ICM-9307-55 The Accelerated Integer GCD Algorithm, Ken Weber.

ABSTRACT The accelerated integer gcd algorithm is based on a reduction step proposed by Sorenson (k-ary reduction), coupled with the dmod operation similar to Norton's smod. Some practical limitations of Sorenson's reduction have been eliminated. Worst case complexity is still $O(n^2)$ for n-bit input, but actual implementations given input about 4096 bits long perform over 5.5 times as fast as the binary gcd on one computer architecture having a multiply instruction. Independent research by Jebelean points to the same conclusions.