Hoja 2: Teorema chino del residuo

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Problema 2.1 (Teorema chino del residuo)**.** Sean m y n dos enteros coprimos ($\mathrm{mcd}(m,n)=1$).

a) Demuestre que existen enteros e_1, e_2 tales que

$$\begin{aligned} e_1 &\equiv 1 \pmod{m}, \quad & e_1 &\equiv 0 \pmod{n}, \\ e_2 &\equiv 0 \pmod{m}, \quad & e_2 &\equiv 1 \pmod{n}. \end{aligned}$$

Sugerencia: identidad de Bézout.

b) Dados $a, b \in \mathbb{Z}$, encuentre c tal que

$$c \equiv a \pmod{m}, \quad c \equiv b \pmod{n}.$$

Problema 2.2. De nuevo, supongamos que $\mathrm{mcd}(m,n)=1$.

a) Demuestre que si $a \equiv 0 \pmod{m}$ y $a \equiv 0 \pmod{n}$, entonces $a \equiv 0 \pmod{mn}$.

b) En el problema anterior, demuestre que el resto que corresponde a los restos $a = b = 0$ es $c = 0$.

c) Deduzca que si $a \equiv b \pmod{m}$ y $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{mn}$.

Podemos reformular el resultado de arriba de la siguiente manera.

Para $\mathrm{mcd}(m,n)=1$ la aplicación

$$\begin{aligned} \Phi\colon \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \\ [c]_{mn} &\mapsto ([c]_m, [c]_n) \end{aligned}$$

es biyectiva.

Demostración. El problema 2.1 establece la sobreyectividad, y el problema 2.2 establece la inyectividad[*]. □

Ejemplo. He aquí la aplicación Φ para $(m,n)=(2,3)$:

$$\Phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$
$$0 \mapsto (0,0),\ 1 \mapsto (1,1),\ 2 \mapsto (0,2),\ 3 \mapsto (1,0),\ 4 \mapsto (0,1),\ 5 \mapsto (1,2).$$

[*] Una aplicación $f\colon X \to Y$ es **inyectiva** si $f(x) \neq f(x')$ para $x \neq x'$.
Una aplicación $f\colon X \to Y$ es **sobreyectiva** si para todo $y \in Y$ existe $x \in X$ tal que $f(x) = y$.
En fin, $f\colon X \to Y$ es **biyectiva** si es inyectiva y sobreyectiva; en otras palabras, si para $y \in Y$ hay *único* $x \in X$ tal que $f(x) = y$.

Problema 2.3. Para $(m,n) = (3,5)$ reduzca los residuos mód 15 módulo 3 y 5:

$$\begin{aligned} \mathbb{Z}/15\mathbb{Z} &\to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\ 0 &\mapsto (0,0), \\ 1 &\mapsto (1,1), \\ &\dots \\ 10 &\mapsto (1,0), \\ &\dots \end{aligned}$$

Verifique que en la parte derecha aparecen todos los pares de residuos $([a]_3, [b]_5)$ para $a = 0,1,2$ y $b = 0,1,2,3,4$.

Ejemplo. Vamos a resolver la congruencia $x^2 \equiv 1 \pmod{40}$. Hay cuatro (!) soluciones mód 8:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8.$$

Por otra parte, mód 5 hay solo dos soluciones esperadas $x \equiv \pm 1$. El teorema chino del resto nos permite concluir que mód 40 hay ocho soluciones:

$$\begin{aligned} \mathbb{Z}/40\mathbb{Z} &\to \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \\ 1 &\mapsto (1,1), \\ 9 &\mapsto (1,4), \\ 11 &\mapsto (3,1), \\ 19 &\mapsto (3,4), \\ 21 &\mapsto (5,1), \\ 29 &\mapsto (5,4), \\ 31 &\mapsto (7,1), \\ 39 &\mapsto (7,4). \end{aligned}$$

¿Cómo reconstruir las soluciones mód 40? ¡Esto nos diría la solución del problema 2.1!
Usando $\mathrm{mcd}(8,5) = 1$, escribamos la identidad de Bézout:

$$2 \cdot 8 + (-3) \cdot 5 = 1.$$

De aquí se ve que

$$\begin{aligned} 16 &\equiv 0 \pmod 8, & \qquad 16 &\equiv 1 \pmod 5, \\ -15 &\equiv 1 \pmod 8, & \qquad -15 &\equiv 0 \pmod 5. \end{aligned}$$

Por ejemplo, buscamos x tal que

$$x \equiv 5 \pmod 8, \quad x \equiv 4 \pmod 5.$$

Entonces,

$$x = 5 \cdot (-15) + 4 \cdot 16 = -11 \equiv 29 \pmod{40}.$$

Problema 2.4. Como antes, $\mathrm{mcd}(m,n) = 1$.

a) Demuestre que para $a \in \mathbb{Z}$ se tiene

$$a \text{ es invertible mód } mn \iff \left\{ \begin{array}{c} a \text{ es invertible mód } m \\ y \\ a \text{ es invertible mód } n \end{array} \right\}$$

b) Deduzca que

$$|(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \times |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Ejemplo. Los residuos invertibles mód 3 y 5 son

$$(\mathbb{Z}/3\mathbb{Z})^\times = \{[1],[2]\},$$
$$(\mathbb{Z}/5\mathbb{Z})^\times = \{[1],[2],[3],[4]\}.$$

El ejercicio anterior nos dice que hay 8 residuos invertibles mód 15. Estos se recuperan del teorema chino del resto de $(\mathbb{Z}/3\mathbb{Z})^\times$ y $(\mathbb{Z}/5\mathbb{Z})^\times$. La respuesta es

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{[1],[2],[4],[7],[8],[11],[13],[14]\}.$$

Problema 2.5. Formule y demuestre una versión del teorema chino del residuo para módulos $n_1,\dots,n_s$ tales que $\text{mcd}(n_i,n_j)=1$ para $i\neq j$.

Problema 2.6. Sea $f(x)=a_m x^m+\cdots+a_1x+a_0$ un polinomio con coeficientes enteros.

a) Demuestre que la congruencia $f(x)\equiv 0 \pmod{n}$ tiene solución para $n=p_1^{e_1}\cdots p_s^{e_s}$ si y solamente si $f(x)\equiv 0 \pmod{p_i^{e_i}}$ tiene solución para cada $i=1,\dots,s$.

b) Sea N el número de soluciones de $f(x)\equiv 0 \pmod{n}$ y N_i el número de soluciones de $f(x)\equiv 0 \pmod{p_i^{e_i}}$. Demuestre que $N=N_1\cdots N_s$.

Problema 2.7.

a) Demuestre que $x^2\equiv x \pmod{p^e}$ tiene únicas soluciones $x=0$ y 1 para todo primo p y $e=1,2,3,\dots$

b) En general, ¿cuántas soluciones tiene $x^2\equiv x \pmod{n}$?

Problema 2.8.

a) Demuestre que $x^2\equiv 1 \pmod{p^e}$ tiene únicas soluciones $x=\pm 1$ para p impar y $e=1,2,3,\dots$

b) Demuestre que $x^2\equiv 1 \pmod{2^e}$ tiene 4 soluciones para $e\geq 3$. ¿Cuáles son?

c) En general, ¿cuántas soluciones tiene $x^2\equiv 1 \pmod{n}$?

Problema 2.9. Use el teorema chino del residuo para encontrar las soluciones de $x^2\equiv x$ y $x^2\equiv 1$ mód $n=221$.