Special Issue

Computational Aspects of Quadratic and High-Order Residues with Applications in Cryptography

Message from the Guest Editor

Quadratic and high-order residues have increasingly caught researchers' attention due to their applications in computational number theory and especially in cryptography. Some of the fields where they have produced useful results are primality testing, pseudo-random generators, public-key cryptography, secure multiparty computation, etc. However, intense research is still needed to clarify various computational aspects and make them more efficient in cryptographic applications. This Special Issue aims to bring together original contributions to the understanding of the computational aspects of quadratic and high-order residues and their applications in cryptography. Areas of interest include but by no means are restricted to:

- Efficient computation of high-order residues;
- Distribution of quadratic and high-order residues;
- Sums of residues and non-residues;
- Signed residues;
- High-order residuosity problem and its relations with other computationally hard problems;
- Applications in cryptography (pseudo-random generators, public-key cryptography, secure multi-party computation, signcrytion, etc.).

Guest Editor

Prof. Dr. Ferucio Laurentiu Tiplea
Department of Computer Science, Alexandru Ioan Cuza University of Iasi, Iasi 700506, Romania

Deadline for manuscript submissions

closed (20 September 2022)

Mathematics

an Open Access Journal by MDPI

Impact Factor 2.2
CiteScore 4.6

mdpi.com/si/68928

Mathematics
Editorial Office
MDPI, Grosspeteranlage 5
4052 Basel, Switzerland
Tel: +41 61 683 77 34
mathematics@mdpi.com

mdpi.com/journal/mathematics

Mathematics

an Open Access Journal by MDPI

Impact Factor 2.2
CiteScore 4.6

mdpi.com/journal/mathematics

About the Journal

Message from the Editor-in-Chief

The journal *Mathematics* publishes high-quality, refereed papers that treat both pure and applied mathematics. The journal highlights articles devoted to the mathematical treatment of questions arising in physics, chemistry, biology, statistics, finance, computer science, engineering and sociology, particularly those that stress analytical/algebraic aspects and novel problems and their solutions. One of the missions of the journal is to serve mathematicians and scientists through the prompt publication of significant advances in any branch of science and technology, and to provide a forum for the discussion of new scientific developments.

Editor-in-Chief

Prof. Dr. Francisco Chiclana
School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester LE1 9BH, UK

Author Benefits

High Visibility:

indexed within Scopus, SCIE (Web of Science), RePEc, and other databases.

Journal Rank:

JCR - Q1 (Mathematics) / CiteScore - Q1 (General Mathematics)

Rapid Publication:

manuscripts are peer-reviewed and a first decision is provided to authors approximately 18.4 days after submission; acceptance to publication is undertaken in 2.4 days (median values for papers published in this journal in the first half of 2025).

MDPI