Minutes
18/01/2003, 12:00pm

ATTENDENCE: All present

TOPICS DISCUSSED

1. Issues concerning the BigInt Library
    - Two-fold approach for the testing of the BigInt Package:
        - Comparing against the Fortran Suite
        - Multiplying results and checking against original numbers -> verification.
    - Since the Project Briefing Booklet has not undergone much change since the year 2000, there might have been numerous discrepancies in the package; since then, Java BigInt package has considerably improved and perhaps most bugs removed (JCE)

2. How to show that our arithmetic is being performed correctly given exhaustive proof is not achievable:
    - Test that our program works fine with relatively small primes
    - Use more than one primality checker

3. Finding ALL factors
    - Write our own primality checker
    - Check for small numbers. If a number is found to be ?small?, implement factorization locally on server
    - Trial Division for factors up to 8 digits (?small? numbers) using Sieve of Eratosthenes
    - Pollard Rho for up to 16 digits
    - For large numbers, distribute on network
    - Quadratic Sieve is perhaps the easiest and most efficient to implement in our range of ?large? numbers
    - Network latency is very expensive, should take it into account during initial design phase, rather than trying to optimize later on.
    - Black-box design.
    - Extensive modules.

4. Documentation
    - Make resource links on our webpage, collecting all reference material that we use
    - Programmers will document codes as they go along

- Finalise requirement specification first as a group, rest of the documentation can be done by Java doc
- Possibly employ UML specification

5. Role delegation
    - Please refer to LIMA 2003 Organisation Chart

TO DO / AGENDA for Tuesday Meeting:

- Are Pollard Rho and Quadratic Sieve classified as ?probablistic??
- Primality checking methods
- Further study of factorisation algorithms, in particular Pollard Rho, Quadratic Sieve.
- Requirement Specification and module Design (meeting with Ross Anderson set for 3pm on Wednesday 29th!)