Hoja 0: Residuos mód n (breve repaso)

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Definición. Fijemos algún $n = 1, 2, 3, \ldots$ y consideremos la siguiente relación sobre los números enteros: se dice que a y b son **congruentes módulo** n si n divide a $a - b$:

$$a \equiv b \pmod{n} \iff n \mid (a - b).$$

En otras palabras, a y b tienen el mismo residuo de la división por n.

Problema 2.1. Demuestre que la congruencia mód n es una relación de equivalencia: para cualesquiera $a, b, c \in \mathbb{Z}$ se tiene

$$a \equiv a, \quad a \equiv b \Rightarrow b \equiv a, \quad a \equiv b \text{ y } b \equiv c \Rightarrow a \equiv c.$$

Definición. Las clases de equivalencia se llaman los **residuos módulo** n[*]. La clase de equivalencia de a será denotada por $[a]_n$, o simplemente por $[a]$:

$$[a]_n = [b]_n \iff a \equiv b \pmod{n}.$$

El conjunto de los residuos mód n se denota por $\mathbb{Z}/n\mathbb{Z}$. Note que este tiene precisamente n elementos, representados por los posibles residuos de división por n:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

Problema 2.2. Demuestre que si $a \equiv a'$, $b \equiv b'$, entonces

$$a + b \equiv a' + b', \quad a \cdot b \equiv a' \cdot b'.$$

Esto quiere decir que la adición y multiplicación tiene sentido para los residuos mód n: podemos definir

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [a \cdot b].$$

En lugar de $[0]_n$ y $[1]_n$ será conveniente escribir simplemente 0 y 1.

Ejemplo. He aquí las tablas de adición y multiplicación módulo 5:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

[*] O también **residuos módulo** n.

Ejemplo. He aquí las tablas de adición y multiplicación módulo 6:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Problema 2.3. Compile las tablas de adición y multiplicación mód $n = 7, 8$.

Problema 2.4. Demuestre que las ecuaciones

$$3x^2 + 2 = y^2, \quad 7x^3 + 2 = y^3$$

no tienen soluciones $x, y \in \mathbb{Z}$, usando reducción módulo algunos p.

Problema 2.5. Sea p un número primo.

a) Demuestre que $p \mid \binom{p}{k}$ para $k = 1, 2, \ldots, p-1$.

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

c) Deduzca de a) la «fórmula del binomio mód p»:

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

para cualesquiera $a, b \in \mathbb{Z}$.

d) Deduzca de c) el **pequeño teorema de Fermat**: $a^p \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}$.
Sugerencia: use inducción con caso base $a = 0$ y el paso inductivo mediante $(a+1)^p \equiv a^p + 1 \pmod{p}$.

Problema 2.6. Demuestre las siguientes congruencias mód p:

$$1 + 2 + 3 + \cdots + (p-1) \equiv 0 \text{ para } p \neq 2,$$
$$1^2 + 2^2 + 3^2 + \cdots + (p-1)^2 \equiv 0 \text{ para } p \neq 2, 3,$$
$$1^3 + 2^3 + 3^3 + \cdots + (p-1)^3 \equiv 0 \text{ para } p \neq 2.$$