Rational approximations over conics

Stefano Barbero

Abstract: We study a general class of conics starting from a quotient field. We give a group structure over these conics generalizing the construction of a group over the Pell hyperbola. Furthermore, we generalize the definition of Rédei rational functions in order to use them for evaluating powers of points over these conics. Then, we study rational approximations of irrational numbers over conics, obtaining a new result for the approximation of quadratic irrationalities. Finally, by means of a convenient parametrization, we define also a group structure over the set of parameters and, in special cases, these groups have finite order and consequently we can construct a novel public key cryptosystem.

References

[1] S. Barbero, U. Cerruti, N. Murru, Solving the Pell equation via Rédei rational functions, *The Fibonacci Quarterly*, Vol.**48** No. **4** (2010), 348–357.

[2] S. Barbero, U. Cerruti, N. Murru, Generalized Redéi Rational Functions and Rational Approxximations Over Conics, *International Journal of Pure and Applied Mathematics* Vol. **64** No. **2** (2010), 305–316.

[3] E. Bellini, N. Murru, An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics, *Finite Fields and Their Applications* Vol. **39** (2016,) 179–194.

[4] E. B. Burger, A. M. Pillai, On diophantine approximation along algebraic curves, *Proceedings of the American Mathematical Society*, Vol. **136** No. **1** (2008), 11–19.

[5] L. Rédei, Uber eindeuting umkehrbare polynome in endlichen korpen, *Acta Sci. Math.* (Szeged), **11** (1946), 85–92.