

1086-11-2809

**Kjell Wooding\*** (kjell@wooding.org) and **H C Williams** (williams@math.ucalgary.ca),  
Dept. of Mathematics & Statistics, University of Calgary, 2500 University Dr NW, Calgary, AB  
T2N1N4, Canada. *On computing solutions to  $fx^2 + gy^2 = m$ .*

Consider the problem of finding  $x, y \in \mathbb{Z}$  such that for a given  $m, f, g \in \mathbb{Z}^+$ ,  $fx^2 + gy^2 = m$ . Define  $t \in \mathbb{Z}$  to be a solution for  $t^2 \equiv -gf^{-1} \pmod{m}$ . In 1848, Hermite and Serret described an algorithm to solve for  $x$  and  $y$  when  $f = g = 1$  using convergents in the simple continued fraction (SCF) expansion of  $t/m$ . In 1908, Cornacchia suggested an algorithm that could solve the problem for any  $f$  and  $g$  using only the remainders in the Euclidean Algorithm applied to  $t$  and  $m$ . An elementary exposition (due to Nitaj) proving the correctness of Cornacchia's algorithm did not follow until much later, and relied on a modified version of the algorithm which again requires finding the convergents in the SCF expansion of  $t/m$ . Our work shows that these convergents can be recovered, via elementary methods, from the sequence of remainders used by Cornacchia's original algorithm. (Received September 25, 2012)