Teoría de Números para Olímpiadas Matemáticas

Dedicado al profesor Darío Durán, maestro de maestros.

José Heber Nieto Said

jhnieto@gmail.com
www.jhnieto.org

Departamento de Matemática
Facultad de Ciencias
Universidad del Zulia
Maracaibo, Venezuela

1. Introducción

La *Teoría de Números* o *Aritmética* es la rama de la matemática que estudia todo lo relacionado con los números naturales y enteros. El hecho de que estos números se estudien desde los primeros años de la enseñanza escolar podría hacer pensar que se trata de un tema elemental y sin misterios. Pero no es así, por el contrario, la Aritmética encierra algunos de los problemas más difíciles de la matemática, algunos de los cuales permanecen o han permanecido abiertos durante siglos. En la teoría de números avanzada se utilizan toda clase de herramientas matemáticas, como por ejemplo la teoría de funciones de variable compleja. Sin embargo, aún limitándonos a las nociones más básicas y elementales, es posible generar una gama inagotable de problemas de todos los grados de dificultad posibles. Esta es la razón por la cual la Teoría de Números es uno de los temas infaltables y favoritos en todas las olimpiadas matemáticas. Estas notas tratan de cubrir los conocimientos básicos necesarios para resolver problemas olímpicos de aritmética. No olvide sin embargo que lo esencial para convertirse en un buen solucionista es... ¡resolver muchos problemas!

Algunos problemas elementales

Veamos algunos ejemplos de problemas interesantes, para cuya solución no hace falta conocer más que la tabla de multiplicar. Trate de resolverlos usted mismo, y sólo si no lo logra después de un serio esfuerzo consulte las soluciones.

Ejemplo 1. En una de sus clases el profesor Darío escribió en la pizarra el número 12345679012345679, y dijo que era mágico. —¡Profesor, olvidó el 8! — Bueno, sí, pero no importa, dejémoslo así... —Profesor, ¿y qué tiene de mágico ese número? — ´Pues veamos, díganme una cifra del 1 al 9. —¡El 7, el 7! — Multipliquen el número mágico por 63. Los alumnos lo hacen, y obtienen con asombro 777777777777777777. ¿Qué hubiese respondido Darío si los alumnos escogen el 3, o cualquier otra cifra? ¿Qué explicación tiene todo esto?

Ejemplo 2. El producto de dos enteros consecutivos, ¿puede terminar en 8?

Ejemplo 3. ¿En qué dígito termina 2^{2011}?

Ejemplo 4. Juan tiene 5 tarjetas con el número 2, 8 tarjetas con el número 3, 10 tarjetas con el número 7 y 20 tarjetas con el número 8, y las usa para formar números de varias cifras, colocándolas en fila. ¿Puede formar un número que sea un cuadrado perfecto?

Ejemplo 5. Halle un número natural tal que, si su última cifra a la derecha se mueve al primer lugar de la izquierda, se obtiene un número doble del original.

Soluciones

1. El profesor Darío dividió 111111111111111111 entre 9 y así obtuvo el número mágico 12345679012345679. Para cualquier cifra x del 1 al 9, si el número mágico se multiplica por $9x$ el resultado será $xxxxxxxxxxxxxxxxx$.

2. No. Como el último dígito de un producto sólo depende de los últimos dígitos de los factores, basta examinar los productos $1 \times 2 = 2$, $2 \times 3 = 6$,$3 \times 4 = 12$, $4 \times 5 = 20$, $5 \times 6 = 30$, $6 \times 7 = 42$, $7 \times 8 = 56$, $8 \times 9 = 72$ y $9 \times 0 = 0$ para convencerse de que el producto de dos enteros consecutivos sólo puede terminar en 0, 2 ó 6.

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

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

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

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

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

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

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

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

Esta es la solución más pequeña al problema. Comenzando con $z = 3, 4, \ldots, 9$ se obtienen otras soluciones: 157894736842105263, 210526315789473684, 263157894736842105, 315789473684210526, 368421052631578947, 421052631578947368 y 473684210526315789 (observe que todas estas son versiones *rotadas* de la primera que obtuvimos). Finalmente, concatenando dos o más de las soluciones anteriores se obtienen nuevas soluciones, de 36, 54, 72,... cifras.

2. Divisibilidad

En lo que sigue se desarrollan los conceptos y resultados básicos de la aritmética. Cada tema va seguido de una lista de problemas que usted debe sesolver. No se incluyen soluciones, si necesita ayuda recurra a su entrenador.

El conjunto de los números naturales $\{1, 2, 3, \ldots\}$ se denotará $\mathbb{N}$, y el de los enteros $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ se denotará $\mathbb{Z}$. Se dice que

$$\boxed{a \in \mathbb{Z} \text{ es } \textit{múltiplo} \text{ de } b \in \mathbb{Z} \text{ si } a = kb \text{ para algún } k \in \mathbb{Z}.}$$

En este caso también se dice que a es *divisible* entre b o que b *divide* a a, y se escribe $b \mid a$.

Para cualquier $a \in \mathbb{Z}$ se cumple que $1 \mid a$ y que $a \mid a$, ya que $a = 1 \cdot a$. Cualquier entero a divide al 0, ya que $0 = a \cdot 0$. Los enteros múltiplos de 2 se denominan *pares*, y los que no lo son *impares*. Observe que 0 es par.

La divisibilidad es *transitiva*, es decir que si $a \mid b$ y $b \mid c$ entonces $a \mid c$. También es inmediato que si un número divide a otros dos entonces divide tanto a su suma como a su diferencia.

Si a es múltiplo de b y ambos son positivos, entonces es obvio que $a \geq b$. Esto no es cierto en general para números enteros, por ejemplo 0 es múltiplo de 2 pero $0 < 2$, -4 es múltiplo de 2 pero $-4 < 2$.

2.1. Números primos

Si un número natural $p > 1$ sólo tiene como divisores a 1 y p, entonces se dice que es *primo*. La sucesión de los primeros números primos comienza así:

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

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

El 1 es especial: no es ni primo ni compuesto, es simplemente la unidad.

La importancia de los números primos consiste en que cualquier número natural $n > 1$ es primo o puede expresarse como producto de primos. En símbolos,

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

donde $p_1 < p_2 < \cdots < p_k$ son números primos y los exponentes $a_1, a_2, \ldots, a_k$ son números naturales. Más aún, esta descomposición es única excepto por el orden de los factores.

De esta manera los números primos son como los bloques fundamentales que permiten generar, multiplicativamente, a todos los números naturales (del mismo modo que el 1 los genera aditivamente). Este resultado es tan importante que se conoce como **Teorema Fundamental de la Aritmética**, y fue probado por Euclides ($\approx$ 325–265 a.C.), quien dedicó el Libro IX de sus famosos *Elementos* a la Teoría de números.

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

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

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

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

Una consecuencia de lo anterior es que el **número de divisores** de n (incluyendo al 1 y al propio n) es

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

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

Otra consecuencia del Teorema Fundamental es que un número natural es un cuadrado perfecto si y sólo si todos sus factores primos diferentes aparecen elevados a exponentes pares. Más en general, un número natural es una potencia k-sima si y sólo si todos sus factores primos diferentes aparecen elevados a exponentes múltiplos de k.

Problemas

Problema 1 (OJM 2009)**.** Los números desde el l hasta el 2009 se escriben consecutivamente en la pizarra. En una primera pasada se borran el primer número escrito, el tercero, el quinto y así sucesivamente hasta borrar el 2009. En una segunda pasada se aplica el mismo procedimiento a los números que quedaron, borrando el primero de ellos, el tercero, el quinto y así sucesivamente. Esto se repite mientras queden números en la pizarra. ¿En qué pasada se elimina el 1728? ¿Cuál es el último número borrado y en qué pasada se elimina?

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

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

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

Problema 5. Pruebe que para cualquier número natural n el número $n^3 + 2n$ es múltiplo de 3.

Problema 6. (Eötvös 1894) Pruebe que $17|2m + 3n$ si y sólo si $17|9m + 5n$ (m y n enteros).

Problema 7. Caracterice los números naturales que tienen una cantidad impar de divisores.

Problema 8 (Canguro 2007, 9º)**.** Dado un número, una extraña calculadora sólo puede hacer lo siguiente: multiplicarlo por 2 o por 3, o calcular su segunda o tercera potencia. Si comenzamos con el número 15, ¿cuál de los siguientes resultados se puede obtener al usar la calculadora cinco veces consecutivas?

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

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

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

Problema 11. Sea n un entero positivo. Pruebe que si 2^n-1 es primo entonces n es primo.

Problema 12. Sea n un entero positivo. Pruebe que si 2^n+1 es primo entonces n es una potencia de 2.

Problema 13. (Canguro 2010, 10º) En cada lado de un pentágono se escribe un número natural, de manera tal que números adyacentes nunca tienen un factor común mayor que 1, pero números no adyacentes siempre tienen un factor común mayor que 1. Hay muchas posibilidades de hacer esto, pero uno de los números siguientes no aparecerá nunca en los lados del pentágono. ¿Cuál es?

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

Problema 14. (Canguro 2008, 9º) Todos los divisores del entero positivo N, diferentes de N y 1, se escriben en orden creciente. ¿Cuántos números naturales N son tales que el mayor de los divisores escritos es 45 veces más grande que el menor?

Problema 15. Si $56a = 65b$, pruebe que $a + b$ es compuesto.

Problema 16. Pruebe que para cualquier número natural n existen n números naturales consecutivos que son compuestos.

Problema 17 (OJM regional 2008)**.** Halle el menor entero positivo n tal que cada dígito de $15n$ sea 0 ó 2.

Problema 18. Halle todas las soluciones enteras de la ecuación

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

Problema 19 (OIM 1999)**.** Halle todos los enteros positivos que son menores que 1000 y cumplen con la siguiente condición: el cubo de la suma de sus dígitos es igual al cuadrado de dicho entero.

Problema 20. (OIM 1999) Sea B un entero mayor que 10 tal que cada uno de sus dígitos pertenece al conjunto $\{1, 3, 7, 9\}$. Demuestre que B tiene un factor primo mayor o igual que 11.

Algunos problemas abiertos sobre números primos

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

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

¿Existen infinitos números primos de la forma $2^p - 1$, con p primo? (Los primos de esta forma se llaman **números primos de Mersenne**).

¿Existen infinitos números primos de la forma $2^{2^n} + 1$, con n entero no negativo)? (Los primos de esta forma se llaman **números primos de Fermat**).

2.2. División entera

El *algoritmo de la división entera* nos dice que si $a, b \in \mathbb{Z}$ y $b \neq 0$ entonces existen números enteros *únicos* q y r tales que

$$\boxed{a = qb + r \quad \text{y} \quad 0 \leq r < |b|}.$$

A q y r se les llama respectivamente *cociente* y *resto* de la división entera de a entre b. El resto es 0 si y sólo si a es múltiplo de b.

Observe que los restos sólo pueden ser 0, 1, 2,..., $|b| - 1$. Todos los enteros a quedan así particionados en conjuntos disjuntos, según cuál sea el resto al dividirlos entre b. Esos conjuntos se llaman *clases residuales módulo* b. Es muy fácil ver que dos enteros están en una misma clase resdual módulo b si y sólo si su diferencia es divisible entre b. En efecto, si $a = qb+r$ y $a' = q'b+r$ entonces $a' - a = (q' - q)b$ y $b \mid a' - a$. Recíprocamente si $a = qb + r$ y $a' - a = kb$ entonces $a' = a + kb = (q + k)b + r$.

Problemas

Problema 21. (Canguro 2007, 10º) Un entero positivo al ser dividido entre 4 deja resto 1 y al ser dividido entre 5 deja resto 3. ¿Qué resto deja al ser dividido entre 20?

Problema 22. (Canguro 2007, 11º) Si dividimos 336 entre el número natural n el resto es 2. Entonces el resto que se obtiene al dividir 2007 entre n es:
(a) 100; (b) 3; (c) 2; (d) 1; (e) 0.

Problema 23. (Canguro 2007, 8º) Cinco números enteros se escriben alrededor de un círculo de manera que la suma de dos o de tres números adyacentes no sea nunca múltiplo de 3. ¿Cuántos de los cinco números son múltiplos de 3?

Problema 24. Halle el menor entero mayor que 1 tal que al dividirlo entre 2, 3, 4, 5, 6, 7, 8 o 9 deja resto 1.

Problema 25. Halle el menor entero positivo tal que al dividirlo entre 2 deja resto 1, al dividirlo entre 3 deja resto 2, al dividirlo entre 4 deja resto 2, al dividirlo entre 5 deja resto 4, al dividirlo entre 6 deja resto 5, al dividirlo entre 7 deja resto 6, al dividirlo entre 8 deja resto 7 y al dividirlo entre 9 deja resto 8.

Problema 26. ¿Cuál es el exponente de 7 en la descomposición de 2011! en producto de factores primos?

Problema 27. ¿En cuántos ceros termina 2011!?

Problema 28 (XXIII OIM 2008)**.** Demuestre que no existen enteros positivos x e y tales que

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

2.3. Máximo común divisor

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

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

Si se conoce la descomposición en producto de factores primos de a y de b, entonces es muy fácil calcular $\text{mcd}(a, b)$: es igual al producto de los factores

primos comunes elevados al menor de los exponentes con que aparecen en las descomposiciones de a y b. De aquí se deduce que $\mcd(a,b)$ no sólo es el mayor divisor común sino que además cualquier otro divisor común de a y b *divide* a $\mcd(a,b)$. por ejemplo $406 = 2 \cdot 7 \cdot 29$ y $147 = 3 \cdot 7^2$, por lo tanto $\mcd(406, 147) = 7$.

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

Ejemplo 6. Hallar $\mcd(3127, 2491)$ mediante el algoritmo de Euclides.

Solución.

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

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

Del algoritmo de Euclides se sigue que $\mcd(a,b)$ se puede expresar en la forma $sa + tb$ para ciertos enteros s y t (esto se conoce como **Teorema de bezout**). Por ejemplo, aprovechando los cálculos que acabamos de hacer se tiene

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

Una consecuencia importante de esta manera de expresar el máximo común divisor es el **Lema de Euclides**:

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

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

Números coprimos

Dos números a y b se dicen *coprimos*, *primos relativos* o *primos entre sí* si no tienen más divisor común que 1, es decir si $\text{mcd}(a, b) = 1$. Observe que en este caso $mcm(a, b) = ab$.

Si $\text{mcd}(a, b) = d$ entonces $\text{mcd}(a/d, b/d) = 1$, es decir que a/d y b/d son coprimos.

2.4. Mínimo común múltiplo

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

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

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

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

Problemas

Problema 29. Sean $a = \underbrace{999\ldots999}_{\text{40 nueves}}$ y $b = 999999999999$. Halle $\text{mcd}(a, b)$.

Problema 30. Juan, Mario y Pedro entrenan dando vueltas en bicicleta a una pista circular. Juan tarda 8 minutos en dar una vuelta, Mario tarda 9 minutos y Pedro tarda 12 minutos. Si los tres parten del mismo punto a las 6:00 am, ¿a qué hora volverán a encontrarse?

Problema 31. Pruebe que todo número natural tiene un múltiplo cuyos dígitos son solamente unos o ceros.

Problema 32. Pruebe que todo número natural coprimo con 10 tiene un múltiplo cuyos dígitos son todos unos.

Problema 33. Se tiene una hoja rectangular de papel milimetrado de 259×154. Si se traza una diagonal, ¿cuántos cuadraditos atraviesa?

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

Problema 34 (OJM 2009)**.** 'Ana vende galletas, que vienen en cajas pequeñas de 5 unidades y en cajas grandes de 12 unidades. Si, por ejemplo, un cliente quiere 39 galletas, Ana puede despachar el pedido exactamente con tres cajas pequeñas y dos grandes, ya que $3 \times 5 + 2 \times 12 = 39$. Pero hay pedidos que no se pueden despachar exactamente, por ejemplo, cuando un cliente quiere 7, 16 ó 23 galletas. ¿Cuál es el pedido más grande que no se puede despachar exactamente?
Nota: Se supone que Ana tiene o puede pedir a la fábrica todas las galletas que le hagan falta.

Problema 35. Sean a y b naturales coprimos. Pruebe que cualquier natural suficientemente grande puede expresarse en la forma $sa + tb$ con s y t enteros no negativos. ¿Cuál es el mayor entero que no se puede expresar en esa forma?

Problema 36. Pruebe que existen infinitos números primos de la forma $4n+3$.

Problema 37. Los *Números de Fibonacci* se definen recursivamente así:
$F_0 = 0$, $F_1 = 1$ y $F_n = F_{n-1} + F_{n-2}$ para $n \geq 2$.

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

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

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

3. Congruencias

La noción de *congruencia* fue introducida por Gauss (1777–1855). Se dice que dos enteros a y b son *congruentes* módulo m si $m \mid (a - b)$. En ese caso se escribe

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

Las congruencia módulo m tiene muchas propiedades similares a las de la igualdad, entre ellas la reflexividad, la simetría y la transitividad:

$$\begin{aligned} a &\equiv a \pmod{m}, \\ a &\equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}, \\ a &\equiv b \pmod{m} \text{ y } b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}. \end{aligned}$$

También se pueden sumar, restar o multiplicar congruencias (del mismo módulo) miembro a miembro:

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

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

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

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

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

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

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

□

Criterios de divisibilidad

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

2 si y sólo si su última cifra es par.

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

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

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

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

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

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

10 si y sólo si su última cifra es 0.

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

13 si y sólo si al quitarle la cifra u de las unidades y sumarle $4u$ al número resultante, se obtiene un múltiplo de 13.

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

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

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

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

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

de donde se deduce el criterio de divisibilidad entre 11.

Tal vez los criterios menos conocidos (y usados) sean los de divisibilidad entre 7 y 13. El criterio del 7 afirma que $n = 10a + u$ es divisible entre 7 si y sólo si $a - 2u$ lo es. Pero si $10a + u \equiv 0 \pmod 7$, multiplicando por -2

resulta $-20a - 2u \equiv 0 \pmod 7$, es decir $a - 2u \equiv 0 \pmod 7$ (pues $-20 \equiv 1 \pmod 7$), y recíprocamente si $a-2u \equiv 0 \pmod 7$ multiplicando por 10 resulta $10a-20u \equiv 0 \pmod 7$, es decir $10a+u \equiv 0 \pmod 7$. Análogamente se prueba el criterio del 13.

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

Función ϕ de Euler

Si n es un número natural se define $\phi(n)$ como la cantidad de números del conjunto $\{1, 2, \ldots, n\}$ que son coprimos con n. Por ejemplo $\phi(6) = 2$ ya que de los números 1, 2, 3, 4, 5 y 6 solamente 1 y 5 son coprimos con 6. Si p es primo y a natural entonces entre 1 y p^a solamente los números $p, 2p, 3p, \ldots, p^{a-1}p = p^a$ no son coprimos con p^a, es decir que $\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p)$. Más en general se puede probar que si $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ entonces

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

Teorema de Euler-Fermat

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

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

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

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

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

$$c_1c_2\cdots c_{\phi(n)} = r_1r_2\cdots r_{\phi(n)} \equiv a^{\phi(n)}c_1c_2\cdots c_{\phi(n)} \pmod n,$$

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

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

Teorema (pequeño) de Fermat

Si p es primo y $p \nmid a$, entonces

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

Problemas

Problema 38. Un número se escribe con cien ceros, cien unos y cien doses, en algún orden. ¿Puede ser un cuadrado perfecto?

Problema 39. Pedro multiplicó dos enteros de dos cifras cada uno y codificó los factores y el producto con letras, usando letras iguales para dígitos iguales y letras diferentes para dígitos diferentes. Entonces le mostró al maestro su trabajo: $AB \cdot CD = EEFF$. Pero el maestro le contestó: Revisa lo que hiciste, pues cometiste un error. ¿Cómo supo eso el maestro?

Problema 40. Permutando las cifras del número

$$122333444455555666666777777$$

¿podrá obtenerse un cuadrado perfecto?

Problema 41. Si m y n son enteros tales que m^2+n^2 es múltiplo de 3, pruebe que tanto m como n son múltiplos de 3.

Problema 42. Hallar el menor entero positivo x tal que $21x \equiv 2 (\text{mód } 37)$.

Problema 43. Pruebe el siguiente **Criterio general de divisibilidad**: Sea n un entero positivo coprimo con 10. Sea m un inverso multiplicativo de 10 módulo n. Entonces el entero $10a + u$ (donde $0 \leq b \leq 9$) es divisible entre n si y sólo si $a + mu$ lo es.

Nota: Este criterio me fue comunicado por el profesor Darío Durán. Como casos particulares se tiene que $10a + u$ es divisible entre 13 si y sólo si $a + 4u$ lo es, entre 17 si y sólo si $a - 5u$ lo es, entre 19 si y sólo si $a + 2u$ lo es.

Problema 44. Si x, y, z son enteros tales que $x^2 + y^2 = z^2$, pruebe que al menos uno de ellos es múltiplo de 3.

Problema 45. Si tres números primos mayores que 3 están en progresión aritmética, pruebe que la razón (o diferencia común) de la progresión es múltiplo de 6.

Problema 46. Se tienen 7 números enteros tales que la suma de 6 cualesquiera de ellos es divisible entre 5. Pruebe que los 7 números son múltiplos de 5.

Problema 47. Si x, y, z son enteros tales que $x^2 + y^2 + z^2$ es múltiplo de 4, pruebe que tanto x, y, z son los tres pares.

Problema 48. Pruebe que $2222^{5555} + 5555^{2222}$ es divisible entre 7.

Problema 49. ¿Qué resto se obtiene al dividir $2^{3^{2011}}$ entre 17?

Problema 50. Pruebe que existe n tal que 3^n tiene al menos 2011 ceros consecutivos.

Problema 51. Pruebe que, dado cualquier natural N, existe n tal que 2^n tiene al menos N ceros consecutivos.

Problema 52 (Teorema de Wilson)**.** Pruebe que, para cualquier primo p, se cumple

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

Residuos cusdráticos

Si m es un entero, se llama **residuo cuadrático** módulo m a aualquier entero a coprimo con m para el cual tenga solución la congruencia

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

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

El siguiente teorema, probado por Gauss, es uno de los resultados más importantes y profundos de la teoría elemental de números. Para su demostración remitimos al lector a la literatura especializada.

Ley de reciprocidad cuadrática. Si p y q son primos impares y al menos uno de ellos es de la forma $4n+1$, entonces p es un residuo cuadrático módulo q si y sólo si q es un residuo cuadrático módulo p. Si en cambio p y q son ambos de la forma $4n+3$, entonces p es un residuo cuadrático módulo q si y sólo si q no es un residuo cuadrático módulo p.

Problemas

Problema 53. Si p es un primo impar entonces la mitad de los enteros de 1 a $p-1$ son residuos cuadráticos módulo p y la otra mitad no lo son.

Problema 54. Si p es un primo de la forma $4n+3$ entonces -1 no es un residuo cuadrático módulo p.

Problema 55. Si p es un primo de la forma $4n+1$ entonces -1 es un residuo cuadrático módulo p.

Problema 56. Pruebe que existen infinitos primos de la forma $4n+1$.

Problema 57. Si p es un primo de la forma $4n+3$ y $p \mid a^2+b^2$, pruebe que $p \mid a$ y $p \mid b$.

Algunos problemas adicionales

Problema 58. Sea $S(n)$ la suma de los dígitos de la expresión decimal del número natural n (por ejemplo $S(748) = 7+4+8 = 19$). ¿Qué relación existe entre $S(2n)$ y $2S(n)$?

Problema 59 (X OMCC, Honduras, 2008)**.** Halle el menor entero positivo N tal que la suma de sus cifras sea 100, y la suma de las cifras de $2N$ sea 110.

Problema 60. (OM 2005, 1$^{\text{er}}$ Nivel) Un número entero se llama *autodivi* si es divisible entre el número de dos cifras formado por sus dos últimos dígitos (decenas y unidades). Por ejemplo, 78013 es autodivi pues es divisible entre 13, 8517 es autodivi pues es divisible entre 17. Halle 6 números enteros consecutivos que sean autodivi y que tengan las cifras de las unidades, de las decenas y de las centenas distintas de 0.

Problema 61. (IMO 1989) Pruebe que para cualquier n entero positivo existen n enteros positivos consecutivos ninguno de los cuales es primo ni potencia de un primo.

Problema 62. (OMCC 2002) Encuentre un conjunto infinito de enteros positivos S tal que para cada $n \geq 1$ y cualesquiera n elementos distintos $x_1, x_2, \ldots, x_n$ de S, el número $x_1 + x_2 + \cdots + x_n$ no es un cuadrado perfecto.

Problema 63. (IMO 2002) Los divisores positivos del entero $n > 1$ son $d_1 < d_2 < \cdots < d_k$, con $d_1 = 1$ y $d_k = n$. Sea $d = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$. Pruebe que $d < n^2$ y halle todos los n para los cuales d divide a n^2.

Problema 64. (OMCC 2001) Encontrar todos los números naturales N que cumplan las dos condiciones siguientes:

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

Problema 65. (IMO 2003-6) Sea p un número primo. Demostrar que existe un número primo q tal que, para todo entero n, el número $n^p - p$ no es divisible por q.

Problema 66. (IMO 2006-4) Determine todas las parejas de enteros (x, y) tales que $1 + 2^x + 2^{2x+1} = y^2$.

Problema 67. (IMO 2011-5) Sea f una función del conjunto de los enteros al conjunto de los enteros positivos. Se supone que para cualesquiera dos enteros m y n, la diferencia $f(m) - f(n)$ es divisible por $f(m - n)$. Demostrar que para todos los enteros m y n con $f(m) \leq f(n)$, el número $f(n)$ es divisible por $f(m)$.