EL PEQUEÑO TEOREMA DE FERMAT Y APLICACIONES

Un enfoque heurístico, una demostración elemental y algunas aplicaciones del mismo

FRANCISCO BELLOT ROSADO

La lección de preparación olímpica que presento a continuación ha sido expuesta en el Seminario de Problemas de Valladolid, el miércoles 14 de octubre de 2009.

UN PROBLEMA PARA EMPEZAR

Un disco, dividido en p (p, primo) sectores iguales, se desea colorear con n colores, pudiendo estar varios, o todos los sectores, pintados del mismo color. No se consideran distintas dos coloraciones tales que se pueda deducir una de otra girando el disco alrededor de su centro, en un cierto sentido (horario o antihorario, pero no los dos).

¿De cuántas maneras se puede hacer esto?

(Origen del problema : la Olimpiada de la antigua Unión Soviética)

Tras unos momentos de reflexión, hago la siguiente sugerencia a los alumnos:

F.B.: *Por si alguno no se siente cómodo por no haberos dado valores particulares de n y p, sería perfectamente razonable empezar a ver lo que sucede con valores pequeños de n y p, para comprender bien el problema.*

Primer caso: $n=2,\ p=2.$

Varios alumnos contestan en seguida : 3 coloraciones. Las dibujo en el encerado, siguiendo las respuestas de los alumnos.

Segundo caso: $n=2,\ p=3.$

La respuesta es igualmente rápida : 4 coloraciones, que igualmente se dibujan en el encerado.

Tercer caso : $n=3,\ p=3.$

Ahora tarda un poco más en aparecer la respuesta correcta; tras una respuesta de 10, otro alumno justifica que ha de considerarse una más, porque los giros se hacen en un solo sentido : 11 coloraciones.

Cuarto caso : $n=4,\ P=3.$

Alguno aventura 24, sin mucha convicción… les digo que sí, que esa es la respuesta.

Escribo entonces en el encerado las igualdades (¡obvias!)

$$3=1+2;\ 4=2+2;\ 11=8+3;\ 24=20+4$$

Hago ver que el segundo sumando de cada suma coincide con *n*.

Para contar las coloraciones utilizaremos, en todos los casos, el siguiente procedimiento:

Primero se considera el disco fijo, y los sectores numerados, de 1 a *p*; y se cuentan las coloraciones posibles así, que resultan ser n^p.

(Para los no convencidos, hago el típico ejemplo de las quinielas: ¿Cuántas columnas de 14 partidos hay que rellenar para estar seguros de que en una de ellas tenemos 14 aciertos?). Salvo los alumnos de 2º de Bachillerato, en el grupo de Olimpiadas hay alumnos de 3º, 4º de E.S.O. y 1º de Bachillerato; la Combinatoria se estudia en 4º, pero no tan pronto. Por lo tanto, prefiero obviar el tecnicismo de llamarle "número de variaciones con repetición".

Después se restan las que corresponden a un solo color, que son *n.* Así, con el disco fijo y los sectores numerados, tenemos

$$n^p-n$$

coloraciones en donde por lo menos se utilizan dos colores.

A continuación se eliminan los números de los sectores. ¿Qué efecto tiene esto sobre las coloraciones que inicialmente eran diferentes? ¿Cuántas coloraciones que eran diferentes coincidirán al borrar la numeración de los sectores?

Los alumnos van examinando los casos vistos hasta ahora y contestan:

Primer caso: 2

Segundo caso: 3

Tercer caso: 3

Cuarto caso: 3

La supresión de los números de los sectores equivale a hacer giros de

$$\frac{k\bullet 360^o}{p}$$

grados de amplitud alrededor del centro del disco; o lo que es lo mismo, cada coloración no monocromática se cuenta *p* veces: la inicial y las que resultan de los *p-1* giros de amplitudes

$$\frac{1\bullet 360^o}{p},\frac{2\bullet 360^o}{p},\cdots,\frac{(p-1)\bullet 360^o}{p}.$$

Es instructivo ver cuáles son esos giros en los casos particulares estudiados. En el primer caso hay un solo giro (*p-1=1)* y en todos los demás hay 2.

Entonces parece que ya estamos en condiciones de formular la respuesta a la pregunta del problema, con generalidad : **el número de coloraciones es**

$$\frac{n^p - n}{p} + n \,.$$

La respuesta al problema es un número natural; por lo tanto, como consecuencia se obtiene que

n^p-n es múltiplo de p, si p es un número primo.

Doy nombre a esta proposición : “Pequeño teorema de Fermat”, enunciado en una carta de Fermat del 18 de octubre de 1640 a su amigo Frénicle de Bessy, naturalmente sin demostración (en esto, Fermat era un verdadero experto) y con una formulación ligeramente diferente. Leibniz dejó una demostración en un manuscrito no publicado, antes de 1683, y Euler publicó la suya en 1736 (*Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio).* La expresión “Pequeño teorema de Fermat” se usó por primera vez en 1913 en un libro alemán de Teoría de Números.

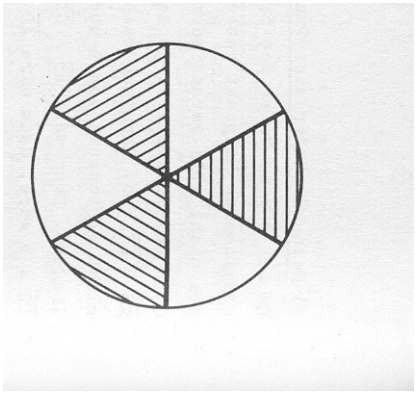
Retrato de Fermat

FB ante la estatua de Fermat en el pueblo natal de Fermat, Beaumont de Lomagne, en el Sur de Francia, verano de 2002

Acto seguido pregunto: ¿qué ocurriría si p no fuera primo, por ejemplo si tenemos el caso $n=2,p=6$?

Una alumna mete los datos en su calculadora para ver el valor de la fracción que da el número de coloraciones no monocromáticas y encuentra un número decimal. Le digo : acabas de comprobar que el resultado no es válido si p no es primo.

Gráficamente la situación se puede visualizar como



y aquí un giro de 120º transforma la figura en sí misma.

A continuación lanzo la pregunta

¿Os parece que hemos demostrado algo?

No hay unanimidad en las respuestas; los que me conocen de años anteriores se inclinan por el NO; a otros les parece que el argumento se debilita al decir que *p* de las coloraciones coinciden cuando se suprimen los números de los sectores; algunos se muestran convencidos de la bondad del argumento. Con objeto de eliminar cualquier sombra de duda, expongo una de las demostraciones del libro *Selected Problems and Thorems in Elementary Mathematics,* de D.O.Schklyarsky, N.N.Chentsov e I.M. Yaglom, MIR, Moscú 1979, que considero al alcance de todos los alumnos de la audiencia.

DEMOSTRACIÓN DEL TEOREMA

Se puede suponer, sin pérdida de la generalidad, que *n* no es divisible por *p* (porque en tal caso el resultado es evidente). Entonces los números

n, 2n, 3n, …, (p-1)n

tampoco son divisibles por *p*, y los restos de su división por *p* son DIFERENTES. Justifiquemos esta última afirmación. Si *kn* y *ln* (con $p-1 \geq k > l$) dieran el mismo resto al ser divididos por *p,* entonces su diferencia $k \bullet n - l \bullet n = (k-l)n$ tendría que ser divisible por *p*, pero eso es imposible porque *p* es primo, *n* no es divisible por *p,* y $k-l < p$.

Como los posibles restos de la división por *p* son 1,2,3,…,p-1, se tiene

$$n = q_1 p + a_1; 2n = q_2 p + a_2, \cdots, (p-1)n = q_{p-1} p + a_{p-1},$$

donde los números $a_1, a_2, \cdots, a_{p-1}$ son 1,2,…,p-1 en algún orden. Multiplicando todas esas igualdades se obtiene

$$\left[1\bullet 2\bullet 3\bullet\cdots\bullet\left(p-1\right)\right]n^{p-1}=Np+a_1\bullet a_2\bullet\cdots\bullet a_{p-1}\,,$$

o lo que es igual

$$\left[1\bullet 2\bullet 3\bullet\cdots\bullet\left(p-1\right)\right]\left(n^{p-1}-1\right)=Np\,.$$

De aquí que $\left(n^{p-1}-1\right)$es divisible por *p* (esta es la forma en que Fermat formuló su teorema) y multiplicando por *n* se obtiene el resultado.

Finalizada la demostración, pido a los alumnos que enuncien el resultado recíproco (para algunos era la primera vez que oían esa expresión) . Se formula como

Si n^p-n es múltiplo de p, entonces p es primo.

Acto seguido señalo que, desafortunadamente, esta proposición es falsa, como lo prueba el contraejemplo (tomado de *Problem Solving strategies,* de Arthur Engel, un libro indispensable en la preparación de Olimpiadas):

341 divide a 2^{341}-2,

pero 341=31x11 no es primo; y la expresión en negrita se justifica escribiendo

$$2^{341}-2=2\left(2^{340}-1\right)=2\left(\left(2^{10}\right)^{34}-1^{34}\right)=2\left(2^{10}-1\right)\left(\cdots\right)=2\bullet 3\bullet 341\bullet\left(\cdots\right).$$

Este es el menor contraejemplo al recíproco, por lo que a mi entender no resultaría conveniente haberles pedido que fueran comprobando algunos casos para valores pequeños de *p* y *n.*

En el libro de Engel antes citado se incluyen tres demostraciones del teorema: por inducción, utilizando congruencias y de tipo combinatorio (con collares, pero utilizando el concepto de permutaciones cíclicas, no apropiado para esta audiencia en este momento). En el de los tres autores rusos mencionados antes se incluye una segunda demostración, por inducción y el teorema del binomio. Una búsqueda en Internet da como resultado siete demostraciones, una de ellas por teoría de grupos, otra sistemas dinámicos y una tercera con la fórmula de Leibniz para la potencia de un polinomio, también conocida como fórmula multinomial. Personalmente, mi favorita es la que acabo de exponer.

ALGUNOS PROBLEMAS DONDE SE APLICA EL TEOREMA

Observación previa

Para agilizar la aplicación del teorema de Fermat es necesario utilizar el concepto y propiedades de las congruencias. Resumo, sin demostración, algunas de sus propiedades.

Si los enteros *a* y *b* dan el mismo resto al ser divididos por el entero *k*, se dice que ambos son congruentes respecto al módulo *k,* y se escribe $a \equiv b(\mathrm{mod}\, k)$. Las principales propiedades de las congruencias son:

$a \equiv a(\mathrm{mod}\, k)$ (propiedad reflexiva)

Si $a \equiv b(\mathrm{mod}\, k)$, entonces $b \equiv a(\mathrm{mod}\, k)$ (propiedad simétrica)

Si $a \equiv b(\mathrm{mod}\, k)$, y $b \equiv c(\mathrm{mod}\, k)$, entonces $a \equiv c(\mathrm{mod}\, k)$ (propiedad transitiva)

Las congruencias se pueden sumar y multiplicar:

Si $a \equiv b(\mathrm{mod}\, k)$ y $c \equiv d(\mathrm{mod}\, k)$, entonces $(a \pm c) \equiv (b \pm d)(\mathrm{mod}\, k)$

Si $a \equiv b(\mathrm{mod}\, k)$ y $c \equiv d(\mathrm{mod}\, k)$, entonces $(ac) \equiv (bd)(\mathrm{mod}\, k)$.

Pero en general no se pueden dividir los términos de una congruencia, salvo por un número que sea primo con el módulo de la congruencia.

1.- Calcular el resto de la división por 13 del número 7^{44}.

Por el pequeño teorema de Fermat, 7^{12}-1 es múltiplo de 13, lo cual significa que 7^{12} da resto 1 al ser dividido por 13. De aquí resulta que $7^{36}=(7^{12})^3$ también da resto 1 al ser dividido por 13. Entonces 7^{44} y 7^8 dan el mismo resto al ser divididos por 13. Pero 7^2 da resto 10 al ser dividido por 13, 7^4 da el mismo resto que 10^2, es decir, 9. Entonces 7^8 da el mismo resto que $9^2=81$, es decir, da resto 3 cuando se divide por 13, y esta es la respuesta.

2.- Demostrar que $2^{70} + 3^{70}$ es divisible por 13.

Por el pequeño teorema de Fermat, 2^{12} da resto 1 al ser dividido por 13, así que $2^{60} = (2^{12})^5$ dará resto $1^5 = 1$. Como 2^5 da resto 6, 2^{10} dará resto -3 al ser dividido por 13. Entonces 2^{70} da resto -3 al ser dividido por 13.

Por otra parte, 3^3 da resto 1, y lo mismo ocurre con 3^{69}. De aquí que 3^{70} dará resto 3. Entonces, sumando $2^{70} + 3^{70}$ dará resto -3+3 =0, es decir, será divisible por 13.

3.- Demostrar que los posibles restos de la división por 7 de un cubo perfecto son 0, 1 ó 6.

Sea *n* un número natural cualquiera. 7 es evidentemente primo.

Si *n* no es divisible por 7, entonces por el teorema de Fermat,

$$n^6 \equiv 1(\mathrm{mod}\,7) \Leftrightarrow n^6 - 1 \equiv 0(\mathrm{mod}\,7) \Leftrightarrow (n^3-1)(n^3+1) \equiv 0(\mathrm{mod}\,7)$$

Luego, o bien $(n^3-1) \equiv 0(\mathrm{mod}\,7)$, o bien $(n^3+1) \equiv 0(\mathrm{mod}\,7)$.

Si $(n^3-1) \equiv 0(\mathrm{mod}\,7)$, esto es lo mismo que $n^3 \equiv 1(\mathrm{mod}\,7)$.

Si $(n^3+1) \equiv 0(\mathrm{mod}\,7)$, esto es lo mismo que $n^3 \equiv -1(\mathrm{mod}\,7) \Leftrightarrow n^3 \equiv 6(\mathrm{mod}\,7)$.

Por último, si *n* es divisible por 7, n^3 también lo es, y $n^3 \equiv 0(\mathrm{mod}\,7)$.

4.- Calcular el resto de la división de 2^{98} por 101.

Como 101 es primo, utilizando el teorema de Fermat tenemos que

$$2^{100} \equiv 1(\mathrm{mod}101) \Leftrightarrow 2^{98} \bullet 4 \equiv 1(\mathrm{mod}101) \Leftrightarrow 2^{98} \bullet 4 \equiv -100(\mathrm{mod}101)$$

Como 4 y 101 son primos entre sí, podemos dividir la última congruencia por 4 y obtenemos

$$2^{98} \equiv -25(\mathrm{mod}101) \Leftrightarrow 2^{98} \equiv 76(\mathrm{mod}101).$$

Por lo tanto, el resto es 76.

5.- Demostrar que si *p* es primo, entonces, cualquiera que sea el número natural *n*, se tiene

$$\sum_{k=1}^{p} n^{mcd(k,p)} \equiv 0(\mathrm{mod}\ p).$$

Se verifica

$\sum_{k=1}^{p} n^{mcd(k,p)} = n + n + \cdots + n + n^p$ (p-1 sumandos iguales a n), es decir

$(p-1)n + n^p = np + n^p - n$. Ahora bien,

$$(1)\ np \equiv 0(\mathrm{mod}\ p)$$

$$(2)\ n^p \equiv n(\mathrm{mod}\ p)(TeoremadeFermat) \Leftrightarrow n^p - n \equiv 0(\mathrm{mod}\ p)$$

Y de (1) y (2) se obtiene el resultado.

6.- Si *p* es un número primo mayor que 5, demostrar que p^4-1 es divisible por 240.

Sea *p* primo mayor que 5. Se tiene que 240 = 8x5x6 = 16x5x3.

$$p^4-1=\left(p^2-1\right)\left(p^2+1\right)=\left(p-1\right)\left(p+1\right)\left(p^2+1\right).$$

Como *p* es impar, entonces *p-1* y *p+1* son dos números pares consecutivos, así que su producto es múltiplo de 8. Pero p^2 + 1 también es par, así que el producto de los tres es múltiplo de 16.

Por el teorema de Fermat, $p^4-1\equiv 0\left(\mathrm{mod}\,5\right)$.

Por otra parte, si *p>5* es primo, *p* no puede ser divisible por 3, así que lo será uno de los números *p-1* ó *p+1.*

Finalmente, 16, 5 y 3 son primos entre sí dos a dos, así que si p^4*-1* es divisible por 16, por 5 y por 3, lo será por su producto, que es 240.

7.- Si *m* es primo, y *a,b* son dos números enteros positivos menores que m, demostrar que

$$a^{m-2}+a^{m-3}b+a^{m-4}b^2+\cdots+b^{m-2}$$

Es múltiplo de m.

Se verifica

$$a^{m-1}-b^{m-1}=\left(a-b\right)\left(a^{m-2}+a^{m-3}b+a^{m-4}b^2+\cdots+b^{m-2}\right).$$

Puesto que *m* es primo, y *a<m,b<m,* por el teorema de Fermat se tiene que

$$a^{m-1}\equiv 1\left(\mathrm{mod}\,m\right);b^{m-1}\equiv 1\left(\mathrm{mod}\,m\right);$$

por lo tanto su diferencia será múltiplo de *m:*

$$a^{m-1}-b^{m-1}\equiv 0\left(\mathrm{mod}\,m\right).$$

Como *a-b* no puede ser múltiplo de m (de hecho, el mcd(*a-b,m)=1),*se obtiene el resultado.

PROCEDENCIA DE LOS PROBLEMAS

El problema 1 está tomado del libro *Introduction to Number Theory and Inequalities,* de C.J. Bradley (publicado por UKMT, 2006).

El problema 2 procede de uno de los libros "míticos" en Teoría de Números: *250 problèmes de théorie élémentaire des nombres,* de Waclaw Sierpinski (publicado en francés por Ed. Jacques Gabay, 1992), y cuya edición original en inglés se publicó en Varsovia en 1970.

Los restantes problemas proceden de una lección de Olimpiadas de la Prof. hispano-cubana María Emilia Santibáñez Piñera sobre el teorema de Fermat, no publicada (sin fecha; probablemente alrededor de 1987).

BIBLIOGRAFÍA

Además de las tres fuentes recién mencionadas, presento a continuación algunos libros válidos para la preparación de Olimpiadas en lo que se refiere a Teoría de Números:

1) Arthur Engel: *Problem solving strategies*; Springer 1998.

2) Enzo Gentile : *Aritmética Elemental en la formación matemática; Olimpiada Matemática Argentina, 1991.*

3) Saulo Rada Aranda : *Aritmética;* CENAMEC, Caracas 1992.

4) Waclaw Sierpinski: *Elementary Theory of Numbers;* North Holland&PNN, Amsterdam y Varsovia 1988.

5) Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery : *An Introduction to the Theory of Numbers;* John Wiley, 1991.