Hoja 5: Orden multiplicativo mód n

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Problema 5.1. Consideremos $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.

a) Demuestre que existen $k > \ell$ tales que $x^k = x^\ell$ en $(\mathbb{Z}/n\mathbb{Z})^\times$.

b) Concluya que $x^k = 1$ para algún $k = 1, 2, 3, \ldots$

Definición. Sea $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ un residuo invertible mód n. Su **orden** (**multiplicativo**) es el mínimo $k = 1, 2, 3, \ldots$ tal que $x^k = 1$.

Ejemplo. Consideremos las potencias de 2 módulo 5:

$$2^2 = 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1 \pmod 5.$$

Entonces, $[2]_5$ tiene orden 4. Por otra parte, módulo 7 tenemos

$$2^2 = 4,\ 2^3 = 8 \equiv 1 \pmod 7.$$

Esto significa que el orden de $[2]_7$ es 2.

Problema 5.2. Para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, sea $k = \operatorname{ord}(x)$.

a) Si $\ell = qk + r$, demuestre que $x^\ell = 1$ si y solamente si $x^r = 1$.

b) Deduzca que $x^\ell = 1$ si y solamente si $k \mid \ell$.
(Use la división $\ell = qk + r$.)

c) Demuestre que $\operatorname{ord}(x) \mid \phi(n)$ para todo $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.
(Recuerde la congruencia de Euler.)

d) Demuestre que $x^\ell = x^m$ si y solamente si $\ell \equiv m \pmod k$.

Problema 5.3. Para $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ y $\ell = 1, 2, 3, \ldots$ deduzca la fórmula

$$\operatorname{ord}(x^\ell) = \frac{\operatorname{ord}(x)}{\operatorname{mcd}(\operatorname{ord}(x), \ell)}.$$

Problema 5.4. Consideremos $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$.

a) Demuestre que $\operatorname{ord}(xy) = \operatorname{ord}(x) \operatorname{ord}(y)$ si $\operatorname{mcd}(\operatorname{ord}(x), \operatorname{ord}(y)) = 1$.

b) ¿Qué pasa si $\operatorname{mcd}(\operatorname{ord}(x), \operatorname{ord}(y)) \neq 1$?