Teorema Chino del Resto, Pequeño Teorema de Fermat

Juan Pablo De Rasis

25 de mayo de 2019

Nos proponemos ilustrar algunos ejemplos donde la utilización del Teorema Chino del Resto o el Pequeño Teorema de Fermat juega un papel fundamental.

Comenzaremos con un ejercicio donde la clave consiste en armar un sistema de ecuaciones lineales de congruencia adecuado y resolverlo.

Ejercicio 1. *Una banda de* 13 *piratas asaltó un barco mercantil y se hizo con una gran cantidad de monedas de oro, todas idénticas entre sí. Cuando trataron de distribuirlas equitativamente entre ellos, les sobraron* 8 *monedas. Por lo tanto, decidieron no repartirlas. Imprevistamente, dos de ellos contrajeron sarampión y murieron. Al volver a intentar repartir las monedas, les sobraron* 3*, y por lo tanto volvieron a cancelar la distribución. Posteriormente murieron otros* 3 *piratas ahogados. Los restantes volvieron a intentar distribuir las monedas, pero les sobraron* 5*. Cansados de tanto intentar distribuir sin poder ser equitativos, optaron por guardar las monedas hasta que se les ocurriese una solución.*

Tiempo después, los piratas se arrepintieron de todas sus fechorías y decidieron hacer un acto caritativo a modo de redención. Se dirijeron a un pueblo muy pobre en el que había exactamente 1136 *personas viviendo, y decidieron integrarse al pueblo para iniciar una nueva vida. Más aún, decidieron que repartirían equitativamente todas las monedas entre todos los habitantes del pueblo, incluyéndose a ellos. Pero, para su sorpresa, volvieron a sobrar monedas. ¿Cuántas monedas sobraron?*

Solución. Sea x la cantidad de monedas robadas. En el primer intento de distribución sobraron 8 monedas al intentar distribuirlas entre 13 piratas, por lo tanto $x \equiv 8 \pmod{13}$. Tras la muerte de dos piratas por sarampión, se intentó distribuir la misma cantidad de monedas entre los 11 piratas restantes pero sobraron 3, es decir, $x \equiv 3 \pmod{11}$. Finalmente, tras la muerte de tres piratas por ahogamiento, el intento de distribución entre los 8 piratas restantes dejó un sobrante de 5 monedas, por lo tanto $x \equiv 5 \pmod{8}$.

Cuando los piratas se integraron al pueblo con 1136 personas, se buscó distribuir las monedas equitativamente entre $1136 + 8 = 1144$ personas. Por consiguiente, se nos está preguntando por el resto de x en la división por 1144. Como $1144 = 13 \times 11 \times 8$ y estos tres factores son coprimos dos a dos, la respuesta será inducida por la solución del siguiente sistema de ecuaciones lineales de congruencia:

$$\begin{cases} x \equiv 8 \pmod{13} \\ x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{8} \end{cases}$$

De la primera ecuación surge que existe $k \in \mathbb{N}_0$ tal que $x = 13k + 8$. Sustituyendo en la segunda ecuación, obtenemos $13k + 8 \equiv 3 \pmod{11}$, que equivale a $2k \equiv 6 \pmod{11}$. Como 2 y 11 son coprimos, esto equivale a $k \equiv 3 \pmod{11}$[1]. Por lo tanto existe $m \in \mathbb{N}_0$

[1]Recordar la siguiente propiedad: Si a, b, c, m son enteros tales que $m \neq 0$ y $(m : c) = 1$, entonces se tiene que $a \equiv b \pmod{m}$ si y solo si $ac \equiv bc \pmod{m}$.

tal que $k = 11m + 3$. Sustituyendo en nuestra expresión para x obtenemos

$$x = 13k + 8 = 13\,(11m + 3) + 8 = 143m + 47$$

Reemplazando en la última ecuación, obtenemos $143m + 47 \equiv 5 \pmod 8$, que equivale a $7m \equiv 6 \pmod 8$, que a su vez equivale a $-m \equiv -2 \pmod 8$, y esto, finalmente, equivale a $m \equiv 2 \pmod 8$. Por lo tanto existe $j \in \mathbb{N}_0$ tal que $m = 8j + 2$. De esta forma, obtenemos

$$x = 143m + 47 = 143\,(8j + 2) + 47 = 1144j + 333$$

Por lo tanto $x \equiv 333 \pmod{1144}$, que por el **Teorema Chino del Resto** es la única solución. Concluimos que, cuando se intentó distribuir las monedas entre los habitantes del pueblo, sobraron 333 monedas.

El ejercicio anterior tuvo la ventaja de que el sistema armado de ecuaciones lineales de congruencia satisfacía las hipótesis del Teorema Chino del Resto para garantizar la existencia de la solución. El siguiente ejercicio ilustra una situación donde esto no ocurre.

Ejercicio 2. *¿Existe $n \in \mathbb{N}$ tal que su dígito de las unidades es igual a 9 y además $n^3 + 3^n$ es divisible por 5?*

Solución. Supongamos que existe $n \in \mathbb{N}$ como en el enunciado. Que su dígito de las unidades sea igual a 9 equivale a la congruencia $n \equiv 9 \pmod{10}$. En particular, se tiene que $n \equiv 9 \equiv 4 \pmod 5$[2]. Por lo tanto, la condición $5 \mid n^3 + 3^n$ equivale a

$$4^3 + 3^n \equiv 0 \pmod 5$$

$$3^n \equiv -4^3 \equiv 1 \pmod 5$$

Analizaremos entonces el comportamiento de las potencias de 3 módulo 5. Comenzamos observando que $3^4 \equiv 1 \pmod 5$, por lo tanto $3^{4k} \equiv 1 \pmod 5$ para todo $k \in \mathbb{N}_0$. Multiplicando sucesivamente por 3 esta congruencia, obtenemos

$$3^{4k} \equiv 1 \pmod 5$$

$$3^{4k+1} \equiv 3 \pmod 5$$

$$3^{4k+2} \equiv 9 \equiv 4 \pmod 5$$

$$3^{4k+3} \equiv 12 \equiv 2 \pmod 5$$

Si volvemos a multiplicar por tres obtendremos $3^{4(k+1)}$, y volvemos al primer caso, donde el exponente es múltiplo de 4.

En consecuencia, $3^n \equiv 1 \pmod 5$ si y solo si $n \equiv 0 \pmod 4$.

Resumiendo, las condiciones del enunciado equivalen a $n \equiv 9 \pmod{10}$ y $n \equiv 0 \pmod 4$. Sin embargo, el sistema

$$\begin{cases} x \equiv 9 \pmod{10} \\ x \equiv 0 \pmod 4 \end{cases} \Rightarrow \begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 4 \end{cases}$$

no admite ninguna solución, ya que las últimas dos relaciones son incompatibles entre sí. Concluimos que no existe ningún $n \in \mathbb{N}$ que satisfaga las condiciones del enunciado.

[2]Recordar la siguiente propiedad: Si $m, n \in \mathbb{Z}$ son no nulos y tales que $m \mid n$, y además existen $a, b \in \mathbb{Z}$ que satisfacen $a \equiv b \pmod n$, entonces $a \equiv b \pmod m$.

Veamos un ejercicio donde requeriremos tanto del Pequeño Teorema de Fermat como del Teorema Chino del Resto.

Ejercicio 3. *Hallar el resto de* 7^{7^7} *en la división por* 3864.[3]

Solución. Factorizamos 3864 como $3 \times 7 \times 8 \times 23$. Llamamos $x = 7^{7^7}$. Hallaremos el resto de x en la división por 3, 7, 8 y 23 y encontraremos el resto módulo $3 \times 7 \times 8 \times 23 = 3864$ mediante el Teorema Chino del Resto.

Es claro que $x \equiv 0 \pmod 7$. Por otra parte, como $7 \equiv 1 \pmod 3$, entonces

$$x \equiv 1^{7^7} = 1 \pmod 3$$

Además, como $7 \equiv -1 \pmod 8$, entonces

$$x \equiv (-1)^{7^7} = -1 \equiv 7 \pmod 8$$

Solamente nos queda hallar el resto de x en la división por 23. Por el **Pequeño Teorema de Fermat** tenemos que $7^{22} \equiv 1 \pmod{23}$. Como $7^7 \equiv 17 \pmod{22}$, entonces $7^7 = 22k + 17$ con $k \in \mathbb{N}$. De esta manera,

$$7^{7^7} = 7^{22k+17} = \left(7^{22}\right)^k \cdot 7^{17} \equiv 1^k \cdot 7^{17} = 7^{17} \pmod{23}$$

Para calcular el resto de 7^{17} en la división por 23, podemos reescribirlo como

$$x \equiv 7^{17} = 7^9 \cdot 7^8 = \left(7^3\right)^3 \left(7^4\right)^2 \equiv (-2)^3 \cdot 9^2 = -648 \equiv 19 \pmod{23}$$

Concluimos que x satisface

$$\begin{cases} x \equiv 0 \pmod 7 \\ x \equiv 1 \pmod 3 \\ x \equiv 7 \pmod 8 \\ x \equiv 19 \pmod{23} \end{cases}$$

Este sistema puede resolverse rutinariamente, obteniendo como resultado $x \equiv 847 \pmod{3864}$. Concluimos que 7^{7^7} tiene resto 847 en la división por 3864.

Finalizaremos con un último ejercicio tomado del Certamen Nacional de la Olimpíada Matemática Argentina llevado a cabo en el año 2000 (Problema 5 del Nivel 3).

Ejercicio 4. *Un programa de computadora genera una sucesión de números con la siguiente regla: el primer número lo escribe Camilo; a partir de entonces, el programa calcula la división entera del último número generado por 18; obtiene así un cociente y un resto. La suma de ese cociente más ese resto es el siguiente número generado. Por ejemplo, si el número de Camilo es* 5291*, la computadora hace* $5291 = 293 \times 18 + 17$*, y genera el* $310 = 293 + 17$*. El siguiente número generado será* 21*, pues* $310 = 17 \times 18 + 4$ *y* $17 + 4 = 21$*; etc. Cualquiera sea el número inicial de Camilo, a partir de algún momento, la computadora genera siempre un mismo número. Determinar cuál es ese número que se repetirá indefinidamente, si el número inicial de Camilo es igual a* 2^{110}.

Solución. Podemos modelizar el problema con la siguiente sucesión recursiva: para cada $n \in \mathbb{N}$ definimos $a_n \in \mathbb{N}$ inductivamente, de la siguiente manera: $a_1 = 2^{110}$ y, para todo $n \in \mathbb{N}$, a_{n+1} es igual a la suma entre el cociente y el resto de dividir a_n por 18.

[3] Téngase presente que, si $a, b, c \in \mathbb{N}$, entonces a^{b^c} puede no ser lo mismo que $\left(a^b\right)^c$. Por ejemplo, no es lo mismo $3^{5^2} = 3^{25}$ que $\left(3^5\right)^2 = 3^{10}$.

Si $n \in \mathbb{N}$ es arbitrario, escribimos $a_n = 18k + r$ donde $k \in \mathbb{N}_0$ es el cociente y $r \in \mathbb{N}_0$ el resto de la división de a_n por 18. Entonces $a_{n+1} = k + r$, luego

$$a_n - a_{n+1} = (18k + r) - (k + r) = 17k$$

Eso implica que **nuestra sucesión decrece de a múltiplos de diecisiete**. En particular, el resto módulo 17 no cambia en ningún paso de la sucesión: *todos los elementos de la sucesión son congruentes módulo* 17.

Más aún, si $a_n \geq 18$ entonces su cociente k en la división por 18 es estrictamente positivo, es decir, $k > 0$, por lo tanto $a_n - a_{n+1} = 17k > 0$, es decir, $a_n > a_{n+1}$. Si, en cambio, $a_n < 18$, entonces $k = 0$ y

$$a_n = 18 \cdot 0 + r = 0 + r = k + r = a_{n+1}$$

Es decir, **en el momento en que un elemento de la sucesión es menor que 18, ese elemento se repetirá indefinidamente en los siguientes pasos de la sucesión**.

Resumimos nuestras conclusiones. Dado $n \in \mathbb{N}$, se cumple:

(1) Si $a_n \geq 18$, entonces $a_{n+1} < a_n$.

(2) Si $a_n < 18$, entonces $a_{n+1} = a_n$ y este número se repetirá indefinidamente en la sucesión.

(3) Todos los elementos de la sucesión tienen el mismo resto en la división por 17.

Por lo tanto, a partir de estas tres conclusiones, podemos razonar de la siguiente manera:

- La sucesión comienza en 2^{110}.
- Por (1), la sucesión comenzará a decrecer hasta llegar a un número menor que 18.
- Una vez que llegamos a un número menor que 18, por (2) ese será el número que se repetirá indefinidamente.
- Ese número que se repite indefinidamente no puede ser igual a 17, porque si lo fuera, entonces, como $17 \equiv 0 \pmod{17}$, por (3) tendríamos que $2^{110} \equiv 0 \pmod{17}$, lo cual es trivialmente falso. Por lo tanto el número que se repite indefinidamente está acotado entre 0 y 16.
- Ese número que se repite indefinidamente, que está entre 0 y 16, por (3) es congruente con 2^{110} módulo 17.
- Por lo tanto, el número que se repite indefinidamente es $r_{17}\left(2^{110}\right)$, ya que es un número entre 0 y 16 congruente con 2^{110} módulo 17.

Eso significa que debemos calcular el resto de 2^{110} en la división por 17. Por el **Pequeño Teorema de Fermat** tenemos que $2^{16} \equiv 1 \pmod{17}$. Escribimos $110 = 16 \cdot 6 + 14$, luego

$$2^{110} = 2^{16 \cdot 6 + 14} = \left(2^{16}\right)^6 2^{14} \equiv 2^{14} \equiv 13 \pmod{17}$$

Concluimos que la respuesta a nuestro problema es 13.