CUNNINGHAM CHAINS MINING

PASCAL GIORGI, LAURENT IMBERT, BASTIEN VIALLA
ÉQUIPE ARITH, LIRMM, MONTPELLIER

Context

Problems and puzzles involving prime numbers have always fascinated humans. A Cunningham chain (of the first kind) is a sequence of the form $p, 2p+1, 4p+3, \dots$ such that each term in the sequence is prime. Similarly, sequences of primes built using the relation $p_{i+1} = 2p_i - 1$ are known as Cunningham chain of the second kind.

Following Dickson's conjecture, it is widely believed that for every k there are infinitely many Cunningham chains of length k. Apart from proving this conjecture, there exists various interesting challenges associated to Cunningham chains. For example, one may want to find the largest prime starting a chain of a given length. Another interesting problem consists in finding Cunningham chains of longest length ; a problem which has recently been proposed as the setting for primecoin mining, a mining process associated to a virtual money similar to bitcoin.

Internship project

Investigating efficient algorithms and implementations for addressing the above challenges is the main objective of the internship project. The algorithms involved are related to sieving techniques, primality proving and the associated arithmetic primitives. If time permits, highly optimized implementation of the proposed algorithms on GPU and/or multi-core processors will also be considered.

Links

http://primecoin.org
http://primecoin.org/static/primecoin-paper.pdf
http://primes.utm.edu/glossary/page.php?sort=CunninghamChain
http://users.cybercity.dk/~dsl522332/math/Cunningham_Chain_records.htm
http://en.wikipedia.org/wiki/Cunningham_chain