El Teorema Chino del Resto y El Pequeño Teorema de Fermat

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Segundo cuatrimestre de 2020

Parte I

El Teorema Chino del Resto

Congruencias respecto a módulos que son primos entre sí

Proposición

Sean $m_1, m_2 \in \mathbb{N}$ *dos números coprimos,* $a, b \in \mathbb{Z}$ *y* $m = m_1 m_2$*. Entonces* $a \equiv b \pmod{m}$ *si y sólo si se tiene simultáneamente que:*

$$\begin{cases} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{cases}$$

Demostración

Primero supongamos que $a \equiv b \pmod{m}$ Entonces, como $m_1|m$ y $m_2|m$, deducimos que se satisface

$$\begin{cases} a & \equiv & b & \pmod{m_1} \\ a & \equiv & b & \pmod{m_2} \end{cases} \tag{1}$$

Recíprocamente supongamos que se satisface (1) entonces, $m_1|b-a$ y $m_2|b-a$. Dado que m_1 y m_2 son coprimos, deducimos que $m_1 m_2|b-a$, es decir que $a \equiv b \pmod{m}$.

Sistemas congruencias con módulos coprimos

Ahora consideremos un sistema de congruencias respecto a dos módulos que son coprimos, por ejemplo:

$$\begin{cases} x & \equiv & 2 & (\text{mód } 3) \\ x & \equiv & 4 & (\text{mód } 5) \end{cases} \tag{2}$$

¿Será posible reducirlo a una única congruencia módulo $3 \times 5 = 15$?. Veremos que la respuesta a esta pregunta es afirmativa. Para ello, notemos que el sistema (2) significa que existen $q_1, q_2 \in \mathbb{Z}$ tales que:

$$\begin{cases} x & = & 3q_1 + 2 \\ x & = & 5q_2 + 4 \end{cases}$$

Comenzamos multiplicando la primer ecuación por 5 y a la segunda por 3 (para que aparezca 15 como factor):

$$\begin{cases} 5x & = & 15q_1 + 10 \\ 3x & = & 15q_2 + 12 \end{cases}$$

Sistemas congruencias con módulos coprimos (2)

Ahora notemos lo siguiente: como los módulos 3 y 5 son coprimos, por el algoritmo de Euclides extendido, existen enteros $\alpha, \beta \in \mathbb{Z}$ tales que:

$$3\alpha + 5\beta = 1$$

De hecho, utilizando el algoritmo de Euclides, es fácil ver que podemos tomar $\alpha = 2$ y $\beta = -1$. Multiplicando entonces a la primera ecuación por β y a la segunda por α, tenemos que:

$$\begin{cases} \beta \cdot 5x &= 15\beta q_1 + 10\beta \\ \alpha \cdot 3x &= 15\alpha q_2 + 12\alpha \end{cases}$$

y sumándolas obtenemos que:

$$(5\beta + 3\alpha)x = 15(\beta q_1 + \alpha q_2) + (10\beta + 12\alpha)$$

o sea, teniendo en cuenta la manera en que hemos elegido α y β,

$$x = 15(\beta q_1 + \alpha q_2) + (10\beta + 12\alpha)$$

Sistemas congruencias con módulos coprimos (3)

Pero entonces:

$$x \equiv 10\beta + 12\alpha = 14 \pmod{15}$$

Recíprocamente, si $x \equiv 14 \pmod{15}$, entonces

$$\begin{cases} x \equiv 14 \equiv 4 \pmod{5} \\ x \equiv 14 \equiv 2 \pmod{3} \end{cases}$$

Por lo que vemos que el sistema (2) es equivalente a la congruencia

$$x \equiv 14 \pmod{15}.$$

El teorema Chino del Resto

Ahora generalizaremos este ejemplo, en un teorema general:

Teorema (Teorema Chino del resto)

Consideramos el sistema de congruencias:

$$\begin{cases} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \end{cases} \tag{3}$$

donde $a_1, a_2 \in \mathbb{Z}$, $m_1, m_2 \in \mathbb{N}$ *y,* m_1 *y* m_2 *son coprimos. Entonces existe un* $a \in \mathbb{Z}$ *tal que el sistema (10) es equivalente a la congruencia:*

$$x \equiv a \pmod{m} \text{ donde } m = m_1 m_2$$

Demostración (1)

Procedemos como en el ejemplo anterior: Notamos que el sistema (10) significa que existen $q_1, q_2 \in \mathbb{Z}$ tales que:

$$\begin{cases} x &= q_1 m_1 + a_1 \\ x &= q_2 m_2 + a_2 \end{cases}$$

Por otra parte, como m_1 y m_2 son coprimos, por el algoritmo de Euclides extendido, existen $\alpha, \beta \in \mathbb{Z}$ tales que:

$$\alpha m_1 + \beta m_2 = 1$$

Entonces multiplicando a la primer ecuación por $m_2\beta$ y a la segunda por $m_1\alpha$, deducimos que:

$$\begin{cases} m_2\beta x &= \beta q_1 m_1 m_2 + \beta m_2 a_1 \\ m_1\alpha x &= \alpha q_2 m_1 m_2 + \alpha m_1 a_2 \end{cases}$$

y sumando estas ecuaciones, tenemos que:

$$(m_2\beta + m_1\alpha)x = (\beta q_1 + \alpha q_2)m_1 m_2 + (\beta m_2 a_1 + \alpha m_1 a_2)$$

Demostración (2)

Teniendo en cuenta la forma en que elegimos α y β, obtenemos:

$$x = (\beta q_1 + \alpha q_2) m_1 m_2 + (\beta m_2 a_1 + \alpha m_1 a_2)$$

Llamando a a

$$a = \beta m_2 a_1 + \alpha m_1 a_2$$

esta ecuación implica que:

$$x \equiv a \pmod{m} \tag{4}$$

donde $m = m_1 m_2$.
Así pues hemos probado que cualquier solución del sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

es una solución de $x \equiv a \pmod{m}$.

Demostración (2)

Recíprocamente, vamos a probar que cualquier solución de $x \equiv a$ (mód m), es una solución del sistema. Para ello notemos primero que a satisface que:

$$\begin{cases} a & \equiv & a_1 & (\text{mód } m_1) \\ a & \equiv & a_2 & (\text{mód } m_2) \end{cases} \tag{5}$$

Para verlo notemos que por la definición de a:

$$a = \beta m_2 a_1 + \alpha m_1 a_2 \Rightarrow \begin{cases} a & \equiv & \beta m_2 a_1 & (\text{mód } m_1) \\ a & \equiv & \alpha m_1 a_2 & (\text{mód } m_2) \end{cases}$$

pero por definición de α, β tenemos también que:

$$\alpha m_1 + \beta m_2 = 1 \Rightarrow \begin{cases} \beta m_2 & \equiv & 1 & (\text{mód } m_1) \\ \alpha m_1 & \equiv & 1 & (\text{mód } m_2) \end{cases}$$

(o sea que m_2 y β son inversos módulo m_1, y del mismo modo m_1 y α son inversos módulo m_2)

Demostración (3)

Utilizando entonces la propiedad multiplicativa de las congruencias podemos concluir que se verifica

$$\begin{cases} a & \equiv & a_1 & \pmod{m_1} \\ a & \equiv & a_2 & \pmod{m_2} \end{cases}$$

lo que dice que a es una solución de nuestro sistema (10).

$$\begin{cases} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \end{cases}$$

Demostración (4)

Cualquier otra solución x de

$$\begin{cases} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \end{cases} \tag{6}$$

verificará entonces (por transitividad de la relación de congruencia) que:

$$\begin{cases} x & \equiv & a & \pmod{m_1} \\ x & \equiv & a & \pmod{m_2} \end{cases}$$

y entonces por la proposición que vimos al comienzo, tendremos que:

$$x \equiv a \pmod{m} \tag{7}$$

Esto demuestra que que el sistema (6) y la congruencia (7) son equivalentes.

Varias conguencias

Consideremos el sistema

$$\begin{cases} x & \equiv & 2 & \text{(mód 3)} \\ x & \equiv & 4 & \text{(mód 5)} \\ x & \equiv & 1 & \text{(mód 7)} \end{cases} \tag{8}$$

formado por las dos congruencias del ejemplo anterior, más una tercera congruencia. Nuestro objetivo es encontrar una congruencia módulo $105 = 3 \times 5 \times 7$ que sea equivalente al sistema (8).
Notemos que en el ejemplo anterior vimos que las dos primeras congruencias eran equivalentes a la congruencia:

$$x \equiv 14 \quad \text{(mód 15)}$$

Sustituyendo, vemos que (8) es equivalente a

$$\begin{cases} x & \equiv & 14 & \text{(mód 15)} \\ x & \equiv & 1 & \text{(mód 7)} \end{cases}$$

Varias conguencias (2)

Como nuevamente 15 y 7 son coprimos, podemos volver a aplicarle el teorema chino a este sistema. Nuevamente buscamos α y β, tales que:

$$15\alpha + 7\beta = 1$$

Encontramos que $\alpha = 1$, $\beta = -2$ y procediendo como en la demostración del teorema chino, encontramos que $a = -181$, es decir que el sistema (8), es equivalente a la única congruencia:

$$x \equiv -181 \quad (\text{mód } 105)$$

El Teorema Chino del Resto

Teorema (Teorema Chino del resto, versión general)

Consideramos el sistema de congruencias:

$$\begin{cases} x & \equiv & a_1 & \pmod{m_1} \\ x & \equiv & a_2 & \pmod{m_2} \\ \dots & & & \\ x & \equiv & a_k & \pmod{m_k} \end{cases} \tag{9}$$

donde $a_i \in \mathbb{Z}$, $m_i \in \mathbb{N}$ *y,* m_i *y* m_j *son coprimos si* $i \neq j$ $(1 \leq i, j \leq k)$. *Entonces existe un* $a \in \mathbb{Z}$ *tal que el sistema (9) es equivalente a la congruencia:*

$$x \equiv a \pmod{m} \text{ donde } m = m_1 m_2 \dots m_k$$

Parte II

El pequeño teorema de Fermat

El Pequeño Teorema de Fermat

Teorema (Fermat)

Sean p un número primo y $a \in \mathbb{Z}$. Entonces:

i)
$$a^p \equiv a \pmod{p}$$

ii) *Si p no divide a a entonces,*
$$a^{p-1} \equiv 1 \pmod{p}$$

- Las dos afirmaciones son equivalentes.

ii) $\Rightarrow$ *i*): Multiplicamos por a ambos miembros de la congruencia.
i) $\Rightarrow$ *ii*): Escribimos $a^p \equiv a \pmod{p}$ como $a^{p-1} \cdot a \equiv 1 \cdot a \pmod{p}$. Y como a es coprimo con p podemos cancelarlo en la congruencia (multiplicando por el inverso de a módulo p).

Un lema sobre los coeficientes binomiales

Lema

Si p es primo, y $1 < k < p$ entonces

$$\binom{p}{k} \equiv 0 \pmod{p}$$

Demostración.

$$\binom{p}{k} = \frac{p(p-1)(p-2)\dots(p-k+1)}{k!} \in \mathbb{N}$$

En consecuencia:

$$p | k! \binom{p}{k}$$

Pero como $k < p$, los factores primos de $k!$ deben ser exclusivamente primos menores que p, por lo tanto p es coprimo con $k!$, y entonces concluimos que $p | \binom{p}{k}$. □

Demostración (1)

Recordamos que el binomio de Newton afirma que:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Usando el lema anterior, inmediatamente deducimos que

Corolario

Si $a, b \in \mathbb{Z}$ y p es primo, entonces:

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Demostración (2)

Ahora resulta sencillo probar el teorema de Fermat en la forma

$$a^p \equiv a \pmod{p}$$

por inducción en a.

- Caso base: Si $a = 0$ el teorema es evidente:

$$0^p = 0 \equiv 0 \pmod{p}$$

- Paso inductivo: Si el teorema vale para un cierto a, veremos que se verifica también para $a + 1$: en efecto por el corolario 1

$$(a+1)^p \equiv a^p + 1^p \pmod{p}$$

y usando la hipótesis inductiva, deducimos que:

$$(a+1)^p \equiv a + 1 \pmod{p}$$

En virtud del principio de inducción, el teorema queda demostrado para cualquier $a \in \mathbb{N}_0$.

Demostración (3)

- Caso a negativo: Si $a < 0$, notemos que $-a > 0$ luego usando lo que ya demostramos:

$$(-a)^p = (-1)^p a^p \equiv -a \pmod{p}$$

pero

$$(-1)^p \equiv -1 \pmod{p}$$

tanto si p es un primo impar como si $p = 2$ (en este caso $1 \equiv -1$). Por lo tanto

$$a^p \equiv a \pmod{p}$$

Usando los dos teoremas juntos

Supongamos que $n = pq$, donde p y q son primos distintos.
Si a es coprimo con n, ni p ni q dividen a a, tendremos por el teorema de Fermat:

$$a^{p-1} \equiv 1 \pmod{p}$$
$$a^{q-1} \equiv 1 \pmod{q}$$

En consecuencia, elevando la primer congruencia a la potencia $q-1$, y la segunda a la potencia $p-1$, tendremos que:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p}$$
$$a^{(p-1)(q-1)} \equiv 1 \pmod{q}$$

y en virtud de la proposición que vimos al comienzo, tendremos que:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

[Este es el análogo del teorema de Fermat, para el módulo compuesto $n = pq$]