CORR 2001-65

Note on Reduction Operation Modulo $r^n + ar^m + b$

Huapeng Wu

Abstract A continuation to the work proposed in [2], this note presents an efficient method to calculate modular operation $X \pmod N$, where $N = 2^n \pm 2^m \pm 1, 0 < m < n$. It has shown that $X \pmod N$, by $\frac{n}{n-m} \leq k < \frac{n}{n-m} - 1$. Examples are given to illustrate the algorithm proposed in [2]. When $N = r^n + ar^m + b$ where $r \geq 2, 0 < m < n$, and a, b can be any nonzero integers, we have also presented a closed-form incomplete solution for modular operation $X \pmod N$ for $0 \leq X < r^{2n}$.

Keywords Modular arithmetic.