Preparación para la XLIX Olimpiada Matemática Española (III) - Teoría

Abel Naya Forcano y Adrián Franco Rubio

1. El Principio del Palomar

El Principio del Palomar es uno de los principios más sencillos de las matemáticas, pero no por ello tiene poca importancia. Es conocido por multitud de nombres, entre ellos Principio del Palomar de Dirichlet, o Principio de los Cajones, aunque el más utilizado es normalmente el de Principio del Palomar. Básicamente consiste en que si tenemos m palomares (huecos) en los que repartir n palomas (elementos), siempre que haya más palomas que palomares ($n > m$) habrá al menos un palomar con dos palomas. A pesar de su sencillez es muy utilizado e incluso puede llegar a ser difícil de emplear si no se tiene claro qué son 'palomas'y qué son 'palomares'.

Ejemplos:

- Si escogemos 8 personas, podremos asegurar que al menos dos de ellas nacieron el mismo día de la semana ($n = 8$, $m = 7$, $n > m$).
- Si tenemos un triángulo equilátero de lado 2 m y elegimos 5 puntos de su interior, al menos dos de ellos estarán a una distancia igual o inferior a 1 m.

La demostración de este último ejemplo sería como sigue: Dividimos el triángulo en cuatro subtriángulos semejantes de lado 1 m, uniendo los puntos medios de los tres lados. Sabemos, por el Principio del Palomar, que al menos dos de esos puntos estarán en el mismo subtriángulo, luego su distancia será como máximo 1 m. En este caso: $n = 5$ (puntos), $m = 4$ (subtriángulos); $n > m$.

Generalizando: Si se desean colocar n palomas en m palomares, alguno de ellos debe contener al menos $\lceil \frac{n}{m} \rceil$ palomas, siendo $\lceil \frac{n}{m} \rceil$ el menor entero que es mayor o igual que $\frac{n}{m}$.

2. Divisibilidad

La teoría de divisibilidad trabaja principalmente con los números enteros (de modo que de ahora en adelante todos los números que mencionemos pertenecerán a $\mathbb{Z}$), y se sustenta en la definición de divisor de un número, que es ampliamente conocida. Se dice que a divide a b, esto es, que a es un *divisor* de b, si existe otro número entero c tal que

$$b = ac$$

En tal caso escribimos

$$a|b$$

Citemos ahora unas propiedades básicas, fáciles de demostrar. Tenemos que

$$a|b, b|c \Rightarrow a|c$$

$$a|b, a|c \Rightarrow a|b+c$$

$$a|b \Rightarrow a \leq b \qquad (b \neq 0)$$

Otra propiedad importante es la siguiente: si disponemos de una igualdad en la que tan sólo aparecen sumas de diversos términos, *todos ellos enteros*,

$$a_1 + a_2 + \ldots = b_1 + b_2 + \ldots$$

y sabemos que un cierto entero c divide a todos los términos de ambas sumas, salvo quizás a uno, entonces c divide a todos los términos de la igualdad. (¿Sabrías demostrar por qué?) Por otra parte, si en una igualdad de este tipo sabemos que uno de los términos no es divisible por c, entonces existe al menos otro término que tampoco lo es, ya que si no, por lo que acabamos de decir, todos los términos serían divisibles por c.
Por ejemplo, toda solución entera de la ecuación:

$$2x^3 + 4x^2 + x = 16$$

es par, puesto que podemos estar seguros de que $2x^3$, $4x^2$ y 16 son divisibles por 2, lo que implica que x también lo será. (Esto no quiere decir, por supuesto, que dichas soluciones existan).

¿Qué ocurre cuando un número no es divisor de otro? Al realizar la división del segundo por el primero, nos encontraremos que nos quedan un cociente y un resto. Así, tendremos

$$b = ca + r$$

Y los números de los que a sí que es divisor serán los *múltiplos* de a, aquellos tales que dan resto cero al dividirlos por a. Cabe destacar que la descomposición anterior es única con $0 \leq r < a$.
Obsérvese que fijado un número entero no nulo m, podemos clasificar todos los enteros en función del resto que resulta de dividirlos por m. Obtendremos

entonces m conjuntos, en cada uno de los cuales se incluirán los números que dan resto r, para $r = 0, 1, \ldots, m-1$. Por ejemplo, si escogemos el 3, tenemos, por un lado, los enteros

$$\ldots -9, -6, -3, 0, 3, 6, 9, \ldots, 3k, \ldots \qquad k \in \mathbb{Z}$$

por otro lado,

$$\ldots -8, -5, -2, 1, 4, 7, 10, \ldots, 3k+1, \ldots \qquad k \in \mathbb{Z}$$

y por último

$$\ldots -7, -4, -1, 2, 5, 8, 11, \ldots, 3k+2, \ldots \qquad k \in \mathbb{Z}$$

Esta clasificación se suele expresar a través de una relación de equivalencia: la congruencia, de modo que, fijado un entero m que llamaremos módulo, diremos que dos enteros a y b son congruentes módulo m y lo denotaremos:

$$a \equiv b \pmod{m}$$

cuando su diferencia sea un múltiplo de m, lo que equivale a decir que dan el mismo resto al dividir por m:

$$a - b = mk \qquad k \in \mathbb{Z}$$

Volviendo a nuestro ejemplo en el que el módulo es 3, tenemos:

$$\ldots -9 \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \ldots \pmod{3}$$

$$\ldots -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \ldots \pmod{3}$$

$$\ldots -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv 11 \ldots \pmod{3}$$

Con este nuevo lenguaje es más sencillo abordar problemas relacionados con divisibilidad. Entre otras, podemos ayudarnos de las siguientes propiedades:

$$a \equiv b, b \equiv c \Longrightarrow a \equiv c \pmod{m}$$

$$a \equiv 0 \pmod{m} \Longrightarrow m|a$$

$$a \equiv b, c \equiv d \Longrightarrow a + c \equiv b + d \pmod{m}$$

$$a \equiv b, c \equiv d \Longrightarrow ac \equiv bd \pmod{m}$$

Y si se cumple que m y c son primos entre sí $(mcd(m, c) = 1)$

$$ac \equiv bc \Longrightarrow a \equiv b \pmod{m}$$

Por medio de congruencias es sencillo demostrar las reglas de divisibilidad, por ejemplo, la del 9, una de las más empleadas. Ya que $10 \equiv 1 \pmod{9}$, para un

cierto número x cuyas cifras sean (de las unidades en adelante) $a_0, a_1, a_2, \ldots, a_n$ tenemos

$$x = a_0 + 10a_1 + 10^2a_2 + \ldots + 10^n a_n \equiv a_0 + 1a_1 + 1^2a_2 + \ldots + 1^n a_n \equiv$$

$$\equiv a_0 + a_1 + a_2 + \ldots + a_n \pmod 9$$

Lo que demuestra que *todo entero es congruente con la suma de sus cifras, módulo 9*. En particular, si la suma de las cifras de un número es un múltiplo de 9 ($a_0 + a_1 + a_2 + \ldots + a_n \equiv 0 \pmod 9$), también lo será dicho número ($x \equiv 0 \pmod 9$). Es más, tomado cualquier entero, por ejemplo el 132134, podemos saber qué resto da al dividirlo por 9 sin necesidad de hacer la división:

$$132134 \equiv 1 + 3 + 2 + 1 + 3 + 4 \equiv 14 \equiv 1 + 4 \equiv 5 \pmod 9$$

y se comprueba que efectivamente, el resto de dicha división es 5 ($132134 = 146819 + 5$).

En algunos problemas las congruencias pueden ayudar a reducir los casos a estudiar, eliminando todos aquellos en los que de su aplicación deriva una contradicción. Esto se da a menudo cuando hay involucradas potencias de números. Por ejemplo, si escogemos como módulo el 3, tenemos que todo entero es congruente con 0, 1 o 2 (que son los posibles restos al dividir por 3) pues pertenece a uno de los tres conjuntos que vimos arriba, y se da que

$$a \equiv 0 \Rightarrow a^2 \equiv 0^2 \equiv 0 \pmod 3$$

$$a \equiv 1 \Rightarrow a^2 \equiv 1^2 \equiv 1 \pmod 3$$

$$a \equiv 2 \Rightarrow a^2 \equiv 2^2 \equiv 1 \pmod 3$$

En consecuencia, un cuadrado perfecto sólo puede dar resto 0 o 1 al dividir por 3, lo que quiere decir que, por ejemplo, podemos estar seguros de que el número $3^k + 3k + 2$ no es un cuadrado perfecto para ningún valor de k entero positivo, pues $3^k + 3k + 2 \equiv 0^k + 0k + 2 \equiv 2 \pmod 3$. Del mismo modo, se prueba que no existen enteros x,y tales que $x^2 + y^2 = 2002$, pues trabajando módulo 7 nos queda que la única posibilidad para que eso suceda es que $x \equiv y \equiv 0 \pmod 7$, y esto quiere decir que tanto x como y son múltiplos de 7, lo que nos lleva a que $x^2 + y^2$ es múltiplo de 49, y por tanto no puede ser igual a 2002, que no es divisible por 49.

Incluimos también ahora un resultado conocido como el *Pequeño Teorema de Fermat*, que nos dice que dado un número primo p y otro número a, se cumple que

$$a^p \equiv a \pmod p$$

y si a y p son primos entre sí (lo que, puesto que p es primo, equivale a decir que a no es múltiplo de p), podemos «dividir» por a y tenemos

$$a^{p-1} \equiv 1 \pmod p$$

Hablando de primos, recordemos un par de cosas sobre ellos. Un número primo es un número cuyos únicos divisores positivos son él mismo y 1. (Consecuentemente, los únicos divisores enteros de un primo p son $1,-1$, p y $-p$). Por el *Teorema Fundamental de la Aritmética*, todo entero positivo se puede expresar de manera única como producto de números primos, llamándose dicho producto la descomposición en factores primos de dicho número. Generalmente cuando trabajamos con números primos conviene tener productos, para poder aprovecharnos de sus propiedades. Por ejemplo, si p es primo

$$p|ab \Longrightarrow p|a \vee p|b$$

donde con $\vee$ queremos decir que o bien $p|a$, o bien $p|b$ o bien se dan ambas cosas. En algunos casos aún podemos ir más allá: si tenemos un número primo p igualado a un producto de dos enteros, entonces dichos enteros serán forzosamente 1 y p, o -1 y $-p$. Más generalmente, si disponemos de una expresión del tipo $a = bc$, entonces los factores primos de a están distribuidos entre b y c, y en el caso de que $a|b$, los factores primos de a están contenidos en la descomposición en factores primos de b.