1023-11-1191 **Michael J. Jacobson Jr.** and **Renate Scheidler*** (rscheidl@math.ucalgary.ca), Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N3Z4, Canada, and **Andreas Stein**. *Cantor Versus NUCOMP on Hyperelliptic Curves.*

Arithmetic in the Jacobian of an imaginary hyperelliptic curve as well as the infrastructure of a real hyperelliptic curve is done on reduced divisors. The standard way to perform this arithmetic is divisor addition (Cantor's algorithm) with subsequent reduction, although for the cryptographically interesting case of low genus, faster explicit formulas are available for the imaginary scenario. A more efficient general-purpose algorithm, called NUCOMP, was developed by D. Shanks in the late 1980's and subsequently improved by O. Atkin.

A major drawback of arithmetic à la Cantor is that the intermediate step of divisor addition produces operands of double size which are then again reduced to single size by the subsequent reduction. NUCOMP not only avoids this problem, but cleverly replaces the rather expensive reduction steps by the much faster Euclidean Algorithm. As a result, numerical experiments have shown that NUCOMP performs up to 35 percent faster than the conventional algorithm.

In this talk, we briefly review divisor arithmetic on hyperelliptic curves and explain the basic idea of NUCOMP. Details of the algorithm will be provided in Andreas Stein's talk. (Received September 25, 2006)