



## Guía 6 – teoría de números

**Problema 1** Sean  $a, b \in \mathbb{Z}$  tal que  $a \neq 0$ ,  $a|b$ . Demuestre que  $(b/a) \in \mathbb{Z}$  y  $(b/a)|b$ .

**Problema 2** Sea  $a \in \mathbb{Z}$  tal que  $2|a$  y  $4 \nmid a$ . Demuestre que el número de divisores de  $a$  que son pares es igual al número de divisores de  $a$  que son impares (*hint: se puede construir una función biyectiva entre dos conjuntos*)

**Problema 3** Demuestre que  $37|1\underbrace{11\dots1}_{2025}$ .

**Problema 4** Demuestre la siguiente regla de división sobre 37: el número  $\overline{d_{m-1}\dots d_0}$  es divisible por 37 si y sólo si  $(d_0 + 10d_1 - 11d_2 + d_3 + 10d_4 - 11d_5 + \dots)$  es divisible por 37.

**Problema 5** ¿ $111111|\underbrace{11\dots1}_{2025}$ ?

**Problema 6** Encontrar todos los posibles cocientes para el dividendo  $a = 57$ .

**Problema 7** ¿Qué afirmaciones de abajo son verdad para todo  $a, b, c, n \in \mathbb{Z}$ ?

- a)  $6|n^3 - n$ ;
- b)  $3 \nmid n^2 + 1$ ;
- c)  $c|ab \rightarrow (c|a \vee c|b)$ ;
- d)  $(a|b \wedge b|a) \rightarrow |a| = |b|$ .

**Problema 8** Demuestre que la relación de congruencia módulo  $k \equiv_k$  “no respete” potenciación. Es decir, de un ejemplo de  $a_1, a_2, b_1, b_2 \in \mathbb{N}$  tal que  $a_1 \equiv_{10} a_2, b_1 \equiv_{10} b_2$  pero  $a_1^{b_1} \not\equiv_{10} a_2^{b_2}$ .

**Problema 9** Encontrar el último dígito de  $1997^{1997^{1997}}$ .

**Problema 10** Encuentre todos los posibles valores de

- a)  $\text{MCD}(2n + 3, 7n + 6)$
  - b)  $\text{MCD}(n^2, n + 1)$
- cuando  $n$  recorre  $\mathbb{Z}$ .

**Problema 11** Sean  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . Demuestre que  $\text{MCD}(a, b) = |b|$  si y sólo si  $b|a$ .

**Problema 12** Sean  $a, b \in \mathbb{Z}$ ,  $(a, b) \neq (0, 0)$ . Demuestre que  $a/\text{MCD}(a, b), b/\text{MCD}(a, b)$  son coprimos.

**Problema 13** Sean  $a, b \in \mathbb{Z}$ . Demuestre que  $a, b$  son coprimos si y sólo si  $a + b, a - b$  son coprimos.

**Problema 14** Encuentre  $\text{MCD}(2^{2^m} + 1, 2^{2^k} + 1)$  para  $m, k \in \mathbb{N}$ .