Progress report on a Wilson prime search

David Harvey
(with Edgar Costa and Robert Gerbicz)

University of New South Wales

10th July 2012, ANTS X, UC San Diego

Wilson primes

For prime p, define the Wilson quotient

$$w_p = \frac{(p-1)! + 1}{p}.$$

Wilson's theorem:

$$w_p \in \mathbf{Z}.$$

A *Wilson prime* is a prime with $w_p = 0 \pmod{p}$.

Equivalently

$$(p-1)! = -1 \pmod{p^2}.$$

Previous work

Only known Wilson primes: 5, 13, 563.

Crandall–Dilcher–Pomerance (1997): no others for

$$p < 500\,000\,000.$$

Carlisle–Crandall–Rodenkirch (2008, unpublished):

$$p < 6\,000\,000\,000.$$

Heuristically

$$\#\{\text{Wilson primes } p < x\} \sim \sum_{p<x} \frac{1}{p} \sim \log\log x.$$

This does go to infinity... but very slowly.

Algorithms for computing w_p

- Naive:

$$O(p^{1+o(1)}) \text{ bit operations.}$$

- Baby-step/giant-step (Strassen):

$$O(p^{1/2+o(1)}) \text{ bit operations.}$$

- New algorithm: compute w_p for all $p < N$ using only

$$O((\log p)^{4+o(1)})$$

bit operations per prime on average. **Polynomial time!**

Current computation

At this moment running on 500–1000 cores at NYU & UNSW.

We have checked all

$$p < 1\,000\,000\,000\,000$$

and larger p in some intervals.

Goal:

$$p < 10\,000\,000\,000\,000.$$

About 8% chance of success for $10^{12} < p < 10^{13}$.

p	w_p	
11 774 118 061	-1	(largest known p with $\lvert w_p \rvert = 1$)
1 239 053 554 603	-4	(smallest known nonzero $\lvert w_p / p \rvert$)

Table: Some close calls

Another announcement

Our new exascale machine arrived about 7 weeks ago:

Jesse Oliver Harvey