ANC Associate Team

Report for 2009 and Plans for 2010

1 Report for 2009

Visits of Richard Brent and Judy-anne Osborn at LORIA in April-May

Richard Brent and Judy-anne Osborn visited LORIA from April 27 to May 9. Judy-anne gave a talk on the Hadamard maximal determinant problem. Richard and Judy-anne worked together with Paul Zimmermann on that problem (in particular a first version in C of the Gram searching program was written, and a first prototype in Maple of the Gram decomposition program); this work was also done in touch by email with Will Orrick from Indiana University. Richard Brent and Paul Zimmermann also worked on the book "Modern Computer Arithmetic" and on their trinomial project.

On the same trip, Richard Brent and Judy-anne Osborn visited ENS Lyon for one week to work with Nicolas Brisebarre, and various places in UK (Queen Mary, Oxford etc).

Visit of P. Zimmermann at ANU in July

Paul Zimmermann visited ANU from July 1st to 30th. This visit was mainly devoted to the Hadamard maximal determinant problem, with two goals:

- improve the search program for candidate Gram matrices (in the C language);
- write an implementation in C of the Gram decomposition program.

Paul Zimmermann mainly worked on the first task, with many interactions with Richard Brent, Judy-anne Osborn, and Will Orrick (by email). Many versions of the search program were written, and we believe the current version is quite good, given the state of the theory. In particular, the current version can be run in parallel on several nodes of a cluster. Richard Brent mainly worked on the second task, and the current decomposition program is very efficient too. This enabled us to get new results for sizes $n = 19$ and $n = 37$ (see below).

Paul Zimmermann also gave a conference on the book "Modern Computer Arithmetic" at the MSI Colloquium, and two short talks on the Hadamard maximal determinant problem.

Visit of Shi Bai at LORIA in October-November

Shi Bai (PhD student at ANU) will visit LORIA from October 22nd to November 21st. Since this visit did not start yet, here is a preliminary workplan. Shi Bai will consider the large prime variations in the number field sieve algorithm for the discrete logarithm problem. The main work is to implement such algorithm based on existing implementations (CADO-NFS).

The analytic estimates of the large prime variations (using line sieve) follow the previous work based on the extended Brujin function on semismooth numbers. This gives an asymptotic formula for the number of semi-smooth integers with large primes. Next, incomplete (partial or partial-partial) relations can be combined to full relations.

The main work is to modify the existing implementation (CADO-NFS) for the discrete logarithm problems and consider its performance on one large prime and two large primes variations. The major modifications would be two parts:

1. Implement the character map used in NFS for DLP;

2. Modify the linear algebra part over a finite ring.

Shi Bai will start to look at the CADO-NFS code before his visit. The implementation may take three weeks and he hopes to produce a report in the final week of his visit.

Scientific Results

As announced in the 2009 workplan, we have completed the search for primitive trinomials of degree 43112609 over GF(2)[x], with the help of computational resources provided by TU Eindhoven; we found four primitive trinomials. We have also conducted a similar search for degree 42643801, a new Mersenne exponent found in the meantime, which revealed five primitive trinomials.

In 2009, we have cleaned up the BMtR tables up to composites of 146 digits. We have also factored $2^{1790}+1$ (156 digits) in December 2008, $3^{527}-1$ (160 digits) in June 2009, and $2^{1105}-1$ (158 digits) in July 2009, all using CADO-NFS.

For the Hadamard Maximal Determinant problem, we have obtained the following results:

- for size $n = 19$, we have proved that the maximal determinant is $833 \cdot 4^6 \cdot 2^{18}$, which was the best value previously known. This result was obtained by running our search program for candidate Gram matrices with that bound. The search program, run in parallel on 50 machines, found 9 candidate matrices in 188 hours. From those 9 candidate matrices, only two decompose; this later result was obtained with the decomposition program written by Richard Brent. This result closes the question for $n = 19$.

- similarly for $n = 37$, we have proved that the maximal determinant is $72 \cdot 9^{17} \cdot 2^{36}$. Our search program found 807 matrices with determinant larger or equal to that bound (after 78 hours of computation), from which only one matrix was shown to be decomposable. This closes the search for $n = 37$ too.

Publications

Judy-anne Osborn has presented the progress done on the maximal determinant matrices at the Annual Australian Mathematical Society Meeting in Adelaide on October 1st, 2009.

Richard Brent and Paul Zimmermann were invited by Steven Krantz, new Editor-in-Chief of the Notices of the AMS, to submit an article to the Notices. The article entitled "The Great Trinomial Hunt" is almost finished.

As planned, two new versions of the book "Modern Computer Arithmetic" were produced: Version 0.2.1 in March 2009 (215 pages), and Version 0.3 in June 2009 (221 pages). This last version was submitted to a publisher, and the reviews were sent back to the authors. Some work is still needed to address the reviewers comments. We expect to have a revised version around the end of 2009.

Organization and Funding

As planned, we have contacted NICTA to try to get additional funding. Richard Brent has sent a mail to Bob Williamson, the scientific director of NICTA, but got no answer. He then contacted Sylvie Thiebaux from ANU/NICTA who talked to NICTA's international relations office. Their answer was that "NICTA only plans to fund equipes associees applications by teams of NICTA researchers (or university researchers that are contributed to NICTA) that have a direct alignment with NICTA's research." Unfortunately, our equipe associee does not fall into that camp.

For 2010, ANU has budgetted 10000 AUD to support the maximal determinant workshop (that is about 6700 EUR).

2 Plans for 2010

Funding and Scientific Animation

Since the contact with NICTA did not succeed, we will continue to support our associate team with the support of INRIA and Richard Brent's ARC grant.

In 2010 we intend to have a workshop on the Hadamard maximal determinant problem, in the second half of May 2010. This will be funded by ANU and any other sponsors that we can find (we did try NICTA, but apparently the topic was not of sufficient interest to NICTA).

Scientific Objectives and Computational Projects

Integer Factorization. We plan to study how the Number Field Sieve (NFS) can be used in practice for the discrete logarithm problem (DLP), in particular adapting the CADO-NFS code base to the DLP (this will start with hi Bai's visit in October/November 2009). Both teams plan to continue extending the Cunningham and BMtR (Brent-Montgomery-te Riele) factorization tables using GMP-ECM and CADO-NFS. In particular, one goal is to factor all remaining composite numbers up to 155 digits.

Modern Computer Arithmetic. In 2010, we plan to submit the final version of this book to a publisher. Hopefully the book will appear in 2010.

The Hadamard Maximal Determinant problem. We will continue our work on that problem, in collaboration with Will Orrick (Indiana University). In particular we expect to be able to organize a workshop on that topic at ANU in May 2010.

Visits

Paul Zimmermann plans to visit ANU in May 2010, to attend the planned workshop on maximal determinant matrices. Sylvain Chevillard (new postdoctoral fellow at LORIA) plans to visit ANU by the end of 2010. He intends to work (mainly with Richard Brent) on subjects related to the evaluation of functions in arbitrary precision. These works will benefit the MPFR library, supported and actively developed by the CACAO team. The expected results are:

- direct contributions to the source code of the library;

- introduction and/or generalization of the use of new techniques in MPFR (e.g., continued fractions, summation techniques, asymptotically optimal algorithms, etc.)

A PhD student of the CACAO team might also visit ANU.

We also plan two visits to LORIA from members of the ANU group (Paul Leopardi, Judy-anne Osborn, Richard Brent, Joerg Arndt, Shi Bai, Srinivas Subramanya).