

HOJA 2 DE EJERCICIOS: Aritmética 2.

(Para entregar el 31 de enero de 2018.)

Es obvio, pero os recuerdo que, aunque no os salga un problema o un apartado, podéis usarlo para otros. Lo único que hay que evitar son los argumentos circulares.

1. Sean $a < b, c < d$ cuatro números reales. Demuestra que el cardinal del intervalo $I = (a, b)$ es igual al cardinal del intervalo $J = (c, d)$ definiendo una correspondencia biyectiva entre I y J .

2. a) Tenemos dos conjuntos A, B descompuestos en subconjuntos disjuntos:

$$A = A_1 \cup A_2, A_1 \cap A_2 = \emptyset, \quad B = B_1 \cup B_2, B_1 \cap B_2 = \emptyset$$

Supongamos que $|A_1| = |B_1|$ y $|A_2| = |B_2|$. Demuestra que entonces $|A| = |B|$. [Se trata de construir una biyección $A \leftrightarrow B$ a partir de biyecciones conocidas $A_1 \leftrightarrow B_1$ y $A_2 \leftrightarrow B_2$.]

b) Recordemos que $X \setminus Y := \{x \in X : x \notin Y\}$. Llamemos $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}, \mathbb{R}^* := \mathbb{R} \setminus \{0\}$. Observa que $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ y $\mathbb{R}^* = \mathbb{Q}^* \cup (\mathbb{R}^* \setminus \mathbb{Q}^*)$ y demuestra que \mathbb{R} y \mathbb{R}^* tienen el mismo cardinal.

c) Demuestra que los intervalos $(0, 1)$ y $[0, 1)$ tienen el mismo cardinal. [Sugerencia: usar el apartado a).]

3. Demuestra que $\sqrt[3]{2}, \sqrt{3}$ y $\sqrt{2} + \sqrt{3}$ son irracionales.

4. Usa el algoritmo de Euclides para hallar una solución de la ecuación $ax + by = (a, b)$ con $x, y \in \mathbb{Z}$ en los casos siguiente:

$$i) a = 63, b = 49 \quad ii) a = 619, b = 93.$$

5. a) Encuentra el dígito de control c de este código EAN: $5 - 449000 - 00099c$.

b) En este código EAN se ha borrado un número, ¿cuál era?: $5 - 449000 - 03?895$

6. La letra del NIF es un “dígito” de control que sirve para evitar errores. Cada letra se asigna dependiendo del resto que resulta de dividir el número del DNI entre 23 de acuerdo con la siguiente tabla:

Resto:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Letra:	T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E

a) Comprueba lo anterior en tu NIF y calcula la letra que corresponde al DNI 02516341.

b) Observa que si escribimos las 8 cifras del DNI como $a_7a_6a_5a_4a_3a_2a_1a_0$, y llamamos L a la letra, el NIF satisface la ecuación $\sum_{i=0}^7 a_i \cdot 10^i - L \equiv 0 \pmod{23}$. Demuestra que si se introduce un error en un dígito del NIF (número o letra) nos daremos siempre cuenta.

c) ¿Cuál es el dígito borrado en el NIF 00230?34 - Z? ¿Podemos siempre recuperar un dígito (número o letra) que se haya borrado de un NIF si sabemos qué posición ocupaba?

7. Encuentra, y demuestra por qué funciona, una forma de decidir si un número natural N es múltiplo de 11 y, más en general, de encontrar el resto al dividir N entre 11, que no requiera hacer ninguna división. (Es decir, encuentra y demuestra una “regla de divisibilidad entre 11” sencilla).

8. En alemán la prueba del nueve se llama *Neuner- und Elferprobe* (Prueba del nueve y del once) porque, además de comprobar módulo 9, comprueban también módulo 11.

a) Utiliza la prueba del 9 y del 11 para comprobar que las siguientes divisiones están mal hechas:

$$\begin{array}{r} 673\,544\,456\,789 \quad \left| \begin{array}{l} 3\,110 \\ \hline 981 \quad 216\,573\,880 \end{array} \right. \qquad 673\,544\,456\,789 \quad \left| \begin{array}{l} 3\,104 \\ \hline 639 \quad 217\,992\,415 \end{array} \right. \end{array}$$

b) Da un ejemplo de una división incorrecta, con como mucho un dígito mal en el cociente y un dígito mal en el resto, que, sin embargo, pase la prueba del 9 y del 11.

9. Halla la única solución de $133x \equiv 1000 \pmod{2010}$. (Sugerencia: usar el algoritmo de Euclides)

10. Un usuario del criptosistema RSA ha publicado la clave $(n, e) = (629, 419)$ y recibe el mensaje cifrado **251**. ¿Cuál era el mensaje original? [NOTA: para simplificar, los mensajes son números. De hecho la respuesta es **208** y se trata de que justifiques cómo se llega a él.]

11. Llamamos *triángulo rectángulo entero* al que tiene lados $x, y, z \in \mathbb{Z}$, y decimos que es *primitivo* si además satisface $(x, y, z) = 1$.

- a) Encuentra un triángulo rectángulo entero primitivo con un cateto de longitud 20.
- b) Encuentra un triángulo rectángulo entero primitivo con un cateto de longitud 11.
- c) Demuestra que no existe ningún triángulo rectángulo entero (necesariamente primitivo) con un cateto de longitud 1 ni con un cateto de longitud 2.
- d) Dado un entero impar $N \geq 3$, demuestra que existe un triángulo rectángulo entero primitivo con un cateto de longitud N .
- e) Dado un entero $N \geq 4$ que sea múltiplo de 4, demuestra que existe un triángulo rectángulo entero primitivo con un cateto de longitud N .

12. Sea p un número primo.

- a) Demuestra que p divide a $\binom{p}{i}$ para $0 < i < p$.
- b) Demuestra por inducción que $b^p \equiv b \pmod{p}$ para cualquier entero $b \geq 0$.
- c) Demuestra que $b^p \equiv b \pmod{p}$ para cualquier entero b .