CORR 99-39

Generalized Mersenne Numbers

Jerome A. Solinas*

Abstract There is a well known shortcut for modular multiplication modulo a Mersenne number, performing modular reduction without integer division. We generalize this technique to a larger class of primes, and discuss parameter choices which are particularly well suited for machine implementation.

Keywords modular arithmetic, elliptic curves.