JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Un problema sobre números combinatorios

Rosa de Frutos Marín[1]

[1] *Universidad de Valladolid. Departamento de Matemática Aplicada.*

La conjetura de Casas-Alvero afirma que si un polinomio mónico de grado n con coeficientes complejos comparte una raíz con cada una de sus sucesivas derivadas, entonces es una potencia de una forma lineal.

La conjetura ha sido probada para grados del tipo $n = hq$, donde q es la potencia de un número primo p y $h = 1,2$. Para cada uno de los h =3, 4, 5, 6, 7, se ha podido dar un listado finito $L(h)$ de valores de p (llamados *ineficaces*) tales que si p no está en el listado correspondiente a dicho h, entonces se ha podido probar la conjetura para $n = h \cdot q$, siendo q cualquier potencia de p. Esta circunstancia justifica el calificativo ineficaz para los primos que no están los correspondientes listados. En concreto, $L(3)$ está formado solo por el primo 2; $L(4)$, por los tres primos 3, 5, 7; $L(5)$, por los nueve primos 2, 3, 7, 11, 131, 193, 599, 3541, 8009, mientras que $L(6)$ consiste en 53 primos ineficaces concretos, y $L(7)$ de 661, estos últimos calculados utilizando computación. Para $n = 12$ también se ha probado utilizando computación.

No se conoce la validez de la conjetura para otros valores de n; en particular no se conoce para $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$, ni para ningún entero n que tenga cuatro o más divisores primos, ni para los que tienen tres que no sean los del tipo $6 \cdot q$ anteriores. La computación está lejos de poder abordar cualquiera de estos casos para los que se desconoce la validez; de hecho, la prueba para $n = 12$ ha requerido una computación de semanas y altas prestaciones y se ha considerado un hito en ese ámbito.

El único método matemático conocido para tratar la conjetura está lejos de poder abordar estos casos. Para utilizarlo, se formula la conjetura de Casas-Alvero para polinomios de grado n sobre las clausuras algebraicas de los cuerpos F_p, es decir una conjetura $CA(n, p)$ para cada grado n y para cada primo (o característica) p. Existen, de hecho, muchas formas equivalentes de formular $CA(n, p)$, y hay valores de p y n para los cuales $CA(n, p)$ no es válida. Si para un valor de n dado se encuentra un primo p tal que $CA(n, p)$ es válida, entonces se deduce que la conjetura de Casas-Alvero es cierta. En ello consiste el método aludido y es el procedimiento seguido para probar la conjetura para los valores del tipo $h.q$ que se han mencionado anteriormente.

En otras palabras, dicho método consiste en intentar probar la conjetura en aquellos casos en los que su reducción módulo p es válida para algún primo p. Se puede aplicar también a polinomios que tengan solamente un cierto subconjunto de monomios. La dificultad de probar la conjetura se manifiesta también,y en la misma medida, para casos de pocos monomios. Si se trata de un solo monomio, éste es X^n y la prueba de la conjetura es trivial. Si se trata de polinomios con sólo dos monomios, digamos X^n, X^i con $i < n$, resulta fácil probar que la reducción módulo p en este caso es válida para aquellos p tales que el número combinatorio $a = \binom{n}{i}$ no es congruente con 1 módulo p, y se deduce de ello que la conjetura es cierta para polinomios con dos monomios.

Si se consideran polinomios con tres monomios, digamos X^n, X^j, X^i, con $i < j < n$, hemos probado que siempre existen primos p que dividen simultáneamente a los números combinatorios $a = \binom{n}{i}$ y $b = \binom{n}{j}$ y para estos primos p se tiene la validez de la reducción módulo p de la conjetura de Casas-Alvero correspondiente. En realidad, para probar dicha validez, es suficiente encontrar primos p que dividan *a uno* de los enteros a, b, y el otro no sea congruente con 1 módulo p. Incluso si p no divide a ninguno de los dos, hemos probado que la condición necesaria y suficiente para que se tenga la validez es que p no divida a un cierto entero D dado explícitamente en términos de los datos n, j, i y que se puede probar que es no nulo.

A partir de lo anterior se deduce que la conjetura de Casas-Alvero es cierta para todos los polinomios con tres monomios; sin embargo no se conoce si es o no cierta para todos los polinomios con cuatro o más monomios. Si consideramos polinomios con únicos cuatro monomios X^n, X^k, X^j, X^i con $n > k > j > i$, y los números combinatorios $a = \binom{n}{i}$, $b = \binom{n}{j}$, $c = \binom{n}{k}$, y un primo p, entonces podemos probar el resultado siguiente.

Teorema: La reducción módulo p de la conjetura de Casas-Alvero es válida para los polinomios con los cuatro monomios anteriores, si se verifica una de las dos condiciones siguientes:

1. Dos de los tres números combinatorios a, b, c son múltiplos de p y el otro no es congruente con 1 módulo p.
2. Uno de los tres números combinatorios a, b, c es múltiplo de p, los otros dos no son congruentes con 1 módulo p, y el entero D determinado por estos dos números combinatorios no es múltiplo de p.

Se deduce que la conjetura de Casas-Alvero para polinomios con cuatro monomios es cierta si existe algún primo p tal que para los exponentes de sus monomios se satisface alguna de las propiedades (1) o (2) del teorema anterior. Por ejemplo, ello sucede en el caso particular de la condición (1), en el que se dispone de un primo p que divide simultáneamente a los tres números combinatorios a, b, c.

Como consecuencia de este resultado, planteamos los siguientes problemas aritméticos sobre ternas de números combinatorios, cuya solución desconocemos, y que si es afirmativa para cualquiera de ellos, probaría la conjetura de Casas-Alvero para todos los polinomios con cuatro monomios.

Problemas: Para n, k, j, i arbitrarios,

- ¿Existe siempre un número primo p que satisface (1) en el teorema?
- ¿Existe siempre un número primo p que satisface (1) o (2) en el teorema?

El método de reducción de la conjetura módulo p fue utilizado por primera vez en [1]. El artículo [2] ha difundido la conjetura para el público general mostrando diversos indicios de su dificultad. En [3] se encuentra un estudio sistemático, la interpretación numérica y los límites del conocimiento actual sobre la conjetura, y se estudian varias alternativas equivalente para su reducción módulo p.

References

[1] H. Bothmer, O. Labs, J. Schicho, C. Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, J. Algebra **366**, pp. 224-230 (2007).

[2] J. Draisma, J. de Jong, *On the Casas-Alvero conjecture*, Feature, EMS Newsletter **80** pp. 29-33 (2011).

[3] R. de Frutos Marín, *Perspectiva aritméticas para la conjetura de Casas-Alvero*, Tesis Universidad de Valladolid (2013).