Notas de Aritmética para la Olimpiada de Matemáticas.

24 de septiembre de 2001

Índice General

Introducción.

Este libro fue creado para el entrenamiento de la selección estatal de la Olimpiada de Matemáticas en Yucatán. El objetivo que se busca no es crear un curso con el material expuesto, sino que se use como referencia y guía. Esto significa que no es necesario cubrir en clase todo el material que se incluye, pues eso representaría una pérdida enorme de tiempo de entrenamiento, además que se corre el riesgo de enfatizar más la acumulación de conocimiento en vez de la habilidad de problemas.

El entrenamiento consta de aproximadamente seis meses. Durante los dos primeros, es aconsejable revisar los conceptos de divisibilidad y máximo común divisor, realizando la mayor cantidad de ejercicios posibles. Se recomienda que al final de los mismos se empiece a usar la terminología de congruencias esporádicamente para que al abordar el tema a partir del tercer mes ya se tenga una cierta familiaridad con el concepto. El objetivo final de todo el curso es que los alumnos dominen los conceptos y teoremas de congruencia, de manera que los primeros dos meses son sólo una introducción a las ideas principales de la Teoría de los Números.

Es por esto que se recomienda iniciar la resolución de problemas usando los métodos de congruencia a partir del tercer mes, ya que se ha visto que posponer el estudio de las mismas causa que los alumnos no adquieran la familiaridad con los métodos de las mismas, atacando los problemas exclusivamente por los métodos más débiles de la divisibilidad y el Algoritmo de la División.

Finalmente quiero enfatizar que la parte central del presente libro la constituyen las secciones de problemas. Los problemas tienen un nivel de dificultad variado, y en vez de soluciones se incluyen únicamente sugerencias para la resolución en la mayoría de los casos. La razón para este enfoque es que una gran cantidad de problemas pueden resolverse usando distintas técnicas además de que el proceso de análisis y exploración de los problemas es mucho más provechoso que leer la solución misma. Así, se evita “dirigir” al alumno por un camino exclusivo pero al mismo tiempo se proporcionan puntos guía en caso de encontrar dificultades.

Pedro Sánchez.
Mérida, Yucatán. 2001.

— No sólo lee. ¡Combátelo! Haz tus propias preguntas, busca tus propios ejemplos, descubre tus propias pruebas. ¿Es esta hipótesis necesaria? ¿Se cumple el recíproco? ¿Qué pasa en el caso especial clásico? ¿Y qué hay de los casos degenerados? ¿En qué parte usa la prueba la hipótesis?

Paul. R. Halmos, I want to be a mathematician.

— Las Matemáticas consisten en probar la cosa más obvia de la manera menos obvia.

G. Polyá, Mathematical Maxims and Minims.

1 Divisibilidad

1.1 Conceptos básicos.

El concepto fundamental en el que estaremos interesados ahora, será el de divisibilidad, por ello, introducimos la siguiente definición.

No confundir $a \mid b$ con a/b. Por ejemplo, $2 \mid 10$ no es lo mismo que $2/10$. En el primer caso estamos diciendo que 10 es múltiplo de 2, y en el segundo la fracción $\frac{2}{10} = 0.2$.

Definicion 1.1 Sean a y b dos números enteros. Decimos que a *divide a* b (lo que simbolizamos con $a \mid b$) si existe un entero c tal que $b = ac$. Esto equivale a decir a que b es múltiplo de a, o que la división $b \div a$ no deja residuo.

Si a no divide a b, escribimos $a \nmid b$. Esto es lo mismo que decir que la división $b \div a$ deja residuo.

Ejemplos:

i $3 \mid 12$ pues $12 = 4 \cdot 3$

ii $4 \nmid 10$ ya que no existe un entero c tal que $10 = 4c$.

iii $4 \mid 20$ ya que si $c = 5$, $20 = 4c$.

iv $3 \mid 0$ dado que $0 = 3c$ cuando $c = 0$.

v $1 \mid 5$ puesto que $5 = 1 \cdot 5$

vi $5 \nmid 1$ dado que $1 \neq 5c$ para cualquier entero c.

vii Para cualquier entero a, $a + 1 \mid a^2 - 1$, ya que $a^2 - 1 = (a + 1) \cdot k$ con $k = a - 1$.

De la definición, podemos derivar ciertas propiedades básicas:

1. Todo número se divide a sí mismo: $a \mid a \quad \forall a \in \mathbb{Z}$.
2. Si $a \mid b$, entonces $a \mid -b$. Como $4 \mid 8$ ($8 = 4 \cdot 2$), $4 \mid -8$ (pues $-8 = 4(-2)$).

3. Si $a \mid b$, entonces $a \mid bc$ para todo entero c. ($4 \mid 12$, entonces $4 \mid 12{\cdot}5$).
4. Si a, b son positivos y $a \mid b$, entonces $a \leq b$.
5. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$. Ejemplo: $2 \mid 10$ y $10 \mid 30$, entonces $2 \mid 30$.
6. Si $a \mid b$ y $a \mid c$ entonces $a \mid (b + c)$. Así, $2 \mid 4$ y $2 \mid 6$ implica $2 \mid (4 + 6)$.

El recíproco no siempre se cumple: $4 \mid 6{\cdot}2$ *pero* $4 \nmid 6$ *y* $4 \nmid 2$.

El recíproco no siempre se cumple: $4 \mid 5 + 3$ *pero* $4 \nmid 5$ *y* $4 \nmid 3$

La prueba de la última propiedad es típica de las pruebas de problemas de divisibilidad, así que se incluye para tener un modelo.

Prueba. Si $a \mid b$ y $a \mid c$, entonces existen enteros m y n tales que $b = am$ y $c = an$. Entonces $b + c = am + an = a(m + n)$. Como $b + c = ak$ cuando $k = (m + n)$, la definición de divisibilidad nos dice que $a \mid (b + c)$. La prueba queda terminada. ∎

La prueba anterior puede extenderse a varios sumandos:

Teorema 1.1 *Si* $a \mid x_1, a \mid x_2, a \mid x_3, \ldots a \mid x_n$*, entonces*

$$a \Big| \big(c_1x_1 + c_2x_2 + c_3x_3 + \cdots + c_nx_n\big)$$

para cualquier combinación de enteros $c_1, c_2, c_3, \ldots, c_n$*.*

▷ Dados a y b, un número de la forma $ax + by$ se denomina una combinación lineal de a y b. En general, dados $x_1, x_2, \ldots, x_n$, un número de la forma $u_1x_1 + u_2x_2 + \cdots + u_nx_n$ se conoce como una combinación lineal de los números $x_1, x_2, \ldots, x_n$. Entonces el teorema anterior lo enunciamos: "Si un número divide a un conjunto de enteros, divide a cualquier combinación lineal de los mismos".

What?

Por ejemplo, dado que $3 \mid 6$, $3 \mid 12$ y $3 \mid 15$, aplicando el teorema anterior con $c_1 = 5, c_2 = -7, c_3 = 2$, deducimos que $3 \Big| (6{\cdot}5 + 12{\cdot}(-7) + 15{\cdot}2)$

El concepto de divisibilidad puede generalizarse de la siguiente manera:

Teorema 1.2 (Algoritmo de la división.) *Sean* a *y* b *dos enteros con* $b > 0$*. Entonces existen enteros únicos* c *y* r *tales que* $a = bc + r$ *y* $0 \leq r < b$*.*

Si $r = 0$ *obtenemos* $b \mid a$*.*

Lo importante a notar es que el residuo es positivo y cumple $0 \leq r < b$, y si $b \nmid a$ entonces $0 < r < b$. Básicamente, el entero c es el cociente de la división $a \div b$ y r es el residuo.

Ejemplos:

- $a = 12, b = 5$. $a = b{\cdot}2 + 2$.
- $a = 38, b = 8$. $a = b{\cdot}4 + 6$.
- $a = 20, b = 4$. $a = b{\cdot}5 + 0$.
- $a = 7, b = 10$. $a = b{\cdot}0 + 7$.
- $a = -15, b = 4$. $a = b{\cdot}(-4) + 1$.
- $a = 18, b = -5$. $a = b{\cdot}(-3) + 3$.
- $a = -14, b = -3$. $a = b{\cdot}5 + 1$.

Este algoritmo adquirirá mayor importancia en la siguiente sección.

Definicion 1.2 Un número positivo se llama *número primo* si tiene sólo dos divisores positivos distintos. Un número mayor a 1 que no es primo se denomina *compuesto*.

Nota que el 1 no es primo ni compuesto.

Teorema 1.3 *Todo número mayor a 1 es divisible por algún primo.*

Prueba. Sea $n > 1$. Supongamos que no es divisible por ningún primo. En particular, n mismo no puede ser primo pues sería divisible entre sí mismo. Como n no es primo, tiene algún divisor positivo d_1 distinto de 1 y n, es decir, $1 < d_1 < n$. Pero d_1 no puede ser primo porque dividiría a n. Entonces existe un d_2 que divide a d_1 tal que $1 < d_2 < d_1 < n$. Como d_2 no puede ser primo porque divide a n, repetimos el argumento con d_2 para obtener un d_3 tal que $1 < d_3 < d_2 < d_1 < n$. Como d_3 no puede ser primo existe d_4 que divide a d_3 y así sucesivamente. Esto lleva a una contradicción pues no es posible continuar indefinidamente este proceso ya que entre 1 y n sólo hay un número finito de términos. Por tanto, n debe ser divisible entre algún primo. ∎

▷ Este tipo de pruebas se conocen como por descenso infinito y se basa en que si la condición pedida no se cumple se crea una sucesión infinita decreciente de enteros positivos, lo cual es imposible porque los enteros positivos tienen elemento mínimo. Las pruebas por descenso infinito fueron ampliamente usadas por Fermat.

Siempre se puede caer más bajo. - Anónimo.

El teorema anterior será usado en muchas pruebas en la siguiente forma: "Si n es un número compuesto n, hay un primo p que lo divide."

Sea n un entero mayor a 1. Si n es primo, es igual a sí mismo. Si no es primo existe un primo p_1 que lo divide y entonces $p = p_1 n_1$. Si n_1 es primo, n es igual a un producto de primos, de lo contrario existe un primo p_2 que divide a n_1 y así $p = p_1 p_2 n_2$. Si n_2 es primo, n es igual a un producto de primos, en caso contrario existe un primo p_3 que lo divide. Continuamos aplicando este argumento y construimos una sucesión $n_1, n_2, n_3 \ldots$ decreciente de enteros positivos que debe terminar, es decir, en algún momento n_k es un número primo. De esta manera ya probamos el siguiente teorema:

Teorema 1.4 *Todo número mayor a 1 puede escribirse como producto de primos.*

Es decir, un número $n > 1$ puede escribirse de la forma:

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

donde cada p_j es un número primo.

Por ejemplo, $12 = 2^2 \cdot 3$, $60 = 2^4 \cdot 3 \cdot 5$, $101 = 101$, $99 = 3 \cdot 11$. Ahora bien, al igual que $12 = 2 \cdot 6 = 3 \cdot 4$ tiene varias factorizaciones, nada nos garantiza que un número dado no se pueda factorizar de maneras diferentes en producto de primos (sin importar el orden). Pero después probaremos que para cada número dado la factorización en primos sí es única. Así podemos establecer el siguiente teorema (aunque la prueba de la unicidad la posponemos hasta tener las herramientas necesarias).

Teorema 1.5 (Teorema Fundamental de la Aritmética) *Todo número se puede factorizar de manera única como producto de primos.*

Para finalizar la sección probaremos uno de los resultados clásicos de la Teoría de los números y que fue establecido hace cerca de 2000 años.

Teorema 1.6 (Euclides) *Hay una cantidad infinita de números primos.*

Prueba. Supongamos que hay una cantidad finita de números primos y sea $p_1, p_2, \ldots, p_n$ la lista de todos ellos. Consideremos el número $p_1 p_2 \cdots p_n + 1$. Como ese número es mayor a 1 hay un primo que lo divide. Sea p_k tal que $p_k \mid p_1 p_2 \cdots p_n + 1$. Como $p_k \mid p_1 p_2 \cdots p_n$ se sigue que $p_k \mid 1$, lo cual es imposible. Concluimos que debe existir una cantidad infinita de primos. ∎

1.2 Máximo común divisor.

Definicion 1.3 Dados dos números a y b no negativos y no ambos cero, el mayor número que divide a los dos se denomina *máximo común divisor de a y b*. Denotamos a este número como (a, b). En general, dado un conjunto de enteros no negativos y no todos cero $\{a_1, a_2, \ldots, a_n\}$, definimos su máximo común divisor $(a_1, a_2, \ldots, a_n)$ como el mayor entero positivo que los divide a todos.

La definición anterior implica que (a, b) siempre es positivo. Esto es claro pues si (a, b) fuera negativo, $-(a, b)$ también sería un divisor común de a y b, por lo que (a, b) no sería el menor.

Algunas propiedades básicas son:

1. $(a, 1) = 1$ para toda a.
2. $(a, a) = a$ para toda a.
3. $(a, 0) = a$ para toda a.
4. $(a, b) = (b, a)$.
5. $(a, b) = (b, a - b)$.

Para probar la última propiedad notemos que si un número divide a a y a b, divide a $a - b$ por lo que es un divisor común de b y $a - b$. A la inversa, si divide a b y a a $a - b$ divide a $(a-b)+b = a$. Esto implica que los divisores comunes de a y b son los mismos que los de b y $a - b$ y por tanto el mayor de ambos conjuntos es el mismo número.

Esta propiedad también nos permite calcular el MCD de dos números dados. Por ejemplo, sean $a = 24, b = 8$. Entonces

$$(26, 10) = (10, 16) = (16, 10) = (10, 6) = (6, 4) = (4, 2) = (2, 0) = 0.$$

Despacio que llevo prisa.

Estas cuentas se pueden acelerar mediante el uso del algoritmo de la división. Si $a = bq + r$ con $0 \leq r < b$ entonces $(a, b) = (b, a - bq) = (b, r)$. Se deja la prueba de estas igualdades al lector. Así, como $26 = 10 \cdot 2 + 6$ el cálculo anterior se convierte en:

$$(26, 10) = (10, 6) = (6, 4) = (4, 2) = (2, 0) = 0.$$

El proceso arriba mencionado se conoce como **Algoritmo de Euclides**.

Teorema 1.7 *Si g es el máximo común divisor de a y b, entonces existen enteros u, v tales que $g = au + bv$.*

Prueba. Consideremos el conjunto de todos los números de la forma $ax + by$ con x, y enteros (el conjunto de combinaciones lineales de a y b). De este conjunto, escojamos

el menor entero positivo y llamémosle d Sean u, v tales que $d = au + bv$.
Si $d \nmid a$ aplicamos el algoritmo de la división $a = dq + r$ con $0 < r < d$. Pero

$$r = a - dq = a - (au + bv)q = a\big(1 - qu\big) + b\big(-qv\big)$$

significa que r es positivo, está en el conjunto y es menor a d. Esto es una contradicción ya que habíamos supuesto que d era el menor número positivo del conjunto. Por tanto, $d \mid a$. Por un argumento similar obtenemos que $d \mid b$.
Ahora, sea g el máximo común divisor de a y b. Como $g \mid a$ y $g \mid b$, $g \mid au + bv$. Si $g \neq d$ tendríamos que $g < d$, es decir, g no era el mayor de todos los divisores comunes de a y b, lo cual es una contradicción. Concluimos pues, que $g = d$. ∎

Corolario 1.8 *El máximo común divisor de a y b es la combinación lineal positiva más pequeña de ambos.*

Corolario 1.9 *Si $(a, b) = 1$, la ecuación $ax + by = 1$ tiene solución entera.*

Prueba. Hállese los enteros x, y para los que $(a, b) = ax + by$. ∎ *¿Y cómo se hallan esos números?*

Corolario 1.10 $(a, a + 1) = 1$.

Prueba. $(-1)\cdot a + (1)\cdot(a - 1) = 1$, Entonces 1 es la combinación lineal positiva más pequeña y por tanto igual a $(a, a + 1)$. ∎

Teorema 1.11 $(am, bm) = m(a, b)$.

Prueba. (am, bm) es el menor valor positivo de $amx + bmy = m(ax + by)$. Esto es lo mismo que m veces el menor valor positivo de $ax + by$ el cual es (a, b). ∎

Corolario 1.12 *Si $d = (a, b)$ entonces* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Otra manera de caracterizar el máximo común divisor de a y b es como sigue. Supongamos que d es cualquier divisor común de a y de b. Entonces d divide a cualquier combinación lineal de a y b, en particular divide a la menor positiva, es decir, divide a (a, b). Y como $a \mid b$ implica $a \leq b$, (a, b) es el único número con esta propiedad. Esto prueba el siguiente teorema.

Teorema 1.13 *El máximo común divisor de a y b es el único entero positivo que es divisible entre cualquier número que divida tanto a a como a b.*

Definicion 1.4 Dados dos números a, b, decimos que son *primos relativos*, si $(a, b) = 1$. En general, decimos que un conjunto $\{x_1, x_2, \ldots, x_n\}$ de enteros son primos relativos entre sí cuando $(x_1, x_2, \ldots, x_n) = 1$.

Definicion 1.5 Dado un conjunto $\{x_1, x_2, \ldots, x_n\}$ de enteros, decimos que son *primos relativos dos a dos* si $(x_i, x_j) = 1$ para cualquier pareja x_i, x_j.

Ser primos relativos entre sí y ser primos relativos dos a dos no es lo mismo. Por ejemplo, los números $4, 6, 9$ son primos relativos entre sí puesto que $(4, 6, 9) = 1$, pero no son primos relativos dos a dos ya que $(4, 6) = 2$.

A continuación se enuncia uno de los resultados más usados en relación al máximo común divisor y a la vez uno de los más fuertes, ya que será pieza clave en la demostración del Teorema Fundamental de la Aritmética.

Teorema 1.14 *Si $c \mid ab$ y $(c,a) = 1$ entonces $c \mid b$.*

Prueba. Como $c \mid ab$ y $c \mid bc$, $c \mid (ab, bc)$. Pero $(ab, bc) = b(a, c) = b$. Por tanto, $c \mid ab$. ∎

Un caso muy especial se obtiene cuando c es primo.

Teorema 1.15 *Si p es primo y divide a ab, y p no divide a a entonces p divide a b.*

Prueba. Sea $d = (a, p)$. Entonces $d \mid p$ por lo que d sólo puede ser 1 o p. Como $p \nmid a$ tenemos que $d \neq p$ y por tanto $d = 1$. Aplicando el teorema anterior llegamos a que $p \mid b$. ∎

Teorema 1.16 (Teorema Fundamental de la Aritmética) *Todo número se puede factorizar de manera única como producto de primos.*

Prueba. Ya hemos probado que todo número se puede factorizar en primos, y nos resta probar la unicidad de esta factorización. Sean

$$n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} = q_1^{b_1} q_2^{b_2} \cdots q_v^{b_v}$$

dos factorizaciones distintas donde por conveniencia suponemos que los primos aparecen listados en orden creciente. Cada p_i divide a n y por tanto a alguna q_j (aplicando varias veces el resultado anterior. Pero un primo divide a otro si y sólo si son el mismo. Entonces cada p_i es alguna q_k, y por un argumento similar cada q_k es alguna p_i, esto implica que $p_i = q_i$ para cada i.
Falta ver que las potencias son las mismas, pero si por ejemplo $a_j < b_j$ dividimos a ambos lados entre $p_j^{a_j}$ y del lado derecho nos sobran factores p_j que dividen al lado izquierdo y son iguales a alguna p_k, lo cual es imposible. Una contradicción similar elimina el caso $a_j > b_j$.
Así, podemos concluir que las factorizaciones son las mismas. ∎

Ahora, retomemos el problema de expresar el máximo común divisor de dos números como combinación lineal de los mismos. Probamos que siempre es posible escribir (a, b) en la forma $au + bv$ donde u y v son enteros y hemos usado este hecho en diversas pruebas, aunque no mencionamos de manera explícita cómo hallar esos números. El procedimiento para hallar los coeficientes a y b se basa en el algoritmo de la división y más que escribir explícitamente el proceso, lo ilustraremos con un ejemplo. Así, deseamos expresar $(124, 44)$ como combinación lineal de 124 y 44.

$$\begin{aligned} 124 &= 44{\cdot}2 + 36 \\ 44 &= 36{\cdot}1 + 8 \\ 36 &= 8{\cdot}4 + 4 \\ 8 &= 4{\cdot}2 + 0 \end{aligned}$$

Entonces $(124, 44) = 4$ (es el último residuo distinto de cero). Despejamos el 4 y empezamos a sustituir de la siguiente manera:

$$\begin{aligned} 4 &= 36 - 4 \cdot 8 \\ &= 36 - 4\Big(44 - 36\Big) \\ &= 5 \cdot 36 - 4{\cdot}44 \\ &= 5\Big(124 - 44{\cdot}2\Big) - 4{\cdot}44 \\ &= 5{\cdot}124 - 14{\cdot}44 \end{aligned}$$

Así, $4 = 124{\cdot}5 - 44{\cdot}14$. Comparemos esto con el proceso para calcular únicamente $(124, 44)$ (versión rápida):

$$(124, 44) = (44, 36) = (36, 8) = (8, 4) = (4, 0) = 4$$

y notemos que los números que aparecen son los mismos que aparecen al desarrollar todo el algoritmo de la división, con lo que comprobamos que el algoritmo de Euclides es en realidad la aplicación sucesiva del algoritmo de la división.

▷ Vale la pena recalcar que los coeficientes que se encuentran no son únicos, de hecho hay una infinidad de soluciones. Para este caso en particular notamos que

$$\left(5 + \frac{44t}{4}\right) 124 - \left(14 + \frac{124t}{4}\right) = (5 + 11t)124 - (14 + 31t)44 = 4$$

cada entero t nos genera una combinación distinta.

1.3 Mínimo común múltiplo.

Definicion 1.6 Si a, b son enteros (no ambos cero), entonces el *mínimo común múltiplo de a y b* es el menor entero *positivo* que es múltiplo tanto de a com ode b. Este número lo denotamos con $[a, b]$.

Podemos extender la definición a un conjunto $a_1, a_2, a_3, \ldots, a_n$ de enteros que no sean todos cero, definiendo su mínimo común múltiplo como el menor entero positivo que es múltiplo de todos ellos.

Estamos interesados en buscar alguna relación entre el máximo común divisor y el mínimo común múltiplo. Escojamos dos números, digamos

$$a = 252 = 2^2 \cdot 3^2 \cdot 7 \qquad \text{y} \qquad b = 735 = 3 \cdot 5 \cdot 7$$

Para facilitar el análisis, podemos "completar" los factores para que los primos que aparecen en ambas expresiones sean los mismos:

$$\begin{aligned} 252 &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^1 \\ 735 &= 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1 \end{aligned}$$

Si calculamos manualmente (a, b) y $[a, b]$ obtenemos

$$\begin{aligned} (252, 735) &= 21 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1 \\ [252, 735] &= 8820 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^1 \end{aligned}$$

Podemos ver que los primos que aparecen en ambas expresiones son los mismos que los que aparecen en las factorizaciones (acompletadas) de los números variando únicamente los exponentes. Esto lo enunciamos como sigue:

Teorema 1.17 *Sea p un número primo.*
El exponente con el que p aparece en (a, b) es el mínimo de los exponentes con los que aparece en las factorizaciones de a y b.
El exponente con el que p aparece en $[a, b]$ es el máximo de los exponentes con los que aparece en las factorizaciones de a y b.

El teorema anterior puede deducirse del Teorema Fundamental de la Aritmética y de las definiciones de máximo común divisor y mínimo común múltiplo. Ya tenemos la herramienta necesaria para demostrar la siguiente relación, cuya prueba se deja como ejercicio.

Teorema 1.18 *Si a, b son enteros, entonces*

$$ab = (a, b)[a, b].$$

1.4 Ecuaciones lineales diofantinas.

Esta sección es opcional en el sentido de que en el capítulo siguiente se estudiará la Ecuación Lineal de Congruencia que es equivalente a lo que se expondrá a continuación. Sin embargo, se incluye este tema por ser parte del desarrollo clásico del estudio de divisibilidad, además de que puede usarse para reforzar los conocimientos relacionados con el máximo común divisor.

Una ecuación lineal diofantina es una ecuación de la forma

$$ax + by = c$$

donde a, b, c son números enteros y x, y son variables que toman valores enteros. Veamos algunos ejemplos:

La ecuación $4x - 6y = 5$ no tiene soluciones enteras, ya que sin importar el valor de x y y el lado izquierdo siempre es un número par, mientras que el derecho es un número impar.

La ecuación $4x - 6y = 2$ tiene solución, ya que $(4, 6) = 2$ y entonces existe una combinación lineal de 4 y 6 que es igual a dos.

La ecuación $4x - 6y = 10$ tiene solución. Si x_0 y y_0 son solución de $4x - 6y = 2$ entonces $5x_0$ y $5y_0$ son solución de $4x - 6y = 10$.

Podemos generalizar los últimos dos ejemplos. Si $d = (a, b)$ sabemos que existen enteros x_0, y_0 tales que $ax_0 + by_0 = d$, es decir, la ecuación

$$ax + by = (a, b)$$

siempre tiene solución.

Más aún, si c es un múltiplo de d (por ejemplo $c = kd$) entonces

$$a(kx_0) + b(ky_0) = k(ax_0 + by_0) = kd = c$$

es decir, una ecuación de la forma

$$ax + by = k(a, b)$$

siempre tiene solución. Esto constituye el primer teorema de la sección.

Teorema 1.19 *Si $(a, b)|c$ entonces la ecuación lineal diofantina*

$$ax + by = c$$

siempre tiene solución entera.

Un corolario muy importante es:

Corolario 1.20 *Si a y b son primos relativos, la ecuación $ax + by = c$ siempre tiene solución entera.*

Ahora nos preguntamos: ¿Habrá alguna ecuación lineal $ax + by = c$ que tenga solución y en donde (a, b) no divida a c?

Vamos a restringirnos únicamente al caso en que c es positivo, puesto que si u y v son solución de $ax + by = c$ entonces $-u$ y $-v$ son solución de $ax + by = -c$.

Por un lado, como (a, b) es la mínima combinación lineal positiva, si $c = 1, 2, \ldots, (a, b) - 1$ la ecuación $ax + by = c$ no puede tener solución. De esta manera, si existe una solución, necesariamente $c \geq (a, b)$.

Supongamos que la ecuación $ax + by = c$ tiene como solución a x_1 y y_1, que $d = (a, b)$ no divide a c, y sean x_0 y y_0 una solución para $ax + by = d$. De esta manera tenemos

$$\begin{aligned} ax_1 + by_1 &= c \\ ax_0 + by_0 &= d \end{aligned}$$

Por el algoritmo de la división tenemos $c = md + r$ con $0 < r < c$ puesto que d no divide a c. Entonces

$$\begin{aligned} ax_1 + by_1 &= md + r \\ &= m(ax_0 + by_0) + r \\ &= a(mx_0) + b(my_0) + r \end{aligned}$$

y por tanto

$$a(x_1 - mx_0) + b(y_1 - my_0) = r.$$

¡Lo anterior es una contradicción! Puesto que tenemos una combinación lineal positiva de a y b igual a r y $0 < r < d$, eso contradice que d era la combinación lineal mínima positiva (es decir, d no era el máximo común divisor). La contradicción surgió de suponer que $ax + by = c$ podía tener solución aunque (a, b) no dividiera a c, por lo que hemos demostrado el siguiente teorema.

Teorema 1.21 *La ecuación lineal diofantina*

$$ax + by = c$$

tiene solución si y sólo si $(a, b) \mid c$.

Ya estamos en condición de determinar si una ecuación dada tiene solución o no, ahora nos interesa determinar cuáles son las soluciones. Supongamos que la ecuación $ax + by = c$ tiene solución, es decir, $c = kd$ donde $d = (a, b)$.

Si u y v son una solución de $ax + by = d$, entonces $x_0 = ku$ y $y_0 = kv$ son una solución de $ax + by = c$. De este modo podemos encontrar al menos una solución a la ecuación. Sea x_1, y_1 otra solución. Como $x_1 \neq x_0$ existe un entero r tal que $x_1 = x_0 + r$. Sustituyamos en la ecuación

$$a(x_0 + r) + by_1 = c = ax_0 + by_0$$

y al simplificar obtenemos

$$y_1 = \frac{by_0 - ar}{b} = y_0 - \frac{ar}{b}.$$

Un argumento simétrico muestra que si $y_1 = y_0 - s$ entonces

$$x_1 = x_0 + \frac{bs}{a}.$$

Una vez más sustituimos en la ecuación

$$a\big(x_0 + \frac{bs}{a}\big) + b\big(y_0 - \frac{ar}{b}\big) = ax_0 + by_0$$

y al simplificar llegamos a $bs - ar = 0$. Sean

$$a' = \frac{a}{(a,b)} \qquad b' = \frac{b}{(a,b)}$$
$$r' = \frac{r}{(r,s)} \qquad s' = \frac{s}{(r,s)}$$

Entonces $(a', b') = 1$ y (r', s')=1. Además

$$b's' - a'r' = 0.$$

Esto implica que $b's' = a'r'$. Además, la coprimalidad implicará que $r' = b'$ y $s' = a'$. Por tanto tenemos que,

$$r = \frac{b(r,s)}{(a,b)} \qquad s = \frac{a(r,s)}{(a,b)}.$$

Así, toda solución es de la forma

$$x = x_0 + \frac{bt}{(a,b)} \qquad y = y_0 - \frac{at}{(a,b)}$$

donde t es un entero que satisface la relación

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

Para terminar, notemos que

$$\left(\frac{bt}{(a,b)}, \frac{at}{(a,b)}\right) = t\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = t \cdot 1 = t$$

¡Esto quiere decir que todo entero satisface la relación anterior! En otras palabras, los números de la forma $x = x_0 + bt/d$ y $y = y_0 - at/d$ siempre son soluciones y además toda pareja de números que es de esa forma es solución.

Para recapitular todo el trabajo desarrollado en esta sección establecemos el teorema principal.

Teorema 1.22 (Resolución de la ecuación lineal de congruencia.)
La ecuación $ax + by = c$ tiene solución si y sólo si $d = (a, b)$ divide a c. Además, las soluciones son los números de la forma

$$x = x_0 + \frac{bt}{d} \qquad y = y_0 - \frac{at}{d}$$

donde x_0 y y_0 son una solución particular y t es cualquier número entero.

1.5 Ejercicios

1.1 Determine cuáles de las siguientes afirmaciones son verdaderas y cuáles son falsas.

i. Si un número es divisible entre 6, es divisible entre 3.
ii. Si un número es divisible entre 3, es divisible entre 6.
iii. Si un número es divisible entre 2 y entre 3, es divisible entre 6.
iv. Si un entero no es divisible entre 6, no es divisible entre 9.
v. Si un número es divisible entre 6, no es divisible entre 9.

1.2 Indique cuáles afirmaciones son ciertas y provea de una demostración, y para las que no lo sean muestre un contraejemplo.

Recuerda que $x \Rightarrow y$ se lee "Si x entonces y."

i. $a \mid b + c \Rightarrow a \mid b$ o $a \mid c$.
ii. $a \mid b \Rightarrow a \mid b^2$.
iii. $a \mid b^2 \Rightarrow a \mid b$.
iv. $a \mid bc \Rightarrow a \mid b$ o $a \mid c$.
v. $a \mid b$ y $c \mid b \Rightarrow ac \mid b$.
vi. $a \mid b$ y $a \mid c \Rightarrow a \mid b - c$
vii. $a \mid b + c$ y $a \mid b \Rightarrow a \mid c$.
viii. $a \mid b \Rightarrow a + b \mid b$.
ix. $a \mid b \Rightarrow a \mid a + b$
x. $a \mid b \Rightarrow a + x \mid b + x \quad \forall x \in \mathbb{Z}$

El símbolo $\forall$ se lee "Para todo".

1.3 Demostrar que $a - b \mid a^n - b^n$ para toda n.

1.4 ¿Para qué enteros n se cumple $120 \mid n^5 - n$?

1.5 Probar que $n \mid a + b + c$ si y sólo si $n \mid a^2 + b^2$ cuando $n = 3, 7, 21$.

1.6 Si a y b son impares, entonces $a^2 + b^2$ no puede ser un cuadrado.

1.7 Si $3 \mid n$, pruebe que $7 \mid 2^n - 1$.

1.8 Encuentra el menor número por el que hay que multiplicar 2000 para obtener un cuadrado perfecto.

1.9 Probar que todo primo de la forma $3k+1$ es de la forma $6m+1$.

1.10 Demostrar que un 2^n-1 sólo puede ser primo si n es primo.

1.11 `(YUC1994)` Sean a, b, c tres números positivos tales que $2^a + 2^b = 2^c$. Demostrar que $a = b$.

1.12 `(HUN1906)` Los números $a_1, a_2, \ldots, a_n$ representan una permutación de los números $1, 2, 3 \ldots, n$. Si n es impar, muestre que el producto $(a_1-1)(a_2-2)\cdots(a_n-n)$ es par.

1.13 `(MEX1987)` ¿Cuántos números dividen a $20!$?

1.14 Encontrar 100 números consecutivos tal que ninguno de ellos es primo.

1.15 Un número con 3^n dígitos iguales siempre es divisible entre 3^n.

1.16 Probar que hay una cantidad infinita de primos de la forma $4k+3$.

1.17 Demuestra que si p_n es el n-ésimo primo, entonces $p_n \leq 2^{2^{n-1}}$.

1.18 Demuestra que $n^4 + 4^n$ nunca es un primo para $n > 1$.

1.19 Si $a \mid b$, calcule (a, b) y $[a, b]$.

1.20 Si $a \mid c$, $b \mid c$ y $(a, b) = 1$, prueba que $ab \mid c$.

1.21 Si $[a, b, c](a, b, c) = abc$, entonces $(a, b) = (b, c) = (c, a) = 1$.

1.22 Si $(a, b) = p$ con p primo, ¿cuáles son los posibles valores de $(a^2, b), (a^3, b), (a^2, b^3)$?

1.23 Determine para qué enteros positivos n se cumple

$$\sum_{j=1}^{n} j \Big| \prod_{j=1}^{n} j$$

1.24 Sean a, b naturales tales que $a \mid b^2, b^2 \mid a^3, a^3 \mid b^4, b^4 \mid a^5, \ldots$. Pruebe que $a = b$.

1.25 Probar que si $n > 2$, existe un primo p tal que $n < p < n!$.

1.26 Usando el Teorema Fundamental de la Aritmética, indique un procedimiento para calcular (a, b) y $[a, b]$ en base a su factorización en primos. Calcule $(1202456, 1202460)$ con este procedimiento y también con el algoritmo de Euclides.

1.27 `(YUC1996)` Considere un recipiente vacío de 1000 litros de capacidad y una cantidad ilimitada de agua.

a. Con recipientes de capacidad de 13 y 19 litros, medir 24 litros de agua.
b. ¿Será posible medir 3 litros con recipientes con capacidad de 2 y 6 litros?

1.28 `(IMO1959)` Prueba que $\dfrac{21n+4}{14n+3}$ es irreducible para toda n.

1.29 (MEX1987) Demuestra que para toda n, la fracción $\dfrac{n^2+n-1}{n^2+2n}$ es irreducible.

1.30 (MEX1988) Si a y b son primos relativos y n es entero, prueba que $(a^2+b^2-nab, a+b)$ divide a $n+2$.

1.31 Si p es un número primo, demuestra que el exponente de p en la factorización de $n!$ en primos es

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

1.32 ¿Cuántos ceros hay al final de $100!$?

1.33 Demuestra que el número de divisores de $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ es $(a_1+1)(a_2+1)\cdots(a_k+1)$.

1.34 Sea $d(n)$ la suma de los dígitos de n. Si $d(n) = d(2n)$, muestre que $9 \mid 9$.

1.35 (OIM1987) Se define la sucesión $\{p_n\}$ de la siguiente manera:
$p_1 = 2$ y para $n > 1$, p_n es el mayor primo que divide a

$$p_1 p_2 p_3 \ldots p_{n-1} + 1.$$

Pruebe que p_n siempre es distinto a 5.

1.36 (IMO1970) Encuentre el conjunto de números n tales que el conjunto $\{n, n+1, n+2n, n+3, n+4, n+5\}$ puede dividirse en dos grupos de modo que el producto de los números del primer grupo sea igual al del segundo.

1.37 Pruebe que la ecuación $x^2+y^2+z^2 = 2xyz$ no tiene soluciones enteras excepto $x = y = z = 0$.

"Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$."

K. F. Gauss, Disquisitiones Arithmeticae

2 Congruencias.

En muchos problemas, la idea central para encontrar la solución es considerar los residuos de los números que se relacionan al dividirse entre otro número fijo. Esto nos llevará a desarrollar la noción de congruencia de números, la cual unifica y extiende muchos resultados desarrollados hasta ahora.

2.1 Congruencias.

Definicion 2.1 Sean a y b dos números enteros, y sea m un entero distinto de cero. Decimos que a *es congruente a* b *módulo* m si m divide a $b-a$. Esto lo escribimos como

$$a \equiv b \pmod m \quad \Leftrightarrow \quad m \mid (b-a).$$

A grandes rasgos lo que decimos es que dos números a y b son congruentes (equivalentes, iguales) módulo m si ambos son de la forma $mk+r$ con una misma r, esto es, si dejan el mismo residuo al dividirse por m. Para decir que a no es congruente a b módulo m escribimos $a \not\equiv b \pmod m$.

Ejemplos:

- $8 \equiv 23 \pmod 5$ puesto que $5 \mid (23-8) = 15$. Notemos que tanto 23 y 5 son de la forma $5k+3$.
- $36 \equiv 0 \pmod{12}$ pues $12 \mid (36-0) = 36$.
- $-22 \equiv 6 \pmod 7$ dado que $7 \mid (6-(-22)) = 28$.
- $14 \not\equiv 21 \pmod 4$ porque $4 \not\mid (21-14) = 7$.

Las ventajas de usar congruencias es que estas comparten muchas propiedades con la igualdad (de ahí que sea apropiado decir que los números son "congruentes"):

Teorema 2.1 *Si a, b, c, d, n son enteros y $n \neq 0$ entonces:*

i. $a \equiv a \pmod{n}$

ii. *Si* $a \equiv b \pmod{n}$ *entonces* $b \equiv a \pmod{n}$.

iii. *Si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$ *entonces* $a \equiv c \pmod{n}$.

iv. *Si* $a \equiv b \pmod{n}$ *entonces* $a + x \equiv b + x \pmod{x}$ *para todo entero* x.

v. *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces* $a + c \equiv b + d \pmod{n}$.

vi. *Si* $a \equiv b \pmod{n}$ *entonces* $ax \equiv bx \pmod{n}$ *para todo entero* x.

vii. *Si* $a \equiv b \pmod{n}$ *y* $c \equiv b \pmod{n}$ *entonces* $ac \equiv bd \pmod{n}$.

viii. *Si* $a \equiv b \pmod{n}$ *entonces* $a^x \equiv b^x \pmod{n}$ *para* $x \in \mathbb{Z}^+$

ix. *Si $f(x)$ es un polinomio de coeficientes enteros, entonces* $a \equiv b \pmod{n}$ *implica que* $f(a) \equiv f(b) \pmod{n}$

x. *Si* $a \equiv b \pmod{n}$ *y* $d \mid n$ *entonces* $a \equiv b \pmod{d}$.

xi. *Si* $a \equiv b \pmod{m}$, $a \equiv b \pmod{m}$ *y* $(m, n) = 1$ *entonces* $a \equiv b \pmod{mn}$.

xii. $a \equiv 0 \pmod{n}$ *si y sólo si* $n \mid a$.

El teorema anterior se prueba a partir de los teoremas de divisibilidad. Como ejemplo: $a \equiv b \pmod{n}$ entonces $a + x \equiv b + x \pmod{n}$.

Prueba. $a \equiv b \pmod{n}$ quiere decir que $n \mid (b - a)$. Pero $b - a = b + x + a - x = (b + x) - (a + x)$ por lo que $n \mid (b + x) - (a + x)$, lo que significa que $a + x \equiv b + x \pmod{n}$. ∎

Hay, sin embargo, una propiedad que la igualdad no comparte con la congruencia. Si $ax = bx$ ($x \neq 0$) podemos decir que $a = b$, pero con las congruencias no. Por ejemplo $10*6 \equiv 4*6 \pmod{4}$ pero $10 \not\equiv 4 \pmod{4}$. Es decir, no se permite cancelar factores en las congruencias. El siguiente teorema nos proporciona condiciones para poder efectuar tal operación.

Teorema 2.2 *Sean a, b enteros. Entonces*

i. $ax \equiv bx \pmod{n}$ *si y sólo si* $a \equiv b \pmod{\frac{n}{(n,x)}}$.

ii. *Si* $ax = bx \pmod{n}$ *y* $(n, x) = 1$ *entonces* $a \equiv b \pmod{n}$.

iii. $a \equiv b \pmod{n_k}$ *para* $k = 1, 2, \ldots, r$ *si y sólo si* $a \equiv b \pmod{[n_1, n_2, \ldots, n_r]}$.

Prueba. Si $ax \equiv bx \pmod{n}$ entonces $bx - ax = nz$ para algún entero z. Entonces

$$\frac{x}{(n,x)}(b - a) = \frac{n}{(n,x)}z$$

y por tanto

$$\frac{n}{(n,x)} \Big| \frac{x}{(n,x)}(b - a).$$

Pero $\left(\frac{n}{(n,x)}, \frac{x}{(n,x)}\right) = 1$ por lo que $\frac{n}{(n,x)}$ divide a $b - a$, es decir,

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

De este modo hemos probado que $ax \equiv bx \pmod{n}$ implica $a \equiv b \pmod{\frac{n}{(n,x)}}$.

Ahora, supongamos que $a \equiv b \pmod{\frac{n}{(n,x)}}$. Esto quiere decir que

$$b - a = \frac{n}{(n,x)} z$$

de donde $(b-a)(n,x) = nz$, es decir, $n \mid (b-a)(n,x)$. Pero x es un múltiplo de (n,x) lo cual nos dice que $n \mid (b-a)x$. Se sigue que $ax \equiv bx \pmod{n}$.

Recuerda que $a \mid b$ implica $a \mid bx$.

Ya hemos probado el primer inciso. El segundo es una aplicación directa del primero. Para probar el tercero, notemos que $n_i \mid (b-a)$ nos dice que $(b-a)$ es un múltiplo común de todas las n_i, por lo que $[n_1, n_2, \ldots, n_r] \mid b-a$. Ya queda probado que $a \equiv b \pmod{n_k}$ ($k = 1 \ldots r$) implica $a \equiv b \pmod{[n_1, n_2, \ldots, n_r]}$.

Para el regreso, notemos que n_k es un divisor de $[n_1, n_2, \ldots, n_r]$, por lo que $a \equiv b \pmod{[n_1, n_2, \ldots, n_r]}$ implica $a \equiv b \pmod{n_k}$ para cada n_k. ∎

Un caso muy especial y útil del teorema anterior es el siguiente resultado:

Teorema 2.3 *Sea p un número primo y t un número que no es divisible entre p. Si $at \equiv bt \pmod{p}$ entonces $a \equiv b \pmod{p}$*

Para ilustrar el uso de congruencias al resolver problemas, demostremos el siguiente teorema:

Teorema 2.4 *Si a es impar, entonces $a^2 - 1$ es divisible entre 8.*

Prueba. Si a es impar, entonces alguna de las siguientes proposiciones es cierta:

$$\begin{aligned} a &\equiv 1 \pmod{8} \\ a &\equiv 3 \pmod{8} \\ a &\equiv 5 \pmod{8} \\ a &\equiv 7 \pmod{8} \end{aligned}$$

Por otro lado $1^2 \equiv 1 \pmod{8}$, $3^2 \equiv 1 \pmod{8}$, $5^2 \equiv 1 \pmod{8}$, $7^2 \equiv 1 \pmod{8}$, por lo que en cualquier caso, $a^2 \equiv 1 \pmod{8}$, lo que es lo mismo que decir que $a^2 - 1$ es divisible entre 8. ∎

Una prueba ligeramente distinta:

Prueba. Supongamos que a es impar, es decir, $a \equiv 1 \pmod{2}$. Entonces

$$a^2 \equiv 1^2 \equiv 1 \pmod{2}.$$

Por otro lado, si $a^2 - 1$ no fuese divisible entre 8 tendríamos $a^2 \not\equiv 1 \pmod{8}$ y como $2 \mid 8$ esto implicaría que

$$a^2 \not\equiv 1 \pmod{2}.$$

Esto es una contradicción, por lo que concluimos que $a^2 - 1$ debe ser entre 8. ∎

Los teoremas principales sobre divisibilidad pueden formularse con congruencias. El teorema 1.15 se enuncia:

Teorema 2.5 *Si p es primo, $ab \equiv 0 \pmod{p}$ y $a \not\equiv 0 \pmod{p}$ entonces $b \equiv 0 \pmod{p}$.*

El teorema anterior es el análogo (para la igualdad) de la afirmación $ab = 0$ entonces $a = 0$ o $b = 0$. Es importante recalcar que el módulo debe ser primo. Como ejercicio, encontrar un contraejemplo cuando el módulo no es primo.

El teorema que dice que si $a = bq + r$ entonces $(a, b) = (b, r)$ puede reescribirse como

Teorema 2.6 *Si* $x \equiv y \pmod{n}$ *entonces* $(x, n) = (y, n)$.

Para terminar la sección, es importante recalcar que aunque los resultados de congruencia se pueden reescribir como resultados de divisibilidad y viceversa, las congruencias generalmente permiten realizar pruebas más claras y concisas, además de que familiarizarse con ellas permite entender resultados más profundos y poderosos. Por esto es que se recomienda especialmente que en lo posible se intente usar congruencias en vez de divisibilidad para resolver los problemas del libro, e inclusive se sugiere que conforme se adquiera más práctica, tratar de resolver ejercicios del primer capítulo con estas técnicas.

Ejercicios

2.2 Ecuación lineal de congruencia.

2.1 Demostrar el teorema 2.1

2.2 Probar que si p es primo y $a^2 \equiv b^2 \pmod{p}$ entonces $p \mid (a + b)$ o $p \mid (a - b)$.

2.3 Probar que todo cuadrado debe terminar en $0, 1, 4, 5, 6$ o 9 y que toda cuarta potencia debe terminar en $0, 1, 5$ o 6. ¿Qué puedes decir de las octavas potencias?

2.4 Si p es primo, demostrar que $(a + b)^p \equiv a^p + b^p \pmod{p}$.

2.5 Probar que si p es un primo que no divide a a, entonces no hay dos elementos del conjunto $\{a, 2a, 3a, \ldots, (p - 1)a\}$ que sean congruentes módulo p.

2.6 Probar que ninguna de las siguientes ecuaciones tiene soluciones enteras.

$$\begin{aligned} 3x^2 + 2 &= y^2 \\ 7x^3 + 2 &= y^3 \\ x^3 - 2 &= 7y \\ x^3 + 5 &= 7y \end{aligned}$$

2.7 Sean p_1, p_2, p_3 primos tales que $p = p_1^2 + p_2^2 + p_3^2$ también es primo. Probar que algún p_i es igual a 3.

2.8 Sea $p(x)$ un polinomio de coeficientes enteros tal que los números $p(-1), p(0)$ y $p(1)$ no son divisibles entre 3. Probar que $p(a) \neq 0$ para cualquier a entera.

2.9 Calcular el residuo que se obtiene al dividir 7077^{377} entre 11.

2.10 Hallar las últimas dos cifras del número $7^{7^{7^7}}$.

A

Sugerencias y respuestas a ejercicios selectos.

1.1 (i) Verdadero. (ii) Falso. (iii) Verdadero. (iv) Falso. (v) Falso.

1.2 (i) Falso: $4 \mid 5+3$ pero $4 \not\mid 5$ y $4 \not\mid 3$. (ii) Verdadero. (iii) Falso: $9 \mid 3^2$ pero $9 \not\mid 3$. (iv) Falso: $6 \mid 2 \cdot 3$ pero $6 \not\mid 2$ y $6 \not\mid 3$. (v) Falso: $3 \mid 6$ y $6 \mid 6$, pero $18 \not\mid 6$. (vi) Verdadero. (vii) Verdadero. (viii) Falso: $a = b = 1$. (ix) Verdadero. (x) Falso. $a = 2, b = 4, x = 1$.

1.3 Factorícese $a^n - b^n$.

1.5 Piensa en los residuos al dividir entre 3 y 7.

1.6 Considera los residuos al dividir entre 4.

1.7 Como $3 \mid n$, $n = 3k$. Ahora

$$2^n - 1 = 2^{3k} - 1 = (2^3)^k - 1^k = (2^3 - 1)\left((2^3)^{k-1} + (2^3)^{k-2} + \cdots + (2^3) + 1\right)$$

como $2^3 - 1 = 7$ se sigue $7 \mid 2^n - 1$.

1.8 Factoriza 2000.

1.9 Si el primo es de la forma $3k + 1$ entonces es de la forma $6m + 1$ o $6m + 4$, pero en el segundo caso tendríamos que el primo es par, esto es, $6m + 4 = 2$, lo cual es imposible.

1.10 Factorizar $2^n - 1^n$.

1.11 Si $a \neq b$ podemos suponer primero que $a < b$. Factoricemos 2^a de ambos lados y cancelemos. Seguimos un proceso similar cuando $a > b$.

1.12 Proceda por contradicción. Si el producto fuera impar, cada factor también lo sería.

1.13 Factorice $20!$ en primos y aplique un argumento combinatorio.

1.14 Considera $100!$.

1.15 Inducción matemática.

1.16 Procede por contradicción.

1.17 Usando inducción matemática.

1.18 Si n es par, el número también lo es. Si el número es impar, usa la factorización de Sophie-Germain.

1.20 Considera los factores primos de c.

1.25 $(n!, n! - 1) = 1$. Entonces, sea p un primo que divide a $n! - 1$, y verifique que tal número cumple la condición pedida.

1.26 Para (a, b) se toman los factores primos comunes con el exponente menor bajo el que aparezcan en cada factorización. Para $[a, b]$, tome los primos que aparecen en cualquiera de las dos factorizaciones con el mayor exponente de ambas.

1.27 (a) Exprese $(13, 19)$ como combinación lineal de 13 y 19. (b) Podría hacerse si 3 fuese combinación lineal de 2 y 6.

1.28 $(a, b) = (a - b, b)$.

1.32 Usando el problema anterior, determine el exponente de 5 en la factorización única.

1.34 Pruebe que la diferencia $2n - n$ es divisible entre 9.

1.35 Supongamos $p_n = 5$ y $n > 2$. La expresión $p_1 p_2 \dots p_{n-1} + 1$ no puede ser divisible por 2 y tampoco por 3. Entonces es una potencia de 5. Muestre que el producto $p_1 p_2 \dots p_{n-1}$ será divisible por 4 y obtenga una contradicción.

1.36 Si p es un primo que divide al producto de los del primer grupo, debe haber un número en el segundo grupo divisible por p.

1.37 Use descenso infinito.

2.6 Para probar que $3x^2 + 2 = y^2$ no tiene soluciones enteras, notemos que si tal solución hubiera se tendría $y^2 \equiv 2 \pmod 3$. Derive una contradicción.

2.7 Considere los residuos de p_1^2, p_2^2 y p_3^2 módulo 3.

2.8 Todo entero n es congruente a 0, 1, o -1 módulo 3. Entonces $p(n)$ es congruente a $p(-1)$, $p(0)$ o $p(1)$.

Bibliografía

[1] Enzo R. Gentile: *Aritmética elemental*. Univ. de Buenos aires. 1985.

[2] Enzo R. Gentile: *Aritmética elemental en la formación matemática.* Univ. de Buenos Aires. 1994.

[3] G. H. Hardy y E. M. Wright: *An introduction to the Theory of Numbers*. Oxford Univ. Press. 1959.

[4] K. Ireland y M. Rosen: *A classical introduction to Modern Number Theory* Springer. 1990.

[5] Juan Gómez: *100 problemas de teoría de números tipo Olimpiada Mexicana de Matemáticas* UAM. 1991.

[6] Naoki Sato: *Number theory* Sin publicar. 1995.

[7] I.Ñiven y H. S. Zuckerman: *Introducción a la teoría de los números* Limusa. 1976.