Congruencias lineales y el teorema chino del residuo

Por Carlos Jacob Rubio Barrios

Nivel Avanzado

Congruencias lineales

Una de las ecuaciones más simples de resolver en álgebra elemental es la ecuación $ax = b$, cuya única solución es $x = \frac{b}{a}$ suponiendo que $a \neq 0$. De manera análoga, podemos preguntarnos cuándo tiene solución la congruencia lineal $ax \equiv b \pmod{m}$, y en caso de tener solución, cómo son todas sus soluciones. Esperaríamos que la solución sea también una congruencia, esto es, de la forma $x \equiv r \pmod{m}$ para algún entero r. Por ejemplo, si $5x \equiv 7 \pmod{12}$, entonces una solución es $x = 11$ ya que $5 \cdot 11 - 7 = 48$, la cual es divisible entre 12. Pero otras soluciones son $x = 23$, o $x = -13$, o más generalmente, $x = 11 + 12k$ para cualquier entero k. De hecho, si x_0 es una solución de $ax \equiv b \pmod{m}$ y $x \equiv x_0 \pmod{m}$, entonces $ax \equiv ax_0 \equiv b \pmod{m}$. Esto significa que x también es solución de la congruencia. Más aún, tenemos el siguiente resultado.

Teorema 1 *La congruencia $ax \equiv b \pmod{m}$ tiene una solución si y sólo si el máximo común divisor de a y m es un divisor de b, esto es, si $d = mcd(a, m)$, entonces la congruencia tiene una solución si y sólo si $d \mid b$. Si hay una solución x_0, entonces el conjunto de todas las soluciones es el conjunto de todos los x tales que $x \equiv x_0 \pmod{\frac{m}{d}}$.*

Demostración. Sea $d = \text{mcd}(a, m)$. Supongamos que la congruencia $ax \equiv b \pmod{m}$ tiene una solución x_0. Entonces, m divide a $ax_0 - b$. Como $d \mid m$, se sigue que d divide a $ax_0 - b$ y como $d \mid a$, resulta que $d \mid b$.
Recíprocamente, supongamos que $d \mid b$. Tenemos que $a = da'$, $m = dm'$ y $b = db'$ para algunos enteros a', m' y b', con a' y m' primos relativos. Entonces, existen enteros r y s tales que $a'r + m's = 1$. Multiplicando esta ecuación por db' obtenemos que

$a(rb') + m(sb') = b$, esto es, $a(rb') \equiv b \pmod{m}$ y por lo tanto rb' es solución de la congruencia $ax \equiv b \pmod{m}$.
Supongamos que x_0 es solución de la congruencia $ax \equiv b \pmod{m}$. Si x es otra solución, entonces $ax \equiv ax_0 \pmod{m}$ y por lo tanto $x \equiv x_0 \pmod{\frac{m}{d}}$ donde $d = \text{mcd}(a, m)$. Recíprocamente, si $x \equiv x_0 \pmod{\frac{m}{d}}$, con d como antes, entonces $ax \equiv ax_0 \pmod{m}$ y por lo tanto $ax \equiv b \pmod{m}$, pues $ax_0 \equiv b \pmod{m}$.

Supongamos, por ejemplo, que queremos resolver la congruencia $15x \equiv 33 \pmod{69}$. Como $\text{mcd}(15, 69) = 3$ y $3 \mid 33$, sabemos que existe una solución. Luego, la congruencia es equivalente a la ecuación $15x + 69y = 33$. No nos interesamos en y excepto porque nos ayudará a determinar el valor de x. Tenemos que

$$x = \frac{33 - 69y}{15} = 2 - 4y + \frac{3 - 9y}{15}.$$

Luego, $\frac{3-9y}{15}$ debe ser un entero también, digamos que $\frac{3-9y}{15} = z$. Repitiendo el proceso anterior tenemos que

$$15z + 9y = 3 \Rightarrow y = \frac{3 - 15z}{9} = -z + \frac{3 - 6z}{9}$$

de donde $\frac{3-6z}{9} = w$ para algún entero w. De aquí, $9w + 6z = 3$, la cual tiene la solución obvia $w = 1$, $z = -1$. Entonces, $y = 2$ y $x = -7$. Luego, todas las soluciones de la congruencia están dadas por $x \equiv -7 \pmod{23}$, que es lo mismo a $x \equiv 16 \pmod{23}$.

El teorema chino del residuo

Supongamos, que por alguna razón, queremos resolver la complicada congruencia $5x^2 + 6x + 7 \equiv 0 \pmod{35}$. Observemos que si a es solución de esta congruencia, entonces $5a^2 + 6a + 7 \equiv 0 \pmod{35}$, y ya que $5(a + 35k)^2 + 6(a + 35k) + 7 = 5a^2 + 6a + 7 + 35(10ka + 175k^2 + 6k)$, se sigue que $a + 35k$ también satisface la congruencia inicial, para cualquier entero k.
Regresando a nuestro problema, no podemos usar la fórmula cuadrática debido a que las raíces cuadradas son un problema con la aritmética modular (pues necesitamos enteros). Una manera de aproximarnos a la solución es tratando con $x \equiv 0, x \equiv 1, x \equiv 2, \ldots, x \equiv 34$, cada una módulo 35. Otra manera más sofisticada, podría ser simplificando el problema: Si $5x^2 + 6x + 7$ es divisible por 35, entonces es divisible por 5 y 7. En lugar de trabajar módulo 35, analizaremos las congruencias $5x^2 + 6x + 7 \equiv 0 \pmod{5}$ y $5x^2 + 6x + 7 \equiv 0 \pmod{7}$. La primera congruencia se puede simplificar a $x + 2 \equiv 0 \pmod{5}$, o bien $x \equiv 3 \pmod{5}$. La segunda congruencia es equivalente a $5x^2 + 6x \equiv 0 \pmod{7}$, la cual tiene la solución trivial $x \equiv 0 \pmod{7}$ y otra no trivial $x \equiv 3 \pmod{7}$. ¿Cómo usaremos estas soluciones para resolver el problema original? Lo que necesitamos son números que sean congruentes con 3 módulo 5, y también a 0 o 3 módulo 7. Una manera simple de encontrar tales números es la siguiente: comenzando con 3 módulo 5, tenemos la sucesión aritmética

$$3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, 63, 68, 73, 78, \ldots.$$

Los números que son 0 módulo 7 pertenecen a la sucesión

$$0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, \ldots.$$

Si buscamos traslapes, obtenemos al 28 y al 63. Ya que suponemos encontrar soluciones módulo 35, esto significa que $x \equiv 28 \pmod{35}$ es una solución. De hecho todo lo que necesitábamos era calcular parte de la sucesión entre 0 y 35 para ver las coincidencias. De manera análoga, si $x \equiv 3 \pmod 7$, entonces x pertenece a la sucesión $3, 10, 17, 24, 31, \ldots$, y obtenemos una segunda solución $x \equiv 3 \pmod{35}$. Estas soluciones ya son fáciles de verificar, por ejemplo $5 \cdot 28^2 + 6 \cdot 28 + 7 = 4095 = 117 \cdot 35$.

Sería bueno si pudiéramos trabajar con congruencias pequeñas para obtener congruencias grandes por algún método más eficiente que el anterior. Por ejemplo, supongamos que tenemos la congruencia $71x^2 + 72x + 73 \equiv 0 \pmod{5183}$. En este caso $5183 = 71 \cdot 73$, de modo que este ejemplo es similar al anterior, pero las congruencias son más grandes. Si trabajamos módulo 71, obtenemos $x + 2 \equiv 0 \pmod{71}$, o $x \equiv -2 \pmod{71}$. La segunda congruencia es $71x^2 + 72x \equiv 0 \pmod{73}$, la cual tiene la solución trivial $x \equiv 0 \pmod{73}$. De hecho, podemos encontrar una segunda solución: si $x \not\equiv 0 \pmod{73}$, entonces podemos cancelar x para obtener $71x + 72 \equiv 0 \pmod{73}$, la cual es equivalente con $-2x - 1 \equiv 0 \pmod{73}$, o $2x \equiv -1 \equiv 72 \pmod{73}$. Luego, $x \equiv 36 \pmod{73}$. Ahora lo que necesitamos es un número x tal que $x \equiv -2 \pmod{71}$ y $x \equiv 0 \pmod{73}$, y un segundo número x tal que $x \equiv -2 \pmod{71}$ y $x \equiv 36 \pmod{73}$. Sin embargo, buscar por inspección la intersección en las sucesiones aritméticas podría ser muy tedioso.

Existe una aproximación sistemática a la solución de este problema, dada por un resultado conocido como el *teorema chino del residuo*. La razón del nombre se debe a que hay una referencia a este tipo de problemas desde la antigua China. En los escritos de Sun Tsu, está la pregunta de determinar un número que dejara residuo 2 al dividirse entre 3, dejara residuo 3 al dividirse entre 5 y dejara otra vez residuo 2 al dividirse entre 7. En notación de congruencias, Sun Tsu buscaba números x que satisfagan simultáneamente el sistema de congruencias

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

Teorema 2 (Teorema chino del residuo) *Sean $m_1, m_2, \ldots, m_n$ enteros positivos primos relativos por parejas. Sean $a_1, a_2, \ldots, a_n$ cualesquiera números enteros. Entonces, existe un entero x tal que*

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1), \\ x &\equiv a_2 \ (mod\ m_2), \\ &\vdots \\ x &\equiv a_n \ (mod\ m_n). \end{aligned}$$

Además, si $M = m_1 m_2 \cdots m_k$, entonces x es único módulo M.

Demostración. Daremos una demostración poco constructiva cuyo interés es más teórico que práctico. Esto es, demostraremos la existencia de tal entero x. Después de esta demostración veremos un ejemplo de cómo obtener una solución.
La idea es resolver primero casos especiales, donde exactamente uno de los a_i's es 1 y los otros son 0. Comencemos definiendo para cada $i = 1, 2, \ldots, n$, el entero P_i como el producto $m_1 m_2 \cdots m_n$ sin el factor m_i, es decir, $P_i = \frac{m_1 m_2 \cdots m_n}{m_i}$. Entonces, para cada $i = 1, \ldots, n$, los enteros P_i y m_i son primos relativos, ya que cada m_i es primo relativo con m_j para todo $j \neq i$. Luego, por el Teorema 1, la congruencia $P_i x \equiv 1 \pmod{m_i}$ tiene solución, esto es, existe un entero c_i ($0 < c_i < m_i$) tal que $c_i P_i \equiv 1 \pmod{m_i}$. Si ahora, $N_i = c_i P_i$, entonces $N_i \equiv 1 \pmod{m_i}$ y $N_i \equiv 0 \pmod{m_k}$ para $k \neq i$ ya que $P_i \equiv 0 \pmod{m_k}$.
Finalmente, usamos las soluciones $N_1, N_2, \ldots, N_n$ obtenidas en los casos especiales para formar el número $x = a_1 N_1 + a_2 N_2 + \cdots + a_n N_n$. Ahora, es fácil ver que la expresión para x satisface cada una de las congruencias del teorema.
Para ver que x es único módulo M, supongamos que y también es una solución. Entonces $x \equiv a_1 \pmod{m_1}$ y $y \equiv a_1 \pmod{m_1}$, de modo que $x \equiv y \pmod{m_1}$. De manera análoga tenemos que $x \equiv y \pmod{m_i}$ para cada $i = 1, \ldots, n$. Esto significa que $x - y$ es divisible entre cada uno de $m_1, m_2, \ldots, m_n$. Como los m_i's son primos relativos por parejas, $x - y$ es divisible entre $m_1 m_2 \cdots m_n = M$ y por lo tanto $x \equiv y \pmod{M}$.

En la demostración anterior, aunque puede resultar tedioso encontrar los números c_i, lo que sabemos es que existe una solución $x = a_1 c_1 P_1 + \cdots + a_n c_n P_n$.

Existe otra aproximación para resolver sistemas de congruencias. Supongamos que queremos resolver el problema de Sun Tsu. A partir de la congruencia $x \equiv 2 \pmod{3}$, sabemos que $x = 2 + 3k$ para algún entero k. Sustituyendo esta igualdad en la segunda congruencia obtenemos que $2 + 3k \equiv 3 \pmod{5}$ y tratamos de resolver esta congruencia para k. Sumando 3 a cada lado y simplificando, obtenemos $3k \equiv 1 \pmod{5}$. Esta es una congruencia lineal como las descritas al inicio de este escrito. Podríamos trabajar con la ecuación equivalente $3k + 5y = 1$, o sólo notar que $2 \cdot 3 = 6 \equiv 1 \pmod{5}$. Usando esto, multiplicamos la congruencia por 2 y obtenemos que $k \equiv 2 \pmod{5}$. Esto significa que $k = 2 + 5j$ para algún entero j, de modo que $x = 2 + 3k = 2 + 3(2 + 5j) = 8 + 15j$. Ahora sabemos que la solución al sistema de dos congruencias $x \equiv 2 \pmod{3}$ y $x \equiv 3 \pmod{5}$ es $x \equiv 8 \pmod{15}$. Ahora vamos a la tercera congruencia con $8 + 15j \equiv 2 \pmod{7}$. Reduciendo módulo 7 obtenemos $1 + j \equiv 2 \pmod{7}$, de donde $j \equiv 1 \pmod{7}$. Escribiendo $j = 1 + 7k$ tenemos que $x = 8 + 15(1 + 7k) = 23 + 105k$, y de aquí $x \equiv 23 \pmod{105}$. La solución $x = 23$ fue la que Sun Tsu dió como respuesta.

¿Qué sucede si los m_i's no son primos relativos? Pueden suceder varias cosas. En primer lugar, el sistema de congruencias podría no tener solución. En segundo lugar, el sistema podría tener solución, en cuyo caso las soluciones x satisfarán las congruencias, pero no módulo el producto de los m_i's. Veamos un par de ejemplos. Primero

consideremos el sistema

$$x \equiv 8 \pmod{12},$$
$$x \equiv 5 \pmod{9},$$
$$x \equiv 14 \pmod{15}.$$

Comenzando con la primera congruencia, escribimos $x = 8 + 12k$. Sustituyéndola en la segunda, obtenemos $8 + 12k \equiv 5 \pmod 9$. Luego, $3k \equiv -3 \pmod 9$, de donde $k \equiv -1 \equiv 2 \pmod 3$, o bien, $k = 2 + 3j$ para algún entero j. Esto significa que la solución a las primeras dos congruencias es $x = 8 + 12(2 + 3j) = 32 + 36j$, que es lo mismo que $x \equiv 32 \pmod{36}$. Observemos que 36 es menor que el producto $12 \cdot 9 = 108$. Esto se debe a que 12 y 9 no son primos relativos. Continuando, sustituyendo en la tercera congruencia obtenemos $32+36j \equiv 14 \pmod{15}$, de donde $2+6j \equiv 14 \pmod{15}$. Simplificando llegamos a $6j \equiv 12 \pmod{15}$ y por lo tanto $j \equiv 2 \pmod 5$, donde hemos usado el Teorema 1. Ahora, $j = 2 + 5m$ para algún entero m, de modo que $x = 32 + 36(2 + 5m) = 104 + 180m$, lo que significa que 104 es una solución, y las soluciones son únicas módulo 180 en lugar de $12 \cdot 9 \cdot 15 = 1620$.

Como segundo ejemplo, consideremos el sistema de congruencias

$$x \equiv 8 \pmod{12},$$
$$x \equiv 5 \pmod{9},$$
$$x \equiv 13 \pmod{15},$$

donde la única congruencia que cambió fue la última. De lo hecho previamente, tenemos que $x = 32 + 36j$ a partir de las primeras dos congruencias. Sin embargo, ahora cuando la sustituimos en la tercera, obtenemos $32 + 36j \equiv 13 \pmod{15}$, de donde $6j \equiv 11 \pmod{15}$ la cual no tiene solución según el Teorema 1, ya que $\text{mcd}(6, 15) = 3 \nmid 11$. Esto significa que el sistema inicial de congruencias no tiene solución.

Una aplicación: La función ϕ de Euler

En esta sección veremos una bonita aplicación del teorema chino del residuo a la función ϕ de Euler. Si n es un entero positivo, $\phi(n)$ denota el número de enteros positivos menores o iguales que n que son primos relativos con n. Por ejemplo, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, etc. El objetivo es determinar una manera fácil para calcular $\phi(n)$. En general, no hay una manera fácil de hallar $\phi(n)$ para valores grandes de n, pues $\phi(n)$ depende de cómo se factoriza n. Si factorizar n es difícil, entonces determinar $\phi(n)$ también es difícil. Sin embargo, en el caso en que la factorización de n sea relativamente sencilla, podemos decir mucho.

Teorema 3 *Si m y n son enteros positivos primos relativos, entonces $\phi(mn) = \phi(m)\phi(n)$.*

Demostración. Primero, notemos que hay una correspondencia uno a uno entre los números x tales que $0 \leq x \leq mn - 1$ y las parejas ordenadas (a, b) con $0 \leq a \leq m - 1$ y $0 \leq b \leq n - 1$. Esto es, dado un número x ($0 \leq x \leq mn - 1$), podemos elegir a y

b haciendo $a \equiv x \pmod{m}$ y $b \equiv x \pmod{n}$. Para el recíproco, el teorema chino del residuo es la clave: dados a, b, debemos hallar el correspondiente x. Y por supuesto, hay mn valores posibles de x y mn posibles parejas ordenadas (a, b).
Veamos qué sucede cuando m y n son primos relativos. En este caso, hay $\phi(mn)$ valores de x con $0 \leq a \leq mn - 1$ y $\text{mcd}(x, mn) = 1$. Hay $\phi(m)\phi(n)$ parejas ordenadas (a, b) que satisfacen $0 \leq a \leq m - 1$, $0 \leq b \leq n - 1$, $\text{mcd}(a, m) = 1$ y $\text{mcd}(b, n) = 1$. ¿Cómo se relaciona (a, b) con x? Nuevamente, dado x, podemos elegir a y b usando $a \equiv x \pmod{m}$ y $b \equiv x \pmod{n}$. Si $\text{mcd}(x, mn) = 1$ entonces $\text{mcd}(a, m) = 1$ y $\text{mcd}(b, n) = 1$ (ejercicio). Esto demuestra que $\phi(mn) \leq \phi(m)\phi(n)$. Recíprocamente, dados a y b con $0 \leq a \leq m - 1$ y $0 \leq b \leq n - 1$, podemos usar el teorema chino del residuo para encontrar un x tal que $0 \leq x \leq mn - 1$ y $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$. Más aún, si $\text{mcd}(m, a) = 1$ y $\text{mcd}(n, b) = 1$, se sigue que $\text{mcd}(mn, x) = 1$ (ejercicio). Esto nos da la otra desigualdad $\phi(mn) \geq \phi(m)\phi(n)$, y por lo tanto estas dos expresiones deben ser iguales.

Estamos listos para dar una fórmula para $\phi(n)$. Usaremos el siguiente resultado, fácil de probar: *Si p es un número primo, entonces $\phi(p^n) = p^{n-1}(p - 1)$ para todo entero positivo n.* Su demostración se deja de ejercicio al lector.

Dado un entero positivo n, consideremos su descomposición canónica $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ donde $p_1, \ldots, p_k$ son números primos distintos, y $a_1, \ldots, a_k$ son enteros positivos. Entonces, usando el Teorema 3 y la fórmula para $\phi(p^n)$ obtenemos

$$\phi(n) = p_1^{a_1-1}(p_1 - 1)p_2^{a_2-1}(p_2 - 1) \cdots p_k^{a_k-1}(p_k - 1).$$

Usualmente, escribimos la fórmula anterior de manera más compacta. Observemos que $p-1 = p(1-\frac{1}{p})$ y $p^{a-1}(p-1) = p^a(1-\frac{1}{p})$. Si hacemos esto con cada factor en la fórmula anterior, entonces el producto de las potencias de primos es de nuevo n, y obtenemos que

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

Así por ejemplo, si $n = 360 = 2^3 \cdot 3^2 \cdot 5$, entonces

$$\phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96.$$

Resolución de problemas de olimpiada

En esta sección veremos algunas aplicaciones del teorema chino del residuo en la resolución de problemas de olimpiada.

Problema 1. Sea p un número primo. Demuestre que hay una infinidad de enteros positivos n tales que p divide a $2^n - n$.

Solución. Si $p = 2$, todo número n par cumple que p divide a $2^n - n$.
Supongamos que $p \geq 3$. Por el pequeño teorema de Fermat[1], $2^{p-1} \equiv 1 \pmod{p}$. Luego,

[1] Ver en el apéndice el teorema 4.

si $n \equiv 0 \pmod{p-1}$, tenemos que $2^n \equiv 1 \pmod{p}$. Y si $n \equiv 1 \pmod{p}$ tenemos que $2^n \equiv n \pmod{p}$. Por lo tanto, basta garantizar la existencia de una infinidad de enteros n tales que $n \equiv 0 \pmod{p-1}$ y $n \equiv 1 \pmod{p}$. El teorema chino del residuo nos garantiza la existencia de un entero positivo N tal que $N \equiv 0 \pmod{p-1}$ y $N \equiv 1 \pmod{p}$. Por lo tanto, todos los números n tales que $n \equiv N \pmod{p(p-1)}$, satisfacen el problema en este caso.

Problema 2. (IMO, 1989) Demuestre que para cada entero positivo n existen n enteros positivos consecutivos, ninguno de los cuales es la potencia de un número primo.

Solución. Sean $p_1, p_2, \ldots, p_{2n}$ números primos distintos. Ya que $p_1p_2, p_3p_4, \ldots, p_{2n-1}p_{2n}$ son primos relativos por parejas, el teorema chino del residuo implica que existe un entero positivo N tal que

$$\begin{aligned} N &\equiv -1 \pmod{p_1p_2}, \\ N &\equiv -2 \pmod{p_3p_4}, \\ &\vdots \\ N &\equiv -n \pmod{p_{2n-1}p_{2n}}. \end{aligned}$$

Luego, cada uno de los n enteros consecutivos $N+1, N+2, \ldots, N+n$ es divisible por más de un número primo, y por lo tanto, cada uno de ellos no puede ser la potencia de un número primo.

Solución alternativa. Consideremos el conjunto

$$S = \left\{[(n+1)!]^2 + 2, [(n+1)!]^2 + 3, \ldots, [(n+1)!]^2 + (n+1)\right\}.$$

Cada entero del conjunto S es de la forma $[(n+1)!]^2 + k$ donde $k \geq 2$ y k es un divisor de $(n+1)!$. Luego, k^2 divide a $[(n+1)!]^2$ y para algún entero positivo t tenemos que

$$[(n+1)!]^2 + k = k^2t + k = k(kt+1),$$

donde k y $kt+1$ son primos relativos. Ya que cada uno de estos factores es mayor que 1, éstos aportan al menos dos divisores primos distintos del número $[(n+1)!]^2 + k$, haciendo imposible para el número ser una potencia de un número primo.

Problema 3. Demuestre que para todos los enteros positivos n y k, existe un conjunto de n enteros consecutivos tal que cada uno de los elementos de este conjunto es divisible por k primos distintos ninguno de los cuales divide a los otros elementos del conjunto.

Solución. Consideremos $k \cdot n$ números primos distintos

$$p_{11}, p_{12}, \ldots, p_{1k}; p_{21}, p_{22}, \ldots, p_{2k}; \ldots; p_{n1}, p_{n2}, \ldots, p_{nk}$$

cada uno mayor o igual que n.

Por el teorema chino del residuo, existe un número entero N tal que

$$\begin{array}{cccc} N \equiv 0 \pmod{p_{11}}, & N \equiv 0 \pmod{p_{12}}, & \ldots, & N \equiv 0 \pmod{p_{1k}}, \\ N \equiv -1 \pmod{p_{21}}, & N \equiv -1 \pmod{p_{22}}, & \ldots, & N \equiv -1 \pmod{p_{2k}}, \\ \vdots & \vdots & & \vdots \\ N \equiv -n+1 \pmod{p_{n1}}, & N \equiv -n+1 \pmod{p_{n2}}, & \ldots, & N \equiv -n+1 \pmod{p_{nk}}. \end{array}$$

Ahora, $N, N+1, \ldots, N+n-1$ son n enteros consecutivos que satisfacen el problema.

Solución alternativa. La demostración la haremos por inducción sobre k. Si $k = 1$, se deja al lector demostrar que cada uno de los números del conjunto

$$\{n!+2, n!+3, \ldots, n!+n\}$$

es divisible por un primo que no divide a ningún otro elemento del conjunto.
Supongamos que el resultado es cierto para $k \geq 1$, es decir, existen enteros $A+1, A+2, \ldots, A+n$ que satisfacen la condición del problema con k divisores primos. Sean $P = (A+n)!$ y $B = P + A$. Consideremos los números

$$B+1, B+2, \ldots, B+n.$$

Para cada $i = 1, \ldots, n$, tenemos que $A+i \mid B+i$. También, si $p \mid A+i$ donde p es uno de esos divisores primos, entonces $p \mid P$, de modo que $p \mid B+j$ si y sólo si $p \mid A+j$ si y sólo si $i = j$. Así, esos k divisores primos funcionan. Debemos determinar otro divisor primo para cada $B+i$.
Supongamos que, para algún i, $B+i$ no tiene ningún divisor primo (distinto de los k mencionados previamente) que no divida a ningún otro $B+j$. Entonces, no debe tener divisores primos mayores que $A+n$, ya que los k primos originales son menores o iguales que $A+i$ (pues cada uno de ellos divide a $A+i$), y cualquier primo que divide a $B+i$ y a $B+j$ debe dividir a $i-j$, y en consecuencia ser menor que n.
Supongamos ahora que p es uno de los primos que no cumplen, es decir, $p \mid B+i$ y $p \mid B+j$. Entonces $p < n < A+n$. Ya que $(A+n)! = P$ y $p \mid (A+n)!$, tenemos que $p \mid A+i$ y $p \mid A+j$. Se sigue que todos los primos que no cumplen para $B+i$ también dividen a $A+i$. Luego, será suficiente determinar un primo p tal que divide a $B+i$ pero no divide a $A+i$. Supongamos que no existe tal primo p. Entonces, como antes, existe un primo p que divide a $A+i$ tal que $p(A+i) \mid B+i$ (pues $B+i$ es mayor que $A+i$). Por otra parte, si $p \neq A+i$ tenemos que $p(A+i) \mid P$, y por lo tanto $p(A+i) \mid A+i$, lo cual es un absurdo. De esta manera tenemos que $A+i = p$. Esto implica que $k = 1$. Si nuestros números $A+1, \ldots, A+n$ para $k = 1$ fueron $(n+2)!+2, \ldots, (n+2)!+(n+2)$, entonces todos ellos eran compuestos, lo que significa que $A+i = p$ es imposible.

Problema 4. (Lista corta, IMO 2005) Sean a y b enteros positivos tales que $a^n + n$ divide a $b^n + n$ para todo entero positivo n. Demuestre que $a = b$.

Solución. Tomando $n = 1$ tenemos que $a+1 \mid b+1$, lo cual implica que $b \geq a$. Supongamos que $b > a$. Sea $p > b$ un número primo. Por el Teorema Chino del residuo existe un entero positivo N tal que

$$N \equiv 1 \pmod{p-1} \quad \text{y} \quad N \equiv -a \pmod{p}.$$

Aplicando ahora el pequeño teorema de Fermat, tenemos que $a^{p-1} \equiv 1 \pmod{p}$ y de aquí $a^N = a(a^{p-1} \cdots a^{p-1}) \equiv a \pmod{p}$. Por lo tanto, $a^N + N \equiv a - a \equiv 0 \pmod{p}$. De esta manera tenemos que p divide al número $a^N + N$, y en consecuencia divide también a $b^N + N$. Por otra parte, usando nuevamente el pequeño teorema de Fermat, obtenemos de manera análoga que $b^N \equiv b \pmod{p}$. Como $b^N + N \equiv 0 \pmod{p}$, concluimos que $0 \equiv b^N + N \equiv b - a \pmod{p}$, y en consecuencia $p \leq b - a < b < p$, lo cual es una contradicción. Por lo tanto, $a = b$.

Problema 5. Demuestre que para cada entero positivo n, existen enteros a y b tales que $4a^2 + 9b^2 - 1$ es divisible entre n.

Solución. Supongamos primero que n es impar. En este caso, sea $b = 0$ y sea a cualquier entero tal que $2a \equiv 1 \pmod{n}$. Entonces, tenemos que

$$4a^2 + 9b^2 - 1 = 4a^2 - 1 = (2a - 1)(2a + 1),$$

el cual es divisible entre n.
Supongamos ahora que n no es divisible entre 3. En este caso, sea $a = 0$ y sea b cualquier entero tal que $3b \equiv 1 \pmod{n}$. Entonces, tenemos que

$$4a^2 + 9b^2 - 1 = 9b^2 - 1 = (3b - 1)(3b + 1),$$

el cual es divisible entre n.
Finalmente, consideremos el caso general. Escribamos n en la forma $n_1 n_2$, donde n_1 no es divisible entre 2, n_2 no es divisible entre 3, y n_1 y n_2 son primos relativos (por ejemplo, tomamos n_2 como la potencia de 2 en la factorización en primos de n, y n_1 es $\frac{n}{n_2}$). Por lo demostrado previamente, sabemos que existen enteros a_1 y b_1 tales que $4a_1^2 + 9b_1^2 - 1$ es divisible entre n_1, y existen enteros a_2 y b_2 tales que $4a_2^2 + 9b_2^2 - 1$ es divisible entre n_2. Como n_1 y n_2 son primos relativos, el teorema chino del residuo implica que existen enteros a y b tales que $a \equiv a_1 \pmod{n_1}$, $a \equiv a_2 \pmod{n_2}$, $b \equiv b_1 \pmod{n_1}$ y $b \equiv b_2 \pmod{n_2}$. Entonces,

$$4a^2 + 9b^2 - 1 \equiv 4a_1^2 + 9b_1^2 - 1 \equiv 0 \pmod{n_1},$$
$$4a^2 + 9b^2 - 1 \equiv 4a_2^2 + 9b_2^2 - 1 \equiv 0 \pmod{n_2}.$$

Luego, $4a^2 + 9b^2 - 1$ es divisible entre n_1 y n_2. Como n_1 y n_2 son primos relativos, se sigue que $4a^2 + 9b^2 - 1$ es divisible entre $n_1 n_2 = n$.

Para finalizar, dejamos unos ejercicios al lector.

Ejercicios

1. Resuelve la congruencia $35x \equiv 56 \pmod{77}$.

2. Resuelve el sistema de congruencias

$$x \equiv 3 \pmod 5,$$
$$x \equiv 2 \pmod 7,$$
$$x \equiv 3 \pmod 9.$$

3. Sean p y n enteros positivos con p número primo. Demuestra que $\phi(pn) = p\phi(n)$ si $p \mid n$, y que $\phi(pn) = (p-1)\phi(n)$ si $p \nmid n$.

4. Sean m y n enteros positivos. Si d es el máximo común divisor de m y n, demuestra que $\phi(mn) = \frac{d\phi(m)\phi(n)}{\phi(d)}$.

5. ¿Existen $1,000,000$ de enteros consecutivos, cada uno divisible por el cuadrado de un número primo?

6. Sin usar el teorema chino del residuo, demuestra que para cada entero positivo n existen n enteros positivos consecutivos que no son números primos.

7. Resuelve el ejercicio anterior usando el teorema chino del residuo.

8. Sea $n \geq 2$ un entero. Demuestra que cada uno de los elementos del conjunto

$$\{n! + 2, n! + 3, \ldots, n! + n\}$$

es divisible por un primo que no divide a ningún otro elemento del conjunto.

9. Un entero m es una *potencia perfecta* si existen enteros positivos a y n con $n > 1$ tales que $m = a^n$. Demuestra que existe un conjunto A de 2013 enteros positivos distintos tal que los elementos de cada subconjunto de A suman una potencia perfecta.

10. Decimos que un entero positivo n es *sorprendente* si existen enteros positivos a, b y c tales que $n = (b,c)(a,bc) + (c,a)(b,ca) + (a,b)(c,ab)$. Demuestra que existen 2013 enteros positivos consecutivos sorprendentes.
(Nota: (m,n) denota el máximo común divisor de los enteros positivos m y n.)

11. Sean k y n enteros positivos tales que $k \mid n$. Demuestra que para cada entero positivo a menor que k y primo relativo con k, existe un entero positivo b menor que n y primo relativo con n tal que $a \equiv b \pmod k$.

Bibliografía

1. Andreescu, T., Gelca, R. *Putnam and Beyond.* Springer, 2007.

2. Ireland K., Rosen M. *A Classical Introduction to Modern Number Theory.* Springer-Verlag, Second Edition, 1992.