Gaps en polinomios ciclotómicos binarios

Antonio Cafure
Universidad Nacional de General Sarmiento, CONICET, Argentina
acafure@campus.ungs.edu.ar

El conjunto de gaps de un polinomio dado por su representación densa es el conjunto de las distancias entre las potencias de monomios no nulos consecutivos. El máximo gap de un polinomio es el máximo de este conjunto.

En este contexto, el estudio de los gaps de los polinomios ciclotómicos ha cobrado relevancia en los últimos años como consecuencia de las aplicaciones a problemas de criptografía ([1], [2]). El primer caso importante de estudio es el caso de los polinomios ciclotómicos binarios. Un polinomio ciclotómico Φ_n se dice binario si $n = pq$, con $p < q$ números primos. Es sabido que el máximo gap de Φ_{pq} es igual a $p - 1$ y que la cantidad de estos gaps es igual a $2\lfloor q/p \rfloor$ ([1], [2]). De todos modos queda aún por determinar el conjunto completo de gaps de Φ_{pq}.

En esta comunicación presentaremos los dos resultados que siguen.

El primero de ellos da cuenta del segundo gap de Φ_{pq}. En efecto, mostramos que si $3 < p < q$ son primos impares y $r > 0$ es el resto de q módulo p, entonces el segundo gap de Φ_{pq} es igual al máximo entre $p - r - 1$ y $r - 1$.

El segundo resultado proporciona una caracterización combinatoria de los sucesivos gaps de Φ_{pq} cuando $q \equiv \pm 1 \mod p$. En particular, implica el de [3] sobre la existencia de gaps de todas las longitudes.

Para obtener estos resultados apelamos a la interpretación de los polinomios ciclotómicos binarios en términos de una concatenación de palabras sobre el alfabeto $\{-1, 0, 1\}$ que introdujimos en nuestro trabajo [4].

Trabajo en conjunto con Eda Cesaratto (Universidad Nacional de General Sarmiento, CONICET, Argentina).

Referencias

[1] Hong, H.; Lee, E.; Lee, H.; Park, C. Maximum gap in (inverse) cyclotomic polynomial. J. Number Theory 132, No. 10, 2297-2315 (2012).

[2] Zhang, B. Remarks on the maximum gap in binary cyclotomic polynomials. Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér. 59(107), No. 1, 109-115 (2016).

[3] Camburu, O.; Ciolan, E.; Luca, F.; Moree, P.; Shparlinski, I. Cyclotomic coefficients: gaps and jumps. J. Number Theory 163, 211-237 (2016).

[4] Cafure, A.; Cesaratto, E. Binary cyclotomic polynomials: representation via words and algorithms. Lecroq, Thierry (ed.) et al., Combinatorics on words. 13th international conference, WORDS 2021, Rouen, France, September 13–17, 2021. Proceedings. Cham: Springer. Lect. Notes Comput. Sci. 12847, 65-77 (2021).