

Re: Factoring using Lehman's method

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-01/8836.html>

From: Phil Carmody (*thefatphil_demunged_at_yahoo.co.uk*)

Date: 01/31/05

Date: 31 Jan 2005 02:00:11 +0200

Christian Bau <christian.bau@cbau.freemove.co.uk> writes:

> *I am trying to implement Lehman's factoring method, which is probably
> the simplest method that is faster than trial division.*

Pollard P-1 and Pollard Rho (including Brent's version thereof) are at least as simple.

> *I found a small
> amount of info on the internet, so what I have now to factor N is this:
>
> 1. Make sure N has no prime factors $\leq N^{1/3}$
> 2. Find x, k such that $x^2 - 4kN$ is a square; this leads quickly to a
> prime factor of N.
> 3. If enough values x, k have been tried without finding a factor
> then N is prime.
>
> The clever part of the algorithm is that the only values of k and x that
> are considered are $1 \leq k \leq N^{1/3}$, and
>
> $x = \text{ceil}(\text{sqrt}(4kN)) + m$
>
> for integers $m \geq 0$ where $m^2 * k \leq N^{1/3}$; so this requires that
> about $2.6 * N^{1/3}$ values are tried, and there is a proof by Lehman
> that if this doesn't find a prime factor of N, then there are none.
>
> I tried for a huge range of products of moderately sized primes that
> this will (1) actually find a solution, and that (2) the whole range
> actually has to be searched, otherwise factors will be missed. Then I
> tried what happens if I start by excluding prime factors up to say $2 * N^{1/3}$
> first, and it seems that I can always find factors by searching
> through a much smaller range, which would speed up the method by
> slightly more than a factor 2 (if I can prove that it works).
>
> Experimentally, it seems that if I find all prime factors $\leq (c*N)^{1/3}$
> for $1 \leq c \leq 4$, then I only need to consider values k, $m^2*k \leq (N / c^2)^{1/3}$. This will be fun to prove.
>
> Question: Are there any known results about this? (Lehman's method was*

sci.math: Re: Factoring using Lehman's method

> *published in 1974, and I could find only one article describing the*
> *method at all).*

Check Crandall & Pomerance's /Prime Numbers, a Computational Perspective/.
They work through the proof of work-factor for the usual version, perhaps
their proof can be simply adapted for your alterations.

Phil

--

If a religion' is defined to be a system of ideas that contains unprovable
statements, then Godel taught us that mathematics is not only a religion, it
is the only religion that can prove itself to be one. -- John Barrow