

TEMAS DE MATEMATICAS ELEMENTALES 1

ARITMETICA

Saulo Rada Aranda

CENAMEC

**CENTRO NACIONAL PARA EL MEJORAMIENTO DE LA ENSEÑANZA DE LA CIENCIA
CARACAS/VENEZUELA
1992**

Comité Ejecutivo del CENAMEC

Dr. Enrique Planchart
Dr. Rubén Caro
Dra. Maritza Dorta
Dra. Isbelia Martín
Dra. María de Lourdes Vargas
Prof. Mercedes Urbaneja
Dr. Hugo Groening
Dr. Claudio Bifano

Personal Directivo

Director: Dr. Enrique Planchart
Subdirectora: Prof. Dalia Diez de Tancredi

Ediciones CENAMEC. 1995
ISBN: 980-218-039-4
ISNN: 0798-3247
1^a Edición a cargo de Ligia de Lima de Bianchi
Portada: Felix Nakamura

Impreso en Venezuela por: Gráficas Colson, C.A. Av. Panteón cruce con Fuerzas Armadas, San Miguel a San Narciso, Sótano Edificio Tamara, Caracas. Telf. 561-1838

CENAMEC/Sede Central: Edif. Sociedad Venezolana de Ciencias Naturales, Av. Arichuna c/Calle Cumaco, El Marqués, Caracas 1070-A Venezuela. Tlefs: 219133 - 222467 - 229511 228779 - 225246 - 227819 - Fax (02) 225077.

CONTENIDO

p.p.

INTRODUCCION	iii
SECCIONES	
1. EL PRINCIPIO DE INDUCCION MATEMATICA	1
2. EL ALGORITMO DE LA DIVISION	6
3. EL MAXIMO COMUN DIVISOR	11
4. LA ECUACION $ax + by = c$	17
5. EL MINIMO COMUN MULTIPLO	21
6. NUMEROS PRIMOS	23
7. LA FUNCION PARTE ENTERA	29
8. CONGRUENCIAS EN Z	34
9. LA ECUACION $x^2 + y^2 = z^2$	42
10. LAS CONGRUENCIAS DE EULER, FERMAT Y WILSON .	45
11. RESOLUCION DE CONGRUENCIAS	51
12. EL INDICADOR DE EULER	56
SOLUCIONES A LOS PROBLEMAS PROPUESTOS	
Sección 1	61
Sección 2	67
Sección 3	73
Sección 4	76
Sección 5	84
Sección 6	85
Sección 7	94
Sección 8	101
Sección 9	107
Sección 10	112
Sección 11	118
Sección 12	121

INTRODUCCION

Estas notas se originaron a partir del trabajo realizado durante varias sesiones sobre resolución de problemas en teoría de números, en las cuales participaron estudiantes del Ciclo Diversificado y último año de Educación Básica con un rendimiento destacado en la matemática escolar, muchos de ellos ganadores de las Olimpiadas Matemáticas Venezolanas.

Las sesiones formaron parte del programa de entrenamiento que debían cumplir dichos jóvenes antes de someterse a las pruebas de selección para conformar el equipo que representaría a Venezuela en la VI Olimpiada Iberoamericana de Matemática, la cual se realizó en Córdoba, Argentina, en el mes de septiembre de 1991.

En este tipo de competencias internacionales se plantean problemas enmarcados en un temario que, en la mayoría de los países, forman parte de la matemática preuniversitaria. Sin embargo, generalmente los problemas exigen considerable ingenio, creatividad y mucha soltura en el empleo de técnicas matemáticas básicas.

Dado que la educación matemática que reciben los jóvenes en nuestro país (y en muchos otros) en los niveles básicos está lejos de proporcionar tales habilidades, es necesario ofrecer un entrenamiento especial a los estudiantes que van a competir en estos compromisos internacionales.

El programa de entrenamiento comprende temas como funciones, desigualdades, teoría de ecuaciones, combinatoria, teoría de números y geometría. Es de hacer notar que los dos últimos señalados son casi totalmente ignorados en nuestros programas escolares pese al extraordinario valor formativo que tienen por cuanto permiten plantear problemas con muy diversos niveles de complejidad a partir de pocos conocimientos previos, se encuentran en muchas situaciones vinculadas a la vida cotidiana (tangibles y familiares) y apelan a la curiosidad natural del joven. En estos temas, el entrenamiento prácticamente comienza desde cero.

La experiencia de los profesores que han participado en las sesiones de entrenamiento en resolución de problemas con estos estudiantes ha resultado verdaderamente gratificante. Es sorprendente ver el entusiasmo con que los jóvenes ejercitan la imaginación y se dedican al trabajo creativo.

Obviamente, el CENAMEC tiene limitaciones para extender estas experiencias a nivel masivo en forma directa, por lo cual se ha propuesto publicar diversas monografías sobre temas complementarios de matemática escolar que, a la vez de proporcionar a los docentes materiales apropiados para la experimentación, sean útiles para los estudiantes atraídos por el estudio de esta ciencia.

En particular, el presente trabajo contiene los conocimientos básicos que debe poseer el estudiante que aspire a abordar los problemas que, sobre teoría de números, se pueden proponer en competencias matemáticas internacionales. Al final de las diferentes secciones se plantean conjuntos de problemas, los cuales constituyen la parte más importante del entrenamiento. Algunos son bastante sencillos, aplicaciones más o menos rutinarias de la teoría, pero la mayoría se han tomado de olimpiadas matemáticas realizadas en diversos países así como de competencias iberoamericanas e internacionales, y es posible que el

lector se desconcierte un poco cuando se enfrente por primera vez con alguno de los enunciados. Aún cuando en la segunda parte del trabajo se presentan los problemas resueltos, la recomendación es no acudir a las soluciones sino como última instancia. No se debe olvidar que cuando se intenta resolver un problema, el esfuerzo realizado deja huellas subconscientes útiles para la formación del estudiante, aún cuando no se llegue a una solución completa.

Saulo Rada Aranda

Caracas, Noviembre de 1991.

SECCION 1

EL PRINCIPIO DE INDUCCION MATEMATICA

Las reglas aritméticas de los números enteros:

$$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

(al menos de los enteros positivos, también llamados números naturales) están entre los logros más antiguos e importantes de la civilización. Hace más de 5000 años los chinos y los egipcios usaban la aritmética en su vida cotidiana; no obstante, fueron los griegos, principalmente los pitagóricos, quienes dieron inicio formal al estudio de la aritmética superior o teoría de números como la conocemos actualmente.

Algunos ejemplos de problemas planteados y resueltos por los griegos son los siguientes:

- Demostrar que $\sqrt{2}$ no es un número racional (es decir, no puede expresarse como el cociente de dos números enteros $\frac{a}{b}$).

Esto equivale a demostrar que no existen enteros a, b , donde $b \neq 0$, tales que $a^2 - 2b^2 = 0$.

- Hallar todos los triángulos rectángulos tales que las medidas de sus lados son números enteros.

Si las medidas de los catetos de un triángulo rectángulo son a, b y la medida de la hipotenusa es c , de acuerdo con el teorema de Pitágoras se tiene:

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

El problema consiste en hallar todas las ternas (a, b, c) de números enteros que satisfacen esta ecuación. Tales ternas, por ejemplo $(3, 4, 5)$, $(5, 12, 13)$, ... se denominan triples pitagóricos.

- Si a, b, c son tres enteros dados, hallar todos los enteros x, y tales que $ax + by = 0$.

Los tres problemas anteriores conducen a casos de las denominadas ecuaciones diofánticas, llamadas así en honor al matemático griego Diofanto, de Alejandría. En general, una ecuación diofántica es una ecuación con cualquier número de incógnitas en la cual se deben determinar sus soluciones enteras.

Quien se inicia en el estudio de la teoría de números debe tener presente que, para la mayoría de los problemas que se presentan, no existen métodos generales de resolución. Asimismo, debe estar consciente de la dificultad considerable de muchos de estos problemas, los cuales, a veces, tienen una apariencia bastante sencilla pero requieren una buena dosis de ingenio para abordarlos satisfactoriamente.

A continuación damos dos ejemplos de famosos problemas que, hasta ahora, no han sido resueltos:

- La conjetura de Goldbach (ruso); establece que todo número par mayor que 2 puede escribirse como la suma de dos números primos. (Un entero positivo p , mayor que 1, es primo si no tiene divisores positivos diferentes de 1 y de p).

En efecto, si consideramos los primeros números pares mayores que 2 observamos que:

$$\begin{aligned} 4 &= 2 + 2; 6 = 3 + 3; 8 = 3 + 5; 10 = 3 + 7 = 5 + 5; \\ 12 &= 5 + 7; 14 = 3 + 11 = 7 + 7; 16 = 3 + 13 = 5 + 11; \\ 18 &= 5 + 13 = 7 + 11; 20 = 3 + 17 = 7 + 13; \\ 22 &= 3 + 19 = 5 + 17 = 9 + 13 = 11 + 11; \text{ etc.} \end{aligned}$$

Así pues, parece que la conjetura fuera cierta, pero aún no se ha encontrado una demostración general, así como tampoco un caso en el cual no se cumpla.

Es preciso aclarar que si se quiere probar que una proposición es verdadera, la prueba tiene que ser general, es decir, abarcar todos los casos posibles. Ahora bien, si se quiere probar que la proposición es falsa, basta hallar un caso particular en el cual no se cumpla. Esto es lo que se llama un *contraejemplo*. Si quisiéramos demostrar que la conjetura de Goldbach es falsa deberíamos buscar un número entero par, mayor que 2, que no se pueda expresar como la suma de dos números primos.

- La ecuación pitagórica generalizada:

$$x^n + y^n = z^n,$$

donde $n \geq 3$, no tiene soluciones en enteros x, y, z (salvo el caso trivial en que alguno de estos sea igual a cero).

Este problema, planteado por Fermat (francés) hace más de 300 años se conoce como el "Último Teorema de Fermat" y ha desafiado el talento de numerosos matemáticos desde entonces; se ha podido demostrar para muchos valores particulares de n , pero no se ha encontrado una prueba general. Lo llamativo es que Fermat afirmó haber demostrado el teorema, pero nunca publicó tal demostración. Actualmente, la mayoría de los matemáticos piensa que la prueba de Fermat tenía algún error. En todo caso, el problema continúa vigente.

Al iniciar nuestro estudio de la teoría de números, convendremos en usar (salvo que se exprese lo contrario) a las letras del alfabeto latino: a, b, c, d, \dots para designar números enteros. Además, asumiremos dos principios básicos, que serán útiles para demostrar muchas propiedades. Estos son:

1.1. El Principio de Buena Ordenación. Todo subconjunto no vacío de números enteros positivos tiene un menor elemento. Es decir, si $A \subset \mathbb{Z}^+$ y $A \neq \emptyset$ entonces existe un entero $m \in A$ tal que $m \leq x$ para todo $x \in A$.

1.2. El Principio de Inducción Matemática. Supongamos que para todo número entero positivo n se da una proposición $P(n)$. Supongamos que $P(1)$ es cierta y que, siempre que $P(n)$ es cierta también lo es $P(n + 1)$. Entonces $P(n)$ es cierta para todo entero positivo n .

? Se puede demostrar un principio?

1.3. El principio de inducción puede demostrarse a partir del principio de buena ordenación.

En efecto, supongamos que A es un conjunto de enteros positivos que contiene al 1 y que, siempre que $n \in A$ entonces también $(n + 1) \in A$. Para probar que $A = \mathbb{Z}^+$ bastará demostrar que el conjunto A' , formado por todos los enteros positivos que no pertenecen a A , es vacío. Daremos una prueba indirecta (*reducción al absurdo*), que consiste en negar la tesis que se pretende demostrar y, a partir de allí, llegar a un resultado contradictorio.

Supongamos que $A' \neq \emptyset$; entonces, de acuerdo con el principio de buena ordenación, A' contendrá un menor elemento m . Como $1 \in A$, necesariamente $m > 1$ y, en consecuencia, $m - 1$ es positivo. Como además $m - 1 < m$ y m es el menor elemento de A' , se tiene que $(m - 1) \in A$. Pero entonces, por hipótesis, $(m - 1) + 1 = m \in A$. Esta contradicción proviene de haber supuesto que $A' \neq \emptyset$. Esto concluye la prueba.

Las pruebas indirectas se usarán con bastante frecuencia en la demostración de teoremas y resolución de problemas sobre divisibilidad.

A continuación daremos un par de ejemplos sobre cómo se procede para demostrar algunas propiedades usando el principio de inducción.

- Probar que para todo entero positivo n se tiene:

$$1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}. \quad (1)$$

La prueba por inducción requiere, en primer lugar, la demostración para $n = 1$. En este caso es inmediata, por cuanto:

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

En segundo lugar supongamos la igualdad (1) válida para un cierto valor de n (ésta es la llamada *hipótesis de inducción*), e intentemos demostrarla para $n + 1$.

Se tiene, por la propiedad asociativa de la adición:

$$1 + 2 + 3 + \dots + n + (n + 1) = (1 + 2 + 3 + \dots + n) + (n + 1)$$

y, de acuerdo con la hipótesis de inducción:

$$\begin{aligned} 1 + 2 + 3 + \dots + n + (n + 1) &= \frac{n(n + 1)}{2} + (n + 1) = \\ &= \frac{n(n + 1) + 2(n + 1)}{2} = \\ &= \frac{(n + 1)(n + 2)}{2}. \end{aligned}$$

Pero esta es, precisamente, la igualdad (1) para $n + 1$ sumandos, con lo cual completamos la demostración.

Nota. Usualmente, cuando se presentan expresiones como $1 + 2 + 3 + \dots + n$ resulta conveniente abreviarlas mediante el uso del símbolo de sumatoria, que se representa por la letra griega sigma mayúscula (\sum). En este ejemplo se escribe:

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

y se lee suma (o sumatoria) de i donde i va desde 1 hasta n , lo cual indica que el primer sumando se obtiene asignando a i el valor que aparece debajo de la letra \sum (en este caso 1), para los siguientes sumandos se asignan a i los valores 2, 3, 4, ... hasta llegar al valor colocado en la parte superior de la letra \sum . Otros ejemplos serían:

$$\sum_{i=1}^n i^3 = 1^3 + 2^3 + 3^3 + \dots + n^3,$$

$$\sum_{i=1}^n i(1+i) = 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1),$$

$$\sum_{i=0}^{n-1} (2i+1) = 1 + 3 + 5 + 7 + \dots + (2n-1).$$

- Probar que para todo entero positivo n se tiene:

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

Esto es, probar que:

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}. \quad (1)$$

Si $n = 1$ se obtiene inmediatamente:

$$\frac{1}{1 \cdot 3} = \frac{1}{2 \cdot 1 + 1}.$$

Supongamos la propiedad cierta para n sumandos. (1) es nuestra hipótesis de inducción. Para $n+1$ sumandos debemos llegar a la igualdad:

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} + \frac{1}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}.$$

En efecto, si sumamos $\frac{1}{(2n+1)(2n+3)}$ al primer miembro de (1), usando la hipótesis de inducción se tiene:

$$\begin{aligned} & \left(\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} \right) + \frac{1}{(2n+1)(2n+3)} = \\ & = \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} = \frac{n(2n+3)+1}{(2n+1)(2n+3)} = \\ & = \frac{2n^2+3n+1}{(2n+1)(2n+3)} = \frac{2(n+\frac{1}{2})(n+1)}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}. \end{aligned}$$

Problemas.

Demostrar, usando el método de inducción:

$$1.1. \sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$1.2. \sum_{i=1}^n i^3 = \left[\frac{n(n+1)}{2} \right]^2.$$

$$1.3. \sum_{i=1}^n (2i-1) = n^2.$$

$$1.4. \sum_{i=1}^n i(i+1) = \frac{1}{3}n(n+1)(n+2).$$

$$1.5. \sum_{i=1}^n (3i-2) = \frac{n(3n-1)}{2}.$$

$$1.6. 2n^2 > (n+1)^2 \text{ para todo entero } n \geq 3.$$

$$1.7. 2^n > n^2 \text{ para todo entero } n > 4.$$

1.8. El número de diagonales de un polígono de n lados es:

$$\frac{n(n-3)}{2}.$$

1.9. La suma de los ángulos interiores de un polígono de n lados es $(n-2)\pi$ (o bien, $(n-2) \cdot 180^\circ$ en grados sexagesimales).

1.10.

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i,$$

donde

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

Nota. Todas estas propiedades se aplican con frecuencia, por tanto, es conveniente memorizarlas.

SECCION 2

EL ALGORITMO DE LA DIVISION

Dados dos números enteros a, b , con $a \neq 0$, se dice que a divide a b si existe un entero x tal que $b = ax$.

Si a divide a b se usa la notación: $a|b$. Por ejemplo, $4 | 20, 7 | 98, 11 | 242$.

Si a no divide a b se escribe: $a \nmid b$. Por ejemplo, $4 \nmid 10, 5 \nmid 24, 12 \nmid 18$.

Si a divide a b , también se dice que a es un divisor de b , o que a es un factor de b , o que b es divisible por a , o que b es múltiplo de a .

Propiedades Básicas.

A continuación se presentan algunas propiedades básicas de la relación de divisibilidad entre dos enteros.

2.1. Si $a|b$ entonces $a|bc$ para todo entero c .

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

2.3. Si $a|b$ y $a|c$ entonces $a|(bx + cy)$ para todo par de enteros x, y .

2.4. Si $a|b$ y $b|a$ entonces $a = \pm b$.

2.5. Si $a|b, a > 0, b > 0$, entonces $a \leq b$.

Las demostraciones de estas propiedades resultan inmediatas a partir de la definición de divisibilidad. En efecto:

2.1. Si $a|b$ entonces existe un entero x tal que

$$b = ax$$

y multiplicando ambos miembros por c :

$$bc = (ax)c = a(xc),$$

de donde:

$$a|bc.$$

2.2. Si $a|b$ y $b|c$ entonces existen enteros x, y tales que:

$$b = ax, c = by,$$

de donde:

$$c = (ax)y = a(xy),$$

luego

$$a|c.$$

2.3. Si $a|b$ y $a|c$, de acuerdo con 2.1. $a|bx$ y $a|cy$, luego existen enteros m, n tales que:

$$bx = am,$$

$$cy = an.$$

Sumando miembro a miembro ambas desigualdades se tiene:

$$bx + cy = am + an,$$

$$bx + cy = a(m + n);$$

luego

$$a|(bx + cy).$$

Nota. Obsérvese que si, en particular, tomamos $x = y = 1$, se tiene:

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

Similarmente, si tomamos $x = 1, y = -1$, nos queda:

$$a|(b - c).$$

Por tanto, si un entero divide a otros dos divide también a su suma y a su diferencia.

El lector podrá generalizar este resultado por inducción para n enteros. Es decir, si $a|b_1, a|b_2, \dots, a|b_n$, entonces

$$a \left| \sum_{i=1}^n b_i x_i$$

para cualquier conjunto de n enteros x_1, x_2, \dots, x_n .

2.4. Si $a|b$ y $b|a$, entonces existen enteros x, y tales que:

$$b = ax, \quad a = by,$$

de donde:

$$b = (by)x = b(yx)$$

y por consiguiente $yx = 1$. Ahora bien, como x, y son enteros, se tiene necesariamente que $x = y = 1$ ó $x = y = -1$, de manera que $a = \pm b$.

2.5. Si $a|b$, entonces $b = ax$ para algún entero x . Como $a > 0$ y $b > 0$, x necesariamente debe ser positivo; es decir, $x \geq 1$ y, en consecuencia, $a \leq b$.

Cuando dividimos un entero entre otro, de la manera usual, se obtiene un cociente y un resto (este último a veces es nulo, cuando el primer entero es divisible por el segundo). A continuación vamos a probar que este procedimiento siempre es posible. Este resultado es conocido como el

2.6. Algoritmo de la División. Dados dos enteros a y b , con $a > 0$, existen enteros q, r tales que $b = qa + r$, donde $0 \leq r < a$.

Para demostrar la proposición, observemos la progresión aritmética

$$\{\dots, b - 2a, b - a, b, b + a, b + 2a, \dots\}.$$

En esta progresión hay números positivos y negativos y, eventualmente, está el cero en caso de que b sea divisible por a . De acuerdo con el principio de buena ordenación, existe un menor entero no negativo en la progresión. Si llamamos r a este entero, r tiene la forma:

$$r = b - qa,$$

de donde:

$$b = qa + r. \quad (1)$$

Obsérvese que q toma alguno de los valores del conjunto $\{\dots, -2, -1, 0, 1, 2, \dots\}$.

Falta comprobar que $r < a$. Supongamos lo contrario (reducción del absurdo). Entonces tendríamos $r \geq a$ y

$$r = a + r_1, \text{ donde } r_1 \geq 0.$$

Reemplazando en (1) se tiene:

$$\begin{aligned} b &= qa + (a + r_1), \\ b &= (q + 1)a + r_1. \end{aligned}$$

Pero esto indica que r_1 es un elemento de la progresión aritmética considerada, no negativo y menor que r , lo que contradice la definición de r . Esto completa la demostración. q se denomina cociente y r resto de la división.

De acuerdo con este resultado, al dividir cualquier entero por 2, los restos posibles son 0 y 1; al dividirlo por 3, los restos posibles son 0, 1 y 2; al dividirlo por 4, los restos posibles son 0, 1, 2 y 3, y así sucesivamente.

Se dice que un entero n es de la forma $ak + b$ si existe un entero k tal que $n = ak + b$. En virtud de lo expuesto anteriormente, todo entero es de la forma $2k$ ó $2k + 1$ (par o impar); de la forma $3k$, $3k + 1$ ó $3k + 2$; de la forma $4k$, $4k + 1$, $4k + 2$ ó $4k + 3$, etc. En cada caso, k es el cociente que resulta al dividir el entero entre 2, 3 ó 4 respectivamente. Esta consideración resulta útil para resolver diversos problemas de divisibilidad. Veamos dos ejemplos.

- Probar que $n^2 - n$ es divisible por 2 para todo entero n . Probar además que $n^3 - n$ es divisible por 3.

En primer término, tenemos que probar que $n^2 - n$ es de la forma $2k$ para todo entero n . Ahora bien, se tiene que $n^2 - n = n(n-1)$. Si $n = 2k$, entonces $n^2 - n = 2k(2k-1) = 2k_1$, donde $k_1 = k(2k-1)$. Si $n = 2k+1$, entonces $n^2 - n = (2k+1)2k = 2k_2$, donde $k_2 = k(2k+1)$. Luego, en cualquier caso $n^2 - n$ es divisible por 2. Obsérvese que esto nos dice que el producto de dos enteros consecutivos siempre es un número par.

Consideremos ahora el entero $n^3 - n$. Debemos probar que es de la forma $3k$. Ahora bien

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

Veamos los casos posibles. Si $n = 3k$, entonces $n^3 - n = (3k-1)3k(3k+1) = 3k_1$, donde $k_1 = (3k-1)k(3k+1)$. Si $n = 3k+1$, entonces $n^3 - n = 3k(3k+1)(3k+2) = 3k_2$, donde $k_2 = k(3k+1)(3k+2)$. Si $n = 3k+2$, entonces $n^3 - n = (3k+1)(3k+2)(3k+3) = 3k_3$, donde $k_3 = (3k+1)(3k+2)(k+1)$. Por consiguiente, en cualquier caso $n^3 - n$ es divisible por 3. Esto nos dice que el producto de tres enteros consecutivos siempre es múltiplo de 3.

- Si n es impar, entonces $n^2 - 1$ es divisible por 8. Debemos probar que $n^2 - 1$ es de la forma $8k$. Ahora bien,

$$n^2 - 1 = (n+1)(n-1).$$

Si n es impar, entonces n es de la forma $4k+1$ ó $4k+3$. Consideremos ambos casos. Si $n = 4k+1$, entonces $n^2 - 1 = (4k+2)4k = 8k_1$, donde $k_1 = k(2k+1)$. Si $n = 4k+3$, entonces $n^2 - 1 = (4k+4)(4k+2) = 8k_2$, donde $k_2 = (k+1)(2k+1)$. Luego, en ambos casos $n^2 - 1$ es divisible por 8.

Problemas.

2.1. Dos enteros son de la misma paridad si son ambos pares o ambos impares. Dados dos enteros cualesquiera, su suma y su diferencia tienen la misma paridad.

2.2. Si $ac|bc$, entonces $a|b$.

2.3. Si $a|b$ y $c|d$, entonces $ac|bd$.

2.4. $4 \nmid n^2 + 2$ para ningún entero n .

2.5. Si $n \geq 2$ y k es positivo, entonces $(n-1)|(n^k - 1)$.

2.6. Si $n \geq 2$ y k es positivo, entonces

$$(n-1)^2|(n^k - 1) \text{ si y sólo si } (n-1)|k.$$

2.7. Un cuadrado perfecto (es decir, un número entero elevado al cuadrado), no es de la forma $3k+2$.

Además, por la propiedad 2.3., cualquier divisor común de a y b divide también a $d = ax_0 + by_0$, y por la propiedad 2.5., cualquier divisor común será menor o igual que d , luego $d = (a, b)$.

De acuerdo con esto último se observa que el máximo común divisor de a y b puede caracterizarse como el divisor común positivo de a y b que es múltiplo de cualquier divisor común de a y b .

Si $(a, b) = 1$, el teorema demostrado nos garantiza que existen enteros x, y tales que $ax + by = 1$. Este resultado se conoce como *Relación de Bezout*.

Nota. Si $(a, b) = 1$ se dice que a y b son *primos entre sí* (o *coprimos*). En general, si $(a_1, a_2, \dots, a_n) = 1$ se dice que los n enteros a_1, a_2, \dots, a_n son primos entre sí.

Ahora bien, si en un conjunto de n enteros, cada par de ellos son primos entre sí, se dice que los números son *primos dos a dos*. Por ejemplo, los números 4, 11, 35, 39 son primos dos a dos. Lógicamente, si varios números son primos dos a dos entonces serán primos entre sí, pero no necesariamente a la inversa; por ejemplo, $(3, 7, 14) = 1$, pero 3, 7 y 14 no son primos dos a dos ya que $(7, 14) = 7$.

El razonamiento empleado en la demostración del teorema anterior es generalizable para cualquier número n de enteros por inducción (el lector puede hacerlo como ejercicio). Es decir, si $d = (a_1, a_2, \dots, a_n)$ entonces existen enteros x_1, x_2, \dots, x_n tales que:

$$d = a_1x_1 + a_2x_2 + \dots + a_nx_n.$$

Esto pone de manifiesto que el máximo común divisor de varios números enteros puede expresarse como *combinación lineal entera* de dichos números. En particular, es fácil ver que a_1, a_2, \dots, a_n son primos entre sí, si y sólo si 1 es combinación lineal entera de a_1, a_2, \dots, a_n .

A continuación vamos a explicar un procedimiento que permite calcular el máximo común divisor de dos números enteros. Este es conocido como el:

3.2. Algoritmo de Euclides. Dados dos enteros, a y b , siendo $a > 0$, si aplicamos reiteradamente el algoritmo de la división obtenemos una secuencia de ecuaciones:

$$\begin{aligned} b &= q_1a + r_1, \quad 0 < r_1 < a, \\ a &= q_2r_1 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= q_3r_2 + r_3, \quad 0 < r_3 < r_2, \end{aligned}$$

⋮

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1},$$

y como la sucesión de los restos es estrictamente decreciente y todos ellos son no negativos, alguno de ellos, digamos r_n , será el último resto no nulo en la cadena de igualdades. Entonces,

$$r_{n-1} = q_{n+1}r_n.$$

Ahora bien, probaremos que $r_n = (a, b)$.

Para demostrar esto, basta recorrer la secuencia de ecuaciones de abajo hacia arriba e inversamente, de arriba hacia abajo.

En efecto, de la última ecuación se desprende que $r_n|r_{n+1}$, pero subiendo a la precedente se observa que, como $r_n|r_n$ y $r_n|r_{n+1}$, entonces necesariamente $r_n|r_{n+2}$. Continuando el proceso (esto se puede formalizar fácilmente por inducción), llegamos a que $r_n|r_3$ y $r_n|r_2$, luego $r_n|r_1$; de allí concluimos que, como $r_n|r_2$ y $r_n|r_1$, entonces $r_n|a$, y finalmente si $r_n|r_1$ y $r_n|a$ entonces $r_n|b$. Por tanto, r_n es un divisor común de a y de b .

Por otra parte, partiendo de la primera ecuación se ve que todo divisor común de a y b lo es también de r_1 ; todo divisor común de a y r_1 lo es también de r_2 ; todo divisor común de r_1 y r_2 lo es también de r_3 ; y así sucesivamente todo divisor común de r_{n-2} y r_{n-1} lo es también de r_n . Por consiguiente, r_n es justamente el máximo común divisor de a y b .

El siguiente ejemplo ilustra la utilización del algoritmo en un cálculo numérico.

- Calcular (440,252).

Al efectuar las divisiones en la forma usual, se obtienen las siguientes igualdades:

$$440 = 1.252 + 188,$$

$$252 = 1.188 + 64,$$

$$188 = 2.64 + 60,$$

$$64 = 1.60 + 4,$$

$$60 = 15.4.$$

El último resto no nulo en la secuencia es 4, luego $(440,252) = 4$. Ahora, si queremos expresar 4 como combinación lineal entera de 440 y 252, podemos eliminar los restos 60, 64 y 188 de la manera siguiente:

$$\begin{aligned} 4 &= 64 - 60 = \\ &= 64 - (188 - 2.64) = \\ &= -188 + 3.64 = \\ &= -188 + 3.(252 - 188) = \\ &= 3.252 - 4.188 = \\ &= 3.252 - 4.(440 - 252) = \\ &= (-4).440 + 7.252. \end{aligned}$$

El método puede ser útil también en la resolución de algunos problemas. Por ejemplo:

- Demostrar que la fracción $\frac{21n+4}{14n+3}$ es irreducible para todo entero n .

Se quiere probar que, para todo n , $(21n+4)$ y $(14n+3)$ son primos entre sí. Al dividir sucesivamente se tiene:

$$21n+4 = 1.(14n+3) + (7n+1),$$

$$14n+3 = 2.(7n+1) + 1.$$

Luego,

$$(21n + 4, 14n + 3) = 1.$$

Concluimos esta sección demostrando algunas propiedades importantes del máximo común divisor.

Propiedades.

Sea $d = (a, b)$. Se tiene:

3.3. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

3.4. Si $a|bc$ y $d = 1$ entonces $a|c$.

3.5. Si $a|bc$ entonces $\frac{a}{d}|c$.

3.6. Si $m > 0$ entonces $(ma, mb) = m(a, b)$.

En efecto:

3.3. Si $(a, b) = d$, entonces existen enteros x, y tales que

$$ax + by = d,$$

luego,

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

y, en consecuencia

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

3.4. Si $d = 1$, entonces existen enteros x, y tales que:

$$ax + by = 1.$$

Multiplicando ambos miembros por c se tiene:

$$axc + byc = c.$$

Como $a|a$ y $a|bc$ se concluye que $a|c$.

3.5. Si $a|bc$ entonces es inmediato que $\frac{a}{d} \mid \frac{b}{d}c$. De acuerdo con 3.3., $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, luego, por 3.4., $\frac{a}{d} \mid c$.

- 3.6. Es inmediato que md es un divisor común de ma y de mb . Supongamos que d' es otro divisor común. Debemos probar que $d'|md$. En efecto, sabemos que existen enteros x, y tales que

$$ax + by = d.$$

Multiplicando ambos miembros por m se tiene:

$$max + mby = md,$$

luego, si $d'|ma$ y $d'|mb$ entonces $d'|md$; por tanto

$$(ma, mb) = md = m(a, b).$$

Problemas.

3.1. Probar que si $(a, b) = 1, a|c$ y $b|c$ entonces $ab|c$.

3.2. $n^5 - n$ es divisible por 30.

3.3. El producto de cuatro enteros consecutivos es divisible por 24.

3.4. Probar que $((a, b), c) = (a, (b, c))$.

3.5. No existen enteros x, y tales que

$$x + y = 100; \quad (x, y) = 3.$$

3.6. Existen infinitos pares de enteros x, y tales que

$$x + y = 100; \quad (x, y) = 5.$$

3.7. Si $(a, 4) = 2$ y $(b, 4) = 2$ entonces $(a + b, 4) = 4$.

3.8. Dados dos enteros impares, a y b , $a^3 - b^3$ es divisible por 2^n si y sólo si $a - b$ es divisible por 2^n .

3.9. Se define la sucesión de Fibonacci de la siguiente manera:

$$a_0 = a_1 = 1,$$

$$a_2 = a_0 + a_1 = 1 + 1 = 2,$$

$$a_3 = a_1 + a_2 = 1 + 2 = 3,$$

$$a_4 = a_2 + a_3 = 2 + 3 = 5,$$

⋮

$$a_{n+2} = a_n + a_{n+1}.$$

- * a) Probar que dos términos consecutivos cualesquiera de la sucesión de Fibonacci son primos entre sí.
 b) Probar que, si $n \geq 1$, entonces

$$a_{n-1} = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \dots$$

- * 3.10. Sean $d = (a, b)$, $d' = (a', b')$. Probar que

$$dd' = (aa', ab', ba', bb').$$

- 3.11. Sean los enteros a, b, c, d primos con m , donde:

$$m = ad - bc.$$

Probar que las expresiones $ax + by$ y $cx + dy$ son múltiplos de m para el mismo conjunto de números enteros x, y .

- * 3.12. Sean a y b dos enteros positivos tales que $(a, b) = d$. Probar que exactamente d de los números:

$$a, 2a, 3a, \dots, (b-1)a, ba$$

son divisibles por b .

SECCION 4

LA ECUACION $ax+by=c$

Con las propiedades básicas que hemos estudiado hasta ahora sobre divisibilidad, es posible resolver algunas ecuaciones diofánticas, es decir, ecuaciones en las cuales se procura hallar soluciones en números enteros.

Los tipos de ecuaciones diofánticas que se pueden presentar son prácticamente ilimitados, y no existen, usualmente, métodos generales de solución. En la presente sección vamos a resolver el caso más sencillo: la ecuación lineal en dos variables. Al final de la sección se presentan diversos problemas diofánticos, en los cuales se requiere plantear o resolver ecuaciones de otros tipos.

Toda ecuación lineal en dos variables con coeficientes enteros, puede escribirse en la forma:

$$ax + by = c. \quad (1)$$

Si $a = 0$ ó $b = 0$, el problema es inmediato pues se reduce a ver si la solución de una ecuación de primer grado con una incógnita es un número entero. Supongamos entonces que $a \neq 0$ y $b \neq 0$. Sea $d = (a, b)$. Probaremos el siguiente resultado.

4.1. La ecuación $ax + by = c$ tiene solución en enteros si y sólo si $d|c$. Además, si (x_0, y_0) es una solución particular, la solución general tiene la forma:

$$x = x_0 + \frac{b}{d}k, \quad y = y_0 - \frac{a}{d}k \quad \text{donde } k \in \mathbb{Z}.$$

En efecto, si $(a, b) = d$ entonces $d|(ax + by)$ para todo par de enteros x, y ; luego, si $d \nmid c$ entonces la ecuación $ax + by = c$ no tiene solución en enteros.

Supongamos que $d|c$. Sabemos que existen enteros x', y' tales que

$$ax' + by' = d \quad (2)$$

(recordemos que estos valores x', y' pueden obtenerse aplicando apropiadamente el algoritmo de Euclides).

Multiplicando ambos miembros de (2) por $\frac{c}{d}$ se tiene:

$$a\left(x' \frac{c}{d}\right) + b\left(y' \frac{c}{d}\right) = c,$$

por consiguiente: $x_0 = x' \frac{c}{d}$, $y_0 = y' \frac{c}{d}$ es una solución particular de la ecuación (1).

A fin de encontrar todas las soluciones, supongamos que (x, y) es una solución arbitraria de (1). Entonces se tiene:

$$\begin{aligned} ax + by &= ax_0 + by_0, \\ a(x - x_0) &= b(y_0 - y), \end{aligned}$$

de donde,

$$b \mid a(x - x_0)$$

y en consecuencia,

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0)$$

y, como $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, se concluye:

$$\frac{b}{d} \mid (x - x_0).$$

Es decir, $x - x_0 = \frac{b}{d}k$ para algún entero k , luego

$$x = x_0 + \frac{b}{d}k.$$

Sustituyendo este valor de x en (1) y despejando y se obtiene:

$$a(x_0 + \frac{b}{d}k) + by = c,$$

luego

$$\begin{aligned} by &= c - ax_0 - a\frac{b}{d}k = \\ &= by_0 - b\frac{a}{d}k \end{aligned}$$

y entonces

$$y = y_0 - \frac{a}{d}k.$$

Por tanto, toda solución entera de la ecuación (1) puede escribirse en la forma

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

Además, si reemplazamos estas expresiones en (1), se ve inmediatamente que se verifica la igualdad, luego efectivamente hemos hallado la solución general.

Veamos a continuación un par de ejemplos.

- Resolver en enteros $32x + 60y = 30$.

Observemos que $(32, 60) = 4$ y $4 \nmid 30$, por consiguiente la ecuación $32x + 60y = 30$ no tiene soluciones en enteros.

- Resolver en enteros $440x - 252y = 12$.

Aplicando el algoritmo de Euclides, en la sección 3 determinamos que $(440, 252) = 4$. Como $4|12$, la ecuación tiene soluciones enteras. Más aún, determinamos que 4 puede escribirse como combinación lineal entera de 440 y 252 de la siguiente manera:

$$(-4) \cdot 440 + 7 \cdot 252 = 4,$$

luego

$$(-4) \cdot 440 - (-7) \cdot 252 = 4$$

y de acuerdo con la notación que hemos usado se tiene

$$x' = -4, \quad y' = -7,$$

$$x_0 = (-4) \cdot \frac{12}{4} = -12, \quad y_0 = (-7) \cdot \frac{12}{4} = -21,$$

de donde $x_0 = -12, y_0 = -21$ es una solución particular.

La solución general viene dada por:

$$x = -12 - \frac{252}{4}k, \quad y = -21 - \frac{440}{4}k,$$

$$x = -12 - 63k, \quad y = -21 - 110k, \text{ donde } k \in \mathbb{Z}.$$

Problemas.

- 4.1. Si $ax + by = c$ tiene dos soluciones (x_0, y_0) y (x_1, y_1) tales que $x_1 = 1 + x_0$ y $(a, b) = 1$, entonces $b = \pm 1$.
- 4.2. Hallar una condición necesaria y suficiente para que el sistema de ecuaciones diofánticas

$$ax + b_1y + c_1z = d_1,$$

$$ax + b_2y + c_2z = d_2,$$

donde $b_1 \neq b_2$, tenga al menos una solución.

- 4.3. Probar que el sistema de ecuaciones diofánticas

$$3x + 6y + z = 2,$$

$$4x + 10y + 2z = 3,$$

no tiene soluciones.

- 4.4. Resolver el sistema de ecuaciones diofánticas

$$x + 2y + 3z = 4,$$

$$2x - z = -1.$$

+ 4.5. Resolver en enteros el sistema

$$\begin{aligned}x + y - z &= -1, \\x^2 - y^2 + z^2 &= 1, \\-x^3 + y^3 + z^3 &= -1.\end{aligned}$$

4.6. La ecuación $x^3 + 5x + 9 = 0$ no tiene soluciones enteras.

4.7. El producto de dos números que son sumas de dos cuadrados puede también expresarse como la suma de dos cuadrados.

4.8. Dados tres enteros consecutivos, el cubo del mayor no puede ser igual a la suma de los cubos de los otros dos.

4.9. El producto de cuatro enteros positivos consecutivos no puede ser un cuadrado perfecto.

4.10. Si la suma de los cuadrados de tres números enteros se multiplica por tres, el resultado puede expresarse como la suma de cuatro cuadrados perfectos.

4.11. Si $2n$ se puede expresar como la suma de cuatro cuadrados perfectos, entonces n también puede expresarse como la suma de cuatro cuadrados perfectos.

4.12. No existen números enteros x, y que satisfagan la ecuación

$$15x^2 - 7y^2 = 9.$$

4.13. Dado un entero n , existen enteros x, y tales que $x^2 - y^2 = n$ si y sólo si n es el producto de dos enteros de la misma paridad.

4.14. Si p, q son enteros positivos tales que $2^p + 1 = q^2$, entonces $p = q = 3$.

4.15. Dados los enteros a, b, c, d , demostrar que

$$x^2 + ax + b = y^2 + cy + d$$

tiene infinitas soluciones enteras (x, y) si y sólo si

$$a^2 - 4b = c^2 - 4d.$$

4.16. Hallar las soluciones enteras de la ecuación

$$x^2 + 15^a = 2^b.$$

4.17. Dados los enteros positivos n, p , hallar condiciones necesarias y suficientes para que el sistema de ecuaciones

$$\begin{aligned}x + py &= n, \\x + y &= p^z,\end{aligned}$$

tenga solución (x, y, z) de enteros positivos. Demostrar además, que a lo sumo hay una tal solución.

SECCION 5

EL MINIMO COMUN MULTIPLO

Si a, b son dos enteros no nulos, se dice que c es un múltiplo común de a y de b si $a|c$ y $b|c$. Por ejemplo, 24 es un múltiplo común de 4 y de 6 ya que $4|24$ y $6|24$.

Es evidente que todo par de enteros no nulos, a y b , tienen múltiplos comunes; por ejemplo, ab es un múltiplo común de a y de b , así como todos los múltiplos de ab . El principio de buena ordenación garantiza que existe un menor múltiplo común positivo de a y b . A éste se le llama *mínimo común múltiplo* de a y b y se le denota por $[a, b]$.

En general, dados n enteros no nulos, a_1, a_2, \dots, a_n , su mínimo común múltiplo se denota por $[a_1, a_2, \dots, a_n]$.

Propiedades.

5.1. Si c es un múltiplo común de a y b , entonces $[a, b]|c$.

En general, si c es un múltiplo común de a_1, a_2, \dots, a_n , entonces $[a_1, a_2, \dots, a_n]|c$. Luego, el mínimo común múltiplo de varios enteros puede caracterizarse como el múltiplo común positivo que es divisor de cualquier múltiplo común.

5.2. Si $m > 0$ entonces $[ma, mb] = m[a, b]$.

5.3. Si $a > 0$ y $b > 0$ entonces $a, b = ab$. En general, $a, b = |ab|$.

En efecto:

5.1. Sea $m = [a, b]$. De acuerdo con el algoritmo de la división, existen enteros q y r tales que

$$c = qm + r \quad y \quad 0 \leq r < m.$$

Debemos probar que $r = 0$. Ahora bien, si fuese $r > 0$, como $a|c, a|m, b|c, b|m$, tendríamos que a y b serían divisiones de $c - qm = r$, esto es, r sería un múltiplo común de a y b , contradiciendo la definición de mínimo común múltiplo por cuanto $r < m$. La contradicción proviene de haber supuesto que $m \nmid c$; por tanto, queda demostrada la propiedad.

Obsérvese que el mismo razonamiento se puede generalizar, inmediatamente, para el caso de n enteros a_1, a_2, \dots, a_n .

5.2. Como $ma|[ma, mb]$ se tiene que $m|[ma, mb]$, luego $[ma, mb] = mx_1$ para algún entero positivo x_1 .

Sea $[a, b] = x_2$. Entonces $a|x_2$ y $b|x_2$, luego

$$ma|mx_2 \quad y \quad mb|mx_2,$$

es decir, mx_2 es un múltiplo común de ma y mb , y por tanto

$$[ma, mb]|mx_2,$$

luego,

$$\begin{aligned} & mx_1 | mx_2, \\ & x_1 | x_2, \\ & x_1 \leq x_2. \end{aligned} \tag{1}$$

Por otra parte, se tiene que

$$ma | mx_1 \quad \text{y} \quad mb | mx_1,$$

luego,

$$\begin{aligned} & a | x_1 \quad \text{y} \quad b | x_1, \\ & x_2 | x_1, \\ & x_2 \leq x_1. \end{aligned} \tag{2}$$

De (1) y (2) se concluye que $x_1 = x_2$; luego, $[ma, mb] = m[a, b]$.

5.3. Supongamos primero que $(a, b) = 1$. $[a, b]$ es múltiplo de a , luego $[a, b] = ax$ para algún entero positivo x . Pero además $b | ax$, y como $(a, b) = 1$ entonces necesariamente $b | x$, luego $b \leq x$ y $ab \leq ax$. Ahora bien, como ab es un múltiplo común positivo de a y de b , no puede ser menor que su mínimo común múltiplo, por lo cual concluimos que $[a, b] = ab$.

Consideremos ahora el caso general en el cual $(a, b) = d > 1$. Entonces $\frac{a}{d}$ y $\frac{b}{d}$ son

enteros tales que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, luego podemos escribir:

$$\left[\frac{a}{d}, \frac{b}{d}\right] \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{ab}{d^2}.$$

Multiplicando ambos miembros por d^2 y tomando en cuenta las propiedades 5.2.

3.6. nos queda:

$$a, b = ab.$$

Obsérvese que $[a, b] = [a, -b]$ y $(a, b) = (a, -b)$, luego en general, si a o b son negativos, se cumple:

$$a, b = |ab|.$$

Problemas.

- 5.1. Si n es un entero positivo, evaluar $(n, n+1)$ y $[n, n+1]$.

- 5.2. Si a y b son enteros positivos tales que $a | b$, hallar los valores de (a, b) y $[a, b]$.

- 5.3. Hallar todos los enteros positivos a y b tales que

$$(a, b) = 10 \quad \text{y} \quad [a, b] = 100.$$

5.4. Dados los enteros positivos d y m , probar que existen enteros x, y tales que $(x, y) = d$, $[x, y] = m$ si y sólo si $d | m$.

SECCION 6

NUMEROS PRIMOS

En el conjunto de los números enteros positivos, se observa que el número 1 tiene un único divisor: el propio 1.

En este sentido, el 1 constituye un caso particular. Cualquier entero positivo $n > 1$ admite, por lo menos, dos divisores: 1 y n .

Se dice que un entero positivo $p > 1$ es un *número primo* si únicamente admite dos divisores positivos: 1 y p . Por ejemplo, 2, 3, 5, 7, 11, 13, ... son números primos. Si un entero positivo tiene más de dos divisores positivos diferentes, es un *número compuesto*. El número 1 no es ni primo ni compuesto.

El resultado fundamental de esta sección establece que todo entero positivo, mayor que 1, puede ser expresado en forma única como un producto de factores primos (si el entero es un número primo, puede considerarse como producto de un solo factor). Para demostrar esto, necesitamos usar dos propiedades previas. Una propiedad que se prueba para usarla en la demostración de otra, más importante o general, recibe el nombre de *lema*.

6.1. Lema. Si n es un entero mayor que 1, entonces n es un producto de números primos.

Para demostrarlo procederemos por vía indirecta; es decir, supondremos que existen enteros positivos mayores que 1 que no son productos de factores primos. De acuerdo con el principio de buena ordenación, existe un menor entero positivo que satisface tal condición. Llámemos m a este número.

m no es un número primo (de lo contrario sería el producto de un factor primo). Por consiguiente, existe un entero positivo a , diferente de 1 y de m , tal que $a|m$. Luego, $m = ax$ para algún entero positivo x .

Ahora bien, de acuerdo con la propiedad 2.5., se tiene que $a < m$ y $x < m$, por tanto a y x pueden expresarse como productos de números primos. Sean

$$a = p_1 p_2 \dots p_i,$$
$$x = q_1 q_2 \dots q_j,$$

donde $p_1, \dots, p_i, q_1, \dots, q_j$ denotan números primos. Entonces

$$m = p_1 \dots p_i q_1 \dots q_j$$

es también un producto de factores primos, lo cual contradice la forma como hemos definido m . Por consiguiente, concluimos que todo entero mayor que 1 es un producto de factores primos.

6.2. Lema. Si p es un número primo y $p|ab$, entonces $p|a$ ó $p|b$.

Este hecho es una consecuencia directa de la propiedad 3.4. En efecto, si $p \nmid a$, como p es primo se tiene necesariamente que $(a, p) = 1$, luego $p|b$.

Nota Es fácil generalizar, por inducción, este resultado para un producto de n factores. Es decir, si $p|a_1a_2\dots a_n$, entonces $p|a_i$ para algún $i = 1, 2, \dots, n$. Ahora estamos en condiciones de probar el:

6.3. Teorema fundamental de la Aritmética. Todo entero positivo $n > 1$ puede expresarse como un producto de factores primos en forma única (salvo el orden en que aparezcan los factores).

De nuevo, procederemos por reducción al absurdo. El lema 6.1. nos dice que todo entero mayor que 1 puede expresarse como producto de números primos. Admitamos que hay enteros que tienen más de una descomposición en factores primos y supongamos (de acuerdo con el principio de buena ordenación) que m es el menor entero positivo que satisface tal condición. Entonces

$$m = p_1p_2\dots p_i = q_1q_2\dots q_j \quad (1)$$

donde $p_1, \dots, p_i, q_1, \dots, q_j$ son primos (evidentemente, diferentes de m). Entonces $p_1|q_1q_2\dots q_j$ y, de acuerdo con el lema 6.2., p_1 divide a alguno de los factores del producto $q_1q_2\dots q_j$. Podemos suponer (reordenando los factores si es necesario) que $p_1|q_1$. Como p_1 y q_1 son primos, se tiene que necesariamente $p_1 = q_1$ y entonces, simplificando por $p_1 = q_1$ en la expresión (1) se tiene

$$\frac{m}{p_1} = p_2\dots p_i = q_2\dots q_j \quad (2)$$

Como $p_1|m$, $\frac{m}{p_1}$ es un entero m_1 y, de acuerdo con la propiedad 2.5., $m_1 < m$. Pero entonces, la expresión (2) muestra que m_1 es un entero menor que m que tiene más de una descomposición en factores primos. Esta contradicción demuestra el teorema.

Usualmente, cuando se aplica el teorema fundamental de la aritmética, un entero $n > 1$ se escribe en la forma:

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k},$$

donde p_1, p_2, \dots, p_k son primos diferentes y $\alpha_1, \alpha_2, \dots, \alpha_k$ son enteros positivos. Esta es la llamada *forma canónica* del entero n . Por ejemplo,

$$1960 = 2^3 \cdot 5 \cdot 7^2; \quad 1188 = 2^2 \cdot 3^3 \cdot 11.$$

A veces es útil usar una modalidad ligeramente diferente de la forma canónica, cuando se permite que algunos de los exponentes sean nulos. Por ejemplo, si queremos expresar el máximo común divisor y el mínimo común múltiplo de dos enteros a y b , en términos de sus factores primos, podemos escribir

$$a = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k},$$

$$b = p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k},$$

donde los exponentes $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k$ son enteros no negativos. De las definiciones de máximo común divisor y mínimo común múltiplo se deduce inmediatamente que

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \dots p_k^{\min\{\alpha_k, \beta_k\}},$$

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \dots p_k^{\max\{\alpha_k, \beta_k\}},$$

donde $\min\{\alpha_i, \beta_i\}$ denota al menor entre los enteros α_i y β_i , y $\max\{\alpha_i, \beta_i\}$ al mayor entre α_i y β_i . Por ejemplo, si queremos calcular $(1960, 1188)$ y $[1960, 1188]$ se tiene:

$$1960 = 2^3 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 11^0,$$

$$1188 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^0 \cdot 11^1,$$

$$(1960, 1188) = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 4,$$

$$[1960, 1188] = 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^2 \cdot 11^1 = 582120.$$

A continuación, comprobaremos algunos hechos básicos sobre los números primos.

6.4. (Euclides). Existen infinitos números primos.

Se procede por vía indirecta. Supongamos que la sucesión de números primos p_1, p_2, \dots, p_k es finita y consideremos el número $n = p_1 p_2 \dots p_k + 1$. Si n es primo, es diferente de cada uno de los p_1, p_2, \dots, p_k . Si n es compuesto, n admite un divisor primo p . Ahora bien, necesariamente p es distinto de cada uno de los p_1, p_2, \dots, p_k ya que de lo contrario tendríamos que $p | p_1 p_2 \dots p_k$ y, como $p | n$, entonces también $p | 1$. En ambos casos se llega a una contradicción, la cual proviene de haber supuesto que la sucesión de números primos es finita.

Nota. Usando argumentos similares se puede demostrar que existen infinitos primos de las formas $3k + 1, 3k + 2, 4k + 1, 4k + 3, 5k + 1, 5k + 2, 5k + 3, 5k + 4$, etc. Estos son casos particulares del siguiente teorema, debido a Dirichlet, que enunciamos aún cuando no lo demostraremos.

6.5. Toda progresión aritmética de la forma $a, a + b, a + 2b, a + 3b, \dots$ donde $(a, b) = 1$ contiene infinitos números primos.

6.6. Para todo número entero positivo k , existen k números compuestos consecutivos.

En efecto, consideremos los números

$$(k+1)! + 2, (k+1)! + 3, (k+1)! + 4, \dots, (k+1)! + (k+1).$$

En general, si $2 \leq n \leq k+1$, entonces $(k+1)! + n$ es divisible por n y es diferente de n ; por tanto, es un número compuesto.

Esto nos dice que en el conjunto de los números enteros positivos es posible hallar "lagunas", tan grandes como se quiera, en las cuales no aparezca ningún número primo.

Es conveniente tener en cuenta que no existe ningún patrón o ley de formación de los números primos.

6.7. Si n es un número compuesto entonces existe un primo p tal que $p|n$ y $p \leq \sqrt{n}$.
En efecto, si n es un número compuesto entonces existen enteros positivos x, y tales que

$$n = xy, \text{ con } 2 \leq x \leq y < n.$$

Si $x \leq y$ entonces $x^2 \leq xy = n$, de donde $x \leq \sqrt{n}$. Si p es un primo tal que $p|x$ entonces $p \leq x$ y se concluye que $p \leq \sqrt{n}$.

De acuerdo con este resultado se tiene que para verificar si un número dado $n > 1$ es primo o no, es suficiente ver si es divisible o no por alguno de los primos $p \leq \sqrt{n}$. Si no lo es, entonces n es primo.

Por ejemplo, si queremos ver si el número 191 es primo o no, calculamos $\sqrt{191}$ y observamos que

$$13 < \sqrt{191} < 14,$$

luego basta dividir 191 entre todos los primos menores o iguales que 13 (esto es, entre 2, 3, 5, 7 y 13). Al hacer esto, se ve que 191 es primo.

Esta idea sugiere un método sencillo para formar la tabla de los números primos que no excedan a un cierto entero positivo n . Tal método se conoce como criba de Eratóstenes y consta de los siguientes pasos:

- Se escriben los números $1, 2, 3, 4, \dots, n$.
- El 2 es el primer número primo. Se tachan de la lista el 1 y todos los múltiplos de 2 (excepto el mismo 2).
- El 3 es el siguiente número primo (no está tachado porque no es múltiplo de 2). Se tachan todos los múltiplos de 3, excepto el mismo 3, que no hayan sido tachados anteriormente por ser también múltiplos de 2.
- El siguiente número no tachado es el 5. Se tachan los múltiplos de 5, con excepción de él mismo. Obsérvese que el primero en ser tachado será $25 = 5^2$ ya que los múltiplos menores de 5 ya han sido tachados por serlo también de 2 ó de 3.
- Se continúa con el mismo procedimiento, observando que al tachar los múltiplos de un primo p se comienza siempre por p^2 .
- El método termina cuando se han tachado los números compuestos que son múltiplos de los números primos menores o iguales que \sqrt{n} .

Problemas.

- *6.1. Sean $a \geq 2, n' \geq 2$. Si $a^n - 1$ es primo, entonces $a = 2$ y n es primo.

- 6.2. Si $2^n - 1$ es primo y $n > 2$, entonces $2^n + 1$ es compuesto.
- 6.3. Para ningún entero positivo n , $2^n + 1$ es un cubo.
- 6.4. La suma de cuatro enteros consecutivos no puede ser un cuadrado perfecto.
- 6.5. Existe un único primo p tal que $2p + 1$ es un cubo.
- 6.6. Si $2^n + 1$ es primo, con $n > 0$, entonces n debe ser potencia de 2.
- 6.7. Si los términos de una progresión aritmética infinita de enteros positivos no son todos iguales, entonces no todos pueden ser primos.
- 6.8. Sean p_1, p_2 primos tales que $p_2 = p_1 + 2$, con $p_1 > 3$. Probar que $12|(p_1 + p_2)$.
- 6.9. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ escrito en su forma canónica. Entonces el número de divisores de n es $(1 + \alpha_1)(1 + \alpha_2)\dots(1 + \alpha_k)$.
- 6.10. Sea $n = 2^{p-1}(2^p - 1)$ y sea $2^p - 1$ un número primo. Probar que la suma de todos los divisores positivos de n , sin incluir a n , es exactamente n .
- 6.11. Si n es un entero positivo y k la cantidad de primos distintos que dividen a n , probar que
- $$\log n \geq k \log 2.$$
- 6.12. Si p es un primo, entonces $(p - 1)! + 1$ es potencia de p si y sólo si $p = 2, 3$ ó 5 .
- 6.13. Existen infinitos primos de la forma $4k + 3$; de la forma $6k + 5$.
- 6.14. Sea $a_n = 111\dots1$ el número cuya expresión decimal está formada por n unos. Probar que, si a_n es primo entonces n es primo.
- 6.15. ¿Cuántos cuadrados perfectos existen entre 40000 y 640000 que son múltiplos, simultáneamente, de 3, 2 y 5?
- 6.16. Del conjunto $\{1, 2, 3, \dots, 360\}$ escogemos 8 números compuestos. Demostrar que por lo menos 2 de los números escogidos no son primos entre sí.
- 6.17. ¿Cuántas ternas ordenadas de números enteros positivos (a, b, c) verifican que:

$$[a, b] = 1000, [b, c] = 2000, [c, a] = 2000?$$

- 6.18. Probar que

$$\frac{[a', b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}.$$

6.19. Sean a, b, c, d, u enteros tales que cada uno de los números

$$ac, bc + ad, bd$$

es múltiplo de u . Probar que bc y ad son múltiplos de u .

6.20.

Si n es un entero mayor que 1, entonces $4^n + n^4$ no es primo.

6.21. Sea k el número de factores primos distintos de n . Probar que existe n_0 tal que, si $n > n_0$ entonces

$$\frac{k}{n} < \frac{1}{1991}.$$

6.22. Sean a, b, c, d números enteros positivos tales que $a^5 = b^4$, $c^3 = d^2$, $c - a = 19$. Hallar $d - b$.

6.23. Probar que, para todo entero positivo n , el número —

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

es divisible por 1897.

SECCION 7

LA FUNCION PARTE ENTERA

Si x es un número real, el símbolo $[x]$ denota al mayor entero que es menor o igual que x . Por ejemplo,

$$\left[\frac{3}{2} \right] = 1, [\pi] = 3, [0, 7] = 0, [-0, 7] = -1.$$

La función que a cada número real x le hace corresponder $[x]$, se denomina *función parte entera* y juega un papel importante en la teoría de números.

A continuación vamos a probar algunas de las propiedades básicas de la función parte entera.

Propiedades.

Consideremos dos números reales x, y . Se tiene:

7.1. $x - 1 < [x] \leq x, [x] \leq x < [x] + 1, 0 \leq x - [x] < 1.$

7.2. Si n es un entero, $[x + n] = [x] + n$.

7.3. $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$.

7.4. $[x] + [-x] = \begin{cases} 0 & \text{si } x \text{ es un entero,} \\ -1 & \text{si } x \text{ no es un entero.} \end{cases}$

7.5. $\left[\frac{[x]}{m} \right] = \left[\frac{x}{m} \right]$ si m es un entero positivo.

7.6. $-[-x]$ es el menor entero mayor o igual que x .

En efecto:

7.1. $x - 1 < [x] \leq x$ y $[x] \leq x < [x] + 1$ se desprenden inmediatamente de la definición de parte entera de x . Si a los tres miembros de la segunda desigualdad se les resta $[x]$, se tiene: $0 \leq x - [x] < 1$.

Nota. Al número $x - [x]$ se le denomina *parte fraccionaria* de x y usualmente se le denota por $\{x\}$.

7.2. La igualdad $[x + n] = [x] + n$, si n es un entero, es evidente por la definición de $[x]$.

7.3. Escribamos $x = n + \alpha, y = m + \beta$, donde n y m son enteros y α y β son dos números reales tales que

$$0 \leq \alpha < 1, \quad 0 \leq \beta < 1.$$

Se tiene:

$$\begin{aligned}[x] + [y] &= n + m \leq [n + \alpha + m + \beta] = n + m + [\alpha + \beta] \leq \\ &\leq n + m + 1 = [x] + [y] + 1.\end{aligned}$$

7.4. Si $x = n + \alpha$, donde n es un entero y $0 \leq \alpha < 1$, entonces

$$\begin{aligned}-x &= -n - \alpha = -n - 1 + 1 - \alpha, \\ 0 &< 1 - \alpha \leq 1.\end{aligned}$$

En consecuencia,

$$\begin{aligned}[x] + [-x] &= n + [-n - 1 + 1 - \alpha] = \\ &= n - n - 1 + [1 - \alpha] = \begin{cases} 0 & \text{si } \alpha = 0, \\ -1 & \text{si } \alpha > 0. \end{cases}\end{aligned}$$

7.5. Escribamos nuevamente $x = n + \alpha$, donde $0 \leq \alpha < 1$. Se tiene, $n = qm + r$, donde q, r son enteros y $0 \leq r \leq m - 1$. Por consiguiente, como $0 \leq r + \alpha < m$, nos queda:

$$\left[\frac{x}{m} \right] = \left[\frac{qm + r + \alpha}{m} \right] = q + \left[\frac{r + \alpha}{m} \right] = q.$$

Por otra parte

$$\left[\frac{[x]}{m} \right] = \left[\frac{n}{m} \right] = \left[q + \frac{r}{m} \right] = q,$$

luego

$$\left[\frac{[x]}{m} \right] = \left[\frac{x}{m} \right].$$

7.6. Si en la desigualdad $x - 1 < [x] \leq x$ se reemplaza x por $-x$ se tiene

$$-x - 1 < [-x] \leq -x,$$

y multiplicando por -1 nos queda

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

El siguiente teorema proporciona un resultado que es bastante útil para la resolución de algunos problemas.

7.7. Consideremos un entero n y un primo p . El mayor exponente k para el cual $p^k | n!$ es

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

Obsérvese que en realidad la suma es finita ya que a partir de un cierto i , digamos i_0 , se tiene que $p^i > n$ para todo $i \geq i_0$ y, en consecuencia, los términos correspondientes se anulan.

Para la demostración procederemos por inducción sobre n . Si $n = 1$ la igualdad se verifica inmediatamente. Supongamos que la propiedad es cierta para $n!$ y sea j el mayor exponente tal que $p^j|(n+1)$. Como $(n+1)! = (n+1)n!$ debemos probar que

$$\sum_{i=1}^{\infty} \left[\frac{n+1}{p^i} \right] - \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] = j.$$

Ahora bien, esta igualdad se desprende inmediatamente del hecho:

$$\left[\frac{n+1}{p^i} \right] - \left[\frac{n}{p^i} \right] = \begin{cases} 1 & \text{si } p^i|(n+1), \\ 0 & \text{si } p^i \nmid (n+1). \end{cases}$$

A continuación veremos algunos ejemplos en los cuales se aplica esta propiedad.

- ¿Cuál es la mayor potencia de 7 que divide a $100!$?

$$\left[\frac{100}{7} \right] + \left[\frac{100}{7^2} \right] = 14 + 2 = 16,$$

luego $7^{16}|100!$ pero $7^{17} \nmid 100!$. Obsérvese que si $i \geq 3$ entonces $\left[\frac{100}{7^i} \right] = 0$.

- ¿En cuántos ceros termina $1000!$?

Es preciso determinar cuántas veces aparece el factor $10 = 2 \cdot 5$ en el producto $1 \cdot 2 \cdot \dots \cdot 1000$. Como hay menos múltiplos de 5 que múltiplos de 2 en este producto, basta determinar la mayor potencia de 5 que divide a $1000!$. Esta es:

$$\left[\frac{1000}{5} \right] + \left[\frac{1000}{5^2} \right] + \left[\frac{1000}{5^3} \right] + \left[\frac{1000}{5^4} \right] = 200 + 40 + 8 + 1 = 249,$$

luego $1000!$ termina con 249 ceros.

- ¿Cuál es la descomposición canónica de $20!$?

Los números primos menores o iguales que 20 son

$$2, 3, 5, 7, 11, 13, 17 \text{ y } 19,$$

luego, se requiere hallar las máximas potencias de ellos que dividen a $20!$.

$$\left[\frac{20}{2} \right] + \left[\frac{20}{2^2} \right] + \left[\frac{20}{2^3} \right] + \left[\frac{20}{2^4} \right] = 10 + 5 + 2 + 1 = 18,$$

$$\left[\frac{20}{3} \right] + \left[\frac{20}{3^2} \right] = 6 + 2 = 8,$$

$$\left[\frac{20}{5} \right] = 4,$$

$$\left[\frac{20}{7} \right] = 2,$$

$$\left[\frac{20}{11} \right] = \left[\frac{20}{13} \right] = \left[\frac{20}{17} \right] = \left[\frac{20}{19} \right] = 1.$$

Por consiguiente, $20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

- Demostrar que si a_1, a_2, \dots, a_k son enteros no negativos tales que $a_1 + a_2 + \dots + a_k = n$, entonces $\frac{n!}{a_1! a_2! \dots a_k!}$ es un entero.

Es necesario probar que todo primo que divide al denominador divide también al numerador, elevado a un exponente mayor o igual. Es decir,

$$\sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] \geq \sum_{i=1}^{\infty} \left[\frac{a_1}{p^i} \right] + \sum_{i=1}^{\infty} \left[\frac{a_2}{p^i} \right] + \dots + \sum_{i=1}^{\infty} \left[\frac{a_k}{p^i} \right].$$

Ahora bien, como $a_1 + a_2 + \dots + a_k = n$, usando reiteradamente la propiedad 7.3. se tiene

$$\left[\frac{a_1}{p^i} \right] + \left[\frac{a_2}{p^i} \right] + \dots + \left[\frac{a_k}{p^i} \right] \leq \left[\frac{n}{p^i} \right]$$

para todo i . Sumando sobre i se llega al resultado propuesto.

Problemas.

7.1. Determinar el menor entero n para que $30!n$ sea un cuadrado perfecto.

7.2. Si x, y son números reales, entonces

$$[x] + [y] + [x + y] \leq [2x] + [2y].$$

7.3. Si x es un número real, entonces

$$\left[\frac{x}{2} \right] + \left[\frac{x+1}{2} \right] = [x].$$

7.4. Hallar fórmulas para el mayor exponente k del primo p tal que p^k divide a:

- $2 \cdot 4 \cdot 6 \dots (2n)$,
- $1 \cdot 3 \cdot 5 \dots (2n-1)$.

7.5. Si n es un entero positivo, entonces $\frac{(2n)!}{(n!)^2}$ es un número par.

7.6. Demostrar que $\prod_{k=1}^n (a+k)$ es divisible por $n!$.

7.7. Demostrar que, para todo entero positivo n ,

$$\sum_{k=0}^{\infty} \left[\frac{n+2^k}{2^{k+1}} \right] = [n].$$

7.8. Si m y n son enteros no negativos, probar que

$$\frac{(2m)!(2n)!}{m!n!(m+n)!} \text{ es entero.}$$

7.9. Probar que para todo par de enteros a, b ,

$$\frac{(ab)!}{a!(b!)^a} \text{ es entero.}$$

7.10. ¿Cuántos de los primeros 100 números enteros positivos pueden expresarse en la forma

$$[2x] + [4x] + [6x] + [8x]?$$

7.11. Demostrar que la ecuación

$$[x] + [2x] + [4x] + [8x] + [16x] + [32x] = 12345$$

no tiene solución real.

7.12. Sea p un número primo y k un entero positivo. Si p es divisor de $\binom{k}{i}$ para todo i , $1 \leq i \leq k-1$, entonces existe un entero positivo m tal que $k = p^m$.

7.13. Si $2^{n-1}|n!$ entonces $n = 2^k$ para algún entero positivo k .

SECCION 8

CONGRUENCIAS EN \mathbb{Z}

Consideremos un entero positivo m . Se dice que a es congruente con b módulo m , y se escribe $a \equiv b$ (mód. m), si $a - b$ es divisible por m .

Por ejemplo, $7 \equiv 2$ (mód. 5) ya que $5|(7 - 2)$, $3 \equiv -5$ (mód. 4), $-31 \equiv -4$ (mód. 27), etc.

Si $a - b$ no es divisible por m , entonces se dice que a no es congruente con b módulo m y se escribe $a \not\equiv b$ (mód. m).

8.1. a es congruente con b módulo m si y sólo si a y b dejan el mismo resto al ser divididos por m .

En efecto, si

$$a = q_1m + r_1, \quad \text{donde } 0 \leq r_1 < m,$$

$$b = q_2m + r_2, \quad \text{donde } 0 \leq r_2 < m,$$

entonces $a - b = (q_1 - q_2)m + (r_1 - r_2)$, y si $m|(a - b)$ entonces necesariamente $m|(r_1 - r_2)$, y como $|r_1 - r_2| < m$ se tiene que $r_1 - r_2 = 0$, luego $r_1 = r_2$. Recíprocamente, si

$$a = q_1m + r \quad \text{y}$$

$$b = q_2m + r \quad \text{donde } 0 \leq r < m,$$

entonces $a - b = (q_1 - q_2)m$, de donde $m|(a - b)$ y $a \equiv b$ (mód. m).

Por consiguiente, cualquier entero es congruente módulo m con uno y sólo uno de los enteros $0, 1, 2, \dots, m - 1$. Por ejemplo, si $m = 2$, los enteros quedan divididos en dos clases:

$$\dots, -6, -4, -2, 0, 2, 4, 6, \dots \equiv 0 \quad (\text{mód. } 2),$$

$$\dots, -5, -3, -1, 1, 3, 5, \dots \equiv 1 \quad (\text{mód. } 2).$$

Si $m = 3$ se tienen tres clases:

$$\dots, -9, -6, -3, 0, 3, 6, \dots \equiv 0 \quad (\text{mód. } 3),$$

$$\dots, -8, -5, -2, 1, 4, 7, \dots \equiv 1 \quad (\text{mód. } 3),$$

$$\dots, -7, -4, -1, 2, 5, 8, \dots \equiv 2 \quad (\text{mód. } 3).$$

En general, habrá m clases:

$$\dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots \equiv 0 \quad (\text{mód. } m),$$

$$\dots, -2m + 1, -m + 1, 1, m + 1, 2m + 1, \dots \equiv 1 \quad (\text{mód. } m),$$

$$\dots, -2m + 2, -m + 2, 2, m + 2, 2m + 2, \dots \equiv 2 \quad (\text{mód. } m),$$

⋮

$$\dots, -2m - 1, -m - 1, -1, m - 1, 2m - 1, \dots \equiv m - 1 \quad (\text{mód. } m).$$

Por otra parte, decir que $a \equiv b$ (mód. m) es equivalente a la posibilidad de expresar a en la forma $mk + b$, donde b es un entero; decir que $a \equiv 0$ (mód. m) es decir que $m|a$, luego el concepto de congruencia que hemos introducido es otra manera de expresar las nociones de divisibilidad.

Ahora bien, la notación que se emplea es muy ventajosa por cuanto muchas de las propiedades de las congruencias son semejantes a las propiedades de las igualdades y es fácil operar con ellas, como veremos a continuación.

Propiedades.

Sean a, b, c, d números enteros. Para todo $m > 0$ se tiene:

8.2. $a \equiv a$ (mód. m).

8.3. Si $a \equiv b$ (mód. m), entonces $b \equiv a$ (mód. m).

8.4. Si $a \equiv b$ (mód. m) y $b \equiv c$ (mód. m), entonces $a \equiv c$ (mód. m).

8.5. Si $a \equiv b$ (mód. m) y $c \equiv d$ (mód. m), entonces $a+c \equiv b+d$ (mód. m) y $a-c \equiv b-d$ (mód. m).

8.6. Si $a \equiv b$ (mód. m) y $c \equiv d$ (mód. m), entonces $ac \equiv bd$ (mód. m).

Las demostraciones son inmediatas. En efecto,

8.2. $m|(a-a)$.

8.3. Si $m|(a-b)$, entonces $m|(b-a)$.

8.4. Si $m|(a-b)$ y $m|(b-c)$, entonces $m|[(a-b)+(b-c)]$, luego $m|(a-c)$.

8.5. Si $m|(a-b)$ y $m|(c-d)$, entonces $m|[(a-b)+(c-d)]$ y $m|[(a-b)-(c-d)]$, luego $m|[(a+c)-(b+d)]$ y $m|[(a-c)-(b-d)]$.

8.6. Si $m|(a-b)$, entonces $m|c(a-b)$, luego $m|(ac-bc)$. (1)

Si $m|(c-d)$, entonces $m|b(c-d)$, luego $m|(bc-bd)$. (2)

De (1) y (2) se concluye que $m|[(ac-bc)+(bc-bd)]$, luego $m|(ac-bd)$.

Nota. Cuando se tienen varias congruencias como $a \equiv b$ (mód. m), $b \equiv c$ (mód. m), $c \equiv d$ (mód. m), esto usualmente se abrevia escribiendo:

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

Las propiedades 8.5. y 8.6. se pueden generalizar fácilmente por inducción, para cualquier número finito de congruencias. Así se tiene que, si

$$a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m}, \dots, a_n \equiv b_n \pmod{m},$$

entonces

$$a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n \pmod{m}$$

y

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_n \pmod{m}.$$

En particular, si $a \equiv b \pmod{m}$, para todo entero positivo n se tiene:

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

Tomando en cuenta estos hechos, es fácil demostrar el teorema siguiente.

8.7. Sea f un polinomio de coeficientes enteros. Si $a \equiv b \pmod{m}$ entonces $f(a) \equiv f(b) \pmod{m}$.

En efecto, supongamos $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$, donde los a_i son enteros para $i = 1, 2, \dots, n$. De acuerdo con las propiedades 8.5. y 8.6. generalizadas, se tiene

$$a_0 a^n \equiv a_0 b^n \pmod{m},$$

$$a_1 a^{n-1} \equiv a_1 b^{n-1} \pmod{m},$$

⋮

$$a_{n-1} a \equiv a_{n-1} b \pmod{m},$$

$$a_n \equiv a_n \pmod{m}.$$

Por consiguiente,

$$a_0 a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n \equiv a_0 b^n + a_1 b^{n-1} + \dots + a_{n-1} b + a_n \pmod{m}.$$

Veamos a continuación algunas aplicaciones prácticas de estas propiedades.

• ¿Cuál es la última cifra de 3^{400} ?

Basta observar que todo entero x escrito en el sistema decimal: $x = a_0 \cdot 10^n + \dots + a_{n-1} \cdot 10 + a_n$, es congruente con su última cifra módulo 10. Entonces:

$$3 \equiv 3 \pmod{10},$$

$$3^2 \equiv 9 \pmod{10},$$

$$3^3 \equiv 27 \equiv 7 \pmod{10},$$

$$3^4 \equiv 21 \equiv 1 \pmod{10}.$$

De esta última congruencia se deduce:

$$(3^4)^{100} \equiv 1^{100} \pmod{10},$$

$$3^{400} \equiv 1 \pmod{10}.$$

Luego, la última cifra de 3^{400} es 1.

- Si $f(x) = x^4 - 5x^3 + 6x^2 - 3x + 2$, ¿cuál es el resto al dividir $f(1991)$ entre 4?
Obsérvese que $1991 \equiv 3 \pmod{4}$; por consiguiente, $1991^4 - 5 \cdot 1991^3 + 6 \cdot 1991^2 - 3 \cdot 1991 + 2 \equiv 3^4 - 5 \cdot 3^3 + 6 \cdot 3^2 - 3 \cdot 3 + 2 \equiv 81 - 135 + 54 - 9 + 2 \equiv -7 \equiv 1 \pmod{4}$.
Por tanto, el resto es 1.

- Expresando los números enteros en el sistema decimal de numeración, deducir el criterio de divisibilidad por 3.

Sea $x = a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + \dots + a_{n-1} \cdot 10 + a_n$. Obsérvese que

$$10 \equiv 1 \pmod{3},$$

por tanto, para todo entero positivo n ,

$$10^n \equiv 1^n \equiv 1 \pmod{3}.$$

Luego, $x \equiv a_0 + a_1 + \dots + a_{n-1} + a_n \pmod{3}$, es decir, x es divisible por 3 si y sólo si la suma de sus cifras es un múltiplo de 3.

- Expresando los números enteros en el sistema decimal de numeración, deducir el criterio de divisibilidad por 11.

Sea $x = a_0 \cdot 10^n + a_1 \cdot 10^{n-1} + \dots + a_{n-1} \cdot 10 + a_n$. Obsérvese que

$$10 \equiv -1 \pmod{11},$$

$$10^n \equiv (-1)^n \pmod{11}.$$

Por consiguiente, $x \equiv a_0 \cdot (-1)^n + a_1 \cdot (-1)^{n-1} + \dots + a_{n-1} \cdot (-1) + a_n \equiv (a_n + a_{n-2} + a_{n-4} + \dots) - (a_{n-1} + a_{n-3} + a_{n-5} + \dots) \pmod{11}$, por tanto x es divisible por 11 si y sólo si la diferencia entre la suma de las cifras que ocupan lugares impares (contando desde las unidades) y la suma de las cifras que ocupan lugares pares, es un múltiplo de 11.

Seguidamente haremos un par de observaciones que puede ser útil tener en cuenta para resolver algunos problemas.

- Todo cuadrado perfecto es de la forma $4k$ ó de la forma $4k + 1$; asimismo, es de una de las formas $8k, 8k + 1, 8k + 4$. Escrito en términos de congruencias:

$$n^2 \equiv \begin{cases} 0 & \text{(mód. 4)} \\ 1 & \text{(mód. 4)} \end{cases} \quad \begin{array}{l} \text{si } n \text{ es par,} \\ \text{si } n \text{ es impar.} \end{array}$$

$$n^2 \equiv \begin{cases} 0 & \text{(mód. 8)} \\ 4 & \text{(mód. 8)} \\ 1 & \text{(mód. 8)} \end{cases} \quad \begin{array}{l} \text{si } n \equiv 0 \pmod{4}, \\ \text{si } n \equiv 2 \pmod{4}, \\ \text{si } n \text{ es impar.} \end{array}$$

- Si consideramos una ecuación diofántica en dos variables, $f(x, y) = 0$, como 0 es divisible por cualquier entero m , para todo $m > 0$ se tiene que $f(x, y) \equiv 0 \pmod{m}$. Luego, si no

existen enteros x, y tales que $f(x, y) \equiv 0$ (mód. m) para todo $m > 0$, la ecuación diofántica $f(x, y) = 0$ no tiene soluciones.

Por ejemplo, consideremos la ecuación diofántica

$$x^2 - 8y^2 = 3$$

y probemos que no tiene soluciones. Tomemos $m = 8$. Entonces la congruencia $x^2 - 8y^2 - 3 \equiv 0$ (mód. 8) no tiene soluciones. En efecto, de lo contrario se tendría

$$x^2 \equiv 8y^2 - 3 \equiv -3 \equiv 5 \pmod{8},$$

y hemos visto que x^2 siempre es congruente con 0, 1 ó 4 módulo 8.

Otras propiedades importantes de las congruencias son las siguientes.

8.8. $ax \equiv ay \pmod{m}$ si y sólo si $x \equiv y \pmod{\frac{m}{(a, m)}}$.

8.9. Si $ax \equiv ay \pmod{m}$ y $(a, m) = 1$, entonces $x \equiv y \pmod{m}$.

8.10. Dados los enteros positivos m_1, m_2, \dots, m_k , entonces $x \equiv y \pmod{m_1}, x \equiv y \pmod{m_2}, \dots, x \equiv y \pmod{m_k}$ si y sólo si $x \equiv y \pmod{\{m_1, m_2, \dots, m_k\}}$.

En efecto:

8.8. $ax \equiv ay \pmod{m}$ si y sólo si $m | (ax - ay)$; esto es, si y sólo si existe un entero z tal que $mz = a(x - y)$, lo cual ocurre si y sólo si

$$\frac{m}{(a, m)}z = \frac{a}{(a, m)}(x - y),$$

es decir,

$$\frac{m}{(a, m)} \mid \frac{a}{(a, m)}(x - y),$$

y como $\left(\frac{m}{(a, m)}, \frac{a}{(a, m)}\right) = 1$ (propiedad 3.3.), esto último sucede si y sólo si $\frac{m}{(a, m)} \mid (x, y)$, o sea

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

Nota. A diferencia de otras propiedades de las congruencias que hemos demostrado, notese que ésta difiere de la que correspondería en las igualdades. No siempre se puede cancelar un factor común en ambos miembros de una congruencia. Por ejemplo, $3x \equiv 6$ (mód. 9) no es equivalente a $x \equiv 2$ (mód. 9); si lo es a $x \equiv 2$ (mód. 3). $3x \equiv 6$ (mód. 8) es equivalente a $x \equiv 2$ (mód. 8).

8.9. Este es un caso particular de 8.8., cuando $(a, m) = 1$. Se usa con bastante frecuencia.

8.10. Si $x \equiv y \pmod{m_i}$ para todo $i = 1, 2, \dots, k$, entonces $x - y$ es un múltiplo común de m_1, m_2, \dots, m_k y, de acuerdo con la propiedad 5.1., $[m_1, m_2, \dots, m_k] \mid (x - y)$, luego $x \equiv y \pmod{[m_1, m_2, \dots, m_k]}$.

Recíprocamente, si $x \equiv y \pmod{[m_1, m_2, \dots, m_k]}$, entonces $[m_1, m_2, \dots, m_k] \mid (x - y)$, y como cada $m_i \mid [m_1, m_2, \dots, m_k]$, de acuerdo con la propiedad 2.2. se tiene $x \equiv y \pmod{m_i}$ para $i = 1, 2, \dots, k$.

Al principio de esta sección mencionamos que cualquier número entero es congruente con uno y sólo uno de los números $0, 1, 2, \dots, m - 1$ módulo m . Si $y \equiv x \pmod{m}$ se dice que y es un resto de x módulo m . En general, se dice que un conjunto $C = \{x_1, x_2, \dots, x_m\}$ es un sistema completo de restos módulo m si para cualquier número entero y existe un único entero $x_i \in C$ tal que $y \equiv x_i \pmod{m}$.

Obviamente, $\{0, 1, 2, \dots, m - 1\}$ es un sistema completo de restos módulo m y cualquier conjunto que se forme tomando un elemento de cada una de las m clases en las cuales quedan divididos los enteros al considerar los restos que se obtienen al realizar la división por m , es también un sistema completo de restos módulo m .

Ejemplos de sistemas completos de restos módulo 7 son los siguientes:

$$\begin{aligned} &\{0, 1, 2, 3, 4, 5, 6\}, \\ &\{7, 8, 9, 10, 11, 12, 13\}, \\ &\{7, 15, 22, 3, -3, 5, 13\}, \\ &\{-3, -2, -1, 0, 1, 2, 3\}. \end{aligned}$$

Por lo general resulta práctico utilizar sistemas como el último de los indicados, ya que al ser los números más pequeños en valor absoluto, los cálculos son más rápidos. Por ejemplo, si queremos saber cuál es el resto que resulta al dividir 7^{37} entre 17, podemos seleccionar el sistema $\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$ y proceder de la siguiente forma:

$$\begin{aligned} 7^2 &\equiv 49 \equiv -2 \pmod{17}, \\ 7^4 &\equiv (-2)^2 \equiv 4 \pmod{17}, \\ 7^8 &\equiv 4^2 \equiv -1 \pmod{17}, \\ 7^{32} &\equiv (-1)^4 \equiv 1 \pmod{17}, \\ 7^{36} &\equiv 7^{32} \cdot 7^4 \equiv 4 \pmod{17}, \\ 7^{37} &\equiv 7^{36} \cdot 7 \equiv 4 \cdot 7 \equiv 28 \equiv 11 \pmod{17}, \end{aligned}$$

y por tanto, el resto buscado es 11.

Antes de introducir un nuevo concepto, vamos a demostrar el siguiente teorema.

8.11. Si $x \equiv y \pmod{m}$, entonces $(x, m) = (y, m)$.

En efecto, si $x \equiv y \pmod{m}$, entonces $m \mid (x - y)$, luego existe un entero z tal que $x - y = mz$. Ahora bien, de esta igualdad se desprende que $(x, m) \mid y$, luego $(x, m) \mid (y, m)$ y en consecuencia $(x, m) \leq (y, m)$. De la misma manera $(y, m) \mid x$, por tanto $(y, m) \mid (x, m)$ y se tiene $(y, m) \leq (x, m)$. Por consiguiente, $(x, m) = (y, m)$.

Ahora definimos un *sistema reducido de restos módulo m* como un conjunto $R = \{x_1, x_2, \dots, x_k\}$ tal que para cualquier número entero y primo con m existe un único entero $x_i \in R$ tal que $y \equiv x_i \pmod{m}$.

De acuerdo con el teorema anterior, un sistema reducido de restos módulo m puede obtenerse a partir de un sistema completo de restos módulo m , eliminando de este último aquellos enteros que no son primos con m . Por ejemplo, un sistema reducido de restos módulo 8 es: $\{1, 3, 5, 7\}$. Otro sería: $\{-3, -1, 1, 3\}$.

Además, si se tienen dos sistemas reducidos de restos módulo m , R y R' , cada elemento de R es congruente módulo m con un único elemento de R' , y viceversa. Por consiguiente, todos los sistemas reducidos de restos módulo m tienen el mismo número de elementos. A este número se le llama *Indicador de Euler* y se le denota por $\phi(m)$.

Dado que los elementos de un sistema reducido de restos módulo m pueden obtenerse a partir del sistema completo de restos módulo m formado por los números $1, 2, \dots, m-1, m$, $\phi(m)$ indica el número de enteros positivos menores o iguales que m que son primos con m . Por ejemplo, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(10) = 4$. En particular, nótese que si m es un número primo entonces $\phi(m) = m - 1$. Más adelante regresaremos con el indicador de Euler.

Para finalizar esta sección, demostraremos el siguiente resultado.

8.12. Si $X = \{x_1, x_2, \dots, x_k\}$ es un sistema completo (reducido) de restos módulo m y $(a, m) = 1$, entonces $aX = \{ax_1, ax_2, \dots, ax_k\}$ es también un sistema completo (reducido) de restos de módulo m .

En efecto, como X y aX tienen el mismo número de elementos, bastará demostrar que $ax_i \not\equiv ax_j \pmod{m}$ si $i \neq j$ para todo par de elementos de aX . Pero como $(a, m) = 1$, esto se desprende inmediatamente de la propiedad 8.9.

Problemas.

8.1. Escribir una congruencia que sea equivalente al par de congruencias

$$x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{3}.$$

8.2. Expresando los números enteros en el sistema de numeración de base 100, deducir el criterio de divisibilidad por 101.

8.3. Expresando los números enteros en el sistema de numeración de base 1000, deducir los criterios de divisibilidad por 7, 13, 37.

8.4. Demostrar que, si $m > 2$, entonces $\{1^2, 2^2, \dots, m^2\}$ no es un sistema completo de restos módulo m .

8.5. Sean a, b, c, d cuatro enteros. Probar que el producto de las seis diferencias

$$b-a, c-a, d-a, d-c, d-b, c-b,$$

es divisible por 12.

8.6. Si p es un primo tal que $p = x^2 + y^2 = a^2 + b^2$, donde x, y, a, b son números primos tales que $x > y, a > b$, demostrar que $x = a, y = b$.

8.7. Si a_1, a_2, \dots, a_n son enteros y p es un número primo, entonces

$$(a_1 + a_2 + \dots + a_n)^p \equiv a_1^p + a_2^p + \dots + a_n^p \pmod{p}.$$

8.8. Demostrar que para todo entero positivo n ,

$$(x-1)^2 | [x^n - n(x-1) - 1].$$

8.9. Sea d un entero positivo distinto de 2, 3 ó 13. Demostrar que pueden hallarse dos números diferentes a y b pertenecientes al conjunto $\{2, 5, 13, d\}$ tales que $ab - 1$ no es un cuadrado perfecto.

8.10. Si $S(n)$ es la suma de las cifras del entero n escrito en base decimal, entonces

$$S(4891n) - S(1984n)$$

es siempre múltiplo de 9.

8.11. Si a, m, n son enteros positivos, con $m \neq n$, entonces

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

8.12. Las longitudes de los catetos y de la hipotenusa de un triángulo rectángulo son a, b, c respectivamente. a, b y c son números enteros y c no es divisible por 5. Demostrar que el área del triángulo es múltiplo de 10.

8.13. Dados los $2k$ números

$$2^1 - 1, 2^2 - 1, 2^3 - 1, \dots, 2^{2k} - 1,$$

donde $k \geq 1$, demostrar que al menos uno de estos números es múltiplo de $2k + 1$.

8.14. Tomemos la sucesión de los cuadrados perfectos y sumemos 100 a cada término para formar la sucesión

$$101, 104, 109, 116, 125, 136, 149, \dots$$

Sea d_n el máximo común divisor del n -ésimo término y del $(n+1)$ -ésimo término de esta sucesión. ¿Cuál es el mayor valor que puede tener d_n ?

SECCION 9

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

Antes de proseguir con nuestro estudio de las congruencias, vamos a resolver uno de los problemas más antiguos de la teoría de números, que ya mencionamos al inicio de estas notas: hallar todos los triángulos rectángulos cuyos lados son enteros. Esto es, hallar todas las soluciones enteras de la ecuación:

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

Haremos algunos comentarios previos.

Se dice que un conjunto de tres enteros (x, y, z) tales que $x^2 + y^2 = z^2$, es un *triple pitagórico*. Vamos a obviar el caso trivial en donde $x = y = z = 0$. Además, si (x, y, z) es un triple pitagórico, también lo son todas las ternas $(\pm x, \pm y, \pm z)$, luego podemos concretarnos a estudiar el caso en que x, y, z son enteros positivos.

Por otra parte, si (x, y, z) es un triple pitagórico, para cualquier entero k se tiene que (xk, yk, zk) es también un triple pitagórico, luego para resolver la ecuación podemos limitarnos a encontrar todos los triples pitagóricos (x, y, z) que sean primos entre sí (más aún, serán primos dos a dos ya que si d es un divisor común de dos de los enteros x, y, z , de la igualdad $x^2 + y^2 = z^2$ se desprende que lo será también del tercero). Una solución de la ecuación $x^2 + y^2 = z^2$ en la cual x, y, z son primos dos a dos es llamada una *solución primitiva* y el triángulo rectángulo correspondiente es un *triángulo primitivo*. Por ejemplo,

$$(3, 4, 5)$$

es una solución primitiva de la ecuación por cuanto 3, 4 y 5 son primos dos a dos y $3^2 + 4^2 = 5^2$. Para cualquier entero k , $(3k, 4k, 5k)$ es también una solución de $x^2 + y^2 = z^2$. Por ejemplo, $(6, 8, 10), (9, 12, 15), (12, 16, 20), (15, 20, 25), \dots$ son soluciones que se desprenden de la solución primitiva $(3, 4, 5)$.

Además, observemos que en la ecuación $x^2 + y^2 = z^2$, x, y no pueden tener la misma paridad. En efecto, si $(x, y) = 1$, entonces no pueden ser ambos pares. Por otra parte, si suponemos que ambos son impares se tiene:

$$\begin{aligned} x^2 &\equiv 1 \pmod{4}, \\ y^2 &\equiv 1 \pmod{4}, \end{aligned}$$

de donde resulta que $z^2 \equiv 2 \pmod{4}$, lo cual sabemos no es posible. Supondremos, sin pérdida de generalidad, que x es impar e y es par.

Hechas estas consideraciones, procedamos a hallar todas las soluciones primitivas de $x^2 + y^2 = z^2$. Se tiene:

$$y^2 = z^2 - x^2,$$

de donde

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

Dividiendo ambos miembros por 4 se tiene,

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$$

(obsérvese que $z+x$ y $z-x$ son pares). Además,

$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \mid \frac{z+x}{2} + \frac{z-x}{2} = z,$$

y

$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \mid \frac{z+x}{2} - \frac{z-x}{2} = x,$$

por tanto se concluye que

$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1,$$

y como el producto $\left(\frac{z+x}{2}\right) \cdot \left(\frac{z-x}{2}\right)$ es un cuadrado perfecto, cada uno de estos dos factores debe ser un cuadrado perfecto. Escribamos: $\frac{z+x}{2} = m^2$, $\frac{z-x}{2} = n^2$. Observemos que $m > n > 0$; además $(m, n) = 1$ y, al resolver el sistema

$$\frac{z+x}{2} = m^2,$$

$$\frac{z-x}{2} = n^2,$$

se tiene que $x = m^2 - n^2$, $z = m^2 + n^2$. Reemplazando en $y^2 = z^2 - x^2$ nos queda

$$y^2 = (m^2 + n^2)^2 - (m^2 - n^2)^2,$$

$$y^2 = 4m^2n^2,$$

$$y = 2mn.$$

Finalmente, observemos que si m y n fuesen de la misma paridad, de las igualdades $x = m^2 - n^2$, $z = m^2 + n^2$ se tendría que x, z son ambos pares, contradiciendo el hecho que $(x, z) = 1$.

Recíprocamente, es fácil verificar que los tres números $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ satisfacen la ecuación pitagórica $x^2 + y^2 = z^2$, por tanto, tenemos el siguiente

9.1. Todas las soluciones primitivas positivas de la ecuación $x^2 + y^2 = z^2$, donde x es impar e y es par, vienen dadas por:

$$x = m^2 - n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2,$$

donde m y n son enteros arbitrarios que satisfacen las tres condiciones siguientes:

- a) $m > n > 0$,
- b) $(m, n) = 1$,
- c) m y n tienen distinta paridad.

Veamos algunos ejemplos:

- Si $m = 2$ y $n = 1$, se tiene

$$x = 2^2 - 1^2 = 3,$$

$$y = 2 \cdot 2 \cdot 1 = 4,$$

$$z = 2^2 + 1^2 = 5,$$

luego $m = 2$ y $n = 1$ dan origen a la solución primitiva $(3, 4, 5)$.

- Si $m = 3$ y $n = 2$, entonces

$$x = 3^2 - 2^2 = 5,$$

$$y = 2 \cdot 3 \cdot 2 = 12,$$

$$z = 3^2 + 2^2 = 13.$$

$m = 3$ y $n = 2$ dan origen a la solución primitiva $(5, 12, 13)$.

- Si $m = 4$ y $n = 1$, entonces

$$x = 4^2 - 1^2 = 15,$$

$$y = 2 \cdot 4 \cdot 1 = 8,$$

$$z = 4^2 + 1^2 = 17.$$

$m = 4$ y $n = 1$ dan origen a la solución primitiva $(15, 8, 17)$.

Problemas.

- 9.1. Hallar todos los triples pitagóricos cuyos términos forman una progresión aritmética.
- 9.2. Si x, y, z son enteros tales que $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$, entonces $(x, y) > 1$.
- 9.3. Si x, y, z son enteros tales que $x^2 + y^2 = z^2$, entonces xyz es múltiplo de 60.
- 9.4. Si $a \geq 3$ entonces existe un triángulo pitagórico cuyo cateto mide a .
- 9.5. Hallar todos los triángulos pitagóricos cuyo perímetro mide 60.
- 9.6. Resolver la ecuación diofántica

$$5x^2 + 10xy + 10y^2 = z^2 + 2z + 1.$$

- 9.7. Hallar todos los triángulos pitagóricos cuya área es igual a 120.

SECCION 10

LAS CONGRUENCIAS DE EULER, FERMAT Y WILSON

En esta sección estableceremos tres congruencias que, además de tener interés histórico, son bastante útiles para resolver diversos problemas en teoría de números. Comenzaremos probando el:

10.1. Teorema de Euler. Si $(a, m) = 1$, entonces $a^{\phi(m)} \equiv 1$ (mód. m), donde $\phi(m)$ es el indicador de Euler.

En efecto, consideremos un sistema reducido de restos módulo m : $R = \{x_1, x_2, \dots, x_{\phi(m)}\}$. Entonces, como $(a, m) = 1$, el conjunto $aR = \{ax_1, ax_2, \dots, ax_{\phi(m)}\}$ es también un sistema reducido de restos módulo m (propiedad 8.12.). Por consiguiente, a cada $x_i \in R$ le corresponde un y sólo un $ax_j \in aR$ tal que

$$x_i \equiv ax_j \pmod{m}.$$

Además, a elementos diferentes de R les corresponderán elementos diferentes de aR , por tanto $ax_1, ax_2, \dots, ax_{\phi(m)}$ son congruentes con $x_1, x_2, \dots, x_{\phi(m)}$ módulo m (no necesariamente en ese orden). Luego,

$$(ax_1)(ax_2) \dots (ax_{\phi(m)}) \equiv x_1 x_2 \dots x_{\phi(m)} \pmod{m},$$
$$x_1 x_2 \dots x_{\phi(m)} a^{\phi(m)} \equiv x_1 x_2 \dots x_{\phi(m)} \pmod{m},$$

y como $(x_1 x_2 \dots x_{\phi(m)}, m) = 1$, de acuerdo con la propiedad 8.9. se tiene:

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

conforme se quería demostrar.

Dado que, si m es primo entonces $\phi(m) = m - 1$, el siguiente resultado se desprende inmediatamente como un corolario del teorema de Euler.

10.2. Teorema de Fermat. Si p es un primo tal que $p \nmid a$, entonces

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

A veces, éste se llama "pequeño teorema de Fermat", para diferenciarlo del "último teorema de Fermat".

Una aplicación típica del teorema de Fermat es la siguiente.

- Calcular el resto que resulta al dividir 2^{1991} entre 11.

Como 11 es un primo y $11 \nmid 2$, se tiene:

$$2^{10} \equiv 1 \pmod{11}.$$

Ahora bien, $1991 = 10 \cdot 199 + 1$, luego

$$2^{1991} \equiv (2^{10})^{199} \cdot 2 \equiv 1^{199} \cdot 2 \equiv 2 \pmod{11},$$

por consiguiente, el resto buscado es 2.

Al teorema de Fermat se le puede dar otra forma, multiplicando ambos miembros de la congruencia $a^{p-1} \equiv 1 \pmod{p}$ por a . Se tiene entonces la congruencia:

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

la cual se cumple para todos los valores enteros de a , por cuanto también es cierta si $p|a$.

Del teorema de Euler se deduce también el siguiente resultado.

Si $(a, m) = 1$, entonces la congruencia $ax \equiv b \pmod{m}$ tiene una solución $x = x_1$.

En efecto, basta tomar

$$x_1 = a^{\phi(m)-1}b.$$

Además, si x es la solución general de $ax \equiv b \pmod{m}$, se tiene:

$$ax - ax_1 \equiv b - b \pmod{m},$$

$$a(x - x_1) \equiv 0 \pmod{m}$$

y como $(a, m) = 1$,

$$x \equiv x_1 \pmod{m},$$

por consiguiente, $x = x_1 + km$ donde k es un entero. Además, la propiedad 8.7. garantiza que, para todo entero k , $x = x_1 + km$ es una solución de la congruencia $ax \equiv b \pmod{m}$. En conclusión:

10.3. Si $(a, m) = 1$, entonces $ax \equiv b \pmod{m}$ tiene una solución $x = x_1$. Todas las soluciones de la congruencia vienen dadas por $x = x_1 + km$, donde $k \in \mathbb{Z}$.

Veamos un ejemplo.

• Resolver la congruencia $5x \equiv 2 \pmod{7}$.

Como $(5, 7) = 1$, la congruencia tiene una solución particular $x_1 = 5^{\phi(7)-1} \cdot 2 = 5^5 \cdot 2$ y la solución general viene dada por $x = 5^5 \cdot 2 + 7k$ donde $k \in \mathbb{Z}$.

Usualmente resulta más práctico, cuando el módulo es un número pequeño, hallar la solución particular por simple inspección. En el ejemplo anterior, si tomamos el siguiente sistema completo de restos módulo 7:

$$\{-3, -2, -1, 0, 1, 2, 3\},$$

se verifica fácilmente que $x_1 = -1$ es una solución particular.

A continuación vamos a probar el:

10.4. Teorema de Wilson. Si p es un primo, entonces

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

Si $p = 2$ ó $p = 3$, entonces la congruencia se verifica inmediatamente. Supongamos que $p \geq 5$.

Antes de hacer la demostración formal, vamos a dar un ejemplo que ilustra la idea en la cual se apoya aquella. Tomemos $p = 11$ y procuremos agrupar los números $2, 3, 4, 5, 6, 7, 8$ y 9 en parejas de manera que el producto de los dos elementos de cada pareja sea congruente con 1 módulo 11 . Se tiene:

$$\begin{aligned} 2 \cdot 6 &\equiv 1 \pmod{11}, \\ 3 \cdot 4 &\equiv 1 \pmod{11}, \\ 5 \cdot 9 &\equiv 1 \pmod{11}, \\ 7 \cdot 8 &\equiv 1 \pmod{11}, \end{aligned}$$

y además,

$$1 \cdot 10 \equiv -1 \pmod{11}.$$

Multiplicando miembro a miembro estas congruencias nos queda

$$10! \equiv -1 \pmod{11}.$$

Ahora bien, si en general j es un entero tal que $1 \leq j \leq p - 1$, entonces $(j, p) = 1$ y por consiguiente, según 10.3., la congruencia $ji \equiv 1 \pmod{p}$ tiene solución y existe exactamente una solución i tal que $0 \leq i \leq p - 1$. Evidentemente, $i \neq 0$, luego tenemos $1 \leq i \leq p - 1$.

Si a cada j le asignamos el i correspondiente, como $ij \equiv ji \equiv 1 \pmod{p}$ podemos observar que j es el entero asociado con i . Observamos además que

$$\begin{aligned} 1 \cdot 1 &\equiv 1 \pmod{p}, \\ (p-1)^2 &\equiv 1 \pmod{p}, \end{aligned}$$

luego 1 y $p - 1$ se asocian con ellos mismos. Consideraremos los casos en que $2 \leq j \leq p - 2$. Para estos enteros se tiene

$$\begin{aligned} (j-1, p) &= 1 \quad y \\ (j+1, p) &= 1, \end{aligned}$$

por consiguiente $(j^2 - 1, p) = 1$ y entonces

$$j^2 \not\equiv 1 \pmod{p}.$$

Luego, todo j tal que $2 \leq j \leq p - 2$ está asociado con un i tal que $i \neq j$ y $2 \leq i \leq p - 2$. Por tanto, los enteros $2, 3, \dots, p - 2$ pueden ser asociados en parejas $\{i, j\}$ tales que $ji \equiv 1 \pmod{p}$. Multiplicando miembro a miembro estas congruencias nos queda

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

y como

$$1 \cdot (p-1) \equiv -1 \pmod{p}$$

se deduce

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

Los teoremas de Wilson y Fermat pueden usarse para resolver un tipo particular de congruencias cuadráticas, como veremos en el siguiente resultado.

10.5. Si p es un primo, la congruencia $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y sólo si $p = 2$ ó $p \equiv 1 \pmod{4}$. Si $p \equiv 1 \pmod{4}$, entonces $x = \left(\frac{p-1}{2}\right)!$ es una solución.

En efecto, si $p = 2$ se tiene la solución $x = 1$. Supongamos que p es un primo impar y supongamos además que

$$x^2 \equiv -1 \pmod{p} \text{ para algún } x \in \mathbb{Z}.$$

Entonces,

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

Por otra parte, de acuerdo con el teorema de Fermat,

$$x^{p-1} \equiv 1 \pmod{p}$$

ya que $p \nmid x$. Luego,

$$\begin{aligned} 1 &\equiv (-1)^{\frac{p-1}{2}} \pmod{p}, \\ p &\mid \left[1 - (-1)^{\frac{p-1}{2}} \right]. \end{aligned}$$

Si $1 - (-1)^{\frac{p-1}{2}} \neq 0$, entonces necesariamente $1 - (-1)^{\frac{p-1}{2}} = 2$, lo que contradice el hecho de ser p impar. Por tanto,

$$\begin{aligned} 1 - (-1)^{\frac{p-1}{2}} &= 0, \\ (-1)^{\frac{p-1}{2}} &= 1, \\ 2 &\mid \frac{p-1}{2}, \\ 4 &\mid (p-1), \\ p &\equiv 1 \pmod{4}. \end{aligned}$$

Recíprocamente, supongamos que $p \equiv 1 \pmod{4}$. Se tiene

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1) = \\ &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot (p-1)(p-2) \cdots \frac{p+1}{2} \equiv \\ &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot (-1) \cdot (-2) \cdots \left(-\frac{p-1}{2} \right) \pmod{p}. \end{aligned}$$

Luego,

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2 \equiv \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p},$$

ya que $p \equiv 1 \pmod{4}$.

Por otra parte, el teorema de Wilson garantiza que

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

por tanto, si tomamos $x = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!$ se tiene

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

Este resultado puede ser útil en algunos ejercicios, como en el siguiente ejemplo.

- Probar que la ecuación diofántica $x^2 + 1 = 23y$ no tiene soluciones.
Si $x^2 + 1 = 23y$, entonces

$$23|(x^2 + 1),$$

luego,

$$x^2 \equiv -1 \pmod{23},$$

pero 23 es un primo de la forma $4k + 3$, luego no existe ningún entero x tal que $x^2 \equiv -1 \pmod{23}$.

Problemas.

- 10.1. Probar que $n^{12} - a^{12}$ es divisible por 91 si $(n, 91) = (a, 91) = 1$.

- 10.2. Probar que, para todo entero n , $n^7 - n$ es divisible por 42.

- 10.3. Probar que $19 \nmid (4n^2 + 4)$ para ningún entero n .

10.4. Probar que un entero $m > 1$ es primo si y sólo si

$$m|[(m-1)! + 1].$$

- 10.5. Probar que, para todo entero n , $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es entero.

10.6. Probar que, si p es un primo, entonces

$$(p-1)! \equiv p-1 \pmod{1+2+\cdots+[p-1]}.$$

10.7. Si p es un primo impar, entonces:

- a) $2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}}$ (mód. p).
b) $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}}$ (mód. p).

10.8. Si p es un primo diferente de 2 y de 5, entonces p divide a infinitos enteros de la forma 9, 99, 999, 9999, Asimismo, p divide a infinitos enteros de la forma 1, 11, 111, 1111,

10.9. Sean a, b, c enteros consecutivos, donde b es un cubo perfecto. Demostrar que abc es divisible por 504.

10.10. Para cualquier entero positivo n ,

$$1^n + 2^n + 3^n + 4^n$$

es divisible por 5 si y sólo si n no es divisible por 4.

10.11. Hallar todas las soluciones de la ecuación

$$3^n - 5^m = 4,$$

para n, m enteros positivos.

10.12. Demostrar que, para todo primo p , existen infinitos enteros positivos n tales que $2^n - n$ es divisible por p .

10.13. Demostrar que el producto de los primeros n enteros positivos, $n > 1$, es divisible por su suma si y sólo si $n + 1$ no es primo.

SECCION 11

RESOLUCION DE CONGRUENCIAS

Supongamos que se tiene un polinomio de coeficientes enteros:

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

Si x_0 es un número entero tal que, dado un entero positivo m , $f(x_0) \equiv 0 \pmod{m}$, entonces se dice que x_0 es una solución de la congruencia $f(x) \equiv 0 \pmod{m}$.

Recordemos que si a, b son dos enteros tales que $a \equiv b \pmod{m}$, entonces $f(a) \equiv f(b) \pmod{m}$ (propiedad 8.7.), luego si a es una solución de la congruencia $f(x) \equiv 0 \pmod{m}$, entonces b también lo es. De acuerdo con esto, si la congruencia $f(x) \equiv 0 \pmod{m}$ admite una solución x_0 , entonces admite infinitas soluciones (todos los enteros congruentes con x_0 módulo m). No obstante, se considera que dos soluciones son distintas si y sólo si no son congruentes entre sí módulo m . Esta consideración permite definir el *número de soluciones* de la congruencia $f(x) \equiv 0 \pmod{m}$ como el número de enteros de un sistema completo de restos módulo m : $\{x_1, x_2, \dots, x_m\}$ tales que $f(x_i) \equiv 0 \pmod{m}$.

Por ejemplo:

- Resolver la congruencia $x^5 + x + 1 \equiv 0 \pmod{7}$.

Si tomamos el sistema completo de restos módulo 7:

$$\{-3, -2, -1, 0, 1, 2, 3\},$$

observamos que los enteros -3 y 2 satisfacen la congruencia y sólo ellos. Luego, la congruencia tiene dos soluciones, a saber: $x \equiv 3 \pmod{7}$ ó $x \equiv 2 \pmod{7}$.

Por otra parte, obsérvese que si x_0 es una solución de la congruencia $f(x) \equiv 0 \pmod{m}$ y si d es un entero positivo tal que $d|m$, entonces x_0 es también una solución de la congruencia $f(x) \equiv 0 \pmod{d}$. En efecto, si

$$f(x_0) \equiv 0 \pmod{m},$$

entonces

$$m|f(x_0)$$

y como $d|m$ se tiene:

$$d|f(x_0)$$

de donde se concluye que $f(x_0) \equiv 0 \pmod{d}$.

Si $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$, y $a_0 \not\equiv 0 \pmod{m}$, se dice n es el *grado* de la congruencia $f(x) \equiv 0 \pmod{m}$. Ahora bien, si $a_0 \equiv 0 \pmod{m}$ y k es el menor entero positivo tal que $a_k \not\equiv 0 \pmod{m}$, entonces el grado de la congruencia $f(x) \equiv 0 \pmod{m}$ es $n - k$. Si todos los a_i ($i = 0, 1, \dots, n$) son múltiplos de m , entonces no se le asigna grado a la congruencia.

De acuerdo con esta definición, nótese que el grado de la congruencia $f(x) \equiv 0$ (mód. m) no necesariamente coincide con el grado de la ecuación $f(x) = 0$. De hecho, *el grado de la congruencia depende del módulo*. Por ejemplo:

$$8x^3 + 3x + 1 \equiv 0 \pmod{4} \text{ tiene grado 1;}$$

$$8x^3 + 3x + 1 \equiv 0 \pmod{5} \text{ tiene grado 3.}$$

Para congruencias de grado mayor que 1, no se conocen métodos generales de resolución. En esta sección nos limitaremos al estudio de congruencias de primer grado.

11.1. Congruencias de Primer Grado. Toda congruencia de grado 1 puede ser escrita en la forma $ax \equiv b$ (mód. m), donde $a \not\equiv 0$ (mód. m). Podemos considerar dos casos:

a) $(a, m) = 1$. En este caso ya hemos visto, como consecuencia del teorema de Euler, que la congruencia $ax \equiv b$ (mód. m) tiene una solución única módulo m ; ésta es:

$$x \equiv a^{\phi(m)-1}b \pmod{m}.$$

b) $(a, m) = d > 1$. Si x_0 es una solución de $ax \equiv b$ (mód. m), se tiene que x_0 es también una solución de $ax \equiv b$ (mód. d), luego $ax_0 \equiv b$ (mód. d) y, como $ax_0 \equiv 0$ (mód. d), entonces necesariamente $b \equiv 0$ (mód. d). Por consiguiente, si $d \nmid b$ se puede garantizar que la congruencia $ax \equiv b$ (mód. m) no tiene soluciones.

Supongamos que $d \mid b$. Entonces existe un entero x_0 tal que $ax_0 \equiv b$ (mód. m) si y sólo si $\frac{a}{d}x_0 \equiv \frac{b}{d}$ (mód. $\frac{m}{d}$), de acuerdo con la propiedad 8.8. Ahora bien, $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, luego, la congruencia $\frac{a}{d}x \equiv \frac{b}{d}$ (mód. $\frac{m}{d}$) tiene solución única módulo $\frac{m}{d}$. Sea $x \equiv x_1$ (mód. $\frac{m}{d}$) tal solución. Entonces, las soluciones de $ax \equiv b$ (mód. m) son aquellos enteros x_0 tales que $x_0 \equiv x_1$ (mód. $\frac{m}{d}$); es decir, $x_0 = x_1 + k \frac{m}{d}$ donde $k \in \mathbb{Z}$.

Si asignamos a k los valores $0, 1, \dots, d-1$, entonces x_0 toma d valores que no son congruentes entre sí, dos a dos, módulo m . Además, si se le asigna a k cualquier otro valor entero, el x_0 resultante será congruente módulo m con alguno de los d anteriores, luego la congruencia $ax \equiv b$ (mód. m) tiene exactamente d soluciones.

Veamos dos ejemplos.

- Resolver la congruencia $16x \equiv 10$ (mód. 4).

Se tiene $(16, 4) = 4$. Como $4 \nmid 10$, la congruencia no tiene soluciones.

- Resolver la congruencia $16x \equiv 10$ (mód. 10).

$(16, 10) = 2$. Como $2 \mid 4$, la congruencia tiene dos soluciones.

Debemos resolver: $8x \equiv 2$ (mód. 5).

Por inspección en un sistema completo de restos módulo 5 se observa que esta última congruencia tiene la solución:

$$x \equiv 4 \pmod{5},$$

luego las soluciones de $16x \equiv 4$ (mód. 10) vienen dadas por los enteros: $x_0 = 4 + 5k$. Dando a k los valores 0 y 1 (por cuanto $d = 2$) se tiene que las dos soluciones de la congruencia son $x \equiv 4$ (mód. 10) y $x \equiv 9$ (mód. 10).

Cuando el módulo es pequeño, es fácil encontrar la solución de la congruencia, como en el ejemplo anterior. Si el valor de m es grande, este procedimiento puede no resultar práctico; en este caso obsérvese que resolver la congruencia $ax \equiv b$ (mód. m) es equivalente a resolver la ecuación diofántica $ax - b = my$, y restringir nuestra atención a los valores de x . En el ejemplo anterior, si resolvemos por el método usual la ecuación diofántica $8x - 5y = 2$, obtendremos los mismos valores para x .

Si el módulo m es un número compuesto, $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, de acuerdo con la propiedad 8.10. resolver la congruencia $ax \equiv b$ (mód. m) es equivalente a resolver el sistema de congruencias:

$$ax \equiv b \pmod{p_1^{\alpha_1}},$$

$$ax \equiv b \pmod{p_2^{\alpha_2}},$$

⋮

$$ax \equiv b \pmod{p_k^{\alpha_k}},$$

donde los números $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ son menores que m y, por tanto, los cálculos se pueden facilitar. Hay varias formas de resolver un sistema como el anterior. El siguiente resultado nos garantiza que, efectivamente, un sistema de congruencias como el anterior tiene soluciones comunes y nos brinda un método para hallarlas.

11.2. Teorema Chino del Resto. Consideremos k enteros positivos m_1, m_2, \dots, m_k primos dos a dos. Las congruencias

$$x \equiv a_1 \pmod{m_1},$$

$$x \equiv a_2 \pmod{m_2},$$

⋮

$$x \equiv a_k \pmod{m_k},$$

tienen soluciones comunes. Dos soluciones cualesquiera son congruentes entre sí módulo $m_1 m_2 \dots m_k$.

En efecto, si $j = 1, 2, \dots, k$ y $m = m_1 m_2 \dots m_k$, entonces $\frac{m}{m_j}$ es un entero tal que $\left(\frac{m}{m_j}, m\right) = 1$. Por consiguiente, la congruencia $\frac{m}{m_j}x \equiv 1$ (mód. m_j) tiene una solución $x \equiv b_j$ (mód. m_j).

Además, si $i \neq j$ entonces $m_i \mid \frac{m}{m_j}$, luego,

$$\frac{m}{m_j}b_j \equiv 1 \pmod{m_j},$$

$$\frac{m}{m_j}b_j \equiv 0 \pmod{m_i} \text{ si } i \neq j.$$

Consideremos:

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \dots + \frac{m}{m_k} b_k a_k.$$

Entonces, $x_0 \equiv \frac{m}{m_i} b_i a_i$ (mód. m_i) para todo $i = 1, \dots, k$, es decir, x_0 es una solución común del sistema de congruencias. Además, la propiedad 8.10. garantiza que si x_1 es otra solución común de las congruencias, entonces $x_0 \equiv x_1$ (mód. $m_1 m_2 \dots m_k$).

Veamos a continuación dos ejemplos.

- Hallar todos los enteros que dejan restos 1, 2, 3 cuando se dividen por 3, 4 y 5 respectivamente.

Se requiere resolver el sistema:

$$x \equiv 1 \pmod{3},$$

$$x \equiv 2 \pmod{4},$$

$$x \equiv 3 \pmod{5}.$$

De acuerdo con la notación que se ha utilizado, se tiene:

$$a_1 = 1, a_2 = 2, a_3 = 3,$$

$$m_1 = 3, m_2 = 4, m_3 = 5, m = 60,$$

$$\frac{m}{m_1} = 20, \frac{m}{m_2} = 15, \frac{m}{m_3} = 12.$$

En las expresiones $\frac{m}{m_j} b_j \equiv 1$ (mód. m_j) determinamos valores particulares para b_1, b_2 y b_3 :

$$20b_1 \equiv 1 \pmod{3} \implies b_1 = -1,$$

$$15b_2 \equiv 1 \pmod{4} \implies b_2 = -1,$$

$$12b_3 \equiv 1 \pmod{5} \implies b_3 = -2.$$

Por tanto,

$$x_0 = 20(-1).1 + 15(-1).2 + 12(-2).3 = -20 - 30 - 72 = -122 \equiv -2 \pmod{60}.$$

$$x \equiv -2 \pmod{60}.$$

- Hallar todos los enteros que dejan restos 2 ó 3 cuando se dividen por 4, 5 ó 7.
Se trata de hallar todos los enteros x tales que, simultáneamente:

$$\begin{cases} x \equiv 2 \pmod{4} \\ \text{ó} \\ x \equiv 3 \pmod{4}, \end{cases} \quad \begin{cases} x \equiv 2 \pmod{5} \\ \text{ó} \\ x \equiv 3 \pmod{5}, \end{cases} \quad \begin{cases} x \equiv 2 \pmod{7} \\ \text{ó} \\ x \equiv 3 \pmod{7}. \end{cases}$$

Entonces: $m_1 = 4, m_2 = 5, m_3 = 7, m = 140$,

$$\frac{m}{m_1} = 35, \frac{m}{m_2} = 28, \frac{m}{m_3} = 20,$$

$$35b_1 \equiv 1 \pmod{4} \Rightarrow b_1 = -1,$$

$$28b_2 \equiv 1 \pmod{5} \Rightarrow b_2 = 2,$$

$$20b_3 \equiv 1 \pmod{7} \Rightarrow b_3 = -1.$$

$$x \equiv -35a_1 + 56a_2 - 20a_3 \pmod{140}.$$

Como a_1, a_2, a_3 pueden tomar los valores 2 ó 3, se presentan ocho casos, los cuales se resumen en la siguiente tabla.

a_1	a_2	a_3	$x \pmod{140}$
2	2	2	2
2	2	3	-18
2	3	2	58
2	3	3	38
3	2	2	-33
3	2	3	-53
3	3	2	23
3	3	3	3

Problemas.

11.1. ¿Para cuáles valores de x es $(5x+1)(3x+2)$ divisible por 15?

11.2. Hallar todos los enteros que dejan restos 1 ó 2 cuando se dividen por 3, 4 ó 5.

11.3. Resolver la congruencia $x^2 - 1 \equiv 0 \pmod{56}$.

11.4. Resolver la congruencia $11x + 1 \equiv 0 \pmod{210}$.

11.5. Resolver la congruencia $5x^2 + 7x - 3 \equiv 0 \pmod{35}$.

11.6. Si $k > 0$, entonces existen k enteros consecutivos, cada uno de los cuales es divisible por un cuadrado mayor que 1.

SECCION 12

EL INDICADOR DE EULER

En la sección 8 hemos definido al indicador de Euler, $\phi(m)$, como el número de elementos de un sistema reducido de restos módulo m , y hemos visto que éste es el número de enteros positivos menores o iguales que m que son primos con m .

En la presente sección, con el auxilio del teorema chino del resto, deduciremos una fórmula que nos permitirá calcular directamente el valor de $\phi(m)$. Para esto, establecemos el siguiente resultado previo.

12.1. Sean m, n dos enteros positivos tales que $(m, n) = 1$. Entonces, $\phi(mn) = \phi(m)\phi(n)$.

Nota. Toda función $f : \mathbb{Z}^+ \rightarrow C$, donde C es el conjunto de los números complejos, se llama *función aritmética*. Se dice que una función aritmética es *multiplicativa* si, siempre que $(m, n) = 1$ se tiene $f(mn) = f(m)f(n)$. 12.1 establece que la función que a cada $m \in \mathbb{Z}^+$ le asigna $\phi(m)$, es multiplicativa.

Para probar 12.1., supongamos que $R = \{r_1, r_2, \dots, r_{\phi(m)}\}$ es un sistema reducido de restos módulo m y $S = \{s_1, s_2, \dots, s_{\phi(n)}\}$ un sistema reducido de restos módulo n . Si x es un entero que pertenece a un sistema reducido de restos módulo mn entonces $(x, mn) = 1$ y, por consiguiente, $(x, m) = (x, n) = 1$. Por tanto, existen $r_i \in R$ y $s_j \in S$ tales que

$$\begin{aligned} x &\equiv r_i \pmod{m}, \\ x &\equiv s_j \pmod{n}. \end{aligned}$$

Por otra parte, de acuerdo con el teorema chino del resto, cada par (r_i, s_j) determina un único x módulo mn y, evidentemente, diferentes pares (r_i, s_j) determinan diferentes x módulo mn . Ahora bien, hay exactamente $\phi(m)\phi(n)$ de tales pares, luego un sistema reducido de restos módulo mn contiene $\phi(m)\phi(n)$ elementos, y se tiene:

$$\phi(mn) = \phi(m)\phi(n),$$

conforme se quería demostrar.

Es inmediato generalizar, por inducción, este resultado para cualquier número finito de enteros; es decir, si m_1, m_2, \dots, m_k son enteros positivos primos dos a dos, se tiene:

$$\phi(m_1 m_2 \dots m_k) = \phi(m_1)\phi(m_2)\dots\phi(m_k).$$

Por ejemplo, si queremos calcular $\phi(210)$ basta observar que $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Entonces,

$$\phi(210) = \phi(2)\phi(3)\phi(5)\phi(7) = 1 \cdot 2 \cdot 4 \cdot 6 = 48.$$

Nótese que esta propiedad es válida sólo si los m_i son primos dos a dos. Por ejemplo se tiene:

$$\phi(9) = 6,$$

pero

$$\phi(3)\phi(3) = 2 \cdot 2 = 4.$$

Evidentemente, $\phi(1) = 1$. Si n es un entero mayor que 1, entonces se verifica el siguiente resultado.

12.2. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, entonces:

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

En efecto, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, como los $p_i^{\alpha_i}$ son primos dos a dos se puede aplicar el teorema 12.1., y se tiene:

$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k}).$$

Entonces, el problema se reduce a calcular el valor de $\phi(p^\alpha)$, donde p es un número primo y α un entero positivo. Para esto, notamos que $\phi(p^\alpha)$ es el número de enteros positivos que son menores o iguales que p^α y, a la vez, primos con p^α . Estos son todos los enteros menores o iguales que p^α exceptuando los múltiplos de p : $p, 2p, 3p, \dots, p^{\alpha-1}p$. Luego, entre 1 y p^α hay exactamente $p^{\alpha-1}$ múltiplos de p y, en consecuencia:

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

Por consiguiente,

$$\begin{aligned} \phi(n) &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) = \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) = \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right), \end{aligned}$$

conforme se quería demostrar.

Por ejemplo, si queremos calcular $\phi(3600)$, en primer lugar escribimos 3600 en su forma canónica. Se tiene:

$$3600 = 2^4 \cdot 3^2 \cdot 5^2.$$

Entonces,

$$\begin{aligned} \phi(3600) &= 3600 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = \\ &= 3600 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 960. \end{aligned}$$

Nota. Frecuentemente se usa la notación $\prod_{p|n}$ para indicar el producto sobre todos los primos que dividen a n . Si n , escrito en su forma canónica, es $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, entonces $\prod_{p|n} p = p_1 p_2 \dots p_k$; es decir $\prod_{p|n} p = \prod_{i=1}^k p_i$. Utilizando esta notación en el teorema 12.2., se tiene:

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

También es corriente encontrar la notación $\sum_{d|n}$ para indicar la suma sobre todos los divisores de n (sean estos primos o no). Por ejemplo,

$$\sum_{d|24} d = 1 + 2 + 3 + 4 + 6 + 8 + 12 + 24 = 60.$$

Esta notación resultará útil en el siguiente teorema.

12.3. Si $n \geq 1$, entonces $\sum_{d|n} \phi(d) = n$.

Haremos la demostración por inducción sobre el número de factores primos de n . Si $n = p^\alpha$ se tiene:

$$\begin{aligned} \sum_{d|n} \phi(d) &= \phi(1) + \phi(p) + \phi(p^2) + \dots + \phi(p^\alpha) = \\ &= 1 + (p - 1) + (p^2 - p) + \dots + (p^\alpha - p^{\alpha-1}) = \\ &= p^\alpha = n. \end{aligned}$$

Supongamos que la propiedad es cierta para todos los enteros que tienen k o menos factores primos diferentes en su descomposición canónica y consideremos un entero m con $k + 1$ factores primos diferentes. Entonces

$$m = np^\alpha,$$

donde p^α es uno de los factores que aparecen en la descomposición canónica de m , n tiene k factores primos diferentes y $(n, p^\alpha) = 1$.

Obsérvese que si d es un divisor de n , entonces $d, pd, p^2d, \dots, p^\alpha d$ son divisores de m ;

por consiguiente, se puede escribir:

$$\begin{aligned}
 \sum_{d|m} \phi(d) &= \sum_{d|n} \phi(d) + \sum_{d|n} \phi(pd) + \sum_{d|n} \phi(p^2d) + \dots + \sum_{d|n} \phi(p^\alpha d) = \\
 &= \sum_{d|n} \phi(d) + \sum_{d|n} \phi(p)\phi(d) + \sum_{d|n} \phi(p^2)\phi(d) + \dots + \sum_{d|n} \phi(p^\alpha)\phi(d) = \\
 &= \sum_{d|n} \phi(d)[1 + \phi(p) + \phi(p^2) + \dots + \phi(p^\alpha)] = \\
 &= \sum_{d|n} \phi(d)[1 + (p-1) + (p^2-p) + \dots + (p^\alpha - p^{\alpha-1})] = \\
 &= np^\alpha = m.
 \end{aligned}$$

Por tanto, la propiedad es cierta para todo entero positivo n . Por ejemplo, los divisores positivos de 24 son:

$$1, 2, 3, 4, 6, 8, 12 \text{ y } 24$$

y se tiene:

$$\begin{aligned}
 \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(8) + \phi(12) + \phi(24) &= \\
 = 1 + 1 + 2 + 2 + 2 + 4 + 4 + 8 &= 24.
 \end{aligned}$$

Problemas.

12.1. Hallar el número de enteros positivos menores o iguales que 3600 que tienen un factor común con 3600.

12.2. Si p es un número primo y n un entero positivo, entonces

$$\phi(np) = \begin{cases} p\phi(n) & \text{si } p|n, \\ (p-1)\phi(n) & \text{si } p \nmid n. \end{cases}$$

12.3. Si $n|m$, entonces $\phi(nm) = n\phi(m)$.

12.4. ¿Para cuáles valores de n es $\phi(n)$ impar?

12.5. ¿Para cuáles valores de n es

- a) $\phi(2n) = \phi(n)$,
- b) $\phi(2n) > \phi(n)$?

12.6. Probar que existen infinitos enteros n tales que

$$3 \nmid \phi(n).$$

12.7. Hallar el número de enteros positivos menores o iguales que 25200 que son primos con 3600.

12.8. Si m y k son enteros positivos, probar que el número de enteros positivos menores o iguales que mk que son primos con m es $k\phi(m)$.

12.9. Sea g una función aritmética multiplicativa. La función f definida por $f(n) = \sum_{d|n} g(d)$ para todo entero positivo n , es también multiplicativa.

12.10. Sea $n > 1$. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ en su forma canónica, entonces la suma de los divisores de n es:

$$\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

SOLUCIONES A LOS PROBLEMAS PROPUESTOS

Sección 1.

1.1. $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$

Si $n = 1$ se tiene:

$$1^2 = \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6},$$

lo cual obviamente es cierto.

Supongamos ahora que:

$$\dots 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}. \quad (1)$$

Debemos probar que:

$$1^2 + 2^2 + 3^2 + \dots + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

Sumando $(n+1)^2$ al primer miembro de (1) y usando la hipótesis de inducción:

$$\begin{aligned} (1^2 + 2^2 + \dots + n^2) + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} = \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)2(n+2)(n+\frac{3}{2})}{6} = \frac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$

1.2. $\sum_{i=1}^n i^3 = \left[\frac{n(n+1)}{2} \right]^2$

Si $n = 1$ se verifica:

$$1^3 = \left[\frac{1 \cdot (1+1)}{2} \right]^2$$

Supongamos que:

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2. \quad (1)$$

Debemos probar que:

$$1^3 + 2^3 + 3^3 + \dots + (n+1)^3 = \left[\frac{(n+1)(n+2)}{2} \right]^2.$$

Sumando $(n+1)^3$ a ambos miembros de (1) se tiene:

$$\begin{aligned}(1^3 + 2^3 + 3^3 + \dots + n^3) + (n+1)^3 &= \left[\frac{n(n+1)}{2} \right]^2 + (n+1)^3 = \\ &= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2(n^2 + 4n + 4)}{4} = \frac{(n+1)^2(n+2)^2}{4} = \\ &= \left[\frac{(n+1)(n+2)}{2} \right]^2.\end{aligned}$$

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

Si $n = 1$ se verifica:

$$2 - 1 = 1^2.$$

Supongamos que:

$$1 + 3 + 5 + 7 + \dots + (2n-1) = n^2. \quad (1)$$

Debemos probar que:

$$1 + 3 + 5 + 7 + \dots + (2n-1) + (2n+1) = (n+1)^2.$$

Sumando $(2n+1)$ a ambos miembros de (1) se tiene:

$$[1 + 3 + 5 + 7 + \dots + (2n-1)] + (2n+1) = n^2 + (2n+1) = (n+1)^2.$$

1.4. $\sum_{i=1}^n i(i+1) = \frac{1}{3}n(n+1)(n+2).$

Si $n = 1$ se verifica:

$$1 \cdot 2 = \frac{1}{3} \cdot 1 \cdot 2 \cdot 3.$$

Supongamos que:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{1}{3}n(n+1)(n+2). \quad (1)$$

Debemos probar que:

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) + (n+1)(n+2) = \frac{1}{3}(n+1)(n+2)(n+3).$$

Sumando $(n+1)(n+2)$ a ambos miembros de (1) se tiene:

$$\begin{aligned}[1.2 + 2.3 + 3.4 + \dots + n(n+1)] + (n+1)(n+2) &= \\ = \frac{1}{3}n(n+1)(n+2) + (n+1)(n+2) &= \\ = (n+1)(n+2)\left(\frac{1}{3}n + 1\right) &= (n+1)(n+2)\left(\frac{n+3}{3}\right) = \\ = \frac{1}{3}(n+1)(n+2)(n+3). &\end{aligned}$$

1.5. $\sum_{i=1}^n (3i-2) = \frac{n(3n-1)}{2}$.

Si $n = 1$ se verifica:

$$3 - 2 = \frac{1.(3-1)}{2}.$$

Supongamos que:

$$1 + 4 + 7 + 10 + \dots + (3n-2) = \frac{n(3n-1)}{2}. \quad (1)$$

Debemos probar que:

$$1 + 4 + 7 + 10 + \dots + (3n-2) + (3n+1) = \frac{(n+1)(3n+2)}{2}.$$

Sumando $(3n+1)$ a ambos miembros de (1) se tiene:

$$\begin{aligned}[1 + 4 + 7 + 10 + \dots + (3n-2)] + (3n+1) &= \frac{n(3n-1)}{2} + 3n+1 = \\ = \frac{n(3n-1) + 2(3n+1)}{2} &= \frac{3n^2 + 5n + 2}{2} = \\ = \frac{3(n+1)(n+\frac{2}{3})}{2} &= \frac{(n+1)(3n+2)}{2}.\end{aligned}$$

1.6. $2n^2 > (n+1)^2$ para todo entero $n \geq 3$.

Si $n = 3$ se verifica:

$$2.3^2 > (3+1)^2, \text{ por cuanto } 18 > 16.$$

Supongamos que, para un $n \geq 3$ se tiene:

$$2n^2 > (n+1)^2. \quad (1)$$

Debemos probar que:

$$2(n+1)^2 > (n+2)^2.$$

En efecto:

$$2(n+1)^2 = 2(n^2 + 2n + 1) = 2n^2 + 4n + 2,$$

y tomando en cuenta (1):

$$\begin{aligned} 2(n+1)^2 &> (n+1)^2 + 4n + 2 = n^2 + 2n + 1 + 4n + 2 = \\ &= n^2 + 4n + 4 + 2n - 1 = \\ &= (n+2)^2 + 2n - 1 > (n+2)^2. \end{aligned}$$

1.7. $2^n > n^2$ para todo entero $n > 4$.

Si $n = 5$ se verifica:

$$2^5 > 5^2, \text{ por cuanto } 32 > 25.$$

Supongamos que, para un $n > 4$ se tiene:

$$2^n > n^2$$

(1)

Debemos probar que:

$$2^{n+1} > (n+1)^2.$$

De acuerdo con (1), y dado que $2^{n+1} = 2 \cdot 2^n$, se tiene:

$$2^{n+1} > 2n^2,$$

luego, bastará probar que:

$$2n^2 > (n+1)^2.$$

En efecto, como $n > 4$ se tiene:

$$n(n-2) > 1,$$

de donde:

$$n^2 > 2n + 1,$$

$$2n^2 > n^2 + 2n + 1,$$

$$2n^2 > (n+1)^2.$$

1.8. El número de diagonales de un polígono de n lados es:

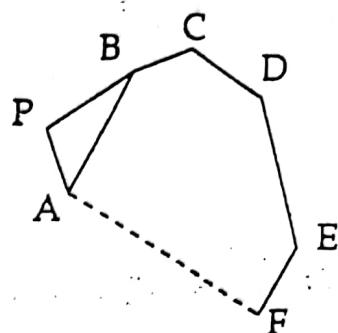
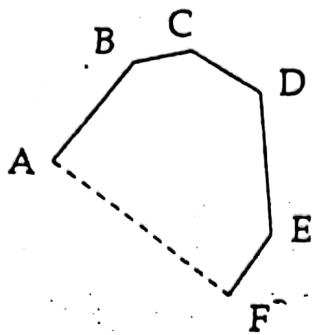
$$\frac{n(n-3)}{2}.$$

Iniciemos la inducción con $n = 3$ (no hay polígonos con menor número de lados). En este caso:

$$\frac{n(n-3)}{2} = \frac{3(3-3)}{2} = 0,$$

y efectivamente, un triángulo no tiene ninguna diagonal.

Consideremos un polígono de n lados, $ABCDEF \dots$, como se muestra en la figura, en donde la línea punteada representa los $n - 5$ lados restantes. Supongamos que este polígono tiene $\frac{n(n-3)}{2}$ lados.



Si le añadimos un lado, como cuando formamos el polígono $APBCDEF \dots$, el nuevo polígono tiene las diagonales del polígono anterior, más el lado \overline{AB} que ha pasado a ser una nueva diagonal, más $n - 2$ diagonales que se originan al unir el punto P con los $n - 2$ vértices no adyacentes; por tanto, el polígono de $n + 1$ lados tiene:

$$\begin{aligned} \frac{n(n-3)}{2} + n - 1 &= \frac{n(n-3) + 2(n-1)}{2} = \\ &= \frac{n^2 - n - 2}{2} = \frac{(n+1)(n-2)}{2} \text{ diagonales.} \end{aligned}$$

1.9. La suma de los ángulos interiores de un polígono de n lados es $(n-2)\pi$.

Al igual que en el problema 1.8., iniciamos la inducción con $n = 3$. En este caso, la suma de los ángulos interiores de un triángulo es justamente $(3-2)\pi = \pi$. Consideremos la misma figura utilizada en el problema 1.8. Si la suma de los ángulos interiores del polígono $ABCDEF \dots$ mide $(n-2)\pi$, al formar el polígono $APBCDEF \dots$ agregamos la suma de los ángulos interiores del triángulo ABP , luego la suma de los ángulos interiores del nuevo polígono mide:

$$(n-2)\pi + \pi = (n-2+1)\pi = (n-1)\pi.$$

1.10. $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$, donde $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.

Si $n = 0$, entonces $(a+b)^n = (a+b)^0 = 1$ y, además,

$$\sum_{i=0}^n \binom{n}{i} a^{n-i} b^i = \binom{0}{0} a^0 b^0 = 1.$$

Supongamos la propiedad cierta para n , esto es:

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Al multiplicar ambos miembros por $(a + b)$ se tiene:

$$(a + b)^{n+1} = \sum_{i=0}^n \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^n \binom{n}{i} a^{n-i} b^{i+1}.$$

Obsérvese que, en general, al multiplicar el término

$$\binom{n}{i+1} a^{n-i-1} b^{i+1}$$

por a , resulta

$$\binom{n}{i+1} a^{n-i} b^{i+1}, \quad (1)$$

mientras que al multiplicar el término

$$\binom{n}{i} a^{n-i} b^i$$

por b , resulta

$$\binom{n}{i} a^{n-i} b^{i+1} \quad (2)$$

y al sumar los dos términos semejantes (1) y (2) nos queda:

$$\left[\binom{n}{i+1} + \binom{n}{i} \right] a^{n-i} b^{i+1} = \binom{n+1}{i+1} a^{n-i} b^{i+1},$$

ya que la suma de dos números combinatorios del mismo numerador y órdenes consecutivos, es otro número combinatorio cuyo numerador es una unidad mayor y cuyo orden es el del sumando de mayor orden.

Por tanto, nos queda:

$$\begin{aligned} (a + b)^{n+1} &= \binom{n}{0} a^{n+1} + \binom{n+1}{1} a^n b + \binom{n+1}{2} a^{n-1} b^2 + \dots + \\ &+ \binom{n+1}{n-1} a^2 b^{n-1} + \binom{n+1}{n} a b^n + \binom{n}{n} b^{n+1}, \end{aligned}$$

y como $\binom{n}{0} = \binom{n+1}{0}$, $\binom{n}{n} = \binom{n+1}{n+1}$, se puede escribir:

$$(a + b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i} b^i,$$

conforme queríamos demostrar.

Sección 2.

2.1. Dados dos enteros, a y b , se pueden presentar tres casos: ambos son pares, ambos son impares, o uno de ellos es par y el otro impar. Consideremos cada uno de estos casos.

a) Si $a = 2k_1$ y $b = 2k_2$, entonces $a + b = 2(k_1 + k_2)$ y $a - b = 2(k_1 - k_2)$, luego $a + b$ y $a - b$ son ambos pares.

b) Si $a = 2k_1 + 1$ y $b = 2k_2 + 1$, entonces $a + b = 2(k_1 + k_2 + 1)$ y $a - b = 2(k_1 - k_2)$, por tanto, en este caso $a + b$ y $a - b$ son también ambos pares.

c) Si $a = 2k_1$ y $b = 2k_2 + 1$, entonces $a + b = 2(k_1 + k_2) + 1$ y $a - b = 2(k_1 - k_2) - 1$, de manera que ambos son impares. El mismo resultado se obtiene si a es impar y b es par, luego la suma y la diferencia de dos enteros siempre tienen la misma paridad.

2.2. Si $ac|bc$ entonces existe un entero x tal que:

$$bc = (ac)x,$$

de donde:

$$\begin{aligned} bc &= (ax)c, \\ b &= ax, \end{aligned}$$

luego:

$$a|b.$$

2.3. Si $a|b$ entonces existe un entero x tal que

$$b = ax. \quad (1)$$

Similarmente, si $c|d$ entonces existe un entero y tal que

$$d = cy. \quad (2)$$

Multiplicando miembro a miembro (1) y (2) se tiene:

$$\begin{aligned} bd &= (ax)(cy), \\ bd &= (ac)(xy), \end{aligned}$$

luego:

$$ac|bd.$$

2.4. Si $n = 2k$ entonces $n^2 + 2 = 4k^2 + 2$. $4k^2$ es múltiplo de 4, luego si $4k^2 + 2$ fuese divisible por 4, también lo sería $4k^2 + 2 - 4k^2 = 2$. Por tanto, si n es par entonces $4 \nmid n^2 + 2$.

Si $n = 2k + 1$ entonces $n^2 + 2 = 4k^2 + 4k + 1 + 2 = 4(k^2 + k) + 3$. Con un razonamiento similar al anterior se concluye que, como $4 \nmid 3$, entonces $4 \nmid n^2 + 2$ si n es impar.

2.5. Basta factorizar:

$$n^k - 1 = (n - 1)(n^{k-1} + n^{k-2} + \dots + n + 1).$$

Nota. Conviene recordar las identidades:

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

para todo entero n , y, si n es impar:

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

2.6. Escribamos:

$$n^k = [(n - 1) + 1]^k.$$

Entonces se tiene:

$$n^k = \binom{k}{0}(n - 1)^k + \binom{k}{1}(n - 1)^{k-1} + \dots + \binom{k}{k-1}(n - 1) + \binom{k}{k},$$

$$n^k - 1 = (n - 1)^2 \left[\binom{k}{0}(n - 1)^{k-2} + \binom{k}{1}(n - 1)^{k-3} + \dots + \binom{k}{k-2} \right] + k(n - 1),$$

por consiguiente, $(n - 1)^2|(n^k - 1)$ si y sólo si $(n - 1)^2|k(n - 1)$, esto es, si y sólo si existe un entero x tal que

$$\begin{aligned} k(n - 1) &= (n - 1)^2 x, \\ k &= (n - 1)x, \end{aligned}$$

luego, $(n - 1)^2|(n^k - 1)$ si y sólo si $(n - 1)|k$.

2.7. Se pueden presentar tres casos:

a) Si $n = 3k$, entonces $n^2 = 9k^2 = 3k_1$, donde $k_1 = 3k^2$.

b) Si $n = 3k + 1$, entonces $n^2 = 9k^2 + 6k + 1 = 3k_2 + 1$, donde $k_2 = 3k^2 + 2k$.

c) Si $n = 3k + 2$, entonces $n^2 = 9k^2 + 12k + 4 = 3k_3 + 1$, donde $k_3 = 3k^2 + 4k + 1$.

Por consiguiente, todo cuadrado perfecto es de la forma $3k$ o de la forma $3k + 1$.

2.8. Si $n = 6k + 5$, entonces:

$$n = 6k + 6 - 1 = 3(2k + 2) - 1 = 3k_1 - 1 \text{ donde } k_1 = 2k + 2.$$

El recíproco no es cierto. Por ejemplo, $2 = 3 \cdot 1 - 1$ es de la forma $3k - 1$ pero no es de la forma $6k + 5$ (de hecho, es de la forma $6k + 2$, tomando $k = 0$). Nótese que todo número de la forma $3k - 1$ es de la forma $3k + 2$.

2.9. Si $n = 5k + 1$, entonces

$$n^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1 = 5k_1 + 1,$$

donde $k_1 = 5k^2 + 2k$.

2.10. Sean $m = 2k_1 + 1, n = 2k_2 + 1$.

a)

$$\begin{aligned}m^2 - n^2 &= (m + n)(m - n) = (2k_1 + 2k_2 + 2)(2k_1 - 2k_2) = \\&= 4(k_1 + k_2 + 1)(k_1 - k_2).\end{aligned}$$

Ahora bien, como $k_1 - k_2$ y $k_1 + k_2$ tienen la misma paridad, el número $(k_1 + k_2 + 1)(k_1 - k_2)$ es de la forma $2k$, luego $8|(m^2 - n^2)$.

b)

$$\begin{aligned}m^4 + n^4 - 2 &= m^4 - 2m^2n^2 + n^4 + 2m^2n^2 - 2 = \\&= (m^2 - n^2)^2 + 2(m^2n^2 - 1).\end{aligned}$$

En (a) hemos visto que $8|(m^2 - n^2)$, luego basta probar que $4|(m^2n^2 - 1)$, es decir, que m^2n^2 es de la forma $4k + 1$. En efecto:

$$\begin{aligned}m^2n^2 &= (4k_1^2 + 4k_1 + 1)(4k_2^2 + 4k_2 + 1) = \\&= (4k_3 + 1)(4k_4 + 1) = \\&= 16k_3k_4 + 4k_3 + 4k_4 + 1 = 4k_5 + 1,\end{aligned}$$

donde hemos hecho: $k_3 = k_1^2 + k_1, k_4 = k_2^2 + k_2, k_5 = 4k_3k_4 + k_3 + k_4$.

2.11. De acuerdo con el algoritmo de la división, si se divide a entre n entonces existen enteros q_0, a_0 tales que

$$a = q_0n + a_0, \quad 0 \leq a_0 < n.$$

Si $a_0 = 0$, hemos terminado. De lo contrario, se aplica nuevamente el algoritmo y se tiene una secuencia de igualdades:

$$q_0 = q_1n + a_1, \quad 0 < a_1 < n,$$

$$q_1 = q_2n + a_2, \quad 0 < a_2 < n,$$

⋮

$$q_{k-3} = q_{k-2}n + a_{k-2}, \quad 0 < a_{k-2} < n,$$

$$q_{k-2} = q_{k-1}n + a_{k-1}, \quad 0 < a_{k-1} < n,$$

en la cual los q_i van decreciendo estrictamente basta que uno de ellos será menor que n , y se tiene:

$$q_{k-1} = a_k.$$

En esta secuencia, podemos despejar a de la siguiente manera:

$$\begin{aligned} q_{k-2} &= a_k n + a_{k-1}, \\ q_{k-3} &= a_k n^2 + a_{k-1} n + a_{k-2}, \end{aligned}$$

⋮

$$q_1 = a_k n^{k-2} + a_{k-1} n^{k-3} + \dots + a_3 n + a_2,$$

$$q_0 = a_k n^{k-1} + a_{k-1} n^{k-2} + \dots + a_3 n^2 + a_2 n + a_1,$$

$$a = a_k n^k + a_{k-1} n^{k-1} + \dots + a_2 n^2 + a_1 n + a_0.$$

Nota. Si $n = 10$, esta es la representación de a en el sistema decimal de numeración (base 10). Se escribe:

$$a = a_k a_{k-1} \dots a_2 a_1 a_0.$$

(Generalmente el contexto evita que haya confusión con la notación de la multiplicación.) Si $n = 2$, la base se llama binaria. Si $n = 16$, la base se llama hexadecimal. Por ejemplo

$$35_{10} = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 = 100011_2 = 2 \cdot 16 + 3 = 23_{16}.$$

2.12. Para $n = 1$ se tiene:

$$A_1 = 5 + 2 \cdot 3^0 + 1 = 8.$$

Supongamos que $8 \mid A_n$.

$$\begin{aligned} A_{n+1} &= 5^{n+1} + 2 \cdot 3^n + 1, \\ A_{n+1} - A_n &= 5^{n+1} + 2 \cdot 3^n + 1 - 5^n - 2 \cdot 3^{n-1} - 1 = \\ &= 5^n \cdot (5 - 1) + 3^{n-1} \cdot (6 - 2) = 4 \cdot (5^n + 3^{n-1}). \end{aligned}$$

Como 5^n y 3^{n-1} son impares, su suma es par, luego $8 \mid (A_{n+1} - A_n)$, y como $8 \mid A_n$ entonces $8 \mid A_{n+1}$.

2.13. Si en la identidad:

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

hacemos $a = 2$ y $b = -1$, se tiene:

$$2^n - (-1)^n = [(2 - (-1))k] = 3k,$$

donde k es un entero. Por consiguiente,

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

Por tanto, si n es impar entonces $2^n + 1$ es de la forma $3k$, pero si n es par entonces $2^n + 1$ es de la forma $3k + 2$. Por ende, $2^n + 1$ es divisible por 3 si y sólo si n es impar.

2.14. Se tiene:

$$4^n = (3 + 1)^n,$$

de donde,

$$4^n = \binom{n}{0} 3^n + \binom{n}{1} 3^{n-1} + \dots + \binom{n}{n-1} 3 + 1.$$

Luego 4^n es un entero de la forma $3k + 1$ y $4^n + 1$ es de la forma $3k + 2$. Por tanto, $3 \nmid (4^n + 1)$.

2.15. Se tiene:

$$n^3 + 100 = n^3 + 1000 - 900 = (n + 10)(n^2 - 10n + 100) - 900.$$

Luego, si $(n + 10)|(n^3 + 100)$ entonces $(n + 10)|900$.

El mayor divisor de 900 es 900, luego el mayor valor para $n + 10$ es 900 y el mayor valor que puede tomar n es 890.

2.16. Si n fuese impar, entonces a_1, a_2, \dots, a_n tendrían que ser todos impares; pero la suma de un número impar de números impares es impar y, por lo tanto, diferente de 0. Por consiguiente, n es par y en consecuencia alguno de los a_i también lo es.

Sea a_k el término par. Entonces,

$$a_1 + a_2 + \dots + a_{k-1} + a_{k+1} + \dots + a_n = -a_k.$$

Como en el primer miembro hay un número impar de términos que sumados dan un número par, alguno de ellos debe ser par. Si a_j es el otro término par, en el producto

$$a_1 a_2 \dots a_n = n$$

hay dos factores pares, a_k y a_j ; por tanto n es divisible por 4.

2.17. Si n es impar se tiene:

$$a_n = (7 - 1)^n + (7 + 1)^n,$$

$$\begin{aligned} a_n &= \left[7^n - \binom{n}{1} 7^{n-1} + \dots - 1 \right] + \left[7^n + \binom{n}{1} 7^{n-1} + \dots + 1 \right] = \\ &= 2 \left[7^n + \binom{n}{2} 7^{n-2} + \dots + \binom{n}{n-3} 7^3 + \binom{n}{n-1} 7 \right] = \\ &= 2 \cdot 49 \left[7^{n-2} + \binom{n}{2} 7^{n-4} + \dots + \binom{n}{n-3} 7 \right] + 14n. \end{aligned}$$

Si $n = 1991$ se tiene:

$$a_{1991} = 49k + 14 \cdot 1991 = 49k + 27874.$$

Al dividir 27874 entre 49, el resto es 42.

2.18. Es necesario probar que al menos uno de los factores es par.

Si n es impar, entonces n es de la forma $2k + 1$, luego el producto tiene $2k + 1$ factores. Además, entre los números $1, 2, 3, \dots, n$ hay exactamente $k + 1$ impares ya que:

$$1 = 2 \cdot 1 - 1,$$

$$3 = 2 \cdot 2 - 1,$$

$$5 = 2 \cdot 3 - 1,$$

⋮

$$2k + 1 = 2(k + 1) - 1.$$

Luego, en los a_i hay también $k + 1$ números impares y entre los $2n$ números $1, 2, \dots, n, a_1, a_2, \dots, a_n$, habrá $2(k + 1) = 2k + 2 = n + 1$ números impares. Pero sólo hay n factores, luego al menos uno de los factores contiene dos números impares, cuya diferencia es un número par.

Nota. En el razonamiento anterior hemos empleado, tácitamente, un argumento extremadamente simple y útil que se conoce como *Principio de las Casillas*; éste establece que, si se colocan $n + 1$ objetos en n casillas, entonces al menos una de estas casillas debe contener más de un objeto.

2.19. Como n es par, n es de la forma $6k$ ó $6k + 2$ ó $6k + 4$. Ahora bien, para todo $k > 1$, $6k$ es abundante pues entre sus divisores diferentes se encuentran:

$$1, k, 2k, 3k, 6k$$

cuya suma es mayor que $2.6k$. Luego, si $n = 6k$ y $k \geq 4$ se tiene:

$$n = 6k = 6 \cdot 2 + 6(k - 2)$$

donde cada término es abundante.

Si $n = 6k + 2$ y $k \geq 5$, se tiene:

$$n = 6k + 2 = 6 \cdot 3 + 6(k - 3) + 2 = 20 + 6(k - 3)$$

donde 20 y $6(k - 3)$ son abundantes.

Si $n = 6k + 4$ y $k \geq 8$, se tiene:

$$n = 6k + 4 = 6 \cdot 6 + 6(k - 6) + 4 = 40 + 6(k - 6)$$

donde 40 y $6(k - 6)$ son abundantes. Esto completa la prueba.

2.20.

$$\begin{aligned} 2^{2^5} + 1 &= 2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = (641 - 5^4) \cdot 2^{28} + 1 = \\ &= 641 \cdot 2^{28} - (5^4 \cdot 2^{28} - 1) = 641 \cdot 2^{28} \cdot (5^2 \cdot 2^{14} + 1) \cdot (5^2 \cdot 2^{14} - 1) = \\ &= 641 \cdot 2^{28} - (5^2 \cdot 2^{14} + 1) \cdot (5 \cdot 2^7 + 1) \cdot (5 \cdot 2^7 - 1) = \\ &= 641 \cdot [2^{28} - (5^2 \cdot 2^{14} + 1) \cdot (5 \cdot 2^7 - 1)]. \end{aligned}$$

2.21. El entero m no es divisible por 5, ya que de lo contrario:

$$am^3 + bm^2 + cm + d = m(am^2 + bm + c) + d$$

sería divisible por 5 sólo si d fuese divisible por 5, en contra de nuestra hipótesis. Por consiguiente m es de la forma $5k + r$, donde r es un entero positivo menor que 5.

Sean:

$$A = am^3 + bm^2 + cm + d,$$

$$B = dn^3 + cn^2 + bn + a.$$

Eliminando d de estas expresiones, se tiene:

$$\begin{aligned} An^3 - B &= a(m^3n^3 - 1) + bn(m^2n^2 - 1) + cn^2(mn - 1) = \\ &= (mn - 1)[a(m^2n^2 + mn + 1) + bn(mn + 1) + cn^2]. \end{aligned}$$

Ahora bien, si $m = 5k + r$ es un entero tal que $5|A$, y si podemos seleccionar n de manera que el último miembro de la igualdad anterior sea divisible por 5, entonces B será divisible por 5.

Tomemos, para cada entero m que no sea divisible por 5, un entero n de manera que el factor $(mn - 1)$ sea divisible por 5.

Como $m = 5k + r$, $mn = 5kn + rn$, luego $mn - 1$ es divisible por 5 si $rn = 5k' + 1$. Por tanto, si $r = 1$, podemos tomar $n = 1$; si $r = 2$, podemos tomar $n = 3$; si $r = 3$, podemos tomar $n = 2$ y, si $r = 4$, podemos tomar $n = 4$. De esta manera, para cada m , hemos hallado un n tal que $mn - 1$ es divisible por 5 y, por consiguiente, la expresión B es divisible por 5.

Sección 3.

3.1. Si $a|c$ entonces existe un número entero x tal que

$$c = ax. \quad (1)$$

Si $b|c$, como $(a, b) = 1$, necesariamente $b|x$, luego existe un entero y tal que

$$x = by. \quad (2)$$

De (1) y (2) se deduce:

$$c = a(by),$$

$$c = (ab)y,$$

$$ab|c.$$

3.2. Tenemos que:

$$n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n - 1)n(n + 1)(n^2 + 1).$$

Como en la descomposición en factores de $n^5 - n$ aparecen tres enteros consecutivos, sabemos que $n^5 - n$ es divisible por 2 y por 3. Veamos que alguno de los cuatro factores: $(n - 1), n, (n + 1)$ ó $(n^2 + 1)$ es divisible por 5. Se presentan cinco casos posibles.

a) Si $n = 5k$, hemos terminado.

b) Si $n = 5k + 1$, entonces $n - 1 = 5k$.

c) Si $n = 5k + 2$, entonces

$$n^2 + 1 = 25k^2 + 20k + 4 + 1 = 5(5k^2 + 4k + 1) = 5k_1,$$

donde $k_1 = 5k^2 + 4k + 1$.

d) Si $n = 5k + 3$, entonces

$$n^2 + 1 = 25k^2 + 30k + 9 + 1 = 5(5k^2 + 6k + 2) = 5k_2,$$

donde $k_2 = 5k^2 + 6k + 2$.

e) Si $n = 5k + 4$, entonces $n + 1 = 5k + 5 = 5(k + 1) = 5k_3$, donde $k_3 = k + 1$.

En cualquiera de los casos $5|(n^5 - n)$. Como 2, 3 y 5 son primos dos a dos, en virtud del problema 3.1. se tiene que $n^5 - n$ es divisible por $2 \cdot 3 \cdot 5 = 30$.

3.3. Consideremos el producto $P = n(n + 1)(n + 2)(n + 3)$. Hemos visto que el mismo es divisible por 3, luego bastará probar que es divisible por 8. En efecto, consideremos los cuatro casos posibles:

a) Si $n = 4k$, entonces $n + 2 = 4k + 2$ y $n(n + 2) = 4k(4k + 2) = 8k(2k + 1)$.

b) Si $n = 4k + 1$, entonces $n + 1 = 4k + 2$ y $n + 3 = 4k + 4$, por tanto $(n + 1)(n + 3) = (4k + 2)(4k + 4) = 8(2k + 1)(k + 1)$.

c) Si $n = 4k + 2$, entonces $n + 2 = 4k + 4$, luego $n(n + 2) = (4k + 2)(4k + 4) = 8(2k + 1)(k + 1)$.

d) Si $n = 4k + 3$, entonces $n + 1 = 4k + 4$ y $n + 3 = 4k + 6$, de donde $(n + 1)(n + 3) = (4k + 4)(4k + 6) = 8(k + 1)(2k + 3)$.

Por consiguiente, $8|P$ en todos los casos posibles.

3.4. Sean $d = ((a, b), c)$ y $d' = (a, (b, c))$.

Si $d|(a, b)$ y $d|c$, entonces $d|a$, $d|b$ y $d|c$, luego $d|a$ y $d|(b, c)$, de donde $d|(a, (b, c))$, o sea $d|d'$ y por consiguiente $d \leq d'$ (1).

Por un razonamiento análogo se ve que $d' \leq d$ (2); de (1) y de (2) se tiene $d = d'$.

3.5. Si $(x, y) = 3$, entonces $3|(x+y)$, por tanto $x+y \neq 100$.

3.6. Una solución inmediata es $x_0 = 5, y_0 = 95$. Si tomamos $x = 5 + 100k, y = 95 - 100k$, para cada valor entero de k se tiene un par diferente de enteros que satisfacen las condiciones.

3.7. Si $(a, 4) = 2$ y $(b, 4) = 2$, entonces a y b son pares. Además, son de la forma $4k+2$ ya que, de lo contrario, sería $(a, 4) = 4$ ó $(b, 4) = 4$. Luego, si $a = 4k_1+2$ y $b = 4k_2+2$, se tiene:

$$a+b = 4(k_1+k_2+1),$$

$$4|(a+b),$$

$$(a+b, 4) = 4.$$

3.8.

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

luego, si $a-b$ es divisible por 2^n , también lo es $a^3 - b^3$. Además, como a y b son impares, $a^2 + ab + b^2$ es impar y $(2^n, a^2 + ab + b^2) = 1$; luego $2^n|(a^3 - b^3)$ sólo si $2^n|(a-b)$.

3.9. a) Procedemos por inducción sobre n . Si $n = 0$, entonces $(a_0, a_1) = (1, 1) = 1$.

Supongamos que $(a_n, a_{n+1}) = 1$. Entonces, si $(a_{n+1}, a_{n+2}) = d$, se tiene que $d|(a_{n+2} - a_{n+1})$, luego $d|a_n$, y como $d|a_{n+1}$ entonces $d|1$, luego $d = 1$.

b) Si $n = 1$ se tiene: $a_0 = \binom{1-1}{0} = \binom{0}{0} = 1$.

Supongamos que la propiedad es cierta hasta n .

$$a_{n-1} = \binom{n-2}{0} + \binom{n-3}{1} + \binom{n-4}{2} + \dots, \quad (1)$$

$$a_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \binom{n-4}{3} + \dots \quad (2)$$

Como $\binom{n-1}{0} = \binom{n}{0}$ y como $\binom{a-1}{b-1} + \binom{a-1}{b} = \binom{a}{b}$, sumando miembro a miembro (1) y (2) se tiene:

$$a_{n+1} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \dots$$

Nota. Se ha usado una versión del principio de inducción equivalente a la que se planteó en la sección 1. Esta es: Supongamos que para cada entero positivo n se da una propiedad

$P(n)$. Supongamos que $P(1)$ es cierta. Supongamos además que siempre que $P(m)$ es cierta para todos los enteros positivos $m \leq n$, entonces $P(m+1)$ es cierta. Entonces $P(n)$ es cierta para todos los enteros positivos n .

3.10. Sean $d = (a, b)$, $d' = (a', b')$. Se tiene:

$$\begin{aligned}(aa', ab', ba', bb') &= ((aa', ab'), (ba', bb')), \\ (aa', ab') &= a(a', b') = ad', \\ (ba', bb') &= b(a', b') = bd', \\ (aa', ab', ba', bb') &= (ad', bd') = d'(a, b) = dd'.\end{aligned}$$

3.11. Sean $u = ax + by$, $v = cx + dy$. Entonces

$$\begin{aligned}du - bv &= (ad - bc)x = mx, \\ bv &= du - mx.\end{aligned}$$

Si x, y son enteros tales que u es múltiplo de m , entonces bv también es múltiplo de m y, como $(b, m) = 1$, se tiene que $m|v$.

El mismo razonamiento muestra que si v es múltiplo de m , también lo es de u .

3.12. Se tiene: $a = dx$, $b = dy$, donde x, y son enteros y $(x, y) = 1$.

Si se dividen $a, 2a, 3a, \dots, (b-1)a, ba$ por b , se obtienen los cocientes

$$\frac{x}{y}, \frac{2x}{y}, \dots, \frac{(b-1)x}{y}, \frac{bx}{y}.$$

Como $(x, y) = 1$, los únicos números enteros entre las fracciones anteriores son aquellos en los cuales el coeficiente de x en el numerador es un múltiplo de y . Como $b = dy$, esto sucede d veces, cuando los coeficientes toman los valores $y, 2y, \dots, dy$.

Sección 4.

4.1. Si $(a, b) = 1$ y $(x_0, y_0), (x_1, y_1)$ son soluciones de la ecuación $ax + by = c$, entonces

$$x_0 + bk_1 = x_1 + bk_2,$$

para dos enteros k_1 y k_2 . Como $x_1 = 1 + x_0$, se tiene

$$x_0 + bk_1 = (1 + x_0) + bk_2,$$

$$b(k_1 - k_2) = 1,$$

$$b = \pm 1.$$

4.2. Restando miembro a miembro las ecuaciones del sistema

$$ax + b_1y + c_1z = d_1,$$
$$ax + b_2y + c_2z = d_2,$$

se tiene

$$(b_1 - b_2)y + (c_1 - c_2)z = d_1 - d_2.$$

Esta última ecuación tiene soluciones enteras si y sólo si

$$(b_1 - b_2, c_1 - c_2) \mid (d_1 - d_2),$$

lo cual nos garantiza que las dos ecuaciones tienen al menos una solución simultánea (para $x = 0$).

4.3. Multiplicando ambos miembros de la primera ecuación por 4 y ambos miembros de la segunda ecuación por 3, se tiene:

$$12x + 24y + 4z = 8,$$
$$12x + 30y + 6z = 9.$$

Obsérvese que $(24 - 30, 4 - 6) = 2$ y $2 \nmid (8 - 9)$, luego, de acuerdo con el resultado obtenido en el problema 4.2., el sistema no tiene soluciones enteras.

4.4. Si en el sistema

$$x + 2y + 3z = 4, \quad (1)$$

$$2x - z = -1, \quad (2)$$

se multiplican los dos miembros de la ecuación (2) por 3 y se suma miembro a miembro con (1), nos queda

$$7x + 2y = 1.$$

Esta ecuación tiene una solución particular: $x_0 = 1, y_0 = -3$ (se puede hallar por inspección), luego la solución general de $7x + 2y = 1$ es

$$x = 1 + 2k, y = -3 - 7k, \quad \text{donde } k \text{ recorre } \mathbb{Z}.$$

Reemplazando estas expresiones en (1) se tiene

$$1 + 2k + 2(-3 - 7k) + 3z = 4,$$
$$1 + 2k - 6 - 14k + 3z = 4,$$
$$3z = 9 + 12k,$$
$$z = 3 + 4k.$$

Por tanto, la solución general del sistema es:

$$x = 1 + 2k, y = -3 - 7k, z = 3 + 4k, \quad \text{donde } k \in \mathbb{Z}.$$

4.5.

$$\begin{aligned}x + y - z &= -1, \\x^2 - y^2 + z^2 &= 1, \\-x^3 + y^3 + z^3 &= -1.\end{aligned}$$

De la primera ecuación del sistema se desprende:

$$x + y = z - 1. \quad (1)$$

De la segunda ecuación se desprende:

$$(x + y)(x - y) + (z + 1)(z - 1) = 0,$$

por tanto

$$(z - 1)(x - y) + (z + 1)(z - 1) = 0,$$

$$(z - 1)(x - y + z + 1) = 0, \quad (2)$$

por consiguiente, $z - 1 = 0$ ó $x - y + z + 1 = 0$. Analicemos ambos casos.

a) Si $z - 1 = 0$, entonces $z = 1$ y de (1) se concluye que $x = -y$. Reemplazando en la tercera ecuación del sistema nos queda:

$$\begin{aligned}-x^3 - x^3 &= -1 - 1, \\-2x^3 &= -2, \\x^3 &= 1, \\x &= 1,\end{aligned}$$

y en consecuencia $y = -1$, luego una solución es:

$$(1, -1, 1).$$

b) Si $x - y + z + 1 = 0$, entonces

$$x - y = -z - 1.$$

Sumando miembro a miembro esta última ecuación con (1) se tiene:

$$\begin{aligned}2x &= -2, \\x &= -1,\end{aligned}$$

y además $z = y$. Reemplazando en la tercera ecuación del sistema, nos queda

$$\begin{aligned}-(-1)^3 + 2y^3 &= -1, \\2y^3 &= -2, \\y^3 &= -1, \\y &= -1.\end{aligned}$$

Entonces, la otra solución del sistema es:

$$(-1, -1, -1).$$

4.6. Si $x = 2k$ entonces $x^3 + 5x + 9 = 8k^3 + 10k + 9 = 2k_1 + 1$, donde $k_1 = 4k^3 + 5k + 4$.

Si $x = 2k + 1$ entonces $x^3 + 5x + 9 = 8k^3 + 12k^2 + 16k + 15 = 2k_2 + 1$, donde $k_2 = 4k^3 + 6k^2 + 8k + 7$.

Luego, $x^3 + 5x + 9$ siempre es un número impar y, por tanto, no puede ser igual a 0.

4.7. Basta verificar la identidad:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

4.8. Sean $n - 1, n, n + 1$ los tres números. Entonces, si

$$(n + 1)^3 = (n - 1)^3 + n^3,$$

se tiene

$$n^3 + 3n^2 + 3n + 1 = n^3 - 3n^2 + 3n - 1 + n^3,$$

$$n^3 - 6n^2 - 2 = 0,$$

$$n^2(n - 6) = 2.$$

El primer miembro es positivo sólo si $n > 6$, y en ese caso $n^2(n - 6) > 36$, luego $n^2(n - 6) \neq 2$.

4.9. Si $x = n(n + 1)(n + 2)(n + 3)$ se tiene:

$$\begin{aligned} x &= [n(n + 3)][(n + 1)(n + 2)] = (n^2 + 3n)(n^2 + 3n + 2) = \\ &= (n^2 + 3n)[(n^2 + 3n) + 2] = (n^2 + 3n)^2 + 2(n^2 + 3n) = \\ &= [(n^2 + 3n)^2 + 2(n^2 + 3n) + 1] - 1 = (n^2 + 3n + 1)^2 - 1. \end{aligned}$$

Luego, $(n^2 + 3n)^2 < x < (n^2 + 3n + 1)^2$ y, en consecuencia, x no es un cuadrado perfecto.

4.10. De las identidades:

$$(a - b)^2 = a^2 - 2ab + b^2,$$

$$(a - c)^2 = a^2 - 2ac + c^2,$$

$$(b - c)^2 = b^2 - 2bc + c^2,$$

$$(a + b + c)^2 = a^2 + b^2 + c^2 + 2ab + 2ac + 2bc,$$

sumando miembro a miembro se tiene:

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

4.11. Supongamos que

$$2n = a^2 + b^2 + c^2 + d^2.$$

Como la suma de los cuadrados de a, b, c, d es par, hay tres casos posibles:

- a) Los cuatro son pares.
- b) Los cuatro son impares.
- c) Hay dos pares y dos impares.

En cualquiera de los casos hay dos parejas de números con la misma paridad de manera que su suma y su diferencia son pares. Supongamos que las parejas de números $\{a, b\}$ y $\{c, d\}$ tienen la misma paridad. Entonces:

$$\frac{a+b}{2}, \frac{a-b}{2}, \frac{c+d}{2}, \frac{c-d}{2} \text{ son enteros}$$

y se tiene:

$$a^2 + b^2 = 2 \left[\left(\frac{a+b}{2} \right)^2 + \left(\frac{a-b}{2} \right)^2 \right],$$

$$c^2 + d^2 = 2 \left[\left(\frac{c+d}{2} \right)^2 + \left(\frac{c-d}{2} \right)^2 \right],$$

$$n = \left(\frac{a+b}{2} \right)^2 + \left(\frac{a-b}{2} \right)^2 + \left(\frac{c+d}{2} \right)^2 + \left(\frac{c-d}{2} \right)^2.$$

4.12. Obsérvese que la cifra de las unidades de un cuadrado perfecto sólo puede ser 0, 1, 4, 5, 6 ó 9. Entonces,

la cifra de las unidades de $15x^2$ es 0 ó 5,

la cifra de las unidades de $7y^2$ es 0, 7, 8, 5, 2 ó 3,

por tanto, la cifra de las unidades de $15x^2 - 7y^2$ no puede ser 9.

4.13. Si $x^2 - y^2 = n$, entonces $(x+y)(x-y) = n$. Pero $x+y, x-y$ tienen la misma paridad (problema 3.1.), luego si $x+y = a, x-y = b$, entonces $n = ab$, con a y b de la misma paridad.

Recíprocamente, supongamos $n = ab$, con a y b de la misma paridad. El sistema

$$x+y = a,$$

$$x-y = b,$$

tiene la solución $x = \frac{a+b}{2}, y = \frac{a-b}{2}$, con x, y enteros. Si $n = ab$, entonces $n = x^2 - y^2$.

4.14. Si $2^p + 1 = q^2$ se tiene $2^p = (q+1)(q-1)$, por consiguiente q es impar. Si $q = 2k+1$, entonces

$$2^p = 4k(k+1).$$

Como k y $k+1$ son dos enteros consecutivos, $k(k+1)$ es una potencia de 2 sólo si $k = 1$, luego

$$2^p = 8,$$

de donde

$$p = 3 \quad y \quad q = 3.$$

4.15. La ecuación $x^2 + ax + b = y^2 + cy + d$ puede escribirse en la forma:

$$\left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} = \left(y + \frac{c}{2}\right)^2 + d - \frac{c^2}{4}.$$

Si $a^2 - 4b = c^2 - 4d$, la ecuación es equivalente a:

$$\left(x + \frac{a}{2}\right)^2 = \left(y + \frac{c}{2}\right)^2,$$

luego

$$x + \frac{a}{2} = \pm \left(y + \frac{c}{2}\right),$$

$$x = -\frac{a}{2} \pm \left(y + \frac{c}{2}\right),$$

$$x = \pm y - \frac{a \mp c}{2}.$$

Como $a^2 - c^2 = 4(b - d)$, entonces $4|(a+c)(a-c)$. Sabemos que $a+c$ y $a-c$ tienen la misma paridad, por consiguiente ambos son pares y, en consecuencia, $\frac{a \mp c}{2}$ son números enteros. Luego, para cada número entero y habrá un entero x que satisfaga la ecuación.

Recíprocamente, supongamos que la ecuación $x^2 + ax + b = y^2 + cy + d$ tiene infinitas soluciones enteras. De la ecuación

$$\left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} = \left(y + \frac{c}{2}\right)^2 + d - \frac{c^2}{4},$$

se tiene

$$\left(x + \frac{a}{2}\right)^2 - \left(y + \frac{c}{2}\right)^2 = \frac{a^2}{4} - b - \frac{c^2}{4} + d,$$

$$(2x + a)^2 - (2y + c)^2 = a^2 - 4b - c^2 + 4d,$$

$$(2x + 2y + a + c)(2x - 2y + a - c) = a^2 - 4b - c^2 + 4d.$$

Si suponemos $a^2 - 4b - c^2 + 4d \neq 0$, este número tendrá un número finito de divisores luego $(2x + 2y + a + c)$ y $(2x - 2y + a - c)$ tendrán un número finito de valores para infinitos enteros x, y que satisfacen la ecuación. Ahora bien, para que $2x + 2y + a + c$ to un número finito de valores, es preciso que $2x + 2y = 0$, es decir, $x = -y$, y en ese caso $2x - 2y + a - c = 4x + a - c$ tomará infinitos valores. Esta contradicción implica que $a^2 - 4b - c^2 + 4d = 0$, luego $a^2 - 4b = c^2 - 4d$.

4.16. Consideraremos tres casos según que a sea menor, igual o mayor que 0.

a) Si $a < 0$ entonces $x^2 = 2^b - \frac{1}{15^{|a|}} = \frac{2^b \cdot 15^{|a|} - 1}{15^{|a|}}$, luego x nunca será entero y la ecuación no tiene soluciones enteras.

b) Si $a = 0$ entonces $x^2 = 2^b - 1$. Para que haya solución entera es necesario que sea $b \geq 0$. Si $b = 0$ entonces $x = 0$ y si $b = 1$ entonces $x = \pm 1$. Si $b \geq 2$ entonces $4 \mid 2^{b-2}$, lo cual es imposible ya que para todo entero x se tiene que $x^2 = 4k$ ó $x^2 = 4k + 1$. Por tanto, en este caso las únicas soluciones son:

$$\begin{aligned} a &= 0, b = 0, x = 0, \\ a &= 0, b = 1, x = 1, \\ a &= 0, b = 1, x = -1. \end{aligned}$$

c) Si $a > 0$, de $15^a = 2^b - x^2$ se desprende que $3 \mid (2^b - x^2)$. Ahora bien, $2^b = (3-1)^b = 3k + (-1)^b$, luego $3 \mid [(-1)^b - x^2]$, de donde $3 \mid [x^2 - (-1)^b]$. Si b es impar, esta relación implica que $3 \mid (x^2 + 1)$, lo cual es imposible porque x^2 es de la forma $3k$ ó $3k + 1$. Por consiguiente, puede haber soluciones sólo si b es par. Supongamos que $b = 2c$; entonces la ecuación es

$$15^a = 2^{2c} - x^2 = (2^c - x)(2^c + x).$$

Nótese que si x es una solución de la ecuación, $-x$ también lo es, luego podemos suponer $x > 0$. (El caso $x = 0$ ya ha sido analizado en (b)).

Ahora bien, $3 \mid 15^a$ y $5 \mid 15^a$, luego 3 y 5 dividen a $(2^c - x)(2^c + x)$. Pero $2^c - x$ y $2^c + x$ no pueden ser ambos divisibles por 3 ya que, en ese caso, también lo sería la suma de ambos, esto es, $3 \mid 2^{c+1}$, lo cual es falso. Similarmente se comprueba que $2^c - x$ y $2^c + x$ no son ambos divisibles por 5. Las posibilidades que quedan son las siguientes:

1) $2^c - x = 1$ y $2^c + x = 15^a$.

Sumando ambas igualdades se tiene:

$$2^{c+1} = 15^a + 1,$$

y debe ser $c \geq 3$. Si $c = 3$, entonces $2^4 = 15 + 1$ y hay las soluciones:

$$\begin{aligned} a &= 1, b = 6, x = 7, \\ a &= 1, b = 6, x = -7. \end{aligned}$$

Si $c > 3$ entonces $32|2^{c+1}$ y, por consiguiente, $32|(15^a + 1)$. Pero $15^2 = 225 = 32 \cdot 7 + 1$, luego si a es par se verifica que 15^a es de la forma $32k + 1$ y si a es impar, entonces 15^a es de la forma $32k + 15$; por tanto, en ningún caso $32|(15^a + 1)$.

$$2^c - x = 3^a \text{ y } 2^c + x = 5^a.$$

Sumando ambas igualdades se tiene:

$$2^{c+1} = 3^a + 5^a.$$

y debe ser $c \geq 2$. Si $c = 2$, $2^3 = 3 + 5$ y hay las soluciones:

$$a = 1, b = 4, x = 1,$$

$$a = 1, b = 4, x = -1.$$

Si $c > 2$ se tiene que $16|2^{c+1}$ y, por consiguiente, $16|(3^a + 5^a)$. Ahora bien, $3^a + 5^a = (4-1)^a + (4+1)^a$ y, desarrollando por el binomio de Newton se llega a que $3^a + 5^a$ es de la forma $16k + 8$ si a es impar y $16k + 2$ si a es par. Por tanto, $16 \nmid (3^a + 5^a)$.

En total la ecuación tiene siete soluciones.

4.17.

$$x + py = n, \quad (1)$$

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

En la ecuación (2) se observa que para que el sistema tenga solución (x, y, z) de enteros positivos, debe ser $p > 1$, luego $p-1 > 0$.

Despejando y en (2) y reemplazando en (1) se tiene:

$$x + p(p^z - x) = n,$$

$$x + p^{z+1} - px = n,$$

$$x(1-p) + p^{z+1} = n,$$

y como $p \neq 1$,

$$x = \frac{p^{z+1} - n}{p-1} = \frac{p^{z+1} - 1 - (n-1)}{p-1},$$

$$x = \frac{p^{z+1} - 1}{p-1} - \frac{n-1}{p-1}. \quad (3)$$

De la ecuación (2) se tiene:

$$y = p^z - x,$$

$$y = p^z - \frac{p^{z+1} - 1}{p-1} + \frac{n-1}{p-1},$$

$$y = \frac{p^{z+1} - p^z - p^{z+1} + 1 + n - 1}{p-1},$$

$$y = \frac{n - p^z}{p-1},$$

$$y = \frac{n-1}{p-1} - \frac{p^z - 1}{p-1}. \quad (4)$$

Como $(p-1)|(p^z - 1)$ para todo entero positivo z , los valores de x, y dados en las igualdades (3) y (4) son enteros si y sólo si $(p-1)|(n-1)$. Además, x es positivo si y sólo si $p^{z+1} - n > 0$, es decir $p^{z+1} > n$, mientras que y es positivo si y sólo si $n - p^z > 0$, luego $n > p^z$. Se tiene entonces

$$p^z < n < p^{z+1}. \quad (5)$$

Por consiguiente, las condiciones que deben satisfacerse para que el sistema tenga soluciones (x, y, z) de enteros positivos son:

- a) $p > 1$,
- b) $(p-1)|(n-1)$,
- c) $p \nmid n$.

Obsérvese que la desigualdad (5) determina z en forma única. Una vez hallado el valor de z , las ecuaciones (1) y (2) determinan, también en forma única, los valores de x, y .

Sección 5.

5.1. $n + 1 = 1 \cdot n + 1$, luego, por el algoritmo de Euclides, $(n, n + 1) = 1$. Por otra parte, $[n, n + 1] = \frac{n(n + 1)}{1} = n(n + 1)$.

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

5.3. Si $(a, b) = 10$ y $[a, b] = 100$, entonces $ab = 1000$.

Como a y b son ambos múltiplos de 10, las soluciones posibles son:

$$\begin{aligned} a &= 10, b = 100, \\ a &= 20, b = 50, \\ a &= 100, b = 10, \\ a &= 50, b = 20. \end{aligned}$$

5.4. Si $d|m$ basta tomar $x = d, y = m$ y entonces se satisfacen las condiciones $(x, y) = d, [x, y] = m$ (problema 5.2.).

Por otra parte, si existen enteros x, y que satisfacen ambas condiciones, entonces d es un divisor de x e y . Como a su vez x e y son divisores de m , entonces necesariamente $d|m$.

Sección 6.

6.1. En la identidad

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1)$$

se observa que

$$(a - 1)|(a^n - 1),$$

luego si $a^n - 1$ es primo entonces necesariamente $a - 1 = 1$, de donde $a = 2$. Además, si n fuese compuesto tendríamos $n = xy$, con x, y enteros tales que $1 < x, y < n$, y de la identidad:

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

se concluye que $2^n - 1$ no es primo. Por consiguiente, n debe ser primo.

Nota. Los primos de esta forma son llamados *primos de Mersenne* (francés).

6.2. Dados los tres números consecutivos

$$2^n - 1, 2^n, 2^n + 1,$$

uno de ellos es de la forma $3k$. Como $2^n - 1$ es primo y $3 \nmid 2^n$, entonces necesariamente $3|(2^n + 1)$. Además, si $n > 2$ entonces $2^n + 1 > 3$, luego $2^n + 1$ es compuesto.

6.3. Si suponemos $2^n + 1 = x^3$, se tiene

$$\begin{aligned} 2^n &= x^3 - 1, \\ 2^n &= (x - 1)(x^2 + x + 1), \end{aligned}$$

pero el factor $x^2 + x + 1$ es impar, y como $x > 1$ (de lo contrario sería $x - 1 \leq 0$), $x^2 + x + 1$ no puede ser un factor de 2^n (teorema fundamental de la aritmética).

6.4. Consideremos los enteros: $n - 1, n, n + 1, n + 2$. Se tiene:

$$(n - 1) + n + (n + 1) + (n + 2) = 4n + 2 = 2.(2n + 1).$$

Ahora bien, como $(2, 2n + 1) = 1$, de acuerdo con el teorema fundamental de la aritmética 2 tendría que ser un cuadrado para que $2.(2n + 1)$ fuese un cuadrado perfecto.

6.5. Si $2p + 1 = x^3$, entonces $2p = (x - 1)(x^2 + x + 1)$.

Ahora bien, como $x^2 + x + 1$ siempre es impar, necesariamente, de acuerdo con el teorema fundamental de la aritmética se tiene $x - 1 = 2$; luego $x = 3$ y $p = 13$.

6.6. Si n no es potencia de 2, podemos escribir $n = 2^k \cdot i$, donde $k \geq 0$ y i es un entero impar mayor o igual que 3. Entonces:

$$2^n + 1 = 2^{2^k \cdot i} + 1 = (2^{2^k})^i + 1 = (2^{2^k} + 1)(2^{2^k(i-1)} - 2^{2^k(i-2)} + \dots - 2^{2^k} + 1).$$

Como cada uno de los dos factores del último miembro de la igualdad es un entero mayor que 1, $2^n + 1$ sería compuesto.

Nota. Los números primos de la forma $2^{2^n} + 1$ se llaman *primos de Fermat*. Los cinco primeros primos de Fermat son: $2^{2^0} + 1 = 3, 2^{2^1} + 1 = 5, 2^{2^2} + 1 = 17, 2^{2^3} + 1 = 257, 2^{2^4} + 1 = 65537$.

Fermat conjeturó que todos los números de la forma $2^{2^n} + 1$ eran primos, aún cuando no realizó los cálculos para números mayores que los cinco anteriores. Posteriormente, el matemático suizo Euler comprobó que el siguiente número de Fermat, $2^{2^5} + 1$, no es primo (ver Problema 2.20). De hecho, se ignora si existen más primos de Fermat.

Los números de Fermat aparecen en un problema completamente diferente, la construcción de polígonos regulares con regla y compás. Se sabe que un polígono regular de n lados, con n primo impar, es constructible con regla y compás si y sólo si n es primo de Fermat.

6.7. Sea d la razón de la progresión. Entonces

$$a_{n+1} = a_n + d \quad y \quad a_{n+k} = a_n + kd.$$

Sea $k = a_n$ y consideremos el k -ésimo término después de a_n . Entonces $a_{n+k} = k + kd = k(1 + d)$ y, por consiguiente, no es primo.

6.8. Si $p_2 = p_1 + 2$ entonces, necesariamente p_1 es de la forma $3k + 2$ y p_2 de la forma $3k + 1$, luego $p_1 + p_2$ es divisible por 3.

Además, como p_1 y p_2 difieren en dos unidades, uno de ellos es de la forma $4k + 1$ y el otro es de la forma $4k + 3$, luego $p_1 + p_2$ es divisible por 4.

Por consiguiente, $12|(p_1 + p_2)$.

6.9. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ y d es un divisor de n , entonces $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ donde los β_i son enteros tales que $0 \leq \beta_i \leq \alpha_i$; luego, cada β_i puede tomar $1 + \alpha_i$ valores: $0, 1, \dots, \alpha_i$, que al combinarlos con los valores que pueden tomar los $k - 1$ exponentes restantes dan un total de

$$(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$$

divisores.

6.10. Si $n = 2^{p-1}(2^p - 1)$ y $2^p - 1$ es un número primo, los divisores de n son los divisores de 2^{p-1} y los divisores de $2^p - 1$ multiplicados por $2^p - 1$. Estos son:

$$1, 2, 2^2, \dots, 2^{p-2}, 2^{p-1}, \quad (1)$$

$$2^p - 1, 2.(2^p - 1), 2^2.(2^p - 1), \dots, 2^{p-2}.(2^p - 1), \quad (2)$$

sin incluir al propio n .

La suma de la progresión geométrica (1) es

$$\frac{2^{p-1}.2 - 1}{2 - 1} = 2^p - 1.$$

La suma de la progresión geométrica (2) es

$$\frac{2^{p-2}.(2^p - 1).2 - (2^p - 1)}{2 - 1} = 2^{p-1}.(2^p - 1) - (2^p - 1) = (2^p - 1).(2^{p-1} - 1).$$

Por consiguiente, la suma deseada es

$$2^p - 1 + (2^p - 1).(2^{p-1} - 1) = (2^p - 1).(1 + 2^{p-1} - 1) = 2^{p-1}.(2^p - 1) = n.$$

Nota. Si un entero positivo n coincide con la suma de todos sus divisores positivos menores que n , se llama un *número perfecto*. El problema anterior proporciona un método para hallar números perfectos pares, a partir de los primos de Mersenne. Más aún, se puede probar que todos los números perfectos pares son de esa forma. Todavía no se sabe si existen infinitos números perfectos pares, ni tampoco si existe algún número perfecto impar.

6.11. Si $n = 1$ se tiene que $k = 0$ y $\log n = k \log 2 = 0$. Supongamos que $n > 1$ y expresémoslo en su forma canónica

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

donde p_1, p_2, \dots, p_k son primos diferentes y $\alpha_1, \alpha_2, \dots, \alpha_k$ son enteros positivos. Como cada uno de los factores primos es mayor o igual que 2, se tiene

$$n \geq 2^{\alpha_1}.2^{\alpha_2} \cdots 2^{\alpha_k} = 2^{\alpha_1 + \alpha_2 + \cdots + \alpha_k} \geq 2^k,$$

por cuanto $\alpha_i \geq 1$ para todo $i = 1, \dots, k$. Por consiguiente,

$$\log n \geq k \log 2.$$

6.12. Si $p = 2, 3$ ó 5 se verifica inmediatamente que $(p - 1)! + 1$ es potencia de p .

Si $p > 5$, $(p - 1)!$ tiene como factores $2, p - 1$ y $\frac{p-1}{2}$, luego $(p - 1)!$ es divisible por $(p - 1)^2$; es decir, existe un entero x tal que $(p - 1)! = x(p - 1)^2$.

Si $(p - 1)! + 1$ es potencia de p , se tiene que

$$(p - 1)! = p^n - 1 \quad \text{donde} \quad n > 1, \quad (1)$$

luego

$$p^n - 1 = x(p - 1)^2$$

y

$$(p-1)^2 | (p^n - 1).$$

Ahora bien, esto se verifica si y sólo si $(p-1) | n$ (problema 2.6.), en cuyo caso sería $n \geq p-1$ de donde

$$\begin{aligned} p^n &> p!, \\ p^n - 1 &> p! - 1, \\ p^n - 1 &> (p-1)! \end{aligned}$$

lo cual contradice a la igualdad (1).

6.13. Supongamos que p_1, p_2, \dots, p_j son todos los primos de la forma $4k + 3$ y consideremos el número

$$n = 4p_1p_2 \dots p_j - 1.$$

n es de la forma $4k + 3$. Si n es primo, hemos terminado, por cuanto es diferente de cada uno de los p_i , $i = 1, \dots, j$. Si n es compuesto entonces n admite un divisor primo de la forma $4k + 3$, ya que el producto de números de la forma $4k + 1$ es también de la forma $4k + 1$. Tal divisor es diferente de cada uno de los p_i ya que, de lo contrario, dividiría a 1.

Similarmente, como los números primos mayores que 3 son de la forma $6k + 1$ ó $6k + 5$ y como el producto de números de la forma $6k + 1$ es de la misma forma, si p_1, p_2, \dots, p_j son números primos de la forma $6k + 5$ entonces el número

$$n = 6p_1p_2 \dots p_j - 1$$

es de la forma $6k + 5$ y tiene un divisor primo que no coincide con ninguno de los p_1, p_2, \dots, p_j .

6.14. Supongamos $n = xy$ con $1 < x, y < n$. Entonces se tiene:

$$\begin{aligned} a_n &= \frac{10^n - 1}{9} = \frac{10^{xy} - 1}{9} = \frac{(10^x - 1)(10^{x(y-1)} + 10^{x(y-2)} + \dots + 10^x + 1)}{9} = \\ &= \frac{10^x - 1}{9} (10^{x(y-1)} + 10^{x(y-2)} + \dots + 10^x + 1), \end{aligned}$$

y, en consecuencia, a_n no sería primo.

6.15. Se requiere hallar el número de enteros n que satisfacen las condiciones:

$$40000 \leq n^2 \leq 640000 \quad (1)$$

y

$$3|n, 2|n \quad y \quad 5|n. \quad (2)$$

La condición (1) es equivalente a

$$200 \leq n \leq 800 \quad (3)$$

y la condición (2) es equivalente a

$$30|n, \quad (4)$$

luego, es fácil ver que los números que satisfacen (3) y (4) son

$$30.7, 30.8, 30.9, \dots, 30.26.$$

En total, 20 enteros.

6.16. Supongamos que hay 8 números compuestos, a_1, a_2, \dots, a_8 , menores que 360 y que son primos dos a dos. Como $\sqrt{360} < 19$, cada uno de estos números debe tener un factor primo menor que 19. Ahora bien, los números primos menores que 19 son

$$2, 3, 5, 7, 11, 13, 17,$$

en total 7, por consiguiente, de acuerdo con el principio de las casillas, por lo menos dos de los ocho números escogidos tienen un factor primo común.

6.17 Se pide hallar todas las ternas ordenadas de números enteros positivos (a, b, c) tales que:

$$[a, b] = 1000, [b, c] = 2000, [c, a] = 2000.$$

Como 1000 y 2000 son de la forma $2^\alpha \cdot 5^\beta$, entonces a, b y c deben ser de la misma forma. Luego:

$$a = 2^{\alpha_1} \cdot 5^{\beta_1}, b = 2^{\alpha_2} \cdot 5^{\beta_2}, c = 2^{\alpha_3} \cdot 5^{\beta_3},$$

donde los α_i y los β_i son enteros no negativos para $i = 1, 2, 3$. Además, como $[a, b] = 2^3 \cdot 5^3$, $[b, c] = 2^4 \cdot 5^3$, $[c, a] = 2^4 \cdot 5^3$, debe tenerse que:

$$\max\{\alpha_1, \alpha_2\} = 3, \max\{\alpha_2, \alpha_3\} = 4, \max\{\alpha_1, \alpha_3\} = 4, \quad (1)$$

$$\max\{\beta_1, \beta_2\} = 3, \max\{\beta_2, \beta_3\} = 3, \max\{\beta_1, \beta_3\} = 3. \quad (2)$$

Para satisfacer (1) se tiene que $\alpha_3 = 4$ y además α_1 ó α_2 es igual a 3, mientras que el otro puede tomar cualquiera de los valores 0, 1, 2 ó 3. Hay siete ternas ordenadas que satisfacen estas condiciones:

$$(3, 0, 4), (3, 1, 4), (3, 2, 4), (3, 3, 4), (0, 3, 4), (1, 3, 4), (2, 3, 4).$$

Para satisfacer (2), dos de los β_i son iguales a 3, mientras que el otro puede tomar cualquiera de los valores 0, 1, 2 ó 3. Hay diez ternas ordenadas que satisfacen estas condiciones:

$$(0, 3, 3), (1, 3, 3), (2, 3, 3), (3, 3, 3), (3, 3, 0), \\ (3, 3, 1), (3, 3, 2), (3, 0, 3), (3, 1, 3), (3, 2, 3).$$

Como la elección de los α_i es independiente de la de los β_i , se puede escoger un total de $7 \cdot 10 = 70$ maneras diferentes. Esto corresponde al número de ternas ordenadas (a, b, c) .

$$bc + ad = p_i^{\alpha_i} y, \quad (2)$$

$$bd = p_i^{\alpha_i} z, \quad (3)$$

para tres enteros x, y, z . Por consiguiente, de (1) y (3) se tiene

$$(bc)(ad) = p_i^{2\alpha_i} xz.$$

Esta relación se cumple si y sólo si p_i aparece elevado a un exponente mayor o igual que α_i en bc o en ad , pero entonces la ecuación (2) muestra que p_i aparece elevado a un exponente mayor o igual que α_i en bc y en ad ; por tanto bc y ad son múltiplos de $p_i^{\alpha_i}$.

El mismo razonamiento se aplica a todos los factores que aparecen en la expresión canónica de u .

6.20. Si n fuese un número par, entonces $4^n + n^4$ sería un número par mayor que 2 y, en consecuencia, sería compuesto.

Supongamos que n es impar y procuremos escribir $4^n + n^4$ como un producto de dos factores. Para ello, hacemos uso de la identidad

$$x^4 + y^4 = (x^2 + y^2 + \sqrt{2}xy)(x^2 + y^2 - \sqrt{2}xy).$$

Si $n = 2k + 1$, entonces $4^n = 4^{2k+1} = 4 \cdot 4^{2k} = (\sqrt{2} \cdot 2^k)^4$, luego $4^n + n^4 = (\sqrt{2} \cdot 2^k)^4 + n^4 = (2^n + n^2 + 2^{k+1}n)(2^n + n^2 - 2^{k+1}n)$.

Para finalizar la prueba, debemos ver que ambos factores son diferentes de 1. De hecho, basta probar que el menor de ellos es mayor que 1. En efecto,

$$\begin{aligned} 2^n + n^2 - 2^{k+1}n &= 2^{2k+1} + (2k+1)^2 - 2^{k+1}(2k+1) = \\ &= 2 \cdot 2^{2k} - 2 \cdot 2^k \cdot (2k+1) + (2k+1)^2 = \\ &= [2^k - (2k+1)]^2 + 2^{2k} \geq 5, \end{aligned}$$

ya que $k > 0$.

6.21. Supongamos que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. como $p_i \geq 2$ para todo $i = 1, \dots, k$, podemos escribir

$$n \geq 2^{\alpha_1} \cdot 2^{\alpha_2} \dots 2^{\alpha_k} \geq 2^k.$$

Ahora bien, todo entero positivo está comprendido entre dos potencias consecutivas de 2; por consiguiente

$$2^{m-1} \leq n < 2^m$$

para algún entero positivo m , y se tiene

$$k < m \quad y \quad \frac{1}{n} \leq \frac{1}{2^{m-1}}.$$

Multiplicando miembro a miembro ambas desigualdades:

$$\frac{k}{n} \leq \frac{m}{2^{m-1}}. \quad (1)$$

Por otra parte, si $m > 6$ se verifica que

$$m^2 < 2^{m-1}$$

(esta desigualdad puede demostrarse por inducción), luego

$$\frac{m}{2^{m-1}} < \frac{1}{m}$$

y reemplazando en (1) se tiene

$$\frac{k}{n} < \frac{1}{m}.$$

$\frac{1}{m} < \frac{1}{1991}$ equivale a $m > 1991$; luego si tomamos $n_0 = 2^{1991}$, para todo $n > n_0$ se tiene $\frac{k}{n} < \frac{1}{1991}$.

6.22. Como $c - a = 19$, se tiene que $c = a + 19$ y $a = c - 19$. Por consiguiente, $c > 19$; $c > a$.

Como $c^3 = d^2$, c^3 y d^2 contienen los mismos factores primos en sus expresiones canónicas; luego si

$$c = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k},$$

entonces $p_1^{3\alpha_1} p_2^{3\alpha_2} \dots p_k^{3\alpha_k} = p_1^{2\beta_1} p_2^{2\beta_2} \dots p_k^{2\beta_k}$ y se tiene que todos los exponentes de los primos en la descomposición canónica de c^3 ó d^2 son divisibles por 2 y por 3 (es decir, por 6).

Con el mismo razonamiento podemos concluir que todos los exponentes de los primos que aparecen en la descomposición canónica de a^5 ó b^4 son divisibles por 5 y por 4 (es decir, por 20). Tenemos entonces que el valor más pequeño que podría tomar a^5 ó b^4 sería 2^{20} .

Ahora bien, si $a^5 = b^4 = 2^{20}$, se tiene

$$a = 16,$$

luego

$$c = 16 + 19 = 35,$$

$$c = 5.7,$$

$$c^3 = 5^3 \cdot 7^3,$$

y estos exponentes no son divisibles por 6.

El segundo valor que se puede tomar para a^5 ó b^4 es 3^{20} . En este caso se tiene

$$a = 3^4 = 81,$$

$$c = 81 + 19 = 100,$$

$$c = 2^2 \cdot 5^2,$$

$$c^3 = 2^6 \cdot 5^6,$$

exponentes que sí son divisibles por 6. Entonces tenemos:

$$\begin{aligned}a^5 &= b^4, \\81^5 &= b^4, \\3^{20} &= b^4, \\b &= 3^5 = 243.\end{aligned}$$

Por otra parte

$$\begin{aligned}d^2 &= c^3, \\d^2 &= (10^2)^3, \\d^2 &= 10^6, \\d &= 10^3 = 1000.\end{aligned}$$

Por consiguiente,

$$d - b = 1000 - 243 = 757.$$

6.23. Tomando en cuenta la identidad:

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

en el número

$$a_n = (2903^n - 464^n) - (803^n - 261^n)$$

observamos que $2903^n - 464^n$ es divisible por

$$2903 - 464 = 2439 = 9.271$$

mientras que $803^n - 261^n$ es divisible por

$$803 - 261 = 542 = 2.271,$$

luego a_n es divisible por 271; es decir, $a_n = 271b_n$ donde b_n es un entero.

Pero a_n también es igual a:

$$(2903^n - 803^n) - (464^n - 261^n)$$

donde $2903^n - 803^n$ es divisible por

$$2903 - 803 = 2100 = 7.300$$

y $464^n - 261^n$ es divisible por

$$464 - 261 = 203 = 7.29,$$

luego a_n es también divisible por 7.

Como $7 \nmid 271$, $a_n = 271b_n$ es divisible por 7 sólo si $b_n = 7c_n$ para algún entero c_n ; por consiguiente,

$$a_n = 271 \cdot 7c_n = 1897c_n.$$

Sección 7.

7.1. Es preciso hallar la descomposición canónica del número $30!$. Los números primos menores o iguales que 30 son

$$2, 3, 5, 7, 11, 17, 19, 23 \text{ y } 29.$$

Procedamos a determinar las máximas potencias de estos primos que dividen a $30!$.

$$\left[\frac{30}{2} \right] + \left[\frac{30}{4} \right] + \left[\frac{30}{8} \right] + \left[\frac{30}{16} \right] = 15 + 7 + 3 + 1 = 26,$$

$$\left[\frac{30}{3} \right] + \left[\frac{30}{9} \right] + \left[\frac{30}{27} \right] = 10 + 3 + 1 = 14,$$

$$\left[\frac{30}{5} \right] + \left[\frac{30}{25} \right] = 6 + 1 = 7,$$

$$\left[\frac{30}{7} \right] = 4,$$

$$\left[\frac{30}{11} \right] = \left[\frac{30}{13} \right] = 2,$$

$$\left[\frac{30}{17} \right] = \left[\frac{30}{19} \right] = \left[\frac{30}{23} \right] = \left[\frac{30}{29} \right] = 1.$$

Por consiguiente, $30! = 2^{26} \cdot 3^{15} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29$. Entonces el menor entero n de manera que $30!n$ sea un cuadrado perfecto es:

$$n = 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29 = 1077205.$$

7.2. Sean $x = n + \alpha$, $y = m + \beta$, donde m, n son enteros y α, β números reales tales que $0 \leq \alpha, \beta < 1$. Entonces

$$[x] + [y] + [x + y] = m + n + m + n + [\alpha + \beta] = 2(m + n) + [\alpha + \beta],$$

$$[2x] + [2y] = 2m + [2\alpha] + 2n + [2\beta] = 2(m + n) + ([2\alpha] + [2\beta]).$$

Por consiguiente, bastará probar que $[\alpha + \beta] \leq [2\alpha] + [2\beta]$. Si $\alpha + \beta < 1$ entonces $[\alpha + \beta] = 0$ y se cumple la desigualdad. Si $\alpha + \beta \geq 1$, entonces $\alpha \geq \frac{1}{2}$ ó $\beta \geq \frac{1}{2}$ y se tiene $[\alpha + \beta] = 1$ y $[2\alpha] + [2\beta] \geq 1$.

7.3. Se tiene:

$$\left[\frac{x}{2} \right] + \left[\frac{x+1}{2} \right] = \left[\frac{x}{2} \right] + \left[\frac{x+1}{2} \right] = \left[\frac{x}{2} \right] + \left[\frac{x+1}{2} \right].$$

Si $[x]$ es par, entonces

$$\left[\frac{x}{2} \right] = \frac{x}{2} \text{ y } \left[\frac{x+1}{2} \right] = \frac{x+1}{2}.$$

Si $[x]$ es impar, entonces

$$\left[\frac{x}{2} \right] = \frac{x-1}{2} \text{ y } \left[\frac{x+1}{2} \right] = \frac{x+1}{2}.$$

En ambos casos la suma es igual a $[x]$.

7.4. a) $2.4.6 \dots (2n) = 2^n \cdot n!$

La mayor potencia k de un primo p que divide a $n!$ es $\sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right]$, por consiguiente

$$k = \begin{cases} \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] & \text{si } p \text{ es impar,} \\ n + \sum_{i=1}^{\infty} \left[\frac{n}{2^i} \right] & \text{si } p = 2. \end{cases}$$

b) $1.3.5 \dots (2n-1) = \frac{(2n)!}{2.4.6 \dots (2n)} = \frac{(2n)!}{2^n \cdot n!}$; por tanto, para calcular la mayor potencia de p que divide a $1.3.5 \dots (2n-1)$ bastará restar la mayor potencia de p que divide a $2^n \cdot n!$ a la mayor potencia de p que divide a $(2n)!$. Esto es:

$$k = \begin{cases} \sum_{i=1}^{\infty} \left(\left[\frac{2n}{p^i} \right] - \left[\frac{n}{p^i} \right] \right) & \text{si } p \text{ es impar,} \\ 0 & \text{si } p = 2. \end{cases}$$

7.5. Hay que demostrar que la mayor potencia de 2 que divide a $(2n)!$ es mayor que la mayor potencia de 2 que divide a $(n!)^2$, es decir:

$$\sum_{i=1}^{\infty} \left[\frac{2n}{2^i} \right] > \sum_{i=1}^{\infty} 2 \left[\frac{n}{2^i} \right]. \quad (1)$$

Ahora bien, en virtud de la propiedad 7.3. siempre se verifica $\left[\frac{2n}{2^i} \right] \geq 2 \left[\frac{n}{2^i} \right]$. Además, si j es el mayor entero tal que $2^j \leq n$, entonces $2^{j+1} \leq 2n$ y se tiene $\left[\frac{n}{2^{j+1}} \right] = 0 < \left[\frac{2n}{2^{j+1}} \right]$. De aquí se concluye (1).

7.6. Multiplicando y dividiendo $\prod_{k=1}^n (a+k)$ por $a!$ se tiene:

$$\prod_{k=1}^n (a+k) = \frac{(a+n)!}{a!},$$

y $n! \left| \prod_{k=1}^n (a+k)$ por cuanto $\frac{(a+n)!}{a!n!} = \binom{a+n}{a}$ es entero.

7.7. En la identidad

$$[x] - \left[\frac{x}{2} \right] = \left[\frac{x+1}{2} \right]$$

(problema 7.3.), hacemos sucesivamente x igual a $n, \frac{n}{2}, \frac{n}{2^2}, \dots$. Se tiene

$$[n] - \left[\frac{n}{2} \right] = \left[\frac{n+1}{2} \right],$$

$$\left[\frac{n}{2} \right] - \left[\frac{n}{2^2} \right] = \left[\frac{\frac{n}{2} + 1}{2} \right] = \left[\frac{n+2}{2^2} \right],$$

$$\left[\frac{n}{2^2} \right] - \left[\frac{n}{2^3} \right] = \left[\frac{\frac{n}{2^2} + 1}{2} \right] = \left[\frac{n+2^2}{2^3} \right],$$

⋮

$$\left[\frac{n}{2^h} \right] - \left[\frac{n}{2^{h+1}} \right] = \left[\frac{n+2^h}{2^{h+1}} \right],$$

donde h es tal que $2^h \leq n < 2^{h+1}$; por consiguiente,

$$\left[\frac{n}{2^h} \right] \neq 0, \text{ pero } \left[\frac{n}{2^{h+1}} \right] = 0.$$

Sumando miembro a miembro estas igualdades se tiene que

$$[n] = \sum_{k=0}^{\infty} \left[\frac{n+2^k}{2^{k+1}} \right].$$

7.8. Para cualquier primo p , el mayor exponente a tal que $p^a | (2m)!(2n)!$ es

$$a = \sum_{i=1}^{\infty} \left[\frac{2m}{p^i} \right] + \sum_{i=1}^{\infty} \left[\frac{2n}{p^i} \right] = \sum_{i=1}^{\infty} \left(\left[\frac{2m}{p^i} \right] + \left[\frac{2n}{p^i} \right] \right),$$

mientras que el mayor exponente b tal que $p^b | m!n!(m+n)!$ es

$$\begin{aligned} b &= \sum_{i=1}^{\infty} \left[\frac{m}{p^i} \right] + \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right] + \sum_{i=1}^{\infty} \left[\frac{m+n}{p^i} \right] = \\ &= \sum_{i=1}^{\infty} \left(\left[\frac{m}{p^i} \right] + \left[\frac{n}{p^i} \right] + \left[\frac{m+n}{p^i} \right] \right). \end{aligned}$$

Basta demostrar que $b \leq a$; es decir, para todo i ,

$$\left[\frac{m}{p^i} \right] + \left[\frac{n}{p^i} \right] + \left[\frac{m+n}{p^i} \right] \leq \left[\frac{2m}{p^i} \right] + \left[\frac{2n}{p^i} \right].$$

Pero esto se desprende de la identidad

$$[x] + [y] + [x+y] \leq [2x] + [2y],$$

planteada en el problema 7.2.

7.9. Se debe probar que, para todo primo p ,

$$\sum_{i=1}^{\infty} \left[\frac{ab}{p^i} \right] - \sum_{i=1}^{\infty} \left[\frac{a}{p^i} \right] - a \sum_{i=1}^{\infty} \left[\frac{b}{p^i} \right] \geq 0.$$

Denotemos por j y k a los enteros tales que $p^j \leq a < p^{j+1}$ y $p^k \leq b < p^{k+1}$. Se tiene:

$$\begin{aligned} &\sum_{i=1}^{\infty} \left[\frac{ab}{p^i} \right] - \sum_{i=1}^{\infty} \left[\frac{a}{p^i} \right] - a \sum_{i=1}^{\infty} \left[\frac{b}{p^i} \right] = \\ &= \sum_{i=1}^k \left[\frac{ab}{p^i} \right] + \sum_{i=k+1}^{j+k} \left[\frac{ab}{p^i} \right] + \sum_{i=j+k+1}^{\infty} \left[\frac{ab}{p^i} \right] - \sum_{i=1}^j \left[\frac{a}{p^i} \right] - \sum_{i=1}^k a \left[\frac{b}{p^i} \right] = \\ &= \sum_{i=1}^k \left(\left[\frac{ab}{p^i} \right] - a \left[\frac{b}{p^i} \right] \right) + \sum_{i=1}^j \left(\left[\frac{ab}{p^{k+i}} \right] - \left[\frac{a}{p^i} \right] \right) + \sum_{i=j+k+1}^{\infty} \left[\frac{ab}{p^i} \right] \geq \\ &\geq \sum_{i=1}^k \left(\left[\frac{ab}{p^i} \right] - a \left[\frac{b}{p^i} \right] \right) + \sum_{i=1}^j \left(\left[\frac{ap^k}{p^{k+i}} \right] - \left[\frac{a}{p^i} \right] \right) = \\ &= \sum_{i=1}^k \left(\left[\frac{ab}{p^i} \right] - a \left[\frac{b}{p^i} \right] \right) \geq 0, \end{aligned}$$

por cuanto, aplicando reiteradamente la propiedad 7.3. se tiene

$$\left[\frac{ab}{p^i} \right] \geq a \left[\frac{b}{p^i} \right].$$

7.10. Denotemos

$$f(x) = [2x] + [4x] + [6x] + [8x].$$

Si n es un entero positivo, entonces

$$f(x+n) = f(x) + 20n,$$

luego si un entero k puede expresarse como $f(x_0)$ para algún número real x_0 , entonces para $n = 1, 2, 3, \dots$ podemos expresar $k + 20n$ de manera similar, ya que $k + 20n = f(x_0 + n)$. Por consiguiente, basta determinar cuáles de los primeros 20 enteros positivos pueden ser generados por $f(x)$ cuando x recorre el intervalo semiabierto $(0, 1]$.

Obsérvese que cuando x se incrementa, el valor de $f(x)$ cambia únicamente si alguno de los números $2x, 4x, 6x, 8x$ sobrepasa un valor entero. En el intervalo $(0, 1]$ estos cambios ocurren cuando x es de la forma $\frac{m}{n}$, donde $1 \leq m \leq n$ y $n = 2, 4, 6$ u 8 . Existen 12 de estas fracciones, que escritas en forma creciente son

$$\frac{1}{8}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{3}{8}, \frac{1}{2}, \frac{5}{8}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{7}{8}, 1.$$

Por consiguiente, sólo 12 de los primeros 20 enteros positivos pueden ser representados en la forma deseada, y en consecuencia $12 \cdot 5 = 60$ de los primeros 100 enteros positivos pueden representarse así.

7.11. Supongamos que existe una solución x . Podemos escribir

$$x = n + \frac{a}{2} + \frac{b}{4} + \frac{c}{8} + \frac{d}{16} + \frac{e}{32} + f,$$

donde n es un entero, a, b, c, d, e son iguales a 0 ó 1, y $0 \leq f < \frac{1}{32}$. De la ecuación dada se desprende que:

$$63n + 31a + 15b + 7c + d + e = 12345;$$

se tiene además que:

$$63n < 12345 < 64n,$$

donde $n = 195$, $63n = 12285 = 12345 - 60$, y por tanto

$$31a + 15b + 7c + 3d + e = 60.$$

Pero como a, b, c, d, e toman únicamente los valores 0 ó 1, el valor máximo que puede tomar el primer miembro de la igualdad anterior es 57 y, por consiguiente, la ecuación original no tiene solución real.

7.12. El número k está ubicado entre dos potencias consecutivas de p , esto es

$$p^n < k \leq p^{n+1}$$

y por consiguiente, p^n es uno de los valores que puede tomar i . Entonces p es un divisor de

$$\binom{k}{p^n} = \frac{k!}{(p^n)!(k-p^n)!}.$$

Sean p^a, p^b y p^c las mayores potencias de p que dividen a $k!, (p^n)!$ y $(k-p^n)!$ respectivamente. Entonces

$$\begin{aligned} a &= \left[\frac{k}{p} \right] + \left[\frac{k}{p^2} \right] + \dots + \left[\frac{k}{p^n} \right] + \left[\frac{k}{p^{n+1}} \right], \\ b &= \left[\frac{p^n}{p} \right] + \left[\frac{p^n}{p^2} \right] + \dots + \left[\frac{p^n}{p^{n-1}} \right] + \left[\frac{p^n}{p^n} \right] = \\ &= p^{n-1} + p^{n-2} + \dots + p + 1 = \frac{p^n - 1}{p - 1}, \\ c &= \left[\frac{k - p^n}{p} \right] + \left[\frac{k - p^n}{p^2} \right] + \dots + \left[\frac{k - p^n}{p^{n-1}} \right] + \left[\frac{k - p^n}{p^n} \right] = \\ &= \left[\frac{k}{p} - p^{n-1} \right] + \left[\frac{k}{p^2} - p^{n-2} \right] + \dots + \left[\frac{k}{p^{n-1}} - p \right] + \left[\frac{k}{p^n} - 1 \right] = \\ &= \left[\frac{k}{p} \right] + \left[\frac{k}{p^2} \right] + \dots + \left[\frac{k}{p^{n-1}} \right] + \left[\frac{k}{p^n} \right] - (p^{n-1} + p^{n-2} + \dots + p + 1) = \\ &= \left[\frac{k}{p} \right] + \left[\frac{k}{p^2} \right] + \dots + \left[\frac{k}{p^{n-1}} \right] + \left[\frac{k}{p^n} \right] - \frac{p^n - 1}{p - 1}. \end{aligned}$$

La mayor potencia de p que divide a $\binom{k}{p^n}$ es p^{a-b-c} , es decir, $p^{\left[\frac{k}{p^{n+1}} \right]}$. Como $k \leq p^{n+1}$, el exponente $\left[\frac{k}{p^{n+1}} \right]$ es no nulo sólo si $k = p^{n+1}$, y sólo en este caso será p un divisor de $\binom{k}{p^n}$.

7.13. El mayor exponente al cual se puede elevar 2 para que divida a $n!$ es

$$\left[\frac{n}{2} \right] + \left[\frac{n}{2^2} \right] + \left[\frac{n}{2^3} \right] + \dots$$

Escribamos n en base 2, es decir

$$n = a_0 \cdot 2^k + a_1 \cdot 2^{k-1} + \dots + a_{k-1} \cdot 2 + a_k$$

donde $a_0 \neq 0$ y, para todo i tal que $0 \leq i \leq k$ se tiene $a_i = 0$ ó $a_i = 1$. En este caso,

$$\left[\frac{n}{2} \right] = \left[\frac{a_0 \cdot 2^k + a_1 \cdot 2^{k-1} + \dots + a_{k-1} \cdot 2 + a_k}{2} \right].$$

Como $a_k < 2$, se tiene

$$\left[\frac{n}{2} \right] = a_0 \cdot 2^{k-1} + a_1 \cdot 2^{k-2} + \dots + a_{k-1},$$

$$\left[\frac{n}{2^2} \right] = a_0 \cdot 2^{k-2} + a_1 \cdot 2^{k-3} + \dots + a_{k-2},$$

⋮

$$\left[\frac{n}{2^{k-1}} \right] = a_0 \cdot 2 + a_1,$$

$$\left[\frac{n}{2^k} \right] = a_0.$$

Sumando miembro a miembro estas igualdades, se tiene que la mayor potencia de 2 que divide a $n!$ es

$$a_0 \cdot 2^{k-1} + a_1 \cdot 2^{k-2} + \dots + a_{k-1} +$$

$$+ a_0 \cdot 2^{k-2} + a_1 \cdot 2^{k-3} + \dots + a_{k-2} +$$

⋮

$$+ a_0 \cdot 2 + a_1 +$$

$$+ a_0.$$

Por consiguiente, la mayor potencia de 2 que divide a $n!$ es

$$a_0 \cdot (2^k - 1) + a_1 \cdot (2^{k-1} - 1) + a_2 \cdot (2^{k-2} - 1) + \dots + a_{k-1} \cdot (2 - 1).$$

Sumando y restando a_k ,

$$a_0 \cdot (2^k - 1) + a_1 \cdot (2^{k-1} - 1) + a_2 \cdot (2^{k-2} - 1) + \dots + a_{k-1} \cdot (2 - 1) + a_k \cdot (1 - 1) =$$

$$= a_0 \cdot 2^k + a_1 \cdot 2^{k-1} + a_2 \cdot 2^{k-2} + \dots + a_{k-1} \cdot 2 + - (a_0 + a_1 + a_2 + \dots + a_{k-1} + a_k) =$$

$$= n - (a_0 + a_1 + a_2 + \dots + a_{k-1} + a_k).$$

Pero como $a_0 \neq 0$ y $a_i = 0$ ó $a_i = 1$ para todo i , entonces

$$n - (a_0 + a_1 + a_2 + \dots + a_{k-1} + a_k) \leq n - 1.$$

Si 2^{n-1} divide a $n!$ se sigue que la mayor potencia de 2 que divide a $n!$ es 2^{n-1} . Ahora bien, si

$$n - (a_0 + a_1 + a_2 + \dots + a_{k-1} + a_k) = n - 1,$$

entonces necesariamente

$$a_1 = a_2 = \dots = a_{k-1} = a_k = 0$$

ya que $a_0 = 1$, por tanto

$$n = 2^k + 0 \cdot 2^{k-1} + 0 \cdot 2^{k-2} + \dots + 0 \cdot 2 + 0,$$

$$n = 2^k.$$

Sección 8.

8.1. De acuerdo con la propiedad 8.8., la congruencia $x \equiv 1$ (mód. 4) es equivalente a $3x \equiv 3$ (mód. 12) (1), y la congruencia $x \equiv 2$ (mód. 3) es equivalente a $4x \equiv 8$ (mód. 12) (2). Restando miembro a miembro (2) menos (1) se tiene:

$$x \equiv 5 \pmod{12}$$

que es la congruencia buscada.

8.2. Sea $x = a_0 \cdot 100^n + a_1 \cdot 100^{n-1} + \dots + a_{n-1} \cdot 100 + a_n$. Como $100 \equiv -1$ (mód. 101), para todo entero positivo n se tiene:

$$100^n \equiv (-1)^n \pmod{101},$$

luego,

$$x \equiv a_0 \cdot (-1)^n + a_1 \cdot (-1)^{n-1} + \dots + a_{n-1} \cdot (-1) + a_n \pmod{101},$$

$$x \equiv (a_n + a_{n-2} + a_{n-4} + \dots) - (a_{n-1} + a_{n-3} + a_{n-5} + \dots) \pmod{101}.$$

Por tanto, x es divisible por 101 si y sólo si la diferencia entre la suma de las cifras que ocupan lugares impares (contando desde la derecha) y la suma de las cifras que ocupan lugares pares, escrito el número en base 100, es un múltiplo de 101.

8.3. Sea $x = a_0 \cdot 1000^n + a_1 \cdot 1000^{n-1} + \dots + a_{n-1} \cdot 1000 + a_n$. Como $1000 \equiv -1$ (mód. 7.13) se tiene

$$1000^n \equiv (-1)^n \pmod{7.13},$$

para todo entero positivo n . Luego,

$$x \equiv a_0 \cdot (-1)^n + a_1 \cdot (-1)^{n-1} + \dots + a_{n-1} \cdot (-1) + a_n \pmod{7.13},$$

$$x \equiv (a_n + a_{n-2} + a_{n-4} + \dots) - (a_{n-1} + a_{n-3} + a_{n-5} + \dots) \pmod{7.13}.$$

Por tanto, x es divisible por 7 ó por 13 si y sólo si la diferencia entre la suma de las cifras que ocupan lugares impares (contando desde la derecha) y la suma de las cifras que ocupan lugares pares, escrito el número en base 1000, es un múltiplo de 7 ó de 13 respectivamente.

Por otra parte se tiene

$$1000 \equiv 1 \pmod{37},$$

de donde

$$1000^n \equiv 1 \pmod{37}$$

para todo entero positivo n . Luego,

$$x \equiv a_0 + a_1 + \dots + a_{n-1} + a_n \pmod{37}.$$

Por tanto, x es divisible por 37 si y sólo si la suma de sus cifras, escrito el número en base 1000, es un múltiplo de 37.

8.4. Obsérvese que para todo k tal que $1 \leq k \leq m$, se tiene

$$k^2 \equiv (m-k)^2 \pmod{m},$$

luego, si $m > 2$ entonces $\{1^2, 2^2, \dots, m^2\}$ no es un sistema completo de restos módulo m .

8.5. Dados los enteros a, b, c, d , al menos dos de ellos son congruentes entre sí módulo 3, luego el producto de las seis diferencias es divisible por 3. Además, si no hay dos de esos enteros que sean congruentes entre sí módulo 4, entonces necesariamente dos de ellos son pares y los otros dos son impares; por consiguiente, el producto de las seis diferencias es divisible por 4.

8.6. $x^2 + y^2$ es congruente con 0, 1 ó 2 módulo 4, y si p es primo, entonces necesariamente $p \equiv 1 \pmod{4}$. Por consiguiente x^2 ó y^2 es congruente con 0 módulo 4 y al ser x, y primos y $x > y$, se deduce que $y = 2$.

Similarmente se puede ver que $b = 2$, y de

$$x^2 + 4 = a^2 + 4$$

se deduce que $x = a$.

8.7. Si $n = 2$ se tiene:

$$\begin{aligned} (a_1 + a_2)^p &= a_1^p + \binom{p}{1} a_1^{p-1} a_2 + \dots + \binom{p}{p-1} a_1 a_2^{p-1} + a_2^p \equiv \\ &\equiv a_1^p + a_2^p \pmod{p} \end{aligned}$$

Supongamos que se verifica:

$$(a_1 + a_2 + \dots + a_n)^p \equiv a_1^p + a_2^p + \dots + a_n^p \pmod{p}.$$

Entonces tenemos

$$\begin{aligned} (a_1 + a_2 + \dots + a_n + a_{n+1})^p &\equiv [(a_1 + a_2 + \dots + a_n) + a_{n+1}]^p \equiv \\ &\equiv (a_1 + a_2 + \dots + a_n)^p + a_{n+1}^p \equiv \\ &\equiv a_1^p + a_2^p + \dots + a_n^p + a_{n+1}^p \pmod{p}, \end{aligned}$$

por consiguiente la congruencia es cierta para todo entero positivo n .

8.8.

$$\begin{aligned} x^n - n(x-1) - 1 &= (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1) - n(x-1) = \\ &= (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1 - n). \end{aligned}$$

Por consiguiente, basta probar que $(x - 1)|(x^{n-1} + x^{n-2} + \dots + x + 1 - n)$. En efecto, obsérvese que

$$x^{n-1} - x^{n-2} \equiv 0 \pmod{x-1},$$

$$2x^{n-2} - 2x^{n-3} \equiv 0 \pmod{x-1},$$

$$3x^{n-3} - 3x^{n-4} \equiv 0 \pmod{x-1},$$

⋮

$$(n-1)x - (n-1) \equiv 0 \pmod{x-1}.$$

Sumando miembro a miembro las congruencias anteriores se llega a

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

conforme se quería demostrar.

8.9. Sean $a, b \in \{2, 5, 13, d\}$, con $a \neq b$, y supongamos que el número $ab - 1$ es un cuadrado perfecto. En particular tenemos:

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

$$5d - 1 = y^2, \tag{2}$$

$$13d - 1 = z^2, \tag{3}$$

para algunos enteros x, y, z . De la igualdad (1) se deduce que x es impar, luego $2d = x^2 + 1 \equiv 2 \pmod{8}$. Por consiguiente, $d \equiv 1 \pmod{4}$; luego d es impar y, en consecuencia, de acuerdo con (2) y (3), y, z son pares. Sean $y = 2y_1, z = 2z_1$. Como $z^2 - y^2 = 8d$, se tiene que

$$4z_1^2 - 4y_1^2 = 8d,$$

de donde

$$(z_1 - y_1)(z_1 + y_1) = 2d,$$

y en consecuencia

$$z_1 \equiv y_1 \pmod{2},$$

luego

$$(z_1 - y_1)(z_1 + y_1) = 2d \equiv 0 \pmod{4},$$

por tanto, resulta que d es par, lo cual es una contradicción.

8.10. Vamos a demostrar que si $a \equiv b \pmod{9}$ entonces $S(an) \equiv S(bn) \pmod{9}$ donde $S(x)$ es la suma de las cifras del número x . Ahora bien, si $a \equiv b \pmod{9}$ entonces $an \equiv bn \pmod{9}$, es decir, $9|(an - bn)$ y, de acuerdo con el criterio de divisibilidad por 9, $9|S(an - bn)$.

Faltaría probar que

$$S(an - bn) \equiv S(an) - S(bn) \pmod{9}.$$

Sean

$$x = a_0 \cdot 10^k + a_1 \cdot 10^{k-1} + \dots + a_{k-1} \cdot 10 + a_k,$$
$$y = b_0 \cdot 10^k + b_1 \cdot 10^{k-1} + \dots + b_{k-1} \cdot 10 + b_k,$$

agregando, si es necesario, algunos ceros a la izquierda de manera que x, y se escriban con el mismo número de cifras.

Entonces,

$$x - y \equiv S(x - y) \equiv (a_0 - b_0) + (a_1 - b_1) + \dots + (a_k - b_k) \pmod{9},$$

pero

$$S(x) = a_0 + a_1 + \dots + a_k,$$
$$S(y) = b_0 + b_1 + \dots + b_k,$$

de donde

$$S(x) - S(y) = (a_0 - b_0) + (a_1 - b_1) + \dots + (a_k - b_k) \equiv S(x - y) \pmod{9}.$$

En el caso dado, $4891 - 1984 = 2907$ y $9|2907$, luego $S(4891n) - S(1984n)$ es un múltiplo de 9.

8.11. Sea p un divisor común de $a^{2^m} + 1$ y $a^{2^n} + 1$. Supongamos que $n > m$. De la congruencia

$$a^{2^m} \equiv -1 \pmod{p},$$

elevando ambos miembros a la 2^{n-m} se tiene

$$(a^{2^m})^{2^{n-m}} \equiv (-1)^{2^{n-m}} \pmod{p}.$$

$$a^{2^n} \equiv 1 \pmod{p}.$$

Por otra parte

$$a^{2^m} \equiv -1 \pmod{p},$$

luego

$$2 \equiv 0 \pmod{p},$$

de donde $p|2$, por consiguiente, si a es par se tiene $(a^{2^m} + 1, a^{2^n} + 1) = 1$ y si a es impar, entonces $(a^{2^m} + 1, a^{2^n} + 1) = 2$.

8.12. Los enteros a, b, c satisfacen la igualdad $a^2 + b^2 = c^2$. Si c no es múltiplo de 5, hay que probar que $10 \mid \frac{ab}{2}$.

En primer lugar probemos que $5|ab$. Se tiene que c es congruente con 1, 2, 3 ó 4 módulo 5, y por consiguiente c^2 es congruente con 1 ó 4 módulo 5. Si $5 \nmid ab$, entonces $5 \nmid a$ y $5 \nmid b$, y se tiene que a^2 y b^2 son congruentes con 1 ó 4 módulo 5, de manera que $a^2 + b^2$ es congruente con 0, 2 ó 3 módulo 5, lo que contradice el hecho que c^2 es congruente con 1 ó 4 módulo 5. Por consiguiente, $5|ab$.

Veamos ahora que $4|ab$. Como c^2 es congruente con 0 ó 1 módulo 4, se presentan dos casos:

a) $c^2 \equiv 0$ (mód. 4). En este caso $a^2 \equiv 0$ (mód. 4) y $b^2 \equiv 0$ (mód. 4), por tanto a y b son pares y $4|ab$.

b) $c^2 \equiv 1$ (mód. 4). Como $c^2 = a^2 + b^2$ se tiene:

$$(a+b)^2 = a^2 + 2ab + b^2 = c^2 + 2ab,$$

luego

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

$$ab = \frac{(a+b+c)(a+b-c)}{2}.$$

Además, $a^2 \equiv 0$ (mód. 4) y $b^2 \equiv 1$ (mód. 4), o bien $a^2 \equiv 1$ (mód. 4) y $b^2 \equiv 0$ (mód. 4). Entonces se presentan las siguientes posibilidades.

1) $a \equiv 1$ (mód. 4) ó $a \equiv 3$ (mód. 4) y $b \equiv 0$ (mód. 4) ó $b \equiv 2$ (mód. 4),

2) $a \equiv 0$ (mód. 4) ó $a \equiv 2$ (mód. 4) y $b \equiv 1$ (mód. 4) ó $b \equiv 3$ (mód. 4).

En total, hay ocho casos posibles. Analicemos el primero de ellos.

Si $a \equiv 1$ (mód. 4) y $b \equiv 0$ (mód. 4), entonces $c \equiv 1$ (mód. 4), y se tiene que $a+b+c \equiv 2$ (mód. 4) y $a+b-c \equiv 0$ (mód. 4), por tanto, existen enteros k_1 y k_2 tales que

$$a+b+c = 4k_1 + 2,$$

$$c - b - c = 4k_2.$$

Entonces,

$$ab = \frac{(4k_1 + 2) \cdot 4k_2}{2} = 4k_2 \cdot (2k_1 + 1),$$

luego $4|ab$. Entonces, como $2 \mid \frac{ab}{2}$ y $5 \mid \frac{ab}{2}$ se concluye que $10 \mid \frac{ab}{2}$.

Para los casos restantes se hace un análisis similar.

8.13. Sea $A = \{2^1 - 1, 2^2 - 1, 2^3 - 1, \dots, 2^{2k} - 1\}$.

Si ningún elemento de A es divisible por $2k+1$, cada uno de los elementos de A debe ser congruente módulo $2k+1$ con alguno de los siguientes números:

$$1, 2, 3, \dots, 2k.$$

Se presentan dos casos:

a) Existen dos elementos de A , $2^r - 1$ y $2^t - 1$, con $r > t$, tales que

$$2^r - 1 \equiv 2^t - 1 \pmod{2k+1},$$

de donde

$$2^r - 2^t \equiv 0 \pmod{2k+1},$$

$$2^t(2^{r-t} - 1) \equiv 0 \pmod{2k+1},$$

$$(2k+1)|(2^{r-t} - 1),$$

y se llega a una contradicción por cuanto $2^{r-t} - 1$ es un elemento de A .

b) No existen dos elementos de A congruentes entre sí módulo $2k+1$. En este caso, alguno de los elementos de A debe ser congruente con $2k$ módulo $2k+1$, es decir, existe un entero r , $1 \leq r \leq 2k$, tal que

$$2^r - 1 \equiv 2k \pmod{2k+1},$$

$$2^r \equiv 2k+1 \pmod{2k+1},$$

y entonces $2k+1$ divide a 2^r , con lo cual también se llega a una contradicción. Por consiguiente, alguno de los elementos de A es divisible por $2k+1$.

8.14. Sea $d_n = (100 + n^2, 100 + (n+1)^2)$. Entonces,

$$d_n = (100 + n^2, 2n + 1).$$

Como $2n+1$ es impar, d_n es impar. Supongamos que $d_n = 2k+1$. Entonces se tiene:

$$2n+1 \equiv 0 \pmod{2k+1}, \quad (1)$$

$$100 + n^2 \equiv 0 \pmod{2k+1}. \quad (2)$$

De (1) se deduce:

$$n \equiv k \pmod{2k+1}. \quad (3)$$

De (2) se tiene: $n^2 \equiv -100 \pmod{2k+1}$, luego

$$n^2 \equiv -100 + (2k+1) \cdot 100 \pmod{2k+1},$$

$$n^2 \equiv 200k \pmod{2k+1},$$

y por (3),

$$n^2 \equiv k^2 \pmod{2k+1},$$

luego

$$k^2 \equiv 200k \pmod{2k+1}.$$

Como $(k, 2k + 1) = 1$ para todo entero k , se puede simplificar:

$$k \equiv 200 \pmod{2k + 1},$$

luego

$$\begin{aligned} 2k + 1 &\equiv 400 + 1 \pmod{2k + 1}, \\ 2k + 1 &\equiv 401 \pmod{2k + 1}. \end{aligned}$$

Como 401 es primo, entonces $2k + 1 = 401$ es el máximo valor que puede tomar d_n .
Falta ver que efectivamente d_n alcanza ese valor. Si

$$n \equiv 200 \pmod{2k + 1},$$

entonces

$$n^2 \equiv 301 \pmod{2k + 1},$$

luego

$$100 + n^2 \equiv 401 \pmod{2k + 1},$$

y dado que

$$2n + 1 \equiv 0 \pmod{2k + 1},$$

se tiene

$$100 + (n + 1)^2 \equiv 401 \pmod{2k + 1}.$$

Sección 9.

9.1. Si (x, y, z) es un triple pitagórico primitivo, entonces se tiene:

$$x = m^2 - n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2,$$

donde $m > n > 0$, $(m, n) = 1$ y m y n tienen diferente paridad. Si x, y, z están en progresión aritmética, entonces

$$y - x = z - y,$$

luego

$$2mn - m^2 + n^2 = m^2 + n^2 - 2mn,$$

$$4mn = 2m^2,$$

$$m = 2n.$$

Como $n|m$ y $(m, n) = 1$, se tiene necesariamente $n = 1$, luego $m = 2$ y el único triple pitagórico primitivo cuyos términos forman una progresión aritmética es $(3, 4, 5)$. Todos los triples que satisfacen la condición son de la forma $(3k, 4k, 5k)$, con $k \in \mathbb{Z}$.

9.2. De la igualdad $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ se desprende

$$y^2 z^2 + x^2 z^2 = x^2 y^2, \quad (1)$$

luego

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

y si $(x, y) = 1$, entonces

$$x^2 | z^2. \quad (2)$$

Similarmente, de $x^2 z^2 = x^2 y^2 - y^2 z^2 = y^2 (x^2 - z^2)$ se tiene que

$$y^2 | z^2. \quad (3)$$

Como hemos supuesto $(x, y) = 1$, de (2) y (3) se tiene

$$x^2 y^2 | z^2$$

y, dividiendo por $x^2 y^2$ ambos miembros de (1), nos queda

$$\left(\frac{z}{x}\right)^2 + \left(\frac{z}{y}\right)^2 = 1,$$

lo cual no es posible.

9.3. Si $x^2 + y^2 = z^2$ entonces x ó y es par. Si y es par, es de la forma $2mn$, con m y n de diferente paridad, luego

$$y \equiv 0 \pmod{4}. \quad (1)$$

Si $x \equiv 1$ ó $-1 \pmod{3}$ e $y \equiv 1$ ó $-1 \pmod{3}$, entonces $x^2 \equiv y^2 \equiv 1 \pmod{3}$, luego $z^2 \equiv 2 \pmod{3}$, lo cual no es posible y por tanto

$$x \equiv 0 \pmod{3} \text{ ó } y \equiv 0 \pmod{3}. \quad (2)$$

Por otra parte, si n es un entero se tiene

$$n^2 \equiv \begin{cases} 0 \pmod{5} & \text{si } n \equiv 0 \pmod{5}, \\ 1 \pmod{5} & \text{si } n \equiv 1 \text{ ó } n \equiv 4 \pmod{5}, \\ -1 \pmod{5} & \text{si } n \equiv 2 \text{ ó } n \equiv 3 \pmod{5}. \end{cases}$$

Se presentan los siguientes casos:

a) $x^2 \equiv y^2 \equiv 1 \pmod{5}$, luego $z^2 \equiv 2 \pmod{5}$ (imposible).

b) $x^2 \equiv y^2 \equiv -1 \pmod{5}$, luego $z^2 \equiv -2 \pmod{5}$ (imposible).

c) $x^2 \equiv 1 \pmod{5}$ e $y^2 \equiv -1 \pmod{5}$, o bien $x^2 \equiv -1 \pmod{5}$ e $y^2 \equiv 1 \pmod{5}$. Entonces $z^2 \equiv 0 \pmod{5}$, luego

$$z \equiv 0 \pmod{5}. \quad (3)$$

De (1), (2) y (3) se concluye que $xyz \equiv 0 \pmod{4 \cdot 3 \cdot 5}$, luego $60|xyz$.

9.4. Consideremos dos casos:

a) a impar. De la igualdad

$$a^2 + y^2 = z^2 \quad (1)$$

se desprende

$$\begin{aligned} a^2 &= z^2 - y^2, \\ a^2 &= (z+y)(z-y). \end{aligned}$$

Haciendo

$$\begin{aligned} z+y &= a^2, \\ z-y &= 1, \end{aligned}$$

se obtienen los valores

$$\begin{aligned} y &= \frac{a^2 - 1}{2}, \\ z &= \frac{a^2 + 1}{2}, \end{aligned}$$

que satisfacen la igualdad (1).

b) a par. De la igualdad

$$x^2 + a^2 = z^2$$

se tiene

$$\begin{aligned} a^2 &= z^2 - x^2, \\ a^2 &= (z+x)(z-x). \end{aligned}$$

Como $a^2 = 4k$, con $k > 1$, podemos hacer

$$\begin{aligned} z+x &= 2k, \\ z-x &= 2, \end{aligned}$$

de donde

$$\begin{aligned} 2z &= 2k + 2 = 2(k+1), \\ z &= k+1, \end{aligned}$$

y

$$\begin{aligned} 2x &= 2k - 2 = 2(k-1), \\ x &= k-1, \end{aligned}$$

con lo cual queda resuelto el problema.

9.5. En todo triángulo pitagórico primitivo de catetos x, y e hipotenusa z , se tiene $x^2 + y^2 = z^2$, donde $x = m^2 + n^2, y = 2mn, z = m^2 - n^2$, con $m > n > 0, (m, n) = 1$ y m, n de diferente paridad. Entonces, el perímetro $2p$ del triángulo es:

$$\begin{aligned} 2p &= x + y + z = \\ &= m^2 + n^2 + 2mn + m^2 - n^2 = \\ &= 2m^2 + 2mn = 2m(m + n). \end{aligned}$$

Si $60 = 2m(m + n)$, entonces $30 = m(m + n)$. Ahora bien, 30 se puede escribir como un producto de dos factores positivos de las siguientes maneras:

$$30 = 1.30,$$

$$30 = 2.15,$$

$$30 = 3.10,$$

$$30 = 5.6.$$

Es inmediato verificar que para ninguna de estas descomposiciones se pueden hallar valores de m y n que satisfagan las tres condiciones requeridas. Esto indica que no hay triángulos pitagóricos primitivos de perímetro 60. No obstante, esto no excluye la posibilidad de hallar soluciones no primitivas.

Los divisores propios de 30 son: 1, 2, 3, 5, 6, 10 y 15. De éstos, los únicos que se pueden expresar como producto de dos factores $m(m + n)$ donde m y n satisfagan las condiciones requeridas son: $6 = 2.3$ y $15 = 3.5$. Si $m = 2$ y $n = 1$, esto conduce al triángulo pitagórico primitivo $(3, 4, 5)$, cuyo perímetro es 12, y si $m = 3$ y $n = 2$ se tiene el triángulo pitagórico primitivo $(5, 12, 13)$, cuyo perímetro es 30. Luego, los únicos triángulos pitagóricos cuyo perímetro mide 60 son:

$$(15, 20, 25) \text{ y } (10, 24, 26).$$

9.6.

$$\begin{aligned} 5x^2 + 10xy + 10y^2 &= 4x^2 + 12xy + 9y^2 + x^2 - 2xy + y^2 = \\ &= (2x + 3y)^2 + (x - y)^2, \end{aligned}$$

Luego, la ecuación original puede escribirse como:

$$(2x + 3y)^2 + (x - y)^2 = (z + 1)^2.$$

Si denotamos $a = 2x + 3y, b = x - y, c = z + 1$, entonces las soluciones primitivas de $a^2 + b^2 = c^2$ son:

$$a = m^2 - n^2,$$

$$b = 2mn,$$

$$c = m^2 + n^2,$$

donde m y n son dos enteros arbitrarios, de diferente paridad, tales que $(m, n) = 1$ y $m > n > 0$.

Despejando x, y, z en términos de m y n , se obtienen las soluciones:

$$x = \frac{m^2 - n^2 + 6mn}{5}, \quad (1)$$

$$y = \frac{m^2 - n^2 - 4mn}{5}, \quad (2)$$

$$z = m^2 + n^2 - 1. \quad (3)$$

Por tanto, hay que agregar a m y n la condición adicional que sean tales que $m^2 - n^2 + 6mn \equiv m^2 - n^2 - 4mn \equiv 0$ (mód. 5). Como $m^2 - n^2 + 6mn \equiv m^2 - n^2 - 4mn \equiv m^2 - n^2 + mn \equiv 0$ (mód. 5), esto equivale a estudiar cuándo se verifica que

$$m^2 - n^2 + mn \equiv 0 \text{ (mód. 5)},$$

es decir,

$$m^2 \equiv n(n - m) \text{ (mód. 5)}.$$

Ahora bien, si $m \equiv 0$ (mód. 5) entonces $n \equiv 0$ (mód. 5), posibilidad que se descarta porque en este caso $(m, n) \neq 1$.

Si $m \equiv 1$ (mód. 5), entonces $n \equiv 3$ (mód. 5); si $m \equiv 2$ (mód. 5), entonces $n \equiv 1$ (mód. 5); si $m \equiv 3$ (mód. 5), entonces $n \equiv 4$ (mód. 5); si $m \equiv 4$ (mód. 5), entonces $n \equiv 2$ (mód. 5).

Con estas restricciones para m y n , (1), (2) y (3) dan las soluciones de la ecuación.

9.7. El área de un triángulo pitagórico primitivo viene dada por:

$$A = \frac{1}{2}xy = mn(m - n)(m + n).$$

Como m y n tienen diferente paridad, tres de los cuatro factores son impares. Además, es fácil ver que son primos dos a dos.

La única descomposición de 120 en 4 factores que cumplen con tales condiciones es:

$$120 = 1.3.5.8$$

(nótese que dos factores podrían ser iguales a 1 sólo en el caso de ser $m = 2, n = 1$, luego no es aplicable aquí).

Si $m + n = 8$, entonces $m = 5$ y $n = 3$ que son de la misma paridad y, por consiguiente, no hay soluciones primitivas. Esto no excluye la posibilidad de hallar soluciones no primitivas. Si los lados del triángulo son dx, dy, dz , entonces el área es:

$$A = \frac{1}{2} dxdy = d^2 mn(m-n)(m+n)$$

y $\frac{A}{d^2}$ puede ser el área de un triángulo primitivo. En su descomposición canónica, contiene un cuadrado perfecto (2^2), luego

$$\frac{A}{2^2} = 30,$$

y como

$$30 = 1.2.3.5,$$

haciendo $m+n = 5, m = 3, n = 2$, se tiene:

$$\begin{aligned} x_0 &= 9 - 4 = 5, \\ y_0 &= 12, \\ z_0 &= 9 + 4 = 13, \\ x &= 2x_0 = 10, \\ y &= 2y_0 = 24, \\ z &= 2z_0 = 26. \end{aligned}$$

El triángulo pitagórico de lados 10, 24 y 26 tiene por área 120.

Sección 10.

10.1. Como $91 = 7 \cdot 13$, se tiene $(n, 7) = (a, 7) = (n, 13) = (a, 13) = 1$.

De acuerdo con el teorema de Fermat

$$n^6 \equiv 1 \pmod{7} \text{ y } a^6 \equiv 1 \pmod{7},$$

de donde, elevando al cuadrado:

$$n^{12} \equiv 1 \pmod{7} \text{ y } a^{12} \equiv 1 \pmod{7}.$$

Además,

$$n^{12} \equiv 1 \pmod{13} \text{ y } a^{12} \equiv 1 \pmod{13}.$$

Como $(7, 13) = 1$, de (1) y (2) se concluye

$$n^{12} \equiv 1 \pmod{91} \text{ y } a^{12} \equiv 1 \pmod{91},$$

luego

$$n^{12} \equiv a^{12} \pmod{91},$$

$$91|(n^{12} - a^{12}).$$

10.2. De la igualdad:

$$\begin{aligned} n^7 - n &= n(n^6 - 1) = n(n^3 - 1)(n^3 + 1) = \\ &= n(n-1)(n+1)(n^2 + n + 1)(n^2 - n + 1), \end{aligned}$$

se concluye que $n^7 - n$ es divisible por 6, ya que en el último miembro aparece el producto de 3 enteros consecutivos. Además, de acuerdo con el teorema de Fermat se tiene:

$$n^7 \equiv n \pmod{7},$$

luego $7|(n^7 - n)$. Como $(6, 7) = 1$, se tiene:

$$42|(n^7 - n).$$

10.3. Si $19|(4n^2 + 4)$ entonces, como $(19, 4) = 1$, necesariamente $19|(n^2 + 1)$, es decir:

$$n^2 \equiv -1 \pmod{19},$$

pero hemos visto que esta congruencia no tiene solución cuando el módulo es un primo de la forma $4k + 3$, luego $19 \nmid (4n^2 + 4)$.

10.4. Si m es primo, entonces la parte directa del problema no es más que el teorema de Wilson.

Supongamos que $(m-1)! \equiv -1 \pmod{m}$. Si m es compuesto, entonces $m = ab$, donde a, b son enteros tales que $1 < a \leq b < m-1$.

Se pueden presentar los siguientes casos:

a) $a \neq b$. Entonces $ab|(m-1)!$, luego $(m-1)! \equiv 0 \pmod{m}$.

b) $a = b = 2$. Se verifica inmediatamente que $3! \not\equiv -1 \pmod{4}$.

c) $a = b \neq 2$. Entonces $2a = 2b < m-1$ y también $ab|(m-1)!$.

En conclusión, si m es compuesto, $(m-1)! \not\equiv -1 \pmod{m}$.

Nota. Obsérvese que hemos probado además, que si m es un número compuesto mayor que 4, entonces $(m-1)! \equiv 0 \pmod{m}$.

10.5. Se tiene:

$$\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n = \frac{3n^5 + 5n^3 + 7n}{15}.$$

De acuerdo con el teorema de Fermat, para todo entero positivo n se cumple:

$$n^5 \equiv n \pmod{5}, \text{ luego } 3n^5 \equiv 3n \pmod{15}, \quad (1)$$

$$n^3 \equiv n \pmod{3}, \text{ luego } 5n^3 \equiv 5n \pmod{15}, \quad (2)$$

y además se tiene:

$$7n \equiv 7n \pmod{15}. \quad (3)$$

Sumando miembro a miembro (1), (2) y (3) nos queda:

$$3n^5 + 5n^3 + 7n \equiv 15n \pmod{15},$$

luego

$$15|(3n^5 + 5n^3 + 7n).$$

10.6. Sabemos que

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

Como $\left(p, \frac{p-1}{2}\right) = 1$, basta probar que

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

y

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

Ahora bien, (1) se deduce inmediatamente del teorema de Wilson y (2) también se verifica por cuanto $\frac{p-1}{2} \mid (p-1)!$ y $\frac{p-1}{2} \mid (p-1)$. Esto completa la prueba.

10.7. a) Se tiene:

$$\begin{aligned} 2^2 \cdot 4^2 \cdot 6^2 \dots (p-1)^2 &= [2 \cdot 4 \cdot 6 \dots (p-1)]^2 = \\ \left[2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right) \right]^2 &= 2^{p-1} \cdot \left(\frac{p-1}{2} \right)^2!. \end{aligned}$$

Ahora bien, como p es impar, el teorema de Fermat garantiza que

$$2^{p-1} \equiv 1 \pmod{p}. \quad (1)$$

Por otra parte, como consecuencia del teorema de Wilson hemos probado que

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

de donde, multiplicando ambos miembros por $(-1)^{\frac{p-1}{2}}$ se tiene:

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

Multiplicando miembro a miembro (1) y (2):

$$2^{p-1} \cdot \left(\frac{p-1}{2} \right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

luego

$$2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

b) De acuerdo con el teorema de Wilson:

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

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

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \cdot 2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv 1 \pmod{p}.$$

Tomando en cuenta la parte (a) nos queda:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \cdot (-1)^{\frac{p+1}{2}} \equiv 1 \pmod{p},$$

y multiplicando ambos miembros por $(-1)^{\frac{p+1}{2}}$:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

10.8. Si p es un primo diferente de 2 y de 5, entonces $p \nmid 10$. De acuerdo con el teorema de Fermat se tiene:

$$10^{p-1} \equiv 1 \pmod{p},$$

luego

$$p \mid (10^{p-1} - 1),$$

y $10^{p-1} - 1$ es un número de la forma 999...999. Para todo entero positivo k se tiene $10^{k(p-1)} \equiv 1 \pmod{p}$, de donde $p \mid (10^{k(p-1)} - 1)$, por consiguiente, p divide a infinitos números de esa forma.

Además, si $p \neq 3$ entonces $(p, 9) = 1$, y como un número de la forma 999...999 es igual a $9 \cdot (111\ldots111)$, p divide también a infinitos números de la forma 111...111. Si por el contrario, $p = 3$, entonces p divide a todos los números de la forma 111...111 que tienen un número de cifras múltiplo de 3.

10.9. Sean $a = n, b = n + 1, c = n + 2$. Si $n + 1 = k^3$, entonces

$$a = k^3 - 1, b = k^3, c = k^3 + 1.$$

Debemos probar que $(k^3 - 1)k^3(k^3 + 1) \equiv 0 \pmod{504}$. Ahora bien, como $504 = 7 \cdot 8 \cdot 9$, debemos demostrar que el primer miembro de la congruencia es divisible por 7, por 8 y por 9.

a) Obsérvese que

$$(k^3 - 1)k^3(k^3 + 1) = k^9 - k^3 = k^2(k^7 - k),$$

y de acuerdo con el teorema de Fermat, $k^7 \equiv k$ (mód. 7), luego

$$(k^3 - 1)k^3(k^3 + 1) \equiv 0 \text{ (mód. 7).}$$

b) Si k es par, entonces $k = 2k_1$, luego

$$(k^3 - 1)(2k_1)^3(k^3 + 1) \equiv 0 \text{ (mód. 8).}$$

Si k es impar, entonces $k^3 - 1$ y $k^3 + 1$ son pares y, además, alguno de los dos es congruente con 0 módulo 4, luego

$$(k^3 - 1)k^3(k^3 + 1) \equiv 0 \text{ (mód. 8).}$$

c) Falta demostrar que $k^9 - k^3 \equiv 0$ (mód. 9). Tenemos:

$$k^9 - k^3 = k^3(k^6 - 1).$$

Si $3|k$, entonces $k^3 \equiv 0$ (mód. 9).

Si $3 \nmid k$, entonces $(k, 9) = 1$ y, de acuerdo con el teorema de Euler se tiene:

$$k^{\phi(9)} \equiv 1 \text{ (mód. 9).}$$

Pero $\phi(9) = 6$; por consiguiente:

$$k^6 \equiv 1 \text{ (mód. 9).}$$

10.10. De acuerdo con el teorema de Fermat,

$$1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \text{ (mód. 5).}$$

Sea $n = 4k + r$, donde k, r son enteros y $0 \leq r \leq 3$. Entonces, si a es igual a 1, 2, 3 ó 4, se tiene

$$a^n = a^{4k}a^r \equiv a^r \text{ (mód. 5),}$$

por consiguiente

$$1^n + 2^n + 3^n + 4^n \equiv 1^r + 2^r + 3^r + 4^r \text{ (mód. 5).}$$

De aquí se desprende que:

$$1^n + 2^n + 3^n + 4^n \equiv \begin{cases} 4 \text{ (mód. 5) si } r = 0, \\ 0 \text{ (mód. 5) si } r = 1, \\ 0 \text{ (mód. 5) si } r = 2, \\ 0 \text{ (mód. 5) si } r = 3. \end{cases}$$

Por consiguiente, $1^n + 2^n + 3^n + 4^n$ es divisible por 5 si y sólo si n no es divisible por 4.

10.11. Obsérvese que, si $n = 1$, entonces la ecuación no tiene solución entera, y si $n = 2$ entonces $m = 1$.

Sea $n = 4k + r$, donde k y r son enteros con $0 \leq r \leq 3$. De acuerdo con el teorema de Fermat se tiene

$$3^{4k} \equiv 1 \pmod{5},$$

luego

$$3^{4k+r} = 3^{4k} \cdot 3^r \equiv 3^r \pmod{5}.$$

Por tanto:

$$3^n \equiv \begin{cases} 1 \pmod{5} & \text{si } n \equiv 0 \pmod{4}, \\ 3 \pmod{5} & \text{si } n \equiv 1 \pmod{4}, \\ 4 \pmod{5} & \text{si } n \equiv 2 \pmod{4}, \\ 2 \pmod{5} & \text{si } n \equiv 3 \pmod{4}. \end{cases}$$

De la ecuación $3^n - 5^m = 4$ se tiene

$$3^n \equiv 4 \pmod{5},$$

por consiguiente $n \equiv 2 \pmod{4}$. Entonces podemos tomar $n = 4k + 2 = 2t$, donde $t = 2k + 1$. Luego,

$$3^{2t} - 4 = 5^m,$$

$$(3^t - 2)(3^t + 2) = 5^m,$$

y por tanto, si $n > 2$ entonces ambos factores de la izquierda son diferentes de 1 y deben verificarse, simultáneamente, las congruencias:

$$3^t \equiv 2 \pmod{5} \text{ y } 3^t \equiv -2 \pmod{5},$$

lo cual no es posible. Por consiguiente, la única solución en enteros positivos es $n = 2$, $m = 1$.

10.12. Si $p = 2$, entonces p divide a $2^n - n$ para todo entero par n . Supongamos p impar. Consideremos un entero positivo cualquiera m y tomemos

$$n = (mp - 1)(p - 1).$$

Entonces se tiene:

$$n = mp^2 - mp - p + 1 \equiv 1 \pmod{p}.$$

Por otra parte, aplicando el teorema de Fermat,

$$2^n = (2^{p-1})^{mp-1} \equiv 1^{mp-1} \equiv 1 \pmod{p}.$$

Por consiguiente, $2^n - n \equiv 0 \pmod{p}$ para infinitos valores de n .

10.13. La suma de los primeros n enteros positivos es $S_n = \frac{n(n+1)}{2}$, y su producto es $n!$. Hay que demostrar que $S_n|n!$ si y sólo si $n+1$ no es primo.

Supongamos $n+1$ primo. De acuerdo con el teorema de Wilson se tiene:

$$n! \equiv -1 \pmod{n+1},$$

de donde $(n+1) \nmid n!$. Como $n > 1$ y $n+1$ es primo, entonces $n+1 > 2$ y en consecuencia es impar, luego $S_n = \left(\frac{n}{2}\right)(n+1)$ donde $\frac{n}{2}$ es entero y, por tanto, $S_n \nmid n!$, lo cual contradice la hipótesis. Por consiguiente, $n+1$ no es primo.

Recíprocamente, supongamos que $n+1$ no es primo. Entonces $n+1 = ab$, donde a y b son enteros tales que $1 < a \leq b \leq n+1$. Consideremos dos casos.

a) Si $a < b$ entonces los factores a, b aparecen entre los números $1, 2, \dots, n-1$. Como $n! = n(n-1)!$, se puede escribir

$$n! = nabk.$$

Luego $n(n+1)|n!$ y, en consecuencia, $\frac{n(n+1)}{2} \mid n!$.

b) Si $a = b$ entonces $n+1 = a^2$ y por tanto, entre los números $1, 2, \dots, n+1$ aparece $a = (n+1)^{\frac{1}{2}}$. Debemos ver que a aparece como factor de otro término. El siguiente término que contiene un factor de a es:

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

Es preciso verificar que $2(n+1)^{\frac{1}{2}} < n-1$. Esto es,

$$4(n+1) < n^2 - 2n + 1,$$

$$n^2 - 6n - 3 > 0.$$

La desigualdad se cumple si $n \geq 7$. Ahora bien, los únicos enteros n menores que 7 para los cuales $n+1$ no es primo son 3 y 5. En el caso $n = 3$ se tiene $S_3 = 3! = 6$, luego $S_3|3!$. En el caso $n = 5$, $n+1 = 6$ no es cuadrado perfecto y estamos en el caso (a). Por consiguiente, para todo $n > 1$, si $n+1$ no es primo entonces $S_n|n!$.

Sección 11.

11.1. Si $15|(5x+1)(3x+2)$ entonces $3|(5x+1)(3x+2)$ y $5|(5x+1)(3x+2)$. Ahora bien, $3x+2 \equiv 2 \pmod{3}$ luego $3 \nmid (3x+2)$ y necesariamente se tiene:

$$5x+1 \equiv 0 \pmod{3},$$

de donde

$$\begin{aligned} 5x &\equiv -1 \pmod{3}, \\ -x &\equiv -1 \pmod{3}, \\ x &\equiv 1 \pmod{3}. \end{aligned} \tag{1}$$

Similarmente se observa que

$$3x + 2 \equiv 0 \pmod{5},$$

de donde

$$\begin{aligned} 3x &\equiv -2 \pmod{5}, \\ -2x &\equiv -2 \pmod{5}, \\ x &\equiv 1 \pmod{5}. \end{aligned} \tag{2}$$

De (1) y (2) se deduce inmediatamente que $(5x + 1)(3x + 2)$ es divisible por 15 para todos los x tales que

$$x \equiv 1 \pmod{15}.$$

11.2. Se requiere hallar todos los enteros x tales que, simultáneamente,

$$\begin{cases} x \equiv 1 \pmod{3} \\ \text{ó} \\ x \equiv 2 \pmod{3}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{4} \\ \text{ó} \\ x \equiv 2 \pmod{4}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{5} \\ \text{ó} \\ x \equiv 2 \pmod{5}. \end{cases}$$

Empleando la misma notación usada en el texto, se tiene:

$$m_1 = 3, \quad m_2 = 4, \quad m_3 = 5, \quad m = 60,$$

$$\frac{m}{m_1} = 20, \quad \frac{m}{m_2} = 15, \quad \frac{m}{m_3} = 12,$$

$$20b_1 \equiv 1 \pmod{3} \implies b_1 = -1,$$

$$15b_2 \equiv 1 \pmod{4} \implies b_2 = -1,$$

$$12b_3 \equiv 1 \pmod{5} \implies b_3 = -2.$$

$$x \equiv -20a_1 - 15a_2 - 24a_3 \pmod{60}.$$

Asignándoles a a_1, a_2, a_3 los valores 1 ó 2, se forma la tabla:

a_1	a_2	a_3	$x \pmod{60}$
1	1	1	1
1	1	2	-23
1	2	1	-14
1	2	2	22
2	1	1	-19
2	1	2	17
2	2	1	26
2	2	2	2

11.3. La congruencia $x^2 - 1 \equiv 0$ (mód. 56) es equivalente al par de congruencias:

$$\begin{aligned} x^2 - 1 &\equiv 0 \text{ (mód. 8)}, \\ x^2 - 1 &\equiv 0 \text{ (mód. 7)}. \end{aligned}$$

Por inspección, en sistemas completos de restos módulo 8 y módulo 7 respectivamente, se observa que la primera congruencia tiene por soluciones $x \equiv 1, 3, 5$ ó 7 (mód. 8) mientras que las soluciones de la segunda congruencia son $x \equiv 1$ ó 6 (mód. 7). Por consiguiente la congruencia $x^2 - 1 \equiv 0$ (mód. 56) tiene 8 soluciones, a saber, las soluciones de los siguientes sistemas de congruencias:

$$\begin{cases} x \equiv 1 \pmod{8}, \\ x \equiv 1 \pmod{7}. \end{cases}, \begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 1 \pmod{7}. \end{cases}, \begin{cases} x \equiv 5 \pmod{8}, \\ x \equiv 1 \pmod{7}. \end{cases}, \begin{cases} x \equiv 7 \pmod{8}, \\ x \equiv 1 \pmod{7}. \end{cases}$$

$$\begin{cases} x \equiv 1 \pmod{8}, \\ x \equiv 6 \pmod{7}. \end{cases}, \begin{cases} x \equiv 3 \pmod{8}, \\ x \equiv 6 \pmod{7}. \end{cases}, \begin{cases} x \equiv 5 \pmod{8}, \\ x \equiv 6 \pmod{7}. \end{cases}, \begin{cases} x \equiv 7 \pmod{8}, \\ x \equiv 6 \pmod{7}. \end{cases}$$

Estos sistemas pueden resolverse aplicando el teorema chino del resto, y se obtienen las soluciones:

$$x \equiv 1, -13, -27, 15, -15, 27, 136 - 1 \pmod{56}.$$

11.4. Como $210 = 2 \cdot 3 \cdot 5 \cdot 7$, la congruencia $11x + 1 \equiv 0$ (mód. 210) es equivalente al sistema de congruencias:

$$\begin{aligned} 11x + 1 &\equiv 0 \pmod{2}, \\ 11x + 1 &\equiv 0 \pmod{3}, \\ 11x + 1 &\equiv 0 \pmod{5}, \\ 11x + 1 &\equiv 0 \pmod{7}, \end{aligned}$$

de donde:

$$\begin{aligned} x &\equiv 1 \pmod{2}, \\ x &\equiv 1 \pmod{3}, \\ x &\equiv -1 \pmod{5}, \\ x &\equiv -2 \pmod{7}. \end{aligned}$$

Aplicando el teorema chino del resto a estas cuatro congruencias se obtiene la solución $x \equiv 19$ (mód. 210).

11.5. Como $35 = 5 \cdot 7$, la congruencia $5x^2 + 7x - 3 \equiv 0$ (mód. 35) es equivalente al par de congruencias:

$$5x^2 + 7x - 3 \equiv 0 \pmod{5},$$

$$5x^2 + 7x - 3 \equiv 0 \pmod{7},$$

En virtud de las identidades $5x^2 \equiv 0$ (mód. 5) y $7x \equiv 0$ (mód. 7), las congruencias anteriores se reducen a:

$$7x \equiv 3 \pmod{5},$$

(1)

$$5x^2 \equiv 3 \pmod{7}. \quad (2)$$

De (1) se deduce que $x \equiv 4 \pmod{5}$ y de (2) se tiene que $x \equiv 3 \pmod{7}$ ó $x \equiv 4 \pmod{7}$, luego la congruencia $5x^2 + 7x - 3 \equiv 0 \pmod{35}$ tiene dos soluciones, que son las de los sistemas de congruencias:

$$\begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 3 \pmod{7}. \end{cases} \quad \begin{cases} x \equiv 4 \pmod{5}, \\ x \equiv 4 \pmod{7}. \end{cases}$$

Aplicando el teorema chino del resto se obtienen las soluciones $x \equiv -11 \pmod{35}$ y $x \equiv 4 \pmod{35}$.

11.6. Consideremos k enteros positivos que sean primos dos a dos, por ejemplo, k números primos diferentes: p_1, p_2, \dots, p_k . Entonces, para todo $i, j = 1, \dots, k$, se tiene $(p_i^2, p_j^2) = 1$, de acuerdo con el teorema chino del resto, las congruencias:

$$\begin{aligned} x &\equiv -1 \pmod{p_1^2}, \\ x &\equiv -2 \pmod{p_2^2}, \\ &\vdots \\ x &\equiv -k \pmod{p_k^2}, \end{aligned}$$

tienen soluciones simultáneas. Si x_0 es una de tales soluciones, se tiene:

$$\begin{aligned} p_1^2 | (x_0 + 1), \\ p_2^2 | (x_0 + 2), \\ &\vdots \\ p_k^2 | (x_0 + k), \end{aligned}$$

conforme se quería demostrar.

Sección 12.

12.1. Los enteros positivos menores o iguales que 3600 que tienen un factor común con 3600 son aquellos que no son primos con 3600, luego su número es:

$$3600 - \phi(3600) = 3600 - 960 = 2640.$$

12.2. Sea $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Si $p | n$ entonces p coincide con alguno de los p_i ($i = 1, \dots, k$). Podemos suponer, sin pérdida de generalidad, que $p = p_1$. Entonces se tiene:

$$np = p_1^{\alpha_1 + 1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

$$\{2.3600 + 1, 2.3600 + 2, 2.3600 + 3, \dots, 3.3600\},$$

$$\{6.3600 + 1, 6.3600 + 2, 6.3600 + 3, \dots, 7.3600\},$$

son sistemas completos de restos módulo 3600, luego cada uno de ellos contiene el mismo número de enteros primos con 3600, esto es, $\phi(3600) = 960$. En total hay:

$$7.960 = 6720$$

de tales números.

12.8. Este resultado es una generalización del problema anterior. Los conjuntos:

$$\{1, 2, 3, \dots, m\},$$

$$\{m + 1, m + 2, m + 3, \dots, 2m\},$$

$$\{2m + 1, 2m + 2, 2m + 3, \dots, 3m\},$$

⋮

$$\{(k - 1)m + 1, (k - 1)m + 2, (k - 1)m + 3, \dots, km\},$$

son k sistemas completos de restos módulo m , en cada uno de los cuales hay $\phi(m)$ números primos con m . En total, el número de enteros positivos menores o iguales que mk que son primos con m es $k\phi(m)$.

12.9. Sean m y n dos enteros positivos tales que $(m, n) = 1$. Los divisores de mn son de la forma d_1d_2 , donde $d_1|m$, $d_2|n$ y $(d_1, d_2) = 1$. Entonces,

$$\begin{aligned} f(mn) &= \sum_{d_1 d_2 | mn} g(d_1 d_2) = \sum_{d_1 d_2 | mn} g(d_1)g(d_2) = \\ &= \sum_{d_1 | m} g(d_1) \sum_{d_2 | n} g(d_2) = f(m)f(n). \end{aligned}$$

12.10. Consideremos la función identidad g definida en el conjunto de los enteros positivos; esto es, $g(d) = d$ para todo entero positivo d . Obviamente, g es multiplicativa y, de acuerdo con el problema 12.9., también lo es la función f definida por:

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

Para todo primo p , la suma de los divisores de p^α es

$$1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$

$$\phi(np) = np \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right),$$

$$\phi(np) = p\phi(n).$$

Si $p \nmid n$, entonces $(p, n) = 1$ y se tiene:

$$\phi(np) = \phi(n)\phi(p) = (p-1)\phi(n).$$

12.3. Se sabe que:

$$\phi(mn) = mn \prod_{p|m \wedge p|n} \left(1 - \frac{1}{p}\right).$$

Si $n|m$ entonces todo primo p que divide a n , divide también a m . luego:

$$\prod_{p|m \wedge p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

de donde

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

12.4. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ entonces, de la igualdad

$$\phi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

se deduce: $\phi(n) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} (p_1-1)(p_2-1) \dots (p_k-1)$, donde se observa que si alguno de los p_i ($i = 1, \dots, k$) es impar, entonces $p_i - 1$ es par y, por consiguiente, $\phi(n)$ es par. Además, si $n = 2^\alpha$ y $\alpha > 1$, entonces $2^{\alpha-1}$ es par y $\phi(n)$, en consecuencia, también lo es. Luego, los únicos enteros n para los cuales $\phi(n)$ es impar son 1 y 2.

12.5. De acuerdo con el problema 12.2, $\phi(2n) = 2\phi(n)$ si $2|n$ y $\phi(2n) = \phi(n)$ si $2 \nmid n$, luego $\phi(2n) = \phi(n)$ si n es impar y $\phi(2n) > \phi(n)$ si n es par.

12.6. Si $n = 5^\alpha$, entonces

$$\phi(n) = 5^\alpha \cdot \left(1 - \frac{1}{5}\right) = 4 \cdot 5^{\alpha-1},$$

que no es divisible por 3 para ningún entero α .

12.7. Obsérvese que $25200 = 7 \cdot 3600$. Los conjuntos:

$$\{1, 2, 3, \dots, 3600\},$$

$$\{3600 + 1, 3600 + 2, 3600 + 3, \dots, 2 \cdot 3600\},$$

$$\{2.3600 + 1, 2.3600 + 2, 2.3600 + 3, \dots, 3.3600\},$$

$$\{6.3600 + 1, 6.3600 + 2, 6.3600 + 3, \dots, 7.3600\},$$

son sistemas completos de restos módulo 3600, luego cada uno de ellos contiene el mismo número de enteros primos con 3600, esto es, $\phi(3600) = 960$. En total hay:

$$7.960 = 6720$$

de tales números.

12.8. Este resultado es una generalización del problema anterior. Los conjuntos:

$$\{1, 2, 3, \dots, m\},$$

$$\{m + 1, m + 2, m + 3, \dots, 2m\},$$

$$\{2m + 1, 2m + 2, 2m + 3, \dots, 3m\},$$

$$\{(k-1)m + 1, (k-1)m + 2, (k-1)m + 3, \dots, km\},$$

son k sistemas completos de restos módulo m , en cada uno de los cuales hay $\phi(m)$ números primos con m . En total, el número de enteros positivos menores o iguales que mk que son primos con m es $k\phi(m)$.

12.9. Sean m y n dos enteros positivos tales que $(m, n) = 1$. Los divisores de mn son de la forma d_1d_2 , donde $d_1|m$, $d_2|n$ y $(d_1, d_2) = 1$. Entonces,

$$\begin{aligned} f(mn) &= \sum_{d_1d_2|mn} g(d_1d_2) = \sum_{d_1d_2|mn} g(d_1)g(d_2) = \\ &= \sum_{d_1|m} g(d_1) \sum_{d_2|n} g(d_2) = f(m)f(n). \end{aligned}$$

12.10. Consideremos la función identidad g definida en el conjunto de los enteros positivos; esto es, $g(d) = d$ para todo entero positivo d . Obviamente, g es multiplicativa y, de acuerdo con el problema 12.9., también lo es la función f definida por:

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

Para todo primo p , la suma de los divisores de p^α es

$$1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1},$$