Exposé court

79 *On a congruence arising from permutation polynomials*

Luca, Florian (Wits)

We present an algorithm which given an odd positive integer n finds a solution to the congruence

$$-1 \equiv \prod_{i=1}^{r} (2^{a_i} + 1) \pmod{2^n - 1}.$$

Whenever such a solution exists, the inverse function in $\mathbb{F}_{2^n}$, the finite field with 2^n elements, can be represented as a composition of quadratics. The algorithm produced one such solution for every odd positive integer $n \leq 100$. Along the way we recall old facts about Mersenne numbers and conjecture new ones. We also use a Jacobi symbol formula due to Rotkiewicz. In addition, we show that the positive integers n such that the congruence $n - 1 \equiv 2^a \cdot 3^b \pmod{2^n - 1}$ holds with some integers $a,\ b$ form a subset of asymptotic density zero and give an explicit bound on their counting function.