# Accelerating modular arithmetic with special choice of moduli

Eugene V. Zima

**Abstract.** Several methods of selection of moduli in modular arithmetic are considered [1] – [6]. With the proposed choice of moduli both modular reduction of an integer and reconstruction from modular images are accelerated. Special attention is paid to the moduli of the forms $2^n \pm 1$ and $2^n \pm 2^k \pm 1$. Different schemes of choice of these types of moduli and algorithms for conversion of arbitrary precision integers into the modular representation and back are considered. Results of experimental implementation of the described algorithms in the GMP system are discussed.

## References

[1] J. Doliskani, P. Giorgi, R. Lebreton, E. Schost Simultaneous Conversions with the Residue Number System Using Linear Algebra. *ACM Transactions on Mathematical Software*, Volume 44, Issue 3, Article No.: 27, pp. 1–21, 2018.

[2] H. Garner. The Residue Number System. *IRE Transactions, EC-8.* pp.140–147, 1959.

[3] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for Computer Algebra* ($6^{\text{th}}$ printing). Boston: Kluwer Academic, 1992.

[4] D. E. Knuth. *The Art of Computer Programming*, Vol 2.

[5] M. Křížek, F. Luca, and L. Somer. *17 Lectures on Fermat Numbers: From Number Theory to Geometry.* New York: Springer-Verlag, 2001.

[6] Stewart A.M., Zima E.V. Base-2 Cunningham numbers in modular arithmetic. Program. Comput. Software, 2007, vol. 33, pp.80 -86.

Eugene V. Zima
Physics and Computer Science dept.,
Wilfrid Laurier University,
Waterloo, Ontario, Canada
e-mail: `ezima@wlu.ca`