

TEOREMA CHINO DEL RESIDUO

ALAN REYES-FIGUEROA
TEORÍA DE NÚMEROS

(AULA 16) 29.AGOSTO.2025

Sistemas de Congruencias Lineales

Teorema (Teorema Chino del Residuo)

Sean $b_1, b_2, \dots, b_k \in \mathbb{Z}$ enteros cualesquiera y $n_1, n_2, \dots, n_k \in \mathbb{Z}$, $n_i > 1$, primos relativos dos a dos. Entonces, el sistema de ecuaciones

$$\begin{aligned}x &\equiv b_1 \pmod{n_1}, \\x &\equiv b_2 \pmod{n_2}, \\&\dots \\x &\equiv b_k \pmod{n_k}.\end{aligned}$$

admite solución, y ésta es única módulo $N = n_1 n_2 \cdots n_k$.

Prueba: Consideramos los números de la forma $N_i = \frac{N}{n_i} = \prod_{j \neq i} n_j$, para $i = 1, 2, \dots, k$.

Observe que $(n_i, N_i) = 1$ (ya que los n_i son todos primos relativos). Luego, N_i es invertible módulo n_i , de modo que existe $c_i \in \mathbb{Z}$ tal que $c_i N_i \equiv 1 \pmod{n_i}$.

Además, si $i \neq j$, como $n_j \mid \prod_{j \neq i} n_j = N_i$, se tiene que $c_i N_i \equiv 0 \pmod{n_j}$, para todo $i \neq j$.

Sistemas de Congruencias Lineales

Consideramos el entero

$$x_0 = c_1 N_1 b_1 + c_2 N_2 b_2 + \dots + c_k N_k b_k \in \mathbb{Z}.$$

Afirmamos que x_0 es solución del sistema de congruencias (1). De hecho, para cada $i = 1, 2, \dots, k$ se tiene

$$\begin{aligned} x_0 &\equiv c_1 N_1 b_1 + c_2 N_2 b_2 + \dots + c_k N_k b_k \pmod{n_i} \\ &\equiv (0)b_1 + (0)b_2 + \dots + (1)b_i + \dots + (0)b_k \pmod{n_i} \\ &\equiv b_i \pmod{n_i}. \end{aligned}$$

Así, x_0 es solución del sistema.

Por otro lado, si $x_1 \in \mathbb{Z}$ es otra solución, entonces

$$x_0 \equiv x_1 \pmod{n_i} \iff n_i \mid x_0 - x_1, \quad \text{para todo } i = 1, 2, \dots, k.$$

Como los n_i son todos primos relativos, entonces los coroloarios al Lema de Euclides, más el uso de inducción matemática, implican que $N = n_1 n_2 \cdots n_k \mid x_0 - x_1$. Portanto $x_0 \equiv x_1 \pmod{N}$. $\square$

Sistemas de Congruencias Lineales

Damos una segunda prueba del Teorema Chino, esta vez un tanto más algebraica. Consideramos el mapa natural $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$, dado por

$$f : b \pmod{N} \mapsto (b \pmod{n_1}, b \pmod{n_2}, \dots, b \pmod{n_k}).$$

Este mapa está bien definido, pues si b' es otro representante en la misma clase de congruencia $b \pmod{N}$, entonces $N \mid b - b'$, y portanto $n_i \mid b - b'$, para todo $i = 1, 2, \dots, k$, de modo que $b \equiv b' \pmod{n_i}$, $\forall i$, y se tiene que $f(b) = f(b')$.

Observe que el Teorema Chino es equivalente a mostrar que el mapa f es una biyección: el hecho de f ser sobreyectiva corresponde a la existencia de la solución del sistema (1), mientras que la inyectividad corresponde a la unicidad módulo N .

Como $|\mathbb{Z}/N\mathbb{Z}| = N = n_1 n_2 \cdots n_k = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}|$, basta mostrar que f es inyectiva. Primero note que f es un morfismo de anillos. Suponga que $f(x) = 0 = (0, 0, \dots, 0)$. Entonces $x \equiv 0 \pmod{n_i}$, para todo $i = 1, 2, \dots, k$. Esto implica que $n_i \mid x$, $\forall i$, y de nuevo el lema de Euclides implica que $N \mid x$. Así, $x \equiv 0 \pmod{N}$. Esto muestra que $\text{Ker } f = 0$, luego f es inyectiva, y portanto biyectiva. $\square$

Caso general: Módulos no coprimos

Falta agregar aquí el tema de cuando el sistema de congruencias los módulos no son coprimos.

Ejemplos:

Definición

Un entero $n \in \mathbb{Z}$ es **libre de cuadrados** si n no es divisible por el cuadrado de ningún número mayor que 1.

Ejemplo: Vamos a mostrar que existen intervalos arbitrariamente grandes, de enteros consecutivos, ninguno de los cuales es libre de cuadrados.

Solución: Sea $n \in \mathbb{N}$ un número natural cualquiera, y sean $p_1, p_2, \dots, p_n$ primos distintos. Por el Teorema Chino, existen soluciones al sistema

$$\begin{aligned}x &\equiv -1 \pmod{p_1^2}, \\x &\equiv -2 \pmod{p_2^2}, \\&\dots, \\x &\equiv -n \pmod{p_k^2}.\end{aligned}$$

Si x_0 es una solución positiva, entonces cada uno de los números $x_0 + 1, x_0 + 2, \dots, x_0 + n$ es divisible por el cuadrado de algún primo, y ninguno es libre de cuadrados.

Lema

Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Para todo $k, i \in \mathbb{Z}$, se tiene que

$$P(i) \mid P(kP(i) + i).$$

Prueba: Observe que para todo $n \in \mathbb{N}$

$$(kP(i) + i)^n \equiv \sum_{j=0}^n \binom{n}{j} k^j P(i)^j i^{n-j} \equiv i^n \pmod{P(i)}.$$

Como las congruencias se preservan mediante productos y sumas, entonces para cualquier polinomio $f(x) \in \mathbb{Z}[x]$, se tiene que $f(kP(i) + i) \equiv f(i) \pmod{P(i)}$.

En particular, $P(kP(i) + i) \equiv P(i) \equiv 0 \pmod{P(i)}$. $\square$

Aplicaciones

Ejemplo: Sea $P(x) \in \mathbb{Z}[x]$ un polinomio no constante con coeficientes enteros. Mostramos que para todo entero $n \in \mathbb{N}$, existe un entero i tal que los números son compuestos

$$P(i), P(i+1), P(i+2), \dots, P(i+n),$$

Solución: Supongamos que la secuencia $P(i), P(i+1), \dots, P(i+n)$ contiene un primo para cada i . Entonces la secuencia $P(i)_{i \geq 1}$ contiene sólo números primos.

Consideramos los $n+1$ primeros números primos distintos $P(i_0), P(i_1), \dots, P(i_n)$. Por el Teorema Chino, existen infinitas soluciones al sistema

$$\begin{aligned}x &\equiv i_0 \pmod{P(i_0)}, \\x &\equiv i_1 - 1 \pmod{P(i_1)}, \\&\dots, \\x &\equiv i_n - n \pmod{P(i_n)}.\end{aligned}$$

Si x_0 es una solución de este sistema, entonces $x = x_0 + k(P(i_0)P(i_1) \cdots P(i_n))$ es también solución, $\forall k \geq 0$. Por el lema anterior, $P(x), P(x+1), \dots, P(x+n)$ son compuestos, para k es suficientemente grande, múltiplos respectivamente de $P(i_0), P(i_1), \dots, P(i_n)$. $\square$