El Teorema Chino del Residuo, una herramienta poderosa

Por Víctor Hugo Almendra Hernández

Nivel Avanzado

El manejo de congruencias en teoría de números, juega un papel muy importante dentro de la olimpiada de matemáticas y, dentro de ello, el Teorema Chino del Residuo es una herramienta sumamente útil. Además de hablar del teorema en sí, mostraremos tres maneras en las que este puede ser usado: para construir, para acotar números y para dividir un problema de modo que sea fácil trabajar con los subproblemas resultantes.

Teorema Chino del Residuo

Comenzaremos por enunciar y demostrar el teorema en cuestión.

Teorema Chino del Residuo (TCR). Sean $m_1, m_2, \ldots, m_n$ enteros positivos distintos de 1 y primos relativos por parejas, y sea $M = m_1 m_2 \cdots m_n$. Entonces, para cualesquiera enteros $x_1, x_2, \ldots, x_n$ el sistema de congruencias:

$$\begin{aligned} x &\equiv x_1 \pmod{m_1}, \\ x &\equiv x_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv x_n \pmod{m_n}, \end{aligned}$$

tiene soluciones y cualesquiera dos soluciones tienen la misma congruencia módulo M.

Demostración. Construiremos primero una solución al sistema de congruencias propuesto. Esta construcción es muy clara una vez que se tiene en mente la forma que queremos que tenga nuestra x para que satisfaga las n congruencias. Buscaremos enteros $k_1, k_2, \ldots, k_n$ tales que para cada $i \in \{1, 2, \ldots, n\}$, se cumpla que $k_i \equiv x_i \pmod{m_i}$ y $k_i \equiv 0 \pmod{m_j}$ para todo $j \neq i$, con $i \neq j$. Una vez que determinemos estos enteros, $x = k_1 + k_2 + \cdots + k_n$ será solución al sistema de congruencias, ya que $x = k_1 + k_2 + \cdots + k_n \equiv k_i \equiv x_i \pmod{m_i}$, pues $k_j \equiv 0 \pmod{m_j}$ siempre que j sea distinto de i. Entonces solo resta encontrar los enteros $k_1, k_2, \ldots, k_n$ que cumplan lo mencionado anteriormente. Para esto, sean $r_i = \frac{M}{m_i}$, para $i = 1, 2, \ldots, n$. Como los m_i's son primos relativos por parejas, tenemos que $\text{mcd}(r_i, m_i) = 1$, por lo que para cada i existe c_i entero tal que $c_i r_i \equiv 1 \pmod{m_i}$. Finalmente, los enteros $k_i = x_i c_i r_i$ cumplen lo deseado, ya que si $j \neq i$, m_j divide a r_i y, por lo tanto, $k_i \equiv 0 \pmod{m_j}$ y también se tiene que $k_i = x_i(c_i r_i) \equiv x_i \pmod{m_i}$, como queríamos. Entonces, $x = k_1 + k_2 + \cdots + k_n$ satisface el sistema de congruencias planteado.
Notemos ahora que si x, y son soluciones del sistema de congruencias, tenemos que m_i divide a $x - y$ para cada $i = 1, 2, \ldots, n$ y, como los m_i's son primos relativos por parejas, se sigue que M divide a $x - y$, esto es, $x \equiv y \pmod{M}$. Es fácil ver que si x es solución del sistema, entonces cualquier entero y tal que $y \equiv x \pmod{M}$ es también es solución.
Con esto concluimos que los enteros congruentes módulo M al entero x que construimos, son las únicas soluciones al sistema de congruencias. □

El caso general

El Teorema Chino del Residuo nos dice que bajo ciertas hipótesis nuestro sistema de congruencias tiene solución, ¿pero qué sucede cuando estas hipótesis no se cumplen? Es decir, cómo saber si determinado sistema tiene solución, si el sistema no satisface que los módulos que se están considerando son primos relativos por parejas. Nos gustaría poder resolver este problema con lo que ya tenemos, por lo que pasaremos de un sistema cualquiera a uno que cumpla las hipótesis del teorema.

Se tiene el sistema de congruencias:

$$\begin{aligned} x &\equiv x_1 \pmod{k_1}, \\ x &\equiv x_2 \pmod{k_2}, \\ &\vdots \\ x &\equiv x_n \pmod{k_n}, \end{aligned}$$

donde $x_1, x_2, \ldots, x_n$ son enteros cualesquiera y $k_1, k_2, \ldots, k_n$ son enteros positivos. Una primera observación es que para que el sistema tenga solución, es necesario que para cualesquiera $i, j \in \{1, 2, \ldots, n\}$, se cumpla que $x_i \equiv x_j \pmod{\text{mcd}(k_i, k_j)}$. Para probar esto, basta con notar que si existe x tal que satisface cada una de las congruencias planteadas anteriormente, entonces k_i divide a $x - x_i$ y k_j divide a $x - x_j$, por lo que $\text{mcd}(k_i, k_j)$ divide a ambos números y, en consecuencia, divide a su diferencia,

que es $x_i - x_j$, de donde concluimos que $x_i \equiv x_j \pmod{\text{mcd}(k_i, k_j)}$ para cualesquiera i, j, como se quería.
Veamos que esta condición también es suficiente para garantizar que existe solución al sistema de congruencias. Supongamos que, además de las congruencias presentadas, se cumple que $x_i \equiv x_j \pmod{\text{mcd}(k_i, k_j)}$ para cualesquiera i, j. Sea K el mínimo común múltiplo de $k_1, k_2, \ldots, k_n$. Considerando la descomposición canónica de $K = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, tenemos que existe j_s tal que $p_s^{\alpha_s}$ divide a k_{j_s} y, además, no existe t tal que $p_s^{\alpha_s+1}$ divida a k_t. En otras palabras, α_s es la máxima potencia de p_s que divide a alguno de los k_i's. Definimos $s_i \in \{1, 2, \ldots, n\}$ tal que $p_i^{\alpha_i}$ divide a k_{s_i} para cada $i \in \{1, 2, \ldots, r\}$ (tal entero existe por lo que mencionamos anteriormente). Demostraremos ahora que el sistema de congruencias:

$$\begin{aligned} x &\equiv x_{s_1} \pmod{p_1^{\alpha_1}}, \\ x &\equiv x_{s_2} \pmod{p_2^{\alpha_2}}, \\ &\vdots \\ x &\equiv x_{s_r} \pmod{p_r^{\alpha_r}}, \end{aligned}$$

es equivalente al planteado inicialmente, esto es, x es solución del primer sistema de congruencias si y solo si x es solución del segundo sistema de congruencias. Supongamos primero que x es solución del primer sistema de congruencias y sea $i \in \{1, 2, \ldots, r\}$. Como $x \equiv x_{s_i} \pmod{k_{s_i}}$, se sigue que k_{s_i} divide a $x - x_{s_i}$ y, como $p_i^{\alpha_i}$ divide a k_{s_i}, resulta que $x \equiv x_{s_i} \pmod{p_i^{\alpha_i}}$, por lo que x es, en efecto, una solución del segundo sistema de congruencias. Para el recíproco, consideremos x solución del segundo sistema y sea $i \in \{1, 2, \ldots, n\}$. Como k_i divide a K, tenemos que $k_i = p_{i_1}^{\beta_{i_1}} p_{i_2}^{\beta_{i_2}} \cdots p_{i_t}^{\beta_{i_t}}$, donde $\{i_1, i_2, \ldots, i_t\} \subset \{1, 2, \ldots, r\}$ y, además, $\beta_{i_j} \leq \alpha_{i_j}$ para cada j. Entonces, por Teorema Chino del Residuo tenemos que $x \equiv x_i \pmod{k_i}$ si y solo si $x \equiv x_i \pmod{p_{i_j}^{\beta_{i_j}}}$ para cada $j \in 1, 2, \ldots, t$. Ahora, como $x \equiv x_{s_{i_j}} \pmod{p_{i_j}^{\alpha_{i_j}}}$ y $\beta_{i_j} \leq \alpha_{i_j}$, tenemos que $x \equiv x_{s_{i_j}} \pmod{p_{i_j}^{\beta_{i_j}}}$. Recordemos que $x_i \equiv x_{s_{i_j}} \pmod{\text{mcd}(k_i, k_{s_{i_j}})}$ y, como $p_{i_j}^{\beta_{i_j}}$ divide a k_i y $p_{i_j}^{\alpha_{i_j}}$ divide a $k_{s_{i_j}}$, se sigue que $p_{i_j}^{\beta_{i_j}}$ divide a $\text{mcd}(k_i, k_{s_{i_j}})$, por lo que $x_i \equiv x_{s_{i_j}} \pmod{p_{i_j}^{\beta_{i_j}}}$. Luego, $x \equiv x_{s_{i_j}} \equiv x_i \pmod{p_{i_j}^{\beta_{i_j}}}$ para cada j, lo cual implica que $x \equiv x_i \pmod{k_i}$, como queríamos. Finalmente, como el segundo sistema de congruencias cumple las hipótesis del Teorema Chino del Residuo, este tiene solución y es única módulo K.
Concluimos entonces que el sistema de congruencias planteado tiene solución si y solo si para cualesquiera i, j se cumple que $x_i \equiv x_j \pmod{\text{mcd}(k_i, k_j)}$. Además, la solución es única módulo M, el mínimo común múltiplo de $k_1, k_2, \ldots, k_n$. □

Fórmula de interpolación de Lagrange

Consideremos el siguiente ejemplo. Se quiere encontrar un polinomio $P(x)$ tal que $P(0) = 1$, $P(1) = 7$ y $P(2) = 10$. Lo que haremos será considerar un polinomio de la forma $P(x) = c_1 x(x-1) + c_2(x-1)(x-2) + c_3(x-2)(x)$. Notemos que

$P(0) = 2c_2$, $P(1) = -c_3$ y $P(2) = 2c_1$, entonces basta con hacer $c_1 = 5, c_2 = \frac{1}{2}$ y $c_3 = -7$.

Notemos que la idea con la que construimos el polinomio $P(x)$ es muy similar a la forma en como se construyó una solución al sistema de congruencias, pues nos apoyamos en sumandos que surgen al considerar el producto de todos los elementos en cuestión excepto alguno de ellos. Ciertamente esta es una idea bastante útil para problemas de esta naturaleza. De manera más general, supongamos que tenemos $d + 1$ números reales distintos $x_1, x_2, \ldots, x_{d+1}$ y $d + 1$ valores (no necesariamente distintos) $y_1, y_2, \ldots, y_{d+1}$. Entonces, existe un único polinomio P, de grado menor o igual a d tal que $P(x_i) = y_i$ para $i = 1, 2, \cdots, d+1$ y, además, se conoce la forma de dicho polinomio P, la cual está dada por la *Fórmula de interpolación de Lagrange*. Veamos cómo se construye. Una vez teniendo esto será muy claro que el polinomio construido cumple lo deseado y tiene grado menor o igual a d, y restaría ver que es único.
Para cada $i = 1, \ldots, d + 1$, sea

$$Q_i(x) = \prod_{j \neq i} (x - x_j),$$

esto es, $Q_i(x)$ es el polinomio que resulta de multiplicar todos los $x - x_j$, excepto $x - x_i$. Ahora, veamos que existen números reales $c_1, c_2, \ldots, c_{d+1}$, tales que

$$P(x) = c_1Q_1(x) + c_2Q_2(x) + \cdots + c_{d+1}Q_{d+1}(x).$$

Notemos que el papel que juegan los Q_i's es exactamente el mismo que el de los k_i's en la prueba dada para el Teorema Chino del Residuo, es decir, $Q_i(x_j) = 0$ para todo $j \neq i$ y $Q_i(x_i)$ es distinto de 0, por lo que si hacemos $c_i = \frac{y_i}{Q_i(x_i)}$ tendremos que $P(x_i) = y_i$, como queremos.

El polinomio obtenido,

$$P(x) = y_1\frac{Q_1(x)}{Q_1(x_1)} + y_2\frac{Q_2(x)}{Q_2(x_2)} + \cdots + y_{d+1}\frac{Q_{d+1}(x)}{Q_{d+1}(x_{d+1})},$$

es conocido como la **fórmula de interpolación de Lagrange**. Notemos que el grado de P es en efecto a lo más d, ya que cada uno de los Q_i's tiene grado d. Demostraremos que no existe otro polinomio R, de grado menor o igual a d que cumpla que $R(x_i) = y_i$ para todo i. Supongamos, por contradicción, que sí existe. Entonces, el polinomio $R(x) - P(x)$ es de grado a lo más d. Sin embargo, $R(x_i) - P(x_i) = y_i - y_i = 0$ para $i = 1, 2, \ldots, d+1$, esto nos dice que el polinomio es la constante 0 pues de lo contrario tendría grado mayor que d por tener al menos $d + 1$ raíces. Como $R(x) - P(x) = 0$ para todo x real, se sigue que $R(x) = P(x)$, lo que es una contradicción. Concluimos que el polinomio dado por la fórmula de interpolación de Lagrange, es el único que cumple las $d + 1$ condiciones deseadas y que tiene grado menor o igual a d.

Este tipo de ideas "diagonales" al momento de construir cosas, en donde forzamos que suceda cierta condición cuando $i \neq j$ y otra distinta cuando $i = j$, como en la

solución propuesta en la demostración del Teorema Chino del Residuo, o la forma de llegar a la fórmula de interpolación de Lagrange, resultan muy útiles en el mundo de las matemáticas, incluso fuera de la olimpiada.

Retomando el Teorema Chino del Residuo (TCR), además de las ideas tan útiles que se vieron en la demostración, el resultado que nos da este teorema suele ser muy útil dentro de los problemas de la olimpiada. A continuación, mostraremos tres diferentes técnicas en las que es común utilizar el TCR: para construir números que cumplan ciertas propiedades, para acotar números que satisfagan ciertas condiciones, o para dividir el problema en subproblemas con los que sea más fácil trabajar.

Construcciones

Para construir enteros que satisfagan cierto sistema de congruencias como el planteado por el TCR, muchas veces es suficiente con saber de su existencia para concluir lo que se ande buscando.

Ejemplo 1. (Estados Unidos, 2008) Sea n un entero positivo. Muestra que existen enteros positivos $k_0, k_1, \ldots, k_n$ mayores que 1, primos relativos por parejas tales que $k_0 k_1 \cdots k_n - 1$ es el producto de dos enteros consecutivos.

Solución con el TCR. Notemos que es suficiente demostrar que existe m entero positivo tal que $m(m+1)+1$ tiene al menos $n+1$ factores primos distintos, lo que nos permitirá "repartir" los factores en $k_0, k_1, \ldots, k_n$ de modo que resulte cada uno mayor que 1 y que sean primos relativos. Consideremos el polinomio $P(x) = x^2 + x + 1$. Queremos probar que existe m tal que $P(m)$ tiene tantos divisores primos distintos como queramos, para lo cual primero hay que ver que el conjunto de primos que divide a algún $P(a)$, con a entero, es infinito. Supongamos que tal conjunto es finito, digamos que $p_1, p_2, \ldots, p_r$ son dichos primos, podemos tomar $a = p_1 p_2 \cdots p_r$ y, claramente, ninguno de estos primos divide a $P(a)$, lo que es una contradicción. Entonces, el conjunto de los primos que dividen a algún $P(a)$ es infinito, en particular tiene al menos $n+1$ elementos distintos. Sean $p_0, p_1, \ldots, p_n$ estos primos y $a_0, a_1, \ldots, a_n$ enteros tales que p_i divide a $P(a_i)$ para $i = 0, 1, \ldots, n$. Consideremos ahora el sistema de congruencias dado por $x \equiv a_i \pmod{p_i}$ para cada i. Por el TCR este sistema de congruencias tiene solución, pues $\text{mcd}(p_i, p_j) = 1$ si $i \neq j$ (ya que los p_i's son primos distintos). Sea N una solución de dicho sistema. Tenemos ahora que $P(N)$ es múltiplo de $p_0, p_1, \ldots p_n$, esto es, hemos encontrado un entero tal que $N(N+1)+1$ tiene al menos $p+1$ divisores primos distintos, como queríamos ver.

Solución sin el TCR. Recordando la factorización

$$x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1),$$

podemos generalizarla como sigue:

$$\begin{aligned} x^{2^{k+1}} + x^{2^k} + 1 &= (x^{2^k} + x^{2^{k-1}} + 1)(x^{2^k} - x^{2^{k-1}} + 1) \\ &= (x^{2^{k-1}} + x^{2^{k-2}} + 1)(x^{2^{k-1}} - x^{2^{k-2}} + 1)(x^{2^k} - x^{2^{k-1}} + 1). \end{aligned}$$

Además, la diferencia entre los primeros dos factores es $2x^{2^{k-1}}$, con lo que es fácil concluir que si x es entero, entonces los factores son primos relativos. Con esta observación concluimos que podemos tomar x entero positivo mayor que 1 y un exponente k lo suficientemente grande, de modo que $x^{2^{k+1}} + x^{2^k} + 1$ tenga al menos $n+1$ factores primos relativos por parejas (los que se obtienen al ir factorizando), con lo que hemos concluido, pues $x^{2^{k+1}} + x^{2^k} + 1 = x^{2^k}(x^{2^k} + 1) + 1$. Entonces, los factores obtenidos serán $k_0, k_1, \ldots, k_n$ y, claramente, son mayores que 1 si x es mayor que 1.

La segunda solución del Ejemplo 1, es evidentemente más simple que la primera. Sin embargo, requiere que se recuerde la factorización o que esta sea motivada de algún modo, lo cual ya no parece ser tan sencillo. La primera solución, una vez que se tiene en mente que se quiere que $m^2 + m + 1$ tenga muchos divisores, resulta natural pensar en el TCR, ya que este nos permite construir números, basados en su congruencia módulo ciertos enteros.

Ejemplo 2. Sea $P(x)$ un polinomio con coeficientes enteros tal que existen enteros positivos $a_1, a_2, \ldots, a_n$ tales que para cada entero x, existe $i \in \{1, 2, \ldots, n\}$ tal que a_i divide a $P(x)$. Muestra que existe $m \in \{1, 2, \ldots, n\}$ tal que a_m divide a $P(x)$ para todo entero x.

Solución. Supongamos, por contradicción, que para cada $i \in \{1, 2, \ldots, n\}$ existe x_i tal que a_i no divide a $P(x_i)$. Nos gustaría construir x tal que $P(x)$ no sea divisible por ninguno de $a_1, a_2, \ldots, a_n$, lo que nos daría la contradicción buscada. Como P tiene coeficientes enteros, sabemos que si d no divide a $P(a)$ entonces d no divide a $P(a + kd)$ con k entero. Esto último nos hace pensar que ya estamos cerca, pues si existe x tal que $x \equiv x_i \pmod{a_i}$ para $i = 1, 2, \ldots, n$ se llega a lo deseado. El único problema con esto, es que no sabemos si los enteros $a_1, a_2, \ldots, a_n$ son primos relativos por parejas, por lo que no podemos usar el TCR. Haremos ciertas modificaciones para poder usar este teorema. Como a_i no divide a $P(x_i)$, existe p_i primo tal que si $\alpha_i = v_{p_i}(a_i)$, entonces $p_i^{\alpha_i}$ no divide a $P(x_i)$. Consideremos entonces el sistema de congruencias dado por $x \equiv x_i \pmod{p_i^{\alpha_i}}$ para $i = 1, 2, \ldots, n$. Si existen j, k tales que $p_j = p_k$, omitimos la congruencia que contiene el mayor exponente para tal primo, esto es, si $\alpha_j \leq \alpha_k$, omitimos la congruencia $x \equiv x_k \pmod{p_k^{\alpha_k}}$. En caso contrario, omitimos la congruencia $x \equiv x_j \pmod{p_j^{\alpha_j}}$. Continuamos este proceso hasta que tengamos puras potencias de primos distintos en nuestro sistema de congruencias y, por el TCR, garantizamos que existe solución. Es fácil ver que esta x cumple que ninguno de $a_1, a_2, \ldots, a_n$ divide a $P(x)$, pues para cada $i = 1, 2, \ldots, n$, $p_i^{\alpha_i}$ no divide a $P(x)$, lo que es una contradicción. Concluimos entonces que existe m tal que a_m divide a $P(x)$ para todo entero x, como queríamos.

El ejemplo 2 muestra que hay ocasiones en las que no tenemos inmediatamente un sistema de congruencias que cumpla las hipótesis del Teorema Chino del Residuo, pero no hay que preocuparse. Usualmente con trucos que se adquieren con la práctica, como el de este ejemplo, podemos modificar las cosas para tener un sistema que cumpla tanto las condiciones del TCR como lo que se quiera para el problema en cuestión.

Ejemplo 3. Sea $\mathbb{N}$ el conjunto de los enteros positivos. Sea $f : \mathbb{N} \to \mathbb{N}$ una función que satisface las siguientes condiciones:

- Si m y n son primos relativos, entonces $f(m)$ y $f(n)$ son primos relativos.
- $n \leq f(n) \leq n + 2012$ para todo $n \in \mathbb{N}$.

Muestra que para cualquier $n \in \mathbb{N}$ y cualquier primo p, si p divide a $f(n)$, entonces p divide a n.

Solución. Procederemos por contradicción. Supongamos que existen n entero positivo y p primo tal que p divide a $f(n)$ pero p no divide a n. Sean $p_1, p_2, \ldots, p_{2012}$ números primos distintos y mayores que $2012, n$ y p. Como $1 < p_i \leq f(p_i)$, se tiene que existe q_i primo tal que $q_i \mid f(p_i)$ para cada $i \in \{1, 2, \ldots, 2012\}$. Notemos que si $i \neq j$, entonces $q_i \neq q_j$, pues $p_i \neq p_j$. En particular, $\text{mcd}(p_i, p_j) = 1$, por lo que $\text{mcd}(f(p_i), f(p_j)) = 1$ y, en consecuencia, $q_i \neq q_j$, como queremos. Ahora, por el TCR podemos garantizar que existe un entero positivo m que satisface las siguientes condiciones:

$$m \equiv 0 \pmod{p}, \tag{1}$$

$$m + i \equiv 0 \pmod{q_i} \text{ para cada } i \in \{1, 2, \ldots, 2012\}, \tag{2}$$

$$p_i \nmid m \text{ para cada } i \in \{1, 2, \ldots, 2012\}, \tag{3}$$

$$\text{mcd}(n, m) = 1. \tag{4}$$

Notemos que $p \neq q_i$ para cada $i \in \{1, 2, \ldots, 2012\}$, ya que $p_i > n$ implica que $\text{mcd}(p_i, n) = 1$ y, en consecuencia, $\text{mcd}(f(p_i), f(n)) = 1$; en particular, p no divide a $f(p_i)$ pues divide a $f(n)$. Con esto garantizamos que el sistema de congruencias dado por (1) y (2), tiene solución. Luego, si algún p_i es igual a algún q_j, entonces p_i no divide a las soluciones del sistema de congruencias dado por (1) y (2), ya que si x es solución, entonces $x + j \equiv 0 \pmod{q_j}$ y, como $0 < j \leq 2012$ y $q_j = p_i$, resulta que p_i no puede dividir a x. Concluimos que sí podemos garantizar (1), (2) y (3) simultáneamente, pues si el primo p_i no ha aparecido en (2), podemos pedir que $m \equiv 1 \pmod{p_i}$. Sea x una solución de (1), (2) y (3). Para ver la cuarta condición, basta ver que para cada primo q que divida a n, como p no divide a n, $q \neq p$, y entonces si q aparece en alguna de las condiciones anteriores, q no divide a x, y su q no ha aparecido, pediremos que $m \equiv 1 \pmod{q}$, con lo que se existe m que satisface las cuatro condiciones deseadas. Si $f(m) = m + i$ con $i \in \{1, 2, \ldots, 2012\}$, entonces $q_i \mid f(m)$. Por otro lado, como $\text{mcd}(p_i, m) = 1$, tenemos que $\text{mcd}(f(p_i), f(m)) = 1$ y como $q_i \mid f(p_i)$, q_i no divide a $f(m)$, lo que es una contradicción. Por lo tanto, $f(m) = m$ y, además, $p \mid m$ y $\text{mcd}(n, m) = 1$, con lo que hemos acabado, pues se tiene que entonces $1 = \text{mcd}(f(m), f(n)) = \text{mcd}(m, f(n))$, lo que es una contradicción, ya que $p \mid m$

y $p \mid f(n)$. Concluimos que la suposición de la existencia de n y p nos lleva a una contradicción, por lo que todo primo que divida a $f(n)$ divide a n para todo entero positivo n, como queríamos.

Acotar con TCR

En ciertas ocasiones nos presentamos con problemas en los que el TCR es útil para acotar. Un ejemplo de esto es que si sabemos que se tienen dos soluciones distintas de cierto sistema de congruencias, entonces su diferencia puede ser muy grande, pues será múltiplo del producto de los módulos considerados.

Ejemplo 4. (Olimpiada Nacional de Matemáticas por Internet, 2013) Para cualquier conjunto finito X de enteros, definimos $S(X)$ como la suma de todos los elementos de X y $P(X)$ como el producto de todos los elementos de X. Sean A y B dos conjuntos finitos de enteros positivos tales que $|A| = |B|$, $P(A) = P(B)$ y $S(A) \neq S(B)$. Si para cada $n \in A \cup B$ y cualquier primo p divisor de n se tiene que p^{36} divide a n pero p^{37} no divide a n, demuestra que

$$|S(A) - S(B)| > 5 \cdot 10^7.$$

Solución. De la condición de que para cualquier primo p que divide a $n \in A \cup B$, la mayor potencia de p que divide a n es 36, concluimos que todos los elementos de A y B son potencias 36-ésimas. Sean q un primo y α un entero positivo tales que $36 \mid \varphi(q^\alpha)$. Si $n \in A \cup B$, entonces $n \equiv 1 \pmod{q^\alpha}$ o $n \equiv 0 \bmod q^\alpha$), pues $n = k^{36}$ para algún entero k. Notemos además que A y B tienen la misma cantidad de múltiplos de q, pues como $P(A) = P(B)$, se tiene que $v_q(P(A)) = v_q(P(B))$ y, como $v_q(P(A))$ es 36 veces la cantidad de múltiplos de q en A, y análogamente para B, se sigue que tienen la misma cantidad de múltiplos de q. Como $|A| = |B|$, resulta que A y B tienen la misma cantidad de números que no son múltiplos de q, por lo que $S(A) \equiv S(B) \pmod{q}$, pues los números en A y en B que no son múltiplos de q son congruentes con 1 módulo q.
Por el TCR, tenemos que $S(A) - S(B)$ debe ser múltiplo de $2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$ y, como $S(A) \neq S(B)$, tenemos que $|S(A) - S(B)| > 5 \cdot 10^7$, como queríamos.

Divide y conquistarás

El TCR también nos permite "dividir" el problema, pues si $M = m_1 m_2 \cdots m_n$, donde $\text{mcd}(m_i, m_j) = 1$ para cualesquiera i, j distintos, y tenemos alguna condición dada módulo M, podemos analizar cada congruencia por separado, es decir, analizando módulo m_i para $i = 1, 2, \ldots, n$.

Ejemplo 5. Sea n un entero positivo impar. Encuentra el número de soluciones de la congruencia $x^2 \equiv 1 \pmod{n}$, esto es, cuántos elementos del conjunto $\{0, 1, \ldots, n-1\}$ satisfacen dicha congruencia.

Solución. Consideremos la descomposición canónica de n, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Por el TCR tenemos que $x^2 \equiv 1 \pmod{n}$ si y solo si $x^2 \equiv 1 \pmod{p_i^{\alpha_i}}$ para $i = 1, 2, \ldots, k$. Ahora, $x^2 \equiv 1 \pmod{p_i^{\alpha_i}}$ si y solo si $p_i^{\alpha_i}$ divide a $(x-1)(x+1)$. Como p_i es primo impar, solo puede dividir a uno de $x-1$ o $x+1$, de donde se tiene que $x \equiv 1 \pmod{p_i^{\alpha_i}}$ o $x \equiv -1 \pmod{p_i^{\alpha_i}}$. Se tienen entonces dos posibilidades para cada uno de $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$, lo que nos da un total de 2^k sistemas de congruencias y, por el TCR, sabemos que cada sistema tiene solución. Como los sistemas difieren en al menos una congruencia, estas soluciones serán distintas entre sí. Entonces concluimos que hay 2^k soluciones de la congruencia $x^2 \equiv 1 \pmod{n}$.

Ejemplo 6. Demuestra que para cada entero positivo n, existen enteros a y b tales que $4a^2 + 9b^2 - 1$ es múltiplo de n.

Solución. Por el TCR, basta demostrar la existencia para potencias de primos. Para 2^k, consideremos a y b tales que $a \equiv 0 \pmod{2^k}$ y $3b \equiv 1 \pmod{2^k}$, esto es, b es el inverso multiplicativo de 3 módulo 2^k. Finalmente, para p^k, con p primo impar, sean a y b tales que $2a \equiv 1 \pmod{p^k}$, equivalentemente, a es el inverso multiplicativo de 2 módulo p^k y $b \equiv 0 \pmod{p^k}$. Los enteros a y b satisfacen la condición del problema, por lo que hemos terminado.

Problemas

1) Encuentra el residuo de dividir $2019^{2019^{2019}}$ entre 100.

2) Sea $P(x)$ un polinomio con coeficientes enteros y sean $q_1, q_2, \ldots, q_n$ primos distintos tales que para cada i existe un entero x_i tal que q_i divide a $P(x_i)$. Demuestra que existe un entero x tal que $q_1 q_2 \cdots q_n$ divide a $P(x)$.

3) Sea $\{a_1, a_2, \ldots, a_n\}$ un conjunto de enteros positivos. Muestra que existe b entero positivo tal que todos los elementos de $\{ba_1, ba_2, \ldots, ba_n\}$ son potencias perfectas.

4) (Olimpiada Internacional, 1989) Sea n un entero positivo. Demuestra que existen n enteros positivos consecutivos tales que ninguno de ellos es potencia de un primo.

5) Demuestra que existe una sucesión creciente de enteros tal que para cualquier entero no negativo k se tiene que la sucesión $\{a_n + k\}$ contiene una cantidad finita de números primos.

6) (México, 2017) Un conjunto de n enteros positivos se llama *balanceado* si para cada entero k tal que $1 \leq k \leq n$, el promedio de cualesquiera k números en el conjunto es un entero. Encuentra la mayor suma posible de los elementos de un conjunto balanceado tal que todos sus elementos son menores o iguales que 2017.

7) (Olimpiada Internacional, 2016) Un conjunto de números enteros positivos se llama *fragante* si contiene al menos dos elementos, y cada uno de sus elementos tiene algún factor primo en común con al menos uno de los elementos restantes. Sea $P(n) = n^2 + n + 1$. Determina el menor número entero positivo b para el cual existe

algún entero no negativo a tal que el conjunto $\{P(a+1), P(a+2), \ldots, P(a+b)\}$ es fragante.

8) (Lista corta, Olimpiada Internacional, 2005) Sean a y b enteros positivos tales que $a^n + a$ divide a $b^n + b$ para todo entero positivo n. Muestra que $a = b$.

9) (Taiwan, 2002) Sea O el origen en el plano. A un punto con coordenadas enteras X en el plano le llamamos *visible desde el origen* si el segmento $\overline{OX}$ no contiene ningún otro punto con coordenadas enteras además de O y X. Muestra que para cualquier entero positivo n, existe un cuadrado de n^2 puntos con coordenadas enteras (con lados paralelos a los ejes) tal que ninguno de los puntos con coordenadas enteras dentro del cuadrado es visible desde el origen.

10) (Lista corta, Olimpiada Internacional, 2014) Sean $a_1 < a_2 < \cdots < a_n$ enteros primos relativos por parejas, tales que a_1 es primo y $a_1 \geq n + 2$. En el segmento $I = [0, a_1 a_2 \cdots a_n]$ de la recta real, se marcan todos los enteros que son divisibles por al menos uno de los enteros $a_1, a_2, \ldots, a_n$. Los puntos marcados dividen a I en segmentos más pequeños. Demuestra que la suma de los cuadrados de las longitudes de los segmentos formados es divisible por a_1.

Bibliografía

1) Evan Chen. *The Chinese Remainder Theorem.* 2015.

2) Dorin Andrica, Titu Andreescu. *Number Theory: Structures, Examples and Problems.* Springer, 2009.

3) Naoki Sato. *Number Theory.*