlos entre $p$. Sea*

$$s' = \sum_{i=1}^{\frac{1}{2}(p-1)} \left\lfloor \frac{2mi}{p} \right\rfloor \pmod 2.$$

*Entonces $\left(\frac{m}{p}\right) = (-1)^s = (-1)^{s'}$.*

*Demostración.* Sean $a_1, a_2, \ldots, a_s$ los elementos de $A$ con resto $\geq \frac{1}{2}(p+1)$ módulo $p$ y sean $b_1, b_2, \ldots, b_t$, con $t = \frac{1}{2}(p-1) - s$, los restantes elementos de $A$. Luego $-a_1, -a_2, \ldots, -a_s$ dejan resto $\leq \frac{1}{2}(p-1)$ módulo $p$. Si $-a_i \equiv b_j$ para algún par de índices $i, j$, entonces $p \mid a_i + b_j$, pero esto es imposible pues los restos que dejan $a_i$ y $b_j$ módulo $p$ suman a lo sumo $\frac{1}{2}(p-1) + \frac{1}{2}(p-1) = p - 1$. Luego en el conjunto $\{-a_1, -a_2, \ldots, -a_s, b_1, b_2, \ldots, b_t\}$ están todos los posibles restos módulo $p$ no nulos y $\leq \frac{1}{2}(p-1)$. Por lo tanto

$$\begin{aligned}\prod_{i=1}^{\frac{1}{2}(p-1)} i &\equiv \prod_{i=1}^{s}(-a_i) \prod_{j=1}^{t} b_j \equiv (-1)^s \prod_{i=1}^{s} a_i \prod_{j=1}^{t} b_j \\ &\equiv (-1)^s \prod_{i=1}^{\frac{1}{2}(p-1)} im = (-1)^s m^{\frac{1}{2}(p-1)} \prod_{i=1}^{\frac{1}{2}(p-1)} i \pmod p,\end{aligned}$$

y como $p \nmid \prod_{i=1}^{\frac{1}{2}(p-1)} i$, resulta

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

Finalmente observemos que $im = pq + r$ con $\frac{1}{2}(p+1) \leq r < p$ si y sólo si $\lfloor \frac{2mi}{p} \rfloor$ es impar, luego $s$ y $s'$ tienen la misma paridad. □

**Ejemplo 5.3.** Como aplicación, calculemos $\left(\frac{2}{p}\right)$. Para ello debemos contar el número $s$ de elementos de $A = \{2, 4, 6, \ldots, p-3, p-1\}$ que dejan resto $\geq \frac{1}{2}(p+1)$ al dividirlos entre $p$. Como $2k < \frac{1}{2}(p+1)$ equivale a $2k \leq \frac{1}{2}(p-1)$ y $k \leq \frac{1}{4}(p-1)$, el mayor elemento de $A$ que no cumple la condición es $\lfloor \frac{1}{4}(p-1) \rfloor$ y entonces $s = |A| - \lfloor \frac{1}{4}(p-1) \rfloor = \frac{1}{2}(p-1) - \lfloor \frac{1}{4}(p-1) \rfloor$. Si escribimos $p = 8q + r$, con $r = 1$, 3, 5 ó 7, se construye fácilmente la siguiente tabla:

| $p$ | $s$ |
|---|---|
| $8q+1$ | $2q$ |
| $8q+3$ | $2q+1$ |
| $8q+5$ | $2q+1$ |
| $8q+7$ | $2q+2$. |

De aquí se sigue que $\left(\frac{2}{p}\right) = (-1)^s$ es 1 si $p \equiv \pm 1 \pmod 8$, y $-1$ si $p \equiv \pm 3 \pmod 8$. Equivalentemente:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\lfloor \frac{p+1}{4} \rfloor}.$$

## 5.2. Ley de reciprocidad cuadrática

El siguiente teorema, probado por Gauss, es uno de los resultados más importantes y profundos de la teoría elemental de números.

**Teorema 5.4.** *Si $p$ y $q$ son primos impares diferentes, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

*Demostración.* Comencemos por observar que $\frac{1}{4}(p-1)(q-1)$ es el número de puntos reticulares (es decir, con ambas coordenadas enteras) en el rectángulo $(0, p/2) \times (0, q/2)$ de $\mathbb{R}^2$. En la diagonal $y = \frac{q}{p}x$ del rectángulo no hay puntos reticulares (si hubiese alguno $(x, y)$ entonces $py = qx$, y como $p \neq y$ se tendría que $p \mid x$ y $q \mid y$, absurdo). Los puntos reticulares del rectángulo que se encuentran en la recta $x = i$ y debajo de la diagonal $y = \frac{q}{p}x$, son $\lfloor \frac{qi}{p} \rfloor$. Por tanto los puntos reticulares del rectángulo que se encuentran debajo de la diagonal son $\sum_{i=1}^{\frac{1}{2}(p-1)} \lfloor \frac{qi}{p} \rfloor$. Análogamente los puntos reticulares del rectángulo que se encuentran por encima de la diagonal son $\sum_{i=1}^{\frac{1}{2}(q-1)} \lfloor \frac{pi}{q} \rfloor$. Entonces

$$\frac{1}{4}(p-1)(q-1) = \sum_{i=1}^{\frac{1}{2}(p-1)} \left\lfloor \frac{qi}{p} \right\rfloor + \sum_{i=1}^{\frac{1}{2}(q-1)} \left\lfloor \frac{pi}{q} \right\rfloor. \qquad (*)$$

Ahora, utilizando las propiedades del símbolo de Legendre, se tiene:

$$\begin{aligned}\left(\frac{p}{q}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{(p+q)/2}{p}\right) &= (-1)^{\frac{p^2-1}{8}}(-1)^{\sum_{i=1}^{\frac{1}{2}(p-1)}\lfloor\frac{(p+q)i}{p}\rfloor} \\ &= (-1)^{\frac{p^2-1}{8}}(-1)^{\sum_{i=1}^{\frac{1}{2}(p-1)} i + \sum_{i=1}^{\frac{1}{2}(p-1)}\lfloor\frac{qi}{p}\rfloor} \\ &= (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p^2-1}{8}}(-1)^{\sum_{i=1}^{\frac{1}{2}(p-1)}\lfloor\frac{qi}{p}\rfloor} = (-1)^{\sum_{i=1}^{\frac{1}{2}(p-1)}\lfloor\frac{qi}{p}\rfloor}.\end{aligned}$$

De la misma manera se obtiene que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^{\frac{1}{2}(q-1)}\lfloor\frac{pi}{q}\rfloor}.$$

Multiplicando ambas expresiones y usando (*) queda probado el teorema. □

La ley de reciprocidad cuadrática, junto con las propiedades elementales del símbolo de Legendre, resuelve el problema de calcular $(\frac{a}{p})$.

**Ejemplo 5.5.** Calcular $\left(\frac{17}{47}\right)$.

$$\begin{aligned}\left(\frac{17}{47}\right) &= (-1)^{\frac{16\cdot 46}{4}}\cdot\left(\frac{47}{17}\right) = \left(\frac{13+2\cdot 17}{17}\right) = \left(\frac{13}{17}\right) \\ &= (-1)^{\frac{16\cdot 12}{4}}\left(\frac{17}{13}\right) = \left(\frac{4+13}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{1}{13}\right) = 1.\end{aligned}$$

## 5.3. Problemas

**Problema 5.1.** Si $p$ es un primo impar entonces la mitad de los enteros de 1 a $p-1$ son residuos cuadráticos módulo $p$ y la otra mitad no lo son.

**Problema 5.2.** Si $p$ es un primo de la forma $4n+3$ entonces $-1$ no es un residuo cuadrático módulo $p$.

**Problema 5.3.** Si $p$ es un primo de la forma $4n+1$ entonces $-1$ es un residuo cuadrático módulo $p$.

**Problema 5.4.** Pruebe que existen infinitos primos de la forma $4n+1$.

**Problema 5.5.** Si $p$ es un primo de la forma $4n+3$ y $p \mid a^2+b^2$, pruebe que $p \mid a$ y $p \mid b$.

**Problema 5.6.** Sea $p = 4n+1$ primo. Pruebe que $p \mid n^n - 1$.

# Capítulo 6

# Soluciones a los problemas

Todo problema profana un misterio; a su vez, al problema lo profana su solución.

E. M. Cioran

Advertencia: Se ha determinado que leer la solución de un problema sin haber realizado antes un serio esfuerzo por resolverlo, no mejora para nada nuestra capacidad resolutiva. Si un problema resiste un primer ataque, intente otros caminos. Cada intento fallido dejará una enseñanza. También puede dejar pasar un tiempo y luego volver al ataque, con nuevos bríos. Sólo cuando haya resuelto el problema, o cuando esté convencido de haber hecho todo lo posible por resolverlo, será útil mirar la solución. Tal vez ésta sea diferente a la suya, e iluminará otras posibilidades. Y si sus intentos no tuvieron éxito, probablemente la solución le ayudará a entender porqué.

## Capítulo 1

**1.1** El profesor Darío dividió 1111111111111111 entre 9 y así obtuvo el número mágico 12345679012345679. Para cualquier cifra $x$ del 1 al 9, si el número mágico se multiplica por $9x$ evidentemente el resultado será $xxxxxxxxxxxxxxxxx$.

**1.2** No. Como el último dígito de un producto sólo depende de los últimos dígitos de los factores, basta examinar los productos $1 \times 2 = 2$, $2 \times 3 = 6$,$3 \times 4 = 12$, $4 \times 5 = 20$, $5 \times 6 = 30$, $6 \times 7 = 42$, $7 \times 8 = 56$, $8 \times 9 = 72$ y $9 \times 0 = 0$ para

convencerse de que el producto de dos enteros consecutivos sólo puede terminar en 0, 2 ó 6.

**1.3** Si se escriben Las primeras potencias de 2: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, $2^8 = 256$, $2^9 = 512$,... se observa que la última cifra se repite periódicamente: 2, 4, 8, 6, 2, 4, 8, 6,... Esto es consecuencia de que el último dígito de un producto sólo depende de los últimos dígitos de los factores, así la siguiente a cualquier potencia de 2 que termine en 2 terminará en $2 \times 2 = 4$, la siguiente a cualquiera que termine en 4 terminará en $4 \times 2 = 8$, la siguiente a cualquiera que termine en 8 terminará en 6 (pues $8 \times 2 = 16$ y la siguiente a cualquiera que termine en 4 terminará en 2 (pues $6 \times 2 = 12$. Como $2011 = 502 \times 4 + 3$, $2^{2011}$ termina en 8.

**1.4** No, porque un cuadrado perfecto sólo puede terminar en 0, 1, 4, 5, 6 ó 9.

**1.5** Si $n > 1$, como $n = (n-1) + 1$, $n$ se puede sustituir por $(n-1) \cdot 1 = n - 1$. Es decir que si se puede obtener un número natural $n$, también se pueden obtener todos los naturales menores que él. Como $22 = 10 + 12$ se puede sustituir por $10 \cdot 12 = 120$. Y como $120 = 70 + 50$ se puede sustituir por $70 \cdot 50 = 3500$. Por lo tanto 2001 se puede obtener. En realidad se pueden obtener todos los naturales.

**1.6** Se trata de hallar un número $abc\ldots xyz$ tal que $zabc\ldots xy = 2 \cdot abc\ldots xyz$, o bien

$$\begin{array}{r} abc\ldots vwxyz \\ \times 2 \\ \hline zabc\ldots vwxy \end{array}$$

Observe que $z$ debe ser al menos 2. Supongamos que $z = 2$. Entonces, como $2 \cdot 2 = 4$, debe ser $y = 4$. Ahora, como $4 \cdot 2 = 8$, debe ser $x = 8$. Y como $8 \cdot 2 = 16$, debe ser $w = 6$ y nos llevamos 1. Ahora $6 \cdot 2 + 1 = 13$, por lo tanto $v = 3$.

$$\begin{array}{r} abc\ldots 36842 \\ \times 2 \\ \hline zabc\ldots 3684 \end{array}$$

La idea es continuar de esta manera hasta que, al hacer el producto, se obtenga nuevamente la cifra 2, sin acarreo. Así resulta lo siguiente:

$$\begin{array}{r} 105263157894736842 \\ \times 2 \\ \hline 210526315789473684 \end{array}$$

Esta es la solución más pequeña al problema. Comenzando con $z = 3, 4, \ldots, 9$ se obtienen otras soluciones: 157894736842105263, 210526315789473684, 263157894736842105, 315789473684210526, 368421052631578947, 421052631578947368 y 473684210526315789 (observe que todas estas son versiones

*rotadas* de la primera que obtuvimos). Finalmente, concatenando dos o más de las soluciones anteriores se obtienen nuevas soluciones, de 36, 54, 72,... cifras.

**1.7** 1 (por inducción): Para $n = 1$ es cierto. Supongamos que es cierto para $n$, es decir que $\sum_{i=1}^{n}(2i-1) = n^2$. Entonces

$$\sum_{i=1}^{n+1}(2i-1) = n^2 + 2(n+1) - 1 = (n+1)^2.$$

2:

$$\begin{aligned} 2\sum_{i=1}^{n}(2i-1) &= \sum_{i=1}^{n}(2i-1) + \sum_{i=1}^{n}(2n-2i+1) \\ &= \sum_{i=1}^{n}((2i-1)+(2n-2i+1)) = \sum_{i=1}^{n} 2n = 2n \cdot n = 2n^2, \end{aligned}$$

luego $1 + 3 + \cdots + (2n-1) = n^2$.

**1.8** En la primera pasada se borran todos los impares, quedando los pares del 2 al 2008. La segunda pasada deja todos los múltiplos de 4 desde el 4 hasta el 2008. Así sucesivamente van quedando los múltiplos de 8, luego los de 16, 32, 64, 128, 256, 512 y 1024. Como $1728 = 64 \cdot 27$, sobrevive a la sexta pasada y es borrado en la séptima. Como el único múltiplo de 1024 (no mayor que 2009) es el mismo 1024, éste es el último número borrado y se elimina en la pasada número 11.

**1.9** Uno de los números $n$, $n+1$ y $n+2$ es múltiplo de 3, y al menos uno de ellos es par, por lo tanto el producto es divisible entre $3 \cdot 2 = 6$.

**1.10** Al menos uno de los números $n$, $n+1$, $n+2$ y $n+3$ es múltiplo de 3, y dos de ellos son pares, siendo uno de los dos múltiplo de 4. Por lo tanto, el producto es divisible entre $3 \cdot 2 \cdot 2^2 = 24$.

**1.11** $1 + k^2 + k^4 = (1+k^2)^2 - k^2 = (1+k^2+k)(1+k^2-k)$.

**1.12** Si $n$ es múltiplo de 3 entonces $n^3+2n = n(n^2+2)$ también lo es. De lo contrario $n$ debe ser de la forma $3k+1$ o $3k-1$. Pero entonces $n^2+2 = 9k^2 \pm 6k + 3 = 3(3k^2 \pm 2k + 1)$ es múltiplo de 3.

**1.13** Observe que $9m + 5n + 4(2m+3n) = 17(m+n)$.

**1.14** El número de divisores del número $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ es $(a_1+1)(a_2+1)\cdots(a_k+1)$, que es impar si y sólo si todos los $a_i$ son pares, lo cual ocurre si y sólo si $n$ es un cuadrado perfecto.

**1.15** Como $10^{99} = 2^{99}5^{99}$, $10^{99}$ tiene $(99+1)(99+1) = 100^2 = 10000$ divisores, que son de la forma $2^a5^b$, con $0 \leq a, b \leq 99$. de éstos, los que son múltiplos de

$10^{88}$ son los que cumplen $88 \leq a, b \leq 99$, que son $12^2 = 144$. Luego la probabilidad buscada es $\frac{144}{10000} = \frac{9}{625}$.

**1.16** Son infinitos. Por ejemplo, $\underbrace{11\ldots11}_{2^n-4n}\underbrace{44\ldots44}_{n}$ para $n \geq 4$.

Otra familia infinita de soluciones: $\underbrace{11\ldots11}_{3^n-9n}\underbrace{99\ldots99}_{n}$ para $n \geq 3$.

**1.17** Ninguna operación puede incrementar el exponente de 5 sin hacer lo mismo con el de 3. Eso descarta (b) y (e). A (d) sólo se puede llegar multiplicando por 2 y elevando luego al cubo, o elevando al cubo primero y luego multiplicando por 2 tres veces, es decir en 2 o 4 operaciones, y nunca en 5. Para obtener (c) nabría que elevar una única vez al cuadrado (por el $5^2$), lo cual obliga a realizar al menos cinco operaciones para obtener $2^8$, y al menos otra para obtener $3^4$. Finalmente (a) se obtiene multiplicando dos veces por 2, multiplicando luego por 3, elevando al cubo y multiplicando por 5.

**1.18** Para que $10A$ sea un cuadrado perfecto los factores primos 2 y 5 deben aparecer en la descomposición de $A$ con exponente impar. Para que $6A$ sea un cubo perfecto los exponentes de los factores primos 2 y 3 en la descomposición de $A$ deben ser de la forma $3k + 2$. Además debe aparecer 5 con exponente múltiplo de 3. Como el menor entero impar de la forma $3k+2$ es cinco, $A$ debe ser divisible entre $2^5 \cdot 3^2 \cdot 5^3 = 36000$, y éste es el menor $A$ posible. Es fácil ver que los valores de $A$ que cumplen la condición son todos los de la forma $36000n^6$, para $n$ natural.

**1.19** Hay 9 primos extraños, a saber 2, 3, 5, 7, 23, 37, 53, 73 y 373.

**1.20** El 19. En realidad ningún primo $p$ puede aparecer, pues si aparece los dos números no adyacentes serían múltiplos de $p$, pero como son adyacentes entre sí se llega a una contradicción. Puede probarse que cualquier número compuesto puede aparecer, pues si $p \neq q$ son dos factores primos de $n$ y $r$, $s$ y $t$ son primos que no dividen a $n$, la disposición $pr$, $st$, $n$, $rt$, $qs$ cumple la condición del problema.

**1.21** Si $d$ es el menor divisor de $N$ mayor que 1, entonces el mayor divisor de $N$ menor que $N$ es $45d$ y $d \cdot (45d) = 45d^2 = N$. Es claro que $d$ debe ser primo y que sus únicos valores posibles son 2 y 3. Luego, sólo hay dos números $N$ posibles: $180 = 45 \cdot 2^2$ y $405 = 45 \cdot 3^2$.

**1.22** Veamos qué pasa para valores pequeños de $n$. Por ejemplo para $n = 4$ se tiene $m(5) = 5$, $m(6) = 3$, $m(7) = 7$, $m(8) = 1$. Ensayando otros casos se intuye que los $m(k)$ son 1, 3, 5,... $2n - 1$. En efecto, si $n + 1 \leq k < h \leq 2n$ entonces $m(h)$ no puede ser igual a $m(k)$, pues en ese caso debería ser $h \geq 2k$ y eso es imposible. Entonces los $m(k)$ con $n+1 \leq k \leq 2n$ son todos diferentes, y como son $n$ impares $\leq 2n$ deben ser los primeros $n$ impares, es decir 1, 3, 5,... $2n-1$. Luego $\sum_{k=n+1}^{2n} m(k) = \sum_{k=1}^{n}(2k-1) = n^2$.

**1.23** Descomponiendo cada miembro de la igualdad $56a = 65b$ en producto de factores primos, se ve que $a = 65A$ y $b = 56B$ para ciertos naturales $A$ y $B$, y

sustituyendo en la igualdad queda $56 \cdot 65A = 65 \cdot 56B$, de donde $A = B$. Por lo tanto $a + b = 65A + 56A = 11^2 A$ es compuesto.

**1.24**18 Si $n = 1$ se toma cualquier compuesto, si $n > 1$ entonces por ejemplo $(n+1)! + 2$, $(n+1)! + 3$,..., $(n+1)! + n$.

**1.25** Como $15n = 5(3n)$ es multiplo de 5, debe terminar en 5 ó en 0. En este caso debe terminar en 0. Como $15n = 3(5n)$ es multiplo de 3, la suma de sus dígitos debe ser múltiplo de 3 y, por tanto, la menor cantidad de doses necesarios para obtener un múltiplo de 3 son tres. Ceros, no hace falta más que el último dígito. Luego, el valor más pequeño para $15n$ es $2220 = 15 \cdot 148$ y el menor $n$ posible es 148.

**1.26** Si $n^2$ es un cubo perfecto, entonces también $n$ es un cubo perfecto. Los cubos perfectos menores que 1000 son 1, 8, 27, 64, 125, 216, 343, 512 y 729, de los cuales sólo cumplen la condición 1 y 27.

**1.27** Si no fuera así, los únicos factores primos de $B$ serían 3 y 7. Pero esto contradice el hecho de que todos los números de la forma $3^n 7^m$ tienen la cifra de las decenas par. En efecto, esto es cierto para 3 y 7, y si un número tiene la cifra de las decenas par y termina en 1, 3, 7 ó 9, al multiplicartlo por 3 o por 7 seguirá teniendo la misma característica, ya que el acarreo desde la columna de la derecha será siempre par (0, 2, 4 ó 6).

**1.28** 2014 es tico pues $2014 = 2 \cdot 19 \cdot 53$ y $2 + 19 + 53 = 74$.

Si la suma de tres números primos diferentes es 74, uno de ellos debe ser el 2 (si no los tres serían impares y su suma también). Es decir que los números ticos son los de la forma $2p(72-p)$ con $p$ y $72-p$ primos. Como $p(72-p) = 36^2 - (p-36)^2$ es mayor cuanto más cercano a 36 sea $p$, para hallar los ticos mayores que 2014 debemos buscar los primos $p$ tales que $72 - p$ sea primo y $19 < p < 36$. El 23 no sirve pues $72 - 23 = 49$ no es primo. Aólo quedan $p_1 = 29$ y $p_2 = 31$. Entonces el siguiente año tico será el $2 \cdot 29 \cdot 43 = 2494$ y el siguiente y último será el $2 \cdot 31 \cdot 41 = 2542$.

**1.29** Sea $S = \{10^{2k+1} : k \geq 1\}$. Cualquier suma de elementos distintos de $S$ acaba en un número impar de ceros y por lo tanto no es un cuadrado perfecto. Hay muchas otras soluciones.

**1.30** Supongamos que sólo hubiese un número finito $p_1$, $p_2$,... $p_k$ de primos de la forma $4n+3$, y sea $A = p_1 p_2 \cdots p_k$. Si $k$ es par entonces $A$ es de la forma $4n+1$, $A+2$ es de la forma $4n+3$ y como $A+2$ no es divisible por ningún $p_i$, sus factores primos son de la forma $4n+1$. Pero entonces $A+2$ también sería de esa forma, absurdo.

Si en cambio $k$ es impar entonces $A$ es de la forma $4n+3$, $A+4$ es de la forma $4n+3$ y como $A+4$ no es divisible por ningún $p_i$, sus factores primos son de la forma $4n+1$, y también $A+4$ sería de esa forma, absurdo.

Otra prueba, que no requiere considerar casos, se obtiene considerando el número $A^2+2$.

**1.31** Para todos. Dado $n$ sea $N=(n+1)!^2+1$. Entonces $j+1$ es un factor propio de $j+N$ para $j=1,2,\ldots,n$. Si $j+N=p^m$ entonces $j+1=p^k$ con $k<m$, de donde $N-1=(n+1)!^2$ es divisible al menos entre $p^{k+1}$, pero entonces $j+1=(j+N)-(N-1)$ sería divisible entre $p^{k+1}$, absurdo.

**1.32** Como $d_k \geq k$, se tiene que $d_{k+1-m} \leq n/m$. Por lo tanto,

$$d < n^2\left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(k-1)k}\right)=n^2\left(1-\frac{1}{k}\right)<n^2.$$

Si $n$ es primo, $d=d_1d_2=n$ divide a $n^2$. Si $n$ es compuesto, sea $p$ su menor factor primo. Entonces $d>dk-1d_k=n^2/p$. Pero como el menor divisor de $n^2$ es $p$, el mayor divisor propio de $n^2$ es $n^2/p$. Es decir que si $d$ divide a $n^2$, entonces $d\leq n^2/p$, absurdo. Por lo tanto, $d$ divide a $n^2$ si y sólo si $n$ es compuesto.

# Capítulo 2

**2.1** Sea $n=5k+3$ y pongamos $k=4q+r$, con $0\leq r<4$. Entonces $n=5(4q+r)+3=20q+5r+3$ deja el mismo resto que $5r+3$ al dividirlo entre 4, y para que ese resto sea 1 debe ser $r=2$. Por lo tanto la respuesta es $5\cdot 2+3=13$.

**2.2** Observemos que $n>2$ y que se puede escribir $336=qn+2$. Como $336\cdot 6=2016$ se tiene $2007=336\cdot 6-9=6(qn+2)-9=6qn+3$. Ahora bien, $n$ no puede ser 3 (pues 336 entre 3 deja resto 0 y no 2), es decir que $n>3$ y la igualdad $2007=6qn+3$ muestra que el resto buscado es 3.

**2.3** Fijándonos en los restos al dividir los números entre 3 (que pueden ser 0, 1 ó 2) observamos que no puede haber dos ceros contiguos, ni un 1 y un 2 contiguos, ni tres restos iguales consecutivos, ni restos 0, 1 y 2 (en algún orden) consecutivos. De esto se deduce que debe haber algún 0 (de lo contrario habría un 1 y un 2 contiguos, o serían todos unos o todos ceros). Los vecinos de ese 0 deben ser ambos 1 o ambos 2. En el primer caso, los dos restantes deben ser 1 y 0. En el segundo caso, los dos restantes deben ser 2 y 0. Es decir que la configuración cíclica de restos debe ser $(1,1,0,1,0)$ o $(2,2,0,2,0)$ y dos de los cinco números deben ser múltiplos de 3.

**2.4** Numeremos las filas del 0 al 7, y las columnas del 1 al 8. Entonces el número que se escribe en la fila $i$, columna $j$, es el $8i+j$. Luego de colocar los signos, consideremos los números con signo +. En cada columna hay 4 de ellos, luego hay 4 con $j=1$, 4 con $j=2$,..., 4 con $j=8$. Es decir que las partes $j$ de esos 32 números suman $4(1+2+\cdots+8)=144$. Análogamente como en cada fila hay 4, sus partes $8i$ suman $4\cdot 8(0+1+2+\cdots+7)=816$. Así la suma total de los positivos es 960. El mismo análisis muestra que la suma total de los negativos es $-960$, y por tanto la suma de los 64 números es 0.

**2.5** $n-1$ debe ser múltiplo de 2, 3, 4, 5, 6, 7, 8 y 9, por lo tanto el menor posible cumple $n-1 = \text{mcm}(2,3,4,5,6,7,8,9) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$, y la respuesta es $n = 2521$.

**2.6** Análogamente $n+1 = \text{mcm}(2,3,4,5,6,7,8,9) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$, por lo tanto $n = 2519$.

**2.7** Las cifras de las unidades de $n$ forman una sucesión periódica de período 10, mientras que las cifras de las unidades de $3^n$ forman una sucesión periódica de período 4 (se repiten 3, 9, 7, 1, 3, 9, 7, 1,...). Luego la lista tiene período $\text{mcm}(10,4) = 20$. Examinando las parejas $(n, 3^n)$ para $n = 1, 2, \ldots, 20$ se observa que las subrayadas son $(7, 3^7)$ y $(13, 3^{13})$. Luego en la decena $k$ (desde $10(k-1)$ hasta $10(k-1)+9$) hay una pareja subrayada, que termina en 7 o en 3 según que $k$ sea impar o par. La que ocupa el lugar 2013 es entonces 20127.

**2.8** Desde 1 hasta 2011 hay $\left\lfloor \dfrac{2011}{7} \right\rfloor = 287$ múltiplos de 7, por lo tanto el exponente buscado es al menos 287. Pero los múltiplos de $7^2 = 49$ contribuyen al menos con dos sietes, por lo tanto se debe sumar $\left\lfloor \dfrac{2011}{49} \right\rfloor = 41$. Del mismo modo hay que sumar un siete por cada múltiplo de $7^3 = 343$, es decir $\left\lfloor \dfrac{2011}{343} \right\rfloor = 5$. La respuesta es entonces $287 + 41 + 5 = 333$.

En general, el exponente de un primo $p$ en $n!$ es

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

**2.9** No existe. Supongamos por absurdo que

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = m \in \mathbb{Z}$$

y sea $k$ el mayor entero tal qye $2^k \leq n$. Entonces multiplicando por $2^{k-1}$ y despejando el término $2^{k-1}/2^k = 1/2$ queda

$$\frac{1}{2} = 2^{k-1}m - \sum_{i \neq 2^k} \frac{2^{k-1}}{i}.$$

Al expresar en forma reducida las fracciones del miembro derecho, todas quedan con denominador impar (incluyendo el 1, ya que algunas pueden ser enteros) y su suma también tendrá denominador impar. luego la igualdad con $1/2$ es imposible.

**2.10** El exponente de 5 en 2011! es

$$\left\lfloor \frac{2011}{5} \right\rfloor + \left\lfloor \frac{2011}{25} \right\rfloor + \left\lfloor \frac{2011}{125} \right\rfloor + \left\lfloor \frac{2011}{625} \right\rfloor = 402 + 80 + 16 + 3 = 501$$

y el exponente de 2 es obviamente mayor que el de 5, por lo tanto 2011! termina en 501 ceros.

**2.11** Como en cada posición se usan 9 dígitos, es como si el cuentakilómetros funcionara en base 9, salvo que usa los dígitos 7, 8 y 9 en vez de 6, 7 y 8. Por lo tanto la respuesta es $(2015)_9 = 2 \cdot 9^3 + 0 \cdot 9^2 + 1 \cdot 9^1 + 5 = 2 \cdot 729 + 9 + 5 = 1472$.

**2.12** Es una multiplicación en base 9.

**2.13** No es potencia de 2 porque es múltiplo del impar 11111. En efecto, numeremos las tarjetas de derecha a izquierda como 0, 1, 2,..., 88888. Si el número $A < 55555$ está en la tarjeta $j$ y el número $B = 111110 - A$ está en la tarjeta $k$, entonces la contribución de ambos es

$$A \cdot 10^{5j} + (111110 - A) \cdot 10^{5k} = 11111 \cdot 10^{5k+1} + A(10^{5j} - 10^{5k}),$$

que es múltiplo de 11111 pues la diferencia $10^{5j} - 10^{5k}$ lo es (si por ejemplo $j > k$ entonces $10^{5j} - 10^{5k}$ comienza con $5(j-k)$ nueves y termina en $5k$ ceros, y claramente es múltiplo de 11111). Como 55555 rambién es múltiplo de 11111, está listo.

**2.14** Si $N$ cumple la condición entonces debe ser múltiplo de 100 y termina en 00. La suma de sus dígitos es igual a la suma de los dígitos de $n = N/100$, y el problema se reduce a hallar los enteros positivos $n$ que sean iguales a 7 veces la suma de sus dígitos.

Evidentemente no hay ninguno de éstos de una sola cifra. Si $n = 10a + b$ y $n = 7(a+b)$, entonces $3a = 6b$ y $a = 2b$. Resultan así para $n$ los valores 21, 42, 63 y 84, que generan las soluciones 2100, 4200, 6300 y 8400.

Veamos que no hay más soluciones. Si $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0$, con $k \geq 2$, y $n = 7(a_k + a_{k-1} + \cdots + a_0)$, entonces

$$(10^k - 7)a_k + (10^{k-1} - 7)a_{k-1} + \cdots + 3a_1 = 6a_0.$$

pero $6a_0 \leq 6 \cdot 9 = 54$, mientras que el miembro izquierdo es al menos $10^k - 7 \geq 93$.

En conclusión hay sólo 4 soluciones, a saber: 2100, 4200, 6300 y 8400.

**2.15** Si se divide $a$ entre $b$ el cociente es 10000000000010000000000010000 y el resto 9999. Como obviamente 999999999999 es divisible entre 9999, $\text{mcd}(a, b) = 9999$.

**2.16** Se encontrarán después de $\text{mcm}(8, 9, 12) = 72$ minutos, es decir a las 7:12 am.

**2.17** Dado $n$ considere los $n+1$ números 1, 11, 111,..., $\underbrace{11\ldots11}_{n+1 \text{ unos}}$. Por el Principio de las casillas debe haber dos de ellos, digamos $\underbrace{11\ldots11}_{h \text{ unos}}$ y $\underbrace{11\ldots11}_{k \text{ unos}}$, con $i \leq h < k \leq n+1$, que dejan el mismo resto al dividirlos entre $n$. Por lo tanto su diferencia, es decir $\underbrace{11\ldots11}_{k-h \text{ unos}}\underbrace{00\ldots00}_{h \text{ ceros}}$, es múltiplo de $n$.

**2.18** Si $n$ es natural, por el problema anterior $n \mid \underbrace{11\ldots11}_{k-h \text{ unos}}\underbrace{00\ldots00}_{h \text{ ceros}}$, es decir $n \mid r \cdot 10^h$, donde $r$ tiene todos sus dígitos iguales a 1. Pero como $\text{mcd}(n, 10) = 1$ resulta que $n \mid r$.

**2.19** En general supongamos que la hoja tiene dimensiones $m \times n$ y consideremos un sistema de coordenadas cartesianas en el cual el vértice inferior izquierdo sea $(0, 0)$ y el derecho sea $(m, n)$. Si la diagonal tiene $k$ puntos de intersección con las líneas de la cuadrícula entonces esos puntos determinan $k-1$ segmentos, cada uno contenido en un cuadradito, y el número de cuadraditos atravesados por la diagonal será $k-1$. Como $(0, 0)$ es uno de los puntos de uintersección, el número de cuadraditos atravesados por la diagonal es igual al número de puntos de intersección de la diagonal con las rectas $x = k$ $(k = 1, 2, \ldots, m)$, $y = h$ $(h = 1, 2, \ldots, n)$. Podría pensarse que esos puntos de intersección son $m + n$, pero en esa suma algunos puntos están contados dos veces, a saber los puntos pertenecientes a la diagonal que tengan ambas coordenadas enteras. Si $d = \text{mcd}(m, n)$ pongamos $m = dm'$, $n = dn'$. Ahora bien, la ecuación de la diagonal es $my = nx$, o equivalentemente $m'y = n'x$. Si $x$ e $y$ son enteros positivos, como $\text{mcd}(m', n') = 1$ resulta que $n' \mid y$ y $m' \mid x$. Además, como $y/n' = x/m'$ es claro que las posibles puntos reticulares en la diagonal son $(m', n')$, $(2m', 2n')$,..., $(dm', dn')$. Es decir que hay $d$ de esos puntos y la respuesta es $m + n - \text{mcd}(m, n)$.

Para $m = 259$ y $n = 154$ se tiene $259 + 154 - \text{mcd}(259, 154) = 413 - 7 = 406$.

**2.20** Cualquier $n > 0$ se puede escribir como $n = 5k + r$, con $0 \leq r \leq 4$. Como $5k + 1 = 5(k - 7) + 36$, $5k + 2 = 5(k - 2) + 12$, $5k + 3 = 5(k - 9) + 48$ y $5k + 4 = 5(k - 4) + 24$, resulta que si $k \geq 9$ (o sea $n \geq 45$) el pedido se puede despachar exactamente. Como también $44 = 5 \cdot 4 + 12 \cdot 2$ se puede despachar, el mayor que no se puede despachar exactamente es 43. En efecto, para despachar 43 habría que usar 1, 2 ó 3 cajas grandes, pero ni $43 - 12 = 31$, ni $43 - 24 = 19$, ni $43 - 36 = 7$ son múltiplos de 5, por lo tanto no es posible.

**2.21** Este es la generalización del problema anterior. Cualquier entero $n$ se puede expresar en la forma $sa + tb$, pero $s$ o $t$ podrían ser negativos. Ahora bien, como

$$sa + tb = (s + kb)a + (t - ka)b$$

es claro que siempre se puede lograr una representación con $s \geq 0$. Más aún, si se toma el menor $s$ con esa propiedad se tendrá $s \geq 0$ y $s - b < 0$. Si para ese $s$ fuese $t < 0$ entonces se tendría $s \leq b - 1$ y $t \leq -1$, de donde $n = sa + tb \leq (b-1)a - b = ab - a - b$. Esto muestra que cualquier $n > ab - a - b$ se puede representar como $sa + tb$ con $s \geq 0$ y $t \geq 0$.

Veamos ahora que $ab - a - b$ no se puede representar de esa manera. En efecto, si $ab - a - b = sa + tb$ con $s \geq 0$ y $t \geq 0$ se tendría que $a(b - 1 - s) = (t + 1)b$, y como $\text{mcd}(a, b) = 1$ se deduce que $a \mid t + 1$ y en particular $a \leq t + 1$ y $t \geq a - 1$. Análogamente $b(a - 1 - t) = (s + 1)a$, de donde $b \mid s + 1$, $b \leq s + 1$ y $s \geq b - 1$. Pero entonces $sa + tb \geq (b - 1)a + (a - 1)b = 2ab - a - b > ab - a - b$, absurdo.

**2.22** Es claro que un cubo se puede partir en $k^3$ cubitos idénticos para cualquier $k$ natural. En particular se puede partir en 8 y en 27 cubitos. Tomando uno de esos cubitos y partiéndolo a su vez en 8 o en 27 cubos, y así sucesivamente, es claro que un cubo se puede partir en $1+7x+26y$ cubos, para $x, y$ enteros no negativos cualesquiera. Por el problema anterior, así se pueden obtener todos los enteros del $1+(7-1)(26-1)=151$ en adelante. Es posible con más trabajo probar que el mínimo $n_0$ es 48.

**2.23** a) $\mathrm{mcd}(F_n, F_{n+1}) = \mathrm{mcd}(F_n, F_n + F_{n-1}) = \mathrm{mcd}(F_n, F_{n-1})$ y aplicando esto reiteradamente se tiene

$$\mathrm{mcd}(F_n, F_{n+1}) = \mathrm{mcd}(F_{n-1}, F_n) = \mathrm{mcd}(F_{n-2}, F_{n-1}) = \cdots = \mathrm{mcd}(F_1, F_2) = 1.$$

b) Para $m = 0$ es trivialmente cierto pues $F_1F_n + F_0F_{n-1} = F_n$. Suponiendo que sea cierto para $m < n-1$ entonces para $m+1$ se tiene

$$\begin{aligned} &F_{m+2}F_{n-m-1} + F_{m+1}F_{n-m-2} = (F_{m+1}+F_m)F_{n-m-1} + F_{m+1}F_{n-m-2} \\ &= F_mF_{n-m-1} + F_{m+1}(F_{n-m-1}+F_{n-m-2}) = F_mF_{n-m-1} + F_{m+1}F_{n-m} = F_n. \end{aligned}$$

c) Por (b) se tiene

$$\mathrm{mcd}(F_n, F_m) = \mathrm{mcd}(F_mF_{n-m-1} + F_{m+1}F_{n-m}, F_m) = \mathrm{mcd}(F_{m+1}F_{n-m}, F_m)$$

Pero como $\mathrm{mcd}(F_m, F_{m+1}) = 1$ (por (a)) entonces

$$\mathrm{mcd}(F_{m+1}F_{n-m}, F_m) = \mathrm{mcd}(F_{n-m}, F_m).$$

Por lo tanto $\mathrm{mcd}(F_n, F_m) = \mathrm{mcd}(F_{n-m}, F_m)$. Aplicando esto en forma reiterada resulta que si $n = q_1m + r_1$ con $0 \le r_1 < m$ entonces $\mathrm{mcd}(F_n, F_m) = \mathrm{mcd}(F_{n-q_1m}, F_m) = \mathrm{mcd}(F_m, F_{r_1})$. Supongamos ahora que se aplica el algoritmo de Euclides y $m = q_2r_1 + r_2$ con $0 \le r_2 < r_1$, $r_1 = q_3r_2 + r_3$ con $0 \le r_3 < r_2$,..., $r_{k-1} = q_{k+1}r_k$ con $r_k = \mathrm{mcd}(m, n)$. Entonces

$$\begin{aligned} \mathrm{mcd}(F_n, F_m) &= \mathrm{mcd}(F_m, F_{r_1}) = \mathrm{mcd}(F_{r_1}, F_{r_2}) = \cdots \\ &= \mathrm{mcd}(F_{r_{k-1}}, F_{r_k}) = F_{r_k} = F_{\mathrm{mcd}(m,n)}. \end{aligned}$$

**2.24** Como $\mathrm{mcm}(11, 12, 13, 14, 15, 16) = 240240$, los números $2402411 = 240240 \cdot 10 + 11$, 2402412, 2402413, 2402414, 2402415 y 2402416 satisfacen la condición pedida.

**2.25** Veamos un ejemplo: $S(234) = 2+3+4 = 9$ y $S(468) = 4+6+8 = 18$. Esto parece sugerir que $S(2n)$ es el doble de $S(n)$. Pero $S(372) = 3+7+2 = 12$ y $S(2 \times 372) = S(744) = 7+4+4 = 15$. La diferencia entre los dos ejemplos está en que en el segundo, al calcular $2n$, hay acarreo. De hecho, si todos los dígitos de $n$ son menores que 5 entonces cada dígito de $2n$ es simplemente el doble del

dígito correspondiente de $n$, y por lo tanto $S(2n) = 2S(n)$. Pero por cada dígito de $n$ mayor o igual que 5, al sumar $n + n$ se produce el acarreo de una unidad, lo que hace que $S(2n)$ disminuya 9 unidades respecto de $2S(n)$. En otras palabras, $S(2n) = 2S(n) - 9m$, donde $m$ es el número de unidades *llevadas*, que es igual al número de dígitos de $n$ que son mayores o iguales que 5.

Una prueba más formal: si $a_1a_2 \ldots a_k$ son los dígitos decimales de $n$ y si $2a_i = 10b_i + c_i$, donde $b_i$ es 0 ó 1 según que $a_i < 5$ o $a_i \geq 5$, entonces los dígitos de $2n$ son $b_1$, $c_1 + b_2$, $c_2 + b_3$,. . . , $c_{k-1} + b_k$, $c_k$ y

$$S(2n) = \sum_i b_i + c_i = \sum_i 2a_i - 9b_i = 2S(n) - 9m.$$

**2.26** En este problema $2S(N) - S(2N) = 200 - 110 = 90$, por lo tanto $N$ debe contener exactamente 10 cifras mayores o iguales que 5. Como estamos interesados en el menor $N$ posible, pongamos estas 10 cifras iguales a nueve, para disminuir el número total de cifras. La suma de estos 9 es 90, y para completar $S(N) = 100$ con cifras menores que 5, se necesitan al menos tres cifras, que podrían ser 4, 4 y 2 o 4, 3 y 3. Nos conviene la primera opción para poner el 2 en el primer lugar, y así se obtiene la solución $N = 2449999999999$.

**2.27** Usando el problema p5 se tiene $9S(n) = 16S(2n) = 16(2S(n)-9m)$, donde $m$ es el número de dígitos de $n$ que son mayores o iguales que 5. Entonces $23S(n) = 144m$, y resulta que 23 divide a $m$ y $n$ tiene al menos 23 cifras. Si un número de 23 cifras cumple la condición entonces todas deben ser $\geq 5$, y para hallar el menor tratamos de poner todos los 5 que se pueda a la izquierda. El máximo es 15, pues con 16 suman 80 y deberíamos llegar a 144 con 7 dígitos, lo cual no es posible. Con 15 cincos nos quedan $144 - 75 = 69$ para repartir en 8 dígitos, lo que hacemos con un 6 y 7 nueves para tener una cifra lo menor posible después de los cincos iniciales. Así resulta que el menor $n$ es $\underbrace{55\ldots5}_{15}6\underbrace{99\ldots9}_{7}$.

**2.28** Sean $x$ e $y$ enteros tales que $f(x) \leq f(y)$. Si $f(x) = f(y)$ entonces $f(x) \mid f(y)$, así que supongamos $f(x) < f(y)$. Entonces $f(x - y)$ divide a $f(x) - f(y)$ y por lo tanto también a $f(y) - f(x) > 0$. Por lo tanto

$$f(x - y) \leq f(y) - f(x) < f(y),$$

de donde

$$-f(y) < -f(x - y) < f(x) - f(x - y) < f(x) < f(y).$$

Tomando $m = x$ y $n = x - y$ resulta que $f(y) = f(x - (x - y)) \mid f(x) - f(x - y)$, pero por la desigualdad anterior $|f(x) - f(x - y)| < f(y)$, lo cual implica que $f(x) - f(x - y) = 0$, o $f(x) = f(x - y)$. Por lo tanto $f(x) \mid f(x) - f(y)$, de donde $f(x) \mid f(y)$.

# Capítulo 3

**3.1** Como la suma de sus cifras es 300, el número es divisible entre 3 pero no entre 9 y por lo tanto no puede ser un cuadrado perfecto.

**3.2** Suponiendo que los números hayan sido correctamente codificados, el resultado $EEFF$ es múltiplo de 11 (pues $E-E+F-F=0$). Entonces al menos uno de los factores es múltiplo de 11. Pero los múltiplos de 11 de dos dígitos tienen ambas cifras iguales, mientras que los que escribió Pedro las tienen diferentes.

**3.3** No. Cualquier número que se obtenga es congruente módulo 3 con la suma de los dígitos, que es $1+2\cdot 2+3\cdot 3+4\cdot 4+5\cdot 5+6\cdot 6+7\cdot 7 = 1+4+9+16+25+36+7^2 = 140 \equiv 2 \pmod 3$, pero los cuadrados sólo pueden ser congruentes con 0 ó 1 módulo 3.

**3.4** Solamente para $k=1$. Si $k \geq 2$, se tiene $11\ldots1 \equiv 11 \equiv 3 \pmod 4$, pero los cuadrados sólo pueden ser congruentes con 0 ó 1 módulo 4.

**3.5** No. Como $8+6+4+2+0 = 20 \equiv 2 \pmod 9$, todos esos números son congruentes con 2 módulo 9. Pero los cuadrados sólo pueden ser congruentes con 0, 1, 4, ó 7 módulo 9.

**3.6** A diferencia de los cuadrados, un cubo puede tener cualquier dígito como cifra de las unidades. Pero los restos módulo 7 sólo pueden ser 0, 1 ó 6. Esto se puede ver calculando los restos de los cubos de los números del 0 al 6, o bien observando que si $7 \nmid x$ entonces por el Teorema de Fermat $(x^3+1)(x^3-1) \equiv 0 \pmod 7$, es decir que $x^3 \equiv 1 \pmod 7$ ò $x^3 \equiv -1 \pmod 7$. esto muestra que $n!+5$ no puede ser cubo para $n \geq 7$, pues deja resto 5 (mód 7). Para $0 < n < 7$ una inspección directa muestra que el único cubo se obtiene para $n=5$ $(5!+5 = 125 = 5^3)$.

**3.7** Como los cuadrados sólo pueden ser congruentes con 0 ó 1 módulo 3, $m^2+n^2$ será congruente con 0 módulo 3 sólo cuando lo sean $m$ y $n$.

**3.8** Con el algoritmo de Euclides se halla que $1 = \text{mcd}(37,21) = 4\cdot 37 - 7\cdot 21$, por lo tanto $-7$ es inverso multiplicativo de 21 (mód 37), de donde $x \equiv -7\cdot 21x \equiv -7\cdot 2 \equiv 23 \pmod{37}$ y la solución es $x=23$.

**3.9** Un cuadrado no puede ser congruente con 2 módulo 3, ya que si $3 \mid x$ entonces $x^2 \equiv 0 \pmod 3$ y si $3 \nmid x$ entonces $x^2 \equiv 1 \pmod 3$. Entonces si ni $x$ ni $y$ fuesen múltiplos de 3 se tendría $z^2 = x^2+y^2 \equiv 2 \pmod 3$, absurdo.

**3.10** La razón $d$ es par por ser diferencia de dos impares. Ahora, si los tres términos de la progresión dejan restos diferentes al dividirlos entre 3 entonces uno de ellos dejaría resto 0, lo cual es absurdo pues son primos mayores que 3. Entonces debe haber dos términos $p<q$ tales que $q-p$ es múltiplo de 3, y como $q-p$ es $d$ o $2d$, $d$ es múltiplo de 3 y por lo tanto de 6.

**3.11** Sean $x_1$, $x_2$,..., $x_7$ los números y $S$ su suma. Entonces $S - x_i \equiv 0 \pmod 5$ para $i = 1, 2, \ldots, 7$. Como $\sum_{i=1}^{6}(S - x_i) = 6S - (S - x_7) = 5S + x_7$ se deduce que $x_7 = \sum_{i=1}^{6}(S - x_i) - 5S \equiv 0 \pmod 5$, y análogamente para los demás.

**3.12** Multipliquemos la primera congruencia por 3 (el inverso multiplicativo de 2 módulo 5), la segunda por 5 y la tercera por $-2$ para obtener

$$\begin{aligned} x &\equiv 4 \pmod 5, \\ x &\equiv 4 \pmod 7, \\ x &\equiv -3 \pmod{11}. \end{aligned}$$

De la primera resulta $x = 4+5k$. Sustituyendo en la segunda $4+5k \equiv 4 \pmod 7$, o sea $5k \equiv 0 \pmod 7$, de donde $k = 7h$. Ahora $x = 4 + 5k = 4 + 35h$ y sustituyendo en la tercera resulta $4 + 35h \equiv -3 \pmod{11}$, es decir $2h \equiv -7 \pmod{11}$, y multiplicando por $-5$ resulta $h \equiv 35 \equiv 2 \pmod{11}$, de donde $h = 2 + 11i$. Finalmente $x = 4 + 5k = 4 + 35h = 4 + 35(2 + 11i) = 74 + 385i$. Es decir que la solución es $x \equiv 74 \pmod{385}$.

**3.13** Como los cuadrados sólo pueden ser congruentes con 0 ó 1 módulo 4, $x^2 + y^2 + z^2$ será congruente con 0 módulo 4 sólo cuando lo sean $x^2$, $y^2$ y $z^2$ (de lo contrario sería congruente con 1, 2 ó 3), es decir cuando $x$, $y$, $z$ sean los tres pares.

**3.14** Sea $n$ un número divertido. Observemos que $n$ debe ser impar, ya que $2+2 = 4$ no es primo. Además $n$ no puede tener factores primos $p \equiv 1 \pmod 3$, pues $p+2 \equiv 0 \pmod 3$ no sería primo. Y si tiene un factor primo $p \equiv 2 \pmod 3$, éste debe aparecer en $n$ con exponente 1, ya que $p^2 + 2 \equiv 2 \cdot 2 + 2 \equiv 0 \pmod 3$ no es primo. por la misma razón no puede tener dos factores primos distintos, ambos $\equiv 2 \pmod 3$. Luego $n$ debe ser de alguna de las formas $3^k$, $p$ o $3^k p$, con $p \equiv 2 \pmod 3$ primo.

De la forma $3^k$ se verifica que solamente 3, $3^2$, $3^3$ y $3^4$ son divertidos, y de ellos el que tiene más divisores es $3^4$, con 5 divisores.

Los de la forma $p$ sólo tienen 2 divisores.

De la forma $3^k \cdot 5$ el divertido con más divisores es $3^3 \cdot 5 = 135$, con 8 divisores ($3^4 \cdot 5 = 405$ no es divertido pues $407 = 11 \cdot 37$ no es primo).

Para los de la forma $3^k p$ con $p > 5$, observamos que:

Si $p \equiv 1 \pmod 5$ entonces $3p + 2 \equiv 0 \pmod 5$.

Si $p \equiv 2 \pmod 5$ entonces $3^2 p + 2 \equiv 0 \pmod 5$.

Si $p \equiv 3 \pmod 5$ entonces $p + 2 \equiv 0 \pmod 5$.

Si $p \equiv 4 \pmod 5$ entonces $3^3 p + 2 \equiv 0 \pmod 5$.

Por lo tanto $k \leq 2$ y estos números tienen a lo sumo $3 \cdot 2 = 6$ divisores.

En definitiva el máximo número de divisores que puede tener un número divertido es 8, y se alcanza únicamente para el 135.

**3.15** Como $2222 = 317 \cdot 7 + 3$, $5555 = 793 \cdot 7 + 4$ y $2222^6 \equiv 5555^6 \equiv 1 \pmod 7$, se tiene

$$2222^{5555} + 5555^{2222} \equiv 3^{925 \cdot 6 + 5} + 4^{370 \cdot 6 + 2} \equiv 3^5 + 4^2 \equiv 259 \equiv 0 \pmod 7.$$

**3.16** Como $10^6 \equiv 1 \pmod 7$ el número 999999 es divisible entre 7, y como $999999 = 9 \cdot 111111$ y $\mcd(9, 7) = 1$, 111111 es divisible entre 7, y también lo es 888888. Es inmediato que también son múltiplos de 7 los números

$$a = \underbrace{88 \cdots 88}_{48\ 8's} \quad \text{y} \quad b = \underbrace{99 \cdots 99}_{48\ 9's},$$

y como

$$\underbrace{88 \cdots 88}_{50\ 8's} d \underbrace{99 \cdots 99}_{50\ 9's} = 10^{53} a + 88d99 \cdot 10^{48} + b,$$

este número es divisible entre 7 si y sólo si $88d99$ lo es, pero $-3 \cdot 8 - 8 + 2d + 3 \cdot 9 + 9 = 2d + 4 \equiv 0 \pmod 7$, de donde $d = 5$.

**3.17** Como $2^{16} \equiv 1 \pmod{17}$, busquemos el resto de dividir $3^{2011}$ entre 16. Como $\phi(16) = 2^4 - 2^3 = 8$ se tiene $3^{2011} = 3^{251 \cdot 3 + 3} \equiv 3^3 = 27 \equiv 11 \pmod{16}$, por lo tanto $2^{3^{2011}} \equiv 2^{11} = 2^4 \cdot 2^4 \cdot 2^3 \equiv (-1)(-1)8 = 8 \pmod{17}$.

**3.18** Considere las fracciones $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$. Si cada una de ellas se expresa en forma irreducible, los denominadores son divisores de $n$, y las que tienen denominador $d$ son de la forma $\frac{k}{d}$, con $1 \leq k \leq d$ y $\mcd(k, d) = 1$. Y todas éstas se obtienen realmente, al simplificar $\frac{k(n/d)}{n}$. Por lo tanto son $\phi(d)$, y al sumar para $d \mid n$ se obtiene el resultado buscado.

**3.19** Si $n$ es impar entonces $7^n \equiv (-1)^n \equiv -1 \equiv 3 \pmod 4$. Y como $\phi(10) = 4$ entonces

$$\underbrace{7^{7^{\cdot^{\cdot^{\cdot^7}}}}}_{2015\ 7's} \equiv 7^3 \pmod{10}.$$

**3.20** Debemos evaluar $2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}$. Como $\phi(1000) = \phi(2^3 \cdot 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$, el problema se reduce a evaluar $2002^{2001} \equiv 2^{2001} \pmod{400}$. Ahora bien, si $2^{1997} \equiv x \pmod{25}$, entonces $2^{2001} \equiv 16x \pmod{400}$. Como $\phi(25) = 20$,

$$2^{1997} = 2^{199 \cdot 20 + 17} \equiv 2^{17} = 2^{10} 2^7 = 1024 \cdot 128 \equiv (-1)3 \equiv 22 \pmod{25},$$

luego $2^{2001} \equiv 16 \cdot 22 = 352 \pmod{400}$ y finalmente

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \equiv 3^{352} = 9^{176} \pmod{1000}.$$

Finalmente usamos el teorema del binomio para calcular

$$9^{176} = (-1+10)^{176} \equiv 1 - 176 \cdot 10 + \binom{176}{2} 10^2 = 1 - 1760 + 1540000$$
$$\equiv 1 - 760 = -759 \equiv 241 \pmod{1000}.$$

**3.21** Por el Teorema de Euler se tiene que $3^{\phi(10^{2012})} \equiv 1 \pmod{10^{2012}}$, por lo tanto la cifra de las unidades de $3^{\phi(10^{2012})}$ es un 1 y está precedida de al menos 2011 ceros.

La misma prueba se aplica a cualquier primo $p$ distinto de 2 y 5.

**3.22** El único es el 1. Para verlo basta probar que cada primo $p$ divide a algún $a_n$. Como $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$, esto es cierto para $p = 2$ y $p = 3$. Supongamos $p \geq 5$. Por Fermat se tiene $2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}$. Entonces

$$6(2^{p-2}+3^{p-2}+6^{p-2}-1) = 3\cdot 2^{p-1}+2\cdot 3^{p-1}+6^{p-1}-6 \equiv 3+2+1-6 \equiv 0 \pmod{p}.$$

Y como $p$ es coprimo con 6, resulta $2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 0 \pmod{p}$.

**3.23** Por el Teorema de Euler $2^{\phi(5^j)} \equiv 1 \pmod{5^j}$, es decir que $2^{\phi(5^j)} = A \cdot 5^j + 1$ para cierto natural $A$. Multiplicando por $2^j$ resulta $2^{\phi(5^j)+j} = A \cdot 10^j + 2^j$, y basta escoger $j$ suficientemente grande para que $j$ supere en $N$ al número de cifras de $2^j$. Esto siempre es posible pues $2^j$ tiene $\lfloor \log_{10} 2^j \rfloor + 1 \leq 1 + j \log_{10} 2$ y $j - 1 - j \log_{10} 2 = -1 + j \log_{10} 5$ se puede hacer tan grande como queramos. Con el $j$ adecuado, se toma la potencia de 2 de exponente $\phi(5^j) + j = 4^j + j$.

Una demostración similar se puede aplicar al caso $p = 5$.

**3.24** Se tiene que $a_i a_{i+1} \equiv a_i \pmod{n}$ para $i = 1, 2, \ldots, k-1$, por lo tanto

$$a_1 a_2 \cdots a_k \equiv a_1 a_2 \cdots a_{k-1} \equiv \cdots \equiv a_1 a_2 \equiv a_1 \pmod{n}.$$

Si $n \mid a_k(a_1 - 1)$ entonces $a_k a_1 \equiv a_k \pmod{n}$ y procediendo como antes tendríamos

$$a_k a_1 a_2 \cdots a_{k-1} \equiv a_k a_1 a_2 \cdots a_{k-2} \equiv \cdots \equiv a_k a_1 \equiv a_k \pmod{n}.$$

Pero entonces $a_1 \equiv a_k \pmod{n}$, lo cual es absurdo pues $0 < |a_1 - a_k| < n$.

**3.25.** Observemos que $2^4 \parallel \frac{17^2-1^2}{2}$. Si $2^s \parallel n$ entonces, por el caso $p = 2$ del Lema de Hensel, se tendrá $2^{s+4} \parallel 17^n - 1$. Por lo tanto para que $2^{2007} \mid 17^n - 1$ debe ser $2^{2003} \mid n$ y el mínimo buscado es $n = 2^{2003}$.

**3.26.** Como $n$ es impar $a^n + b^n$ se puede factorizar como

$$(a+b)(a^{n-1}b - a^{n-2}b^2 + \cdots - ab^{n-2} + b^{n-1}.$$

Entonces $a + b = p^r$ para algún entero positivo $r \leq k$. Observemos que se puede suponer que $p \nmid a$ y $p \nmid b$, ya que si $a = Ap^t$, $b = Bp^t$ entonces $A + B = p^{r-t}$ y $A^n + B^n = p^{k-nt}$, etc.

Supongamos ahora que $p^s \parallel n$. Entonces por el corolario $p^{r+s} \parallel a^n + b^n = p^k$, de donde $s = k - r$. Pongamos $n = mp^s$. Como

$$p^k = p^r p^s || a^{p^s} + b^{p^s} \leq a^{mp^s} + b^{mp^s} = p^k$$

se concluye que $m = 1$ y $n$ es una potencia de $p$.

Nota: Para $n$ par no se cumple, por ejemplo $3^2 + 4^2 = 5^2$ y $2 \nmid 5$.

**3.27.** Probaremos que 1 y 3 son las únicas soluciones. Es claro que $n = 1$ es solución. Como $2^n + 1$ es impar, $n$ debe ser impar. Además $2^n \equiv -1 \pmod{n}$, de donde $2^{2n} \equiv 1 \pmod{n}$. Si $n > 1$, sea $p_1$ el menor factor primo de $n$. Entonces $2^{2n} \equiv 1 \pmod{p_1}$. Sea $d_1$ el orden de 2 módulo $p_1$ (es decir el menor entero positivo tal que$2^{d_1} \equiv 1 \pmod{p_1}$). Entonces $d_1 \mid 2n$. Y como $2^{p_1-1} \equiv 1 \pmod{p_1}$ (por pequeño Fermat) debe ser $d_1 < p_1$. Como $p_1$ es el menor divisor de $n$ (exceptuando el 1), $d_1$ sólo puede ser 1 ó 2. Como $2^1 \equiv 1 \pmod{p_1}$ es imposible, debe ser $d_1 = 2$. Entonces $2^2 \equiv 1 \pmod{p_1}$ y $p_1 = 3$. Supongamos que $3^s \parallel n$. Entonces, como $3^1 \parallel 2 + 1$, por el corolario $3^{s+1} \parallel 2^n + 1$. Pero como $3^{2s} \mid n^2 \mid 2^n + 1$, resulta que $2s \leq s + 1$, es decir que $s = 1$ y $n = 3n'$, donde $3 \nmid n'$. Si $n' \neq 1$, sea $p_2$ el menor factor primo de $n'$. Entonces $2^{6n'} \equiv 1 \pmod{p_2}$. Sea $d_2$ el orden de 2 módulo $p_2$. Entonces $d_2 \mid 6n'$ y $d_2 < p_2$, de donde $d_2 \mid 6$. Por lo que ya vimos $d_2$ no puede ser 1 ni 2. Si $d_2 = 3$ entonces $p_2 = 7$. Si $d_2 = 6$ entonces $p_2 \mid 63$, y como $3 \nmid n'$ resulta que también en este caso $p_2 = 7$. En consecuencia si $7^2 \mid 2^n + 1$ y $2^n \equiv -1 \pmod{7}$. Pero $2^3 \equiv 1 \pmod{7}$, por tanto si $n = 3q + r$ con $0 \leq r < 3$ se tiene $2^n \equiv (2^3)^q 2^r \equiv 2^r \pmod{7}$, es decir que $2^n$ es congruente con 1, 2 ó 4 $\pmod{7}$ y $2^n \not\equiv -1 \pmod{7}$. Esta contradicción provino de suponer $n' \neq 1$, en consecuencia $n' = 1$ y $n = 3$.

**3.28.** Observemos que $3 \nmid p$ (si no 3 dividiría a 5). Luego $5^k \equiv p^2 \equiv 1 \pmod{3}$, de donde $k$ es par. Además $3^n + p^2 = 5^k \equiv 1 \pmod{4}$, y como $p$ es par (pues $p^2$ es diferencia de dos impares) resulta que $3^n \equiv 1 \pmod{4}$ y $n$ es par. Pongamos $k = 2a$ y $n = 2b$. Entonces $5^{2a} = p^2 + 3^{2b}$ por lo que $(p, 3^b, 5^a)$ es una terna pitahórica. Entonces existen dos enteros coprimos $x$, $y$ tales que $2xy = p$, $x^2 - y^2 = 3^b$, $x^2 + y^2 = 5^a$. Pero de $(x + y)(x - y) = 3^b$ se sigue que $x + y$ y $x - y$ son potencias de 3. Si $x - y > 1$ entonces se sigue que $x$ e $y$ son múltiplos de 3 y $x^2 + y^2 = 5^a$ es múltiplo de 3, absurdo. Entonces $x - y = 1$ y tenemos

$$3^b = x^2 - (x - 1)^2 = 2x - 1. \qquad (*)$$

Además $5^a = x^2 + (x - 1)^2 = 2x^2 - 2x + 1$, de donde

$$2 \cdot 5^a - 1 = 4x^2 - 4x + 1 = (2x - 1)^2,$$

y en vista de (*)

$$2 \cdot 5^a - 1 = 9^b. \qquad (**)$$

La igualdad anterior implica que $9^b \equiv -1 \pmod{10}$ y por lo tanto $b$ es impar. Además $5^a \parallel 9^b + 1$, y como $5 \parallel 9 + 1$, del lema de Hensel resulta que $5^{a-1} \parallel b$. Pero si $s \geq 2$ entonces $9^s = (1+8)^s \geq 1 + 8s + 8^2 s(s-1)/2 > 40s$, luego si $a > 1$ resulta

$$2 \cdot 5^a = 9^b + 1 \geq 9^{5^{a-1}} + 1 > 40 \cdot 5^{a-1} = 8 \cdot 5^a,$$

absurdo. Luego $a = 1$ y de $2 \cdot 5 - 1 = 9^b$ sale $b = 1$. Entonces $n = k = 2$ y de $p^2 = 5^2 - 3^2 = 16$ resulta $p = 4$.

**3.29** Sea $N = M \cdot 10^t$ donde $M$ es un número entero que no termina en 0 y $t$ es un entero no negativo. Si $N$ es un cuadrado perfecto, necesariamente $M$ debe ser un cuadrado perfecto y $t$ debe ser par. Por lo tanto, podemos suponer inicialmente que $N$ no termina en 0 y sabemos que a partir de los valores que obtengamos con esa suposición, los demás se obtienen agregando un número par de ceros a la derecha.

Como $N$ es un cuadrado perfecto su último dígito sólo puede ser 1, 4, 5, 6 ó 9. Sea $k$ dicho dígito y sea $n$ el número de ceros que tiene $N$. Entonces $N = 3\underbrace{0\ldots0}_{n}k$.

Si $k = 9$ la suma de los dígitos de $k$ sería múltiplo de 3 pero no de 9, luego $N$ sería múltiplo de 3 y no de 9 y no podría ser un cuadrado perfecto.

Si $k = 5$ entonces $N$ dejaría resto 2 al dividirlo entre 3, lo cual no puede ser pues todo cuadrado perfecto es congruente con 0 ó 1 módulo 3.

Si $n > 0$ entonces $N \equiv k \pmod{4}$, lo cual excluye la posibilidad $k = 6$ ya que los cuadrados perfectos son congruentes con 0 ó 1 módulo 4. Si $n = 0$ entonces el único valor de $k$ para el cual $N$ es un cuadrado perfecto es 6, y obtenemos así la solución 36.

Si $k = 1$ o $k = 4$ pongamos $N = a^2$ con $a$ entero positivo. Necesariamente $n > 0$ pues 31 y 34 no son cuadrados perfectos. Se tiene entonces que

$$N - k = 3 \cdot 10^{n+1} = 3 \cdot 5^{n+1} \cdot 2^{n+1} = (a - \sqrt{k})(a + \sqrt{k}).$$

Notemos que al ser $k$ cuadrado perfecto (1 ó 4), los dos factores al lado derecho de la igualdad son enteros positivos y al menos uno de ellos debe ser múltiplo de 5. Pero no pueden ser ambos múltiplos de 5 pues su diferencia es $2\sqrt{k}$, que no es múltiplo de 5. Por lo tanto uno de los factores debe ser múltiplo de $5^{n+1}$. Ese factor es entonces al menos $5^{n+1}$ y el otro es a lo sumo $3 \cdot 2^{n+1}$. Como $n \geq 1$ entonces $2n \geq n + 1$ y

$$5^{n+1} - 3 \cdot 2^{n+1} > 4^{n+1} - 3 \cdot 2^{n+1} \geq 3(2^{2n} - 2^{n+1}) + 4^n \geq 4.$$

Eso significa que la diferencia entre los dos factores es mayor que $2\sqrt{k}$ (que a lo sumo es 4) lo cual es absurdo. Luego no hay solución con $k = 1$ o $k = 4$. Agotadas todas las posibilidades se concluye que las únicas soluciones al problema son los números de la forma $N = 36 \cdot 10^{2t}$ con $t$ entero no negativo.

**3.30.** Probaremos por inducción que para cualquier matural $k$ existe un $n_k$ con exactamente $k$ divisores primos tal que $n_k \mid 2^{n_k}+1$ y un primo $p_k$ tal que $p_k \mid 2^{n_k}+1$

y $p_k \nmid n_k$. Para $k=1$, como $2^9+1=513=3^3\cdot 19$, tomando $n_1=9$ y $p_1=19$ se cumple lo deseado. Suponiendo el resultado cierto para $k$, tomemos $n_{k+1}=n_k p_k$. Es claro que $n_{k+1}$ tiene $k+1$ divisores primos y como $n_k p_k \mid 2^{n_k}+1 \mid 2^{n_k p_k}+1$ resulta que $n_{k+1} \mid 2^{n_{k+1}}+1$. Nos falta probar que hay un $p_{k+1}$. Sea $q$ un factor primo de $n_k$ y supongamos que $q^s \parallel 2^{n_k}+1$. Como $q \nmid p_k$ se tiene $q^s \parallel (2^{n_k})^{p_k}+1 = 2^{n_{k+1}}+1$. Análogamente si $p_k^t \parallel 2^{n_k}+1$, como $p_k^1 \parallel p_k$ se tiene $p_k^{t+1} \parallel 2^{n_{k+1}}+1$. Si probamos que $2^{n_{k+1}}+1 > p_k(2^{n_k}+1)$ entonces $2^{n_{k+1}}+1$ tendrá un factor primo $p_{k+1}$ distinto de $p_k$ y de los de $n_k$, y listo. Ahora bien,

$$\begin{aligned}\frac{2^{n_{k+1}}+1}{2^{n_k}+1} &= 2^{n_k(p_k-1)} - 2^{n_k(p_k-2)} + \cdots + 2^{2n_k} - 2^{n_k} + 1 \\ &= (2^{n_k}-1)(2^{n_k(p_k-2)} + 2^{n_k(p_k-4)} + \cdots + 2^{3n_k} + 2^{n_k}) + 1 \\ &\geq (2^{n_k}-1)(\frac{p_k-1}{2}2^{n_k}+1) > 511\cdot 2^8(p_k-1) > p_k\end{aligned}$$

y listo.

**3.31** Si $p=2$, basta tomar $q=3$, ya que un cuadrado no puede ser congruente con 2 módulo 3. Supongamos entonces que $p$ es impar, y sea $N=1+p+p^2+\cdots+p^{p-1}$. Como hay un número impar de sumandos $(p)$, $N$ es impar. Además $N \equiv p+1 \pmod{p^2}$, que no es 1 módulo $p^2$, luego $N$ debe tener algún factor primo $q \not\equiv 1 \pmod{p^2}$. Veamos que $q$ tiene la propiedad deseada.

Como $p$ no divide a $N$, debe ser $q \neq p$. Si $p \equiv 1 \pmod q$ entonces $N \equiv 1+1+\cdots+1 = p \pmod q$. Como $N \equiv 0 \pmod q$, entonces $q \mid p$, absurdo. Luego $q \nmid p-1$. Supongamos ahora que

$$n^p \equiv p \pmod q \tag{1}$$

Entonces no puede ser $n \equiv 1 \pmod q$ (pues sería $p \equiv 1 \pmod q$). Y como $q \neq p$, tampoco puede ser $n \equiv 0 \pmod q$. Elevemos a la $p$ ambos miembros de (1). Como $(p-1)N = p^p - 1$, se tiene que $p^p \equiv 1 \pmod q$. Entonces $n^{p^2} \equiv 1 \pmod q$. Pero $n^{q-1} \equiv 1 \pmod q$ (por el teorema "pequeño" de Fermat). Por lo tanto, si $d = \mathrm{mcd}(q-1, p^2)$ entonces $n^d \equiv 1 \pmod q$. Como $q$ fue elegido de modo que $q-1$ no es divisible entre $p^2$, $d$ debe ser 1 o $p$. Pero estamos asumiendo que $n \not\equiv 1 \pmod q$, luego $d$ no puede ser 1. Entonces $d=p$ y $n^p \equiv 1 \pmod q$. Pero $n^p \equiv p \pmod q$, luego $p \equiv 1 \pmod q$, absurdo.

# Capítulo 4

**4.1** Como $0 < \frac{1}{y+\frac{1}{z}} < 1$, de $x + \frac{1}{y+\frac{1}{z}} = \frac{10}{7} = 1 + \frac{3}{7}$ se sigue que $x=1$. Ahora $\frac{1}{y+\frac{1}{z}} = \frac{3}{7}$, o $y + \frac{1}{z} = \frac{7}{3} = 2 + \frac{1}{3}$, de donde $y=2$ y finalmente $z=3$.

**4.2** Como $2x+5y=1$ tiene la solución $x=-2$, $y=1$, entonces $2x+5y = 4-3z$ tiene la solución particular $x=-2(4-3z)$, $y=4-3z$, y la solución general

$x = -2(4-3z)+5t$, $y = 4-3z-2t$. Luego la solución general son todas las ternas $(-8+6z+5t, 4-3z-2t, z)$.

**4.3** Los tres términos del miembro izquierdo aparecen al desarrollar el producto $(x-2)(y-3)$, pero también aparece un 6. Entonces sumando 6 a ambos miembros La ecuación se transforma en $(x-2)(y-3) = 21$. Ahora sólo falta expresar 21 de todas las maneras posibles como producto de dos enteros.

| $x-2$ | $y-3$ | $x$ | $y$ |
|---|---|---|---|
| 1 | 21 | 3 | 24 |
| 3 | 7 | 5 | 10 |
| 7 | 3 | 9 | 6 |
| 21 | 1 | 23 | 4 |
| $-1$ | $-21$ | 1 | $-18$ |
| $-3$ | $-7$ | $-1$ | $-4$ |
| $-7$ | $-3$ | $-5$ | 0 |
| $-21$ | $-1$ | $-19$ | 2 |

**4.4** Como $a^2b^2 + b^2c^2 + 3b^2 - a^2 - c^2 - 3 = (a^2 + c^2 + 3)(b^2 - 1)$, la ecuación planteada es equivalente a

$$(a^2 + c^2 + 3)(b^2 - 1) = 2002.$$

Ahora bien, $2002 \equiv 2 \pmod 4$, y como los cuadrados son congruentes con 0 ó 1 módulo 4, el primer factor de la izquierda es congruente con $-1$, 0 ó 1, y el segundo factor con $-1$ ó 0, por lo cual su producto es congruente con $-1$, 0 ó 1, y nunca con 2.

**4.5** Supongamos que ni $p$ ni $q$ sean 3. Entonces si $p \equiv q \pmod 3$ se tiene $p^3 - q^5 \equiv 0 \pmod 3$ y $(p+q)^2 \equiv 1 \pmod 3$. Si en cambio $p \not\equiv q \pmod 3$ entonces $p^3 - q^5 \not\equiv 0 \pmod 3$ pero $(p+q)^2 \equiv 0 \pmod 3$. Por lo tanto, si hay solución, debe ser $p = 3$ o $q = 3$. Pero si $p = 3$ entonces $q^5 < 27$, lo cual es imposible. Si $q = 3$entonces $p^3 - 3^5 = (p+3)^2$, cuya única raíz entera es $p = 7$. Por lo tanto la única solución es $p = 7$ y $q = 3$.

**4.6** Dado que $S(n) - 1$ es entero, $n$ divide a 2010 por lo que tiene a lo sumo cuatro cifras; si suponemos que $n \leq 99$, se tiene que $S(n) - 1 \leq 17$, y por tanto $n = \dfrac{2010}{S(n)-1} \geq 118$, lo cual es una contradicción. Por lo tanto, $n$ tiene tres o cuatro cifras, y como los divisores de 2010 que cumplen esto son 134, 201, 335, 402, 670, 1005, 2010, revisando cada caso se obtiene que la única solución es $n = 402$.

**4.7** Procedamos por inducción. Para $n = 3$ se cumple pues $2^3 = 7 \cdot 1^2 + 1^2$. Supongamos que $2^n = 7a^2 + b^2$, con $a$ y $b$ impares. Sean $a_1 = (a+b)/2$, $b_1 = (7a-b)/2$, $a_2 = (a-b)/2$, $b_2 = (7a+b)/2$. Es inmediato verificar que $a_1$, $b_1$, $a_2$ y $b_2$ son enteros y que se cumple $7a_1^2 + b_1^2 = 7a_2^2 + b_2^2 = 2(7a^2 + b^2) = 2^{n+1}$.

Para terminar probaremos que uno de los pares $(a_1, b_1)$ y $(a_2, b_2)$ tiene las dos componentes impares. En efecto, como $a$ y $b$ son impares, cada uno de ellos es congruente con 1 o con 3 módulo 4. Si $a \equiv b \pmod 4$ entonces $a + b \equiv 2 \pmod 4$ y $a_1 = (a + b)/2$ es impar. En este caso $b_1 = (7a - b)/2 = 4a - a_1$ también es impar. Si en cambio uno de los enteros $a$ y $b$ es congruente con 1 y el otro con 3, módulo 4, su diferencia es congruente con 2 módulo 4 y por tanto $a_2 = (a - b)/2$ es impar. En este caso $b_2 = (7a + b)/2 = 4a - a_2$ también es impar.

**4.8** Observe que $21 = 3 \cdot 7$. La cantidad de factores primos 3 en 2008! es

$$n = \left\lfloor \frac{2008}{3} \right\rfloor + \left\lfloor \frac{2008}{9} \right\rfloor + \cdots < 2008.$$

Como $3 \mid 21$ y $3 \mid 2008!$ resulta que $3 \mid x$ y la cantidad de factores primos 3 en $x^{2008}$ es por lo menos 2008. Por lo tanto la mayor potencia de 3 que divide al miembro izquierdo es $3^n$, de donde $y = n$. Razonando de manera similar con el 7, $y$ debería ser igual a la cantidad de factores 7 en 2008!. Pero eso es imposible, pues ese número es claramente menor que $n$.

**4.9** La ecuación se puede reescribir como

$$(x + y)^2 + (x - y)^2 = 314(x - y),$$

o completando cuadrados

$$(x + y)^2 + (157 - x + y)^2 = 157^2.$$

Poniendo $a = x + y$, $b = 157 - x + y$ la ecuación se reduce a

$$a^2 + b^2 = 157^2.$$

Como deben ser $x > y > 0$, se sigue que $0 < a, b < 157$, y como 157 es primo, debe ser $\text{mcd}(a, b) = 1$. Debe haber entonces enteros $m > n > 0$, $\text{mcd}(m, n) = 1$, con

$$m^2 + n^2 = 157, \quad a = 2mn, \quad b = m^2 - n^2$$

(o bien $a = m^2 - n^2$, $b = 2mn$). Es fácil ver que la única manera de satisfacer $m^2 + n^2 = 157$ es con $m = 11$, $n = 6$. Luego $a = 132$, $b = 11^2 - 6^2 = 85$ o viceversa. Ahora hay dos posibilidades:

1. $x + y = 132$, $157 - x + y = 85$, que nos conduce a $x - y = 72$, $x = 102$, $y = 30$.
2. $x + y = 85$, $157 - x + y = 132$, que nos conduce a $x - y = 25$, $x = 55$, $y = 30$.

Por lo tanto hay dos soluciones, $(72, 30)$ y $(55, 30)$.

**4.10** Es claro que no hay soluciones con $x < 0$. Con $x = 0$ se tienen dos soluciones: (0,2) y (0,−2). Supongamos ahora $x > 0$ y también $y > 0$ (pues $(x, y)$ es solución si y sólo si $(x, -y)$ lo es). Reescribamos la ecuación como

$$2^x(1 + 2^{x+1}) = (y - 1)(y + 1).$$

Los dos factores de la derecha son dela misma paridad, y no pueden ser impares. Luego son pares, y uno de ellos es múltiplo de 4. Luego $x \geq 3$. Ahora, uno de los factores de la derecha debe ser divisible entre $2^{x-1}$ y no entre $2^x$. Es decir que se puede escribir

$$y = 2^{x-1}m + k, \quad m \text{ impar}, \quad k = \pm 1. \tag{1}$$

poniendo esto en la ecuación original queda

$$2^x(1 + 2^{x+1}) = (2^{x-1}m + k)^2 - 1 = 2^{2x-2}m^2 + 2^x km,$$

o bien

$$1 + 2^{x+1} = 2^{x-2}m^2 + km.$$

Por lo tanto

$$1 - km = 2^{x-2}(m^2 - 8). \tag{2}$$

Para $k = 1$ esto da $m^2 - 8 \leq 0$, de donde $m = 1$, que no satisface (2). Para $k = -1$ la ecuación (2) queda

$$1 + m = 2^{x-2}(m^2 - 8) \geq 2(m^2 - 8),$$

de donde $2m^2 - 2m - 17 \leq 0$ y entonces $m \leq 3$. Como $m = 1$ no satisface (2), queda $m = 3$, que conduce a $x = 4$. Entonces de (1) resulta $y = 23$. Como $1 + 2^4 + 2^9 = 529 = 23^2$ se tiene así la solución (4,23). Por supuesto que (4,−23) también es solución, y con (0,2) y (0,−2) son todas.

**4.11** Digamos que los lados son $z-1$, $z$ y $z+1$. Entonces el semiperímetro es $3z/2$ t el área, por la fórmula de Heron, es

$$A = \sqrt{\frac{3z}{2}\frac{z}{2}\left(\frac{z}{2} - 1\right)\left(\frac{z}{2} + 1\right)} = \frac{z}{4}\sqrt{3(z^2 - 4)}.$$

Para que este número sea entero es claro que $z$ debe ser par, digamos $z = 2x$, con lo cual queda $A = x\sqrt{3(x^2 - 1)}$, y debe ser $x^2 - 1 = 3y^2$ para $y$ entero. Aparece así la ecuación de Pell $x^2 - 3y^2 = 1$, que tiene solución fundamental $(x, y) = (2, 1)$ y solución general

$$x_n = \frac{1}{2}\left((2 + \sqrt{3})^n + (2 - \sqrt{3})^n\right), \quad y_n = \frac{1}{2\sqrt{3}}\left((2 + \sqrt{3})^n - (2 - \sqrt{3})^n\right).$$

# Capítulo 5

**5.1** Es fácil ver que cualquier residuo cuadrático módulo $p$ es congruente con uno de los siguientes:

$$1^2,\ 2^2, \ldots,\ \left(\frac{p-1}{2}\right)^2,$$

los cuales no son congruentes dos a dos.

**5.2** Si $p = 4n + 3$ entonces $(-1)^{(p-1)/2} = (-1)^{2n+1} = -1$.

**5.3** Si $p = 4n + 1$ entonces $(-1)^{(p-1)/2} = (-1)^{2n} = 1$.

**5.4** Supongamos que sólo hubiese un número finito $p_1$, $p_2$,... $p_k$ de primos de la forma $4n+1$, y sea $A = 2p_1p_2 \cdots p_k$. Como $A^2+1$ no es divisible por ningún $p_i$, sus factores primos deben ser de la forma $4n + 3$. Pero si $p$ es uno de ellos tendríamos que $A^2 \equiv -1 \pmod{p}$, absurdo por el Problema 5.1.

**5.5** Si $p \nmid a$ entonces $a$ tiene un inverso multiplicativo $c$ módulo $p$, Multiplicando $a^2 + b^2 \equiv 0 \pmod{p}$ por $c^2$ resulta $a^2c^2 + b^2c^2 \equiv 0 \pmod{p}$, es decir $1 + (bc)^2 \equiv 0 \pmod{p}$, y entonces $-1$ sería residuo cuadrático módulo $p$, contradiciendo el Problema 5.2.

**5.6**

$$2^{2n} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = (-1)^{\lfloor \frac{p+1}{4} \rfloor} = (-1)^n \pmod{p}.$$

Por otra parte

$$2^{2n}n^n = (4n)^n \equiv (-1)^n \pmod{p},$$

luego $(-1)^n n^n \equiv (-1)^n \pmod{p}$ y $n^n \equiv 1 \pmod{p}$.

## Identificación de algunas competencias matemáticas mencionadas en esta obra.

**AIME** Examen Invitacional de Matemática (USA)

**Canguro** Canguro Matemático

**IMO** Olimpiada Internacional de Matemática

**OBM** Olimpiada Brasilera de Matemática

**OIM** Olimpiada Iberoamericana de Matemática

**OJM** Olimpiada Juvenil de Matemáticas (Venezuela)

**OM** Olimpiada de Mayo

**OMA** Olimpiada Matemática Argentina

**OMCC** Olimpiada Matemática de Centroamérica y el Caribe

**ORP** Olimpíada Rioplatense

**TT** Torneo de las Ciudades

# Bibliografía


[1] Andreescu, T., Andrica, D., Feng, Z., *104 Number Theory Problems*, Birkhäuser, Boston, 2007.

[2] Andreescu, T., Andrica, D., *An Introduction to Diophantine Equations*, GIL Publishing House, Zalau, 2002.

[3] Brochero, F. E., Restrepo, J. I., *Un Recorrido por la Teoría de Números*, Univ. Antonio Nariño, Bogotá, 2006.

[4] Engel, A., *Problem-Solving Strategies*, Springer, 1998.

[5] Halmos, P. R., *The Heart of Mathematics*, American Mathematical Monthly, **87**(7), 1980, 519–524.

[6] Herstein, I. N., *Topics in algebra*, Blaisdell, Waltham, Mass., 1964. Hay traducción: *Algebra moderna*, Trillas, México, 1976.

[7] Nieto, J. H., Sánchez, R., Ordaz, E., Taylor, S., Vielma, L., *Olimpiada Juvenil de Matemática 2013*, Academia de Ciencias Físicas, Matemáticas y Naturales, Caracas, 2014. Hay versión electrónica en `http://www.acm.ciens.ucv.ve`

[8] Nieto, J. H., Sánchez, R., Vielma, L., *Olimpiada Juvenil de Matemática 2012*, Academia de Ciencias Físicas, Matemáticas y Naturales, Caracas, 2013. Hay versión electrónica en `http://www.acm.ciens.ucv.ve`

[9] Nieto, J. H., Sánchez, R., Vielma, L., *Olimpiada Juvenil de Matemática 2011*, Academia de Ciencias Físicas, Matemáticas y Naturales, Caracas, 2012. Hay versión electrónica en `http://www.acm.ciens.ucv.ve`

[10] Nieto, J. H., Sánchez, R., Vielma, L., *Olimpiada Juvenil de Matemática 2010*, Academia de Ciencias Físicas, Matemáticas y Naturales, Caracas, 2011. Hay versión electrónica en `http://www.acm.ciens.ucv.ve`

[11] Martínez, H., Nieto, J. H., Sánchez L., R., Sarabia, E., Vielma, L., *Olimpiada Juvenil de Matemática 2009*, Academia de Ciencias Físicas, Matemáticas y Naturales, Caracas, 2010.

[12] Nieto, J. H., *Resolución de Problemas Matemáticos*, AFAMac, Mayagüez, Puerto Rico, 2010. Disponible en `http://www.jhnieto.org/libros.htm`

[13] Nieto, J. H., *Resolución de Problemas Matemáticos*, XI Escuela Venezolana para la Enseñanza de la Matemática, Mérida, 2006 y 2007.

[14] Nieto, J. H., *Olimpiadas Matemáticas - El arte de resolver problemas*, Los Libros de El Nacional, Caracas, 2005.

[15] Polya, G., *How to solve it; a new aspect of mathematical method*, Princeton University Press, Princeton, 1945. Hay traducción: *Cómo plantear y resolver problemas*, Trillas, México, 1965.

[16] Shanks, D., *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 1978.

# Índice alfabético