Meeting with Dr Paul Leyland

Project Lima

18th February 2003 3:30 - 4:30 pm

Attendance: Dr Paul C Leyland, all group memebers

Dr Paul Leyland is a researcher at the Microsoft Research Ltd at Cambridge. He is a leading expert in Computational Number Theory among other fields, more specifically in the areas of integer factorisation and primality testing.

http://research.microsoft.com/~pleyland

1 Introduction to Project Lima by group memebers

2 Feedback and Suggestions from Dr Leyland

2.1 Optimising Gaussian Elimination

- Efficiency benchmark: If elimination takes more than 1% of sieving time - consider it inefficient.
- Over-sieving: Collecting about 5-10% more relations than the minimum required to make the matrix. This reduces elimination time.
- Dirty Singleton removal: exoploiting bitmap and heap.
- A 'Structured Gauss' implementation.
- Filtering and Merging: filtering out singletons, merging doubletons.
- Make matrix smaller and denser.

2.2 Server

- Distribution of Block Lanczos is non-trivial. For a 10,000 square matrix, it is better not to distribute it.
- Server must ensure primes are not repeated in the matrix reduction phase.
- Consider how to deal with rogue clients.

3 Recommended books and resources

- Prime Numbers and Computer Methods for Factorisation – Hans, Riesel
- An FFT Extension of the Elliptic Curver Method of Factorization – P.L.Montgomery
- MPQS 4 Linux, HGPL code, University of Bonn
- T Kleinjun
- H Franke