1026-11-174 **P Berrizbetia**, **S Muller** and **Hugh C Williams*** (williams@math.ucalgary.ca), Dr. H. Williams, Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta T2N 1N4, Canada. *Pseudopowers and Primality Proving.*

The so-called pseudosquares yield a very powerful machinery for the primality testing of large integers $N$. In fact, assuming reasonable heuristics (which have been confirmed for numbers to $2^{80}$) this gives a deterministic primality test in time $O((\lg N)^{3+o(1)})$, which many believe to be best possible. In the 1980s D.H. Lehmer posed a question tantamount to whether this could be extended to pseudo r-th powers. Very recently this was accomplished for r=3. In fact, the results obtained indicate that r=3 might lead to an event more powerful algorithm than r=2. This naturally leads to the challenge if an how anything can be achieved for r>3. The extension from r=2 to r=3 relied on properties of the arithmetic of the Eisenstein ring of integers $Z[\zeta_3]$, including the Law of Cubic Reciprocity. In this paper we present a generalization of our result for any odd prime r. The generalization is obtained by studying the properties of Gaussian and Jacobi sums in cyclotomic ring of integers, which are tools from which the r-th power Eisenstein Reciprocity Law is derived, rather than from the law itself. While r=3 seems to lead to a more efficient algorithm than r=2, we show that extending to any r>3 does not appear to lead to any further improvements. (Received February 26, 2007)