Hoja 1: Residuos invertibles mód n

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Definición. Se dice que un residuo $x \in \mathbb{Z}/n\mathbb{Z}$ es **invertible** si existe otro residuo $y \in \mathbb{Z}/n\mathbb{Z}$ tal que $xy = 1$. En este caso también se escribe $y = x^{-1}$.

De manera equivalente, $a \in \mathbb{Z}$ es **invertible mód** n si existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \pmod{n}$.

El conjunto de los residuos invertibles módulo n se denotará por $(\mathbb{Z}/n\mathbb{Z})^\times$.

Ejemplo. He aquí los residuos módulo $n = 15$ y sus inversos; «—» significa que el residuo no es invertible.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
—	1	8	—	4	—	—	13	2	—	—	11	—	7	14

Problema 1.1. Demuestre que si $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$ son residuos invertibles mód n, entonces x^{-1} y xy son también invertibles.

Problema 1.2. Demuestre que si $x \in \mathbb{Z}/n\mathbb{Z}$ es invertible, entonces su inverso x^{-1} es único (como residuo mód n).

Problema 1.3 (Cancelación)**.** Demuestre que si x, y, z son residuos módulo n, y z es invertible, entonces $xz = yz$ implica que $x = y$. ¿Qué pasa si z no es invertible?

Problema 1.4. En este problema vamos a probar que $[a]_n$ es invertible si y solo si $\operatorname{mcd}(a, n) = 1$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid 0 \le a < n,\ \operatorname{mcd}(a,n) = 1\}.$$

a) Si $\operatorname{mcd}(a, n) = 1$, use la identidad de Bézout para encontrar $[a]_n^{-1}$.

b) Demuestre que si $x, y \in \mathbb{Z}/n\mathbb{Z}$ son dos residuos no nulos tales que $xy = 0$, entonces x e y no pueden ser invertibles.

   (En otras palabras, si $n \mid ab$ para $n \nmid a$, $n \nmid b$, entonces a y b no son invertibles módulo n.)

c) Si $\operatorname{mcd}(a, n) > 1$, use el punto anterior para probar que a no es invertible mód n.

Problema 1.5. Para $n = 5, 6, 7, 8$ encuentre cuáles residuos mód n son invertibles y escriba sus inversos correspondientes.

Problema 1.6. Calcule $[6]_{385}^{-1}$.

Problema 1.7 (Teorema de Wilson)**.** Sea p un primo.

a) Demuestre que para todo $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ se tiene $x^{-1} = x$ si y solamente si $x = \pm 1$.

b) Deduzca de a) que $(p-1)! \equiv -1 \pmod{p}$.

c) Demuestre que $(n-1)! \equiv 0 \pmod{n}$ si $n \ge 6$ es compuesto.

Problema 1.8. Demuestre que para todo primo impar p, el numerador de

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

es divisible por p.

Sugerencia: $1, 2, \ldots, p-1$ son invertibles mód p.