CENTRO DE MATEMÁTICA
UNIVERSIDADE DO PORTO

Algebra, Combinatorics and Number Theory Seminar

Date. Tuesday, January 10, 2023 - 3pm

Speaker. Bianca Sosnovski - Queensborough Community College, CUNY

Title. Application of Semi-Primitive Roots to the Computation of the Discrete Logarithm Modulo 2^k

Abstract.

In 2004, Fit-Florea and Matula presented an algorithm for computing the discrete logarithm modulo 2^k with logarithmic base 3. The algorithm is suitable for hardware support of applications where fast arithmetic computation is desirable.

This talk aims to present a connection between semi-primitive roots of the multiplicative group of integers modulo 2^k where $k \geq 3$, and the logarithmic base in the Fit-Florea and Matula's algorithm. Using properties of semi-primitive roots modulo 2^k we generalize the algorithm to find the discrete logarithm modulo 2^k with any semi-primitive root as the base.

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

POPH QUALIFICAR É CRESCER.

QUADRO DE REFERÊNCIA ESTRATÉGICO NACIONAL PORTUGAL 2007.2013

GOVERNO DA REPÚBLICA PORTUGUESA

UNIÃO EUROPEIA
Fundo Social Europeu