

Re: A benchmark comparing ECM and triangle number factoring.

Ps

ECM is still cranking after 3hrs and 15 minutes and >still only showing that the 617 digit is a composite. What gives?

ECM will factor arbitrary composites. Your composite is >far from arbitrary. Can your algorithm factor RSA120? Nowadays, ECM can. (Not that you'd want to, of course.)

No, not with just one computer I would not even attempt it. I just did this as a benchmark test. With many computers starting at different sums and indexes it could be realized. Running so as to not overlap one another.

Normally ECM will handel smaller semiprimes of this nature but my method still wins out against ECM for these type of semi-primes.(ratio slightly \diamond 2)

As I read somewhere as an analogy to factor rsa2048 it would be like searching for one discrete grain of sand in the universe and that grain of sand if found would be one of the factors.

Phil

—

The fact that a believer is happier than a sceptic is >no more to the point than the fact that a drunken man is happier than >a sober one. The happiness of credulity is a cheap and dangerous >quality.
— George Bernard Shaw (1856–1950), Preface to >Androcles and the Lion

.