ANC Associate Team

Report for 2008 and Plans for 2009

1 Report for 2008

Visit of Joerg Arndt at LORIA in April-May

Joerg Arndt did visit the CACAO team in Nancy from April 28 until May 24. His work was on Rabin's irreducibility test for polynomials over finite fields. The results obtained, as described in the research report RR-6542 [5], were as follows: If the degree of the polynomial is a prime, a prime power, or the product of two primes, then the GCD computation can be omitted if linear factors can be excluded (Theorems 1 and 2 of the report). A further result was that if the degree d is of the form $d = r^e \cdot s$ where r and s are primes then the GCD computation can be omitted if d is greater than a certain bound that depends on the characteristic of the ground field (Theorem 3 of the report). He also presented a previous work on finding optimal relations to evaluate π using a sum of rational arc-tangents.

Visit of A. Kruppa and P. Zimmermann at ANU in June

A. Kruppa and P. Zimmermann visited ANU from June 1st to 15th. This visit was organized in the context of the associate team "Algorithms, Numbers, Computers" (`http://www.loria.fr/~zimmerma/anc.html`) sponsored by INRIA and ANU (in particular Richard Brent's Federation Fellowship paid the accomodation, which we want to acknowledge here). This associate team started in 2008, with a first visit of Joerg Arndt from Richard Brent's group in France in April-May.

The goals of this visit were:

- for Alexander Kruppa (AK), to make a first contact with the members of Richard Brent's group, and to present his recent work on the P-1/P+1 integer factoring methods;
- for Paul Zimmermann (PZ), to make progress on the book in preparation with Richard Brent [6];
- for both, to identify potential collaborations between the members of Richard Brent's group and the CACAO team in Nancy.

The group of Richard Brent at ANU/MSI (which is part of the Computational Mathematics Program[1]) consists of the following people:

- Richard Brent (`http://wwwmaths.anu.edu.au/~brent/`) is the big chief. He works on many topics, in particular the book "Modern Computer Arithmetic" [6];
- Paul Leopardi (`http://wwwmaths.anu.edu.au/~leopardi/`) has a postdoc position (in Australia such positions are for several years) and his research interests include empirical testing of pseudo-random number generators, approximation on the sphere, object-oriented numerical analysis, applications of ScaLAPACK, Clifford algebras with links to Hadamard matrices

[1] `http://wwwmaths.anu.edu.au/research.groups/advcomp/people.db.html`

(see below). His PhD was on "Distributing points on the sphere: Partitions, separation, quadrature and energy".

- Judy-anne Osborn (`http://wwwmaths.anu.edu.au/~osborn/`) is interested in particular in Hadamard matrices of maximal determinant (see below).
- Joerg Arndt (`http://wwwmaths.anu.edu.au/~arndt/`), PhD student, he is among other things the author of the famous FXT book [7];
- Shi Bai (`http://people.cecs.anu.edu.au/user/3337`), new chinese PhD student, who is working on ECM (see also `http://cecs.anu.edu.au/seminars/showone.pl?SID=634`);
- Srinivas Subramanya Rao (`http://wwwmaths.anu.edu.au/~subrmnya/`) is a new indian PhD student, working on pairings;
- last but not least, Jim White is interested in smooth triangular numbers and the efficient numerical evaluation of mathematical functions.

On the first week, PZ gave a introductory talk to ECM, where several people (outside Richard's group) attended. In particular there was a guy from the Defence Dept who seemed to know quite well how ECM works. On the 2nd week, AK gave a talk on the new P-1/P+1 algorithm he designed with Peter Montgomery.

During the stay A. Kruppa had the opportunity to meet the members of Prof. Brent's group. One of Brent's postgraduate students, Shi Bai, was particularly interested in the P-1, P+1, ECM factoring methods, and AK and him hope to discuss them in more depth during his planned visit to Nancy next year. AK also discussed the selection of suitable elliptic curves for the Elliptic Curve Method (ECM) with Prof. Brent, pointing out unexpected slight differences in the effectiveness of some of the curves he proposed for ECM, which might be used for improving curve selection for this algorithm.

PZ and AK also attended several talks organized at MSI. There was in particular an interesting talk of Keith Matthews on the link between "nearest square continued fractions" and Pell's equations, in addition to the two colloquium talks (one of Amnon Neeman, and one from Chris Bose). Some informal discussions and presentations were also organized: one from Judy-anne Osborn and Paul Leopardi on Hadamard matrices, and one from Srinivas on exponentiation.

Hadamard matrices. Consider a $n \times n$ matrix with 0,1 entries. You want it to have a maximal determinant. This is sequence A003432 from Sloane's Encyclopedia: 1, 1, 2, 3, 5, 9, 32, ... The maximal determinant corresponds to the maximal volume of a region with integer vectors in $[0, 1]^n$. There is a correspondence that allows to go to matrices with (-1,1) entries, then each vector has norm $\sqrt{n}$, thus the maximal determinant is $n^{n/2}$. Hadamard matrices are those attaining this bound. Hadamard's conjecture is that such a matrix exists for n=1, 2, or n = 0 (mod 4). This was checked up to n = 664. A Hadamard matrix H satisfies H * transpose(H) = n * Id. There are several constructions that allow to construct Hadamard matrices. The simplest one from Sylvester allows you to construct a (2n)x(2n) matrix from an nxn matrix. Williamson's construction builds a (4n)x(4n) matrix from four nxn matrices (which do not have to be Hadamard matrices). This was used to solve the case n=92 and others for larger n. Judy-anne Osborn designed a Williamson-like scheme (which turned out to be already known) which allows to construct Hadamard matrices of order 8n from 8 matrices of order n. It turned out that the 8x8 construction matrix looks very much

like the multiplication table of the octonion (`http://en.wikipedia.org/wiki/Octonion`). Then it was clear that Sylvester's method corresponds to the complex numbers, Williamson's one to the quaternions, and Williamson-like to the octonions. With Richard Brent, using computer search and theoretical arguments, Judy-anne proved that these are the only possible similar constructions (again, this was known but not well-known). Paul Leopardi also presented his work on the subject, with an informal presentation on a Clifford algebra construction for Hadamard matrices. His approach is quite different. Starting from m matrices A_1, ..., A_m of order n, and m matrices B_1, ..., B_m of order p, with some technical conditions that we omit for brevity here, he constructs a Hadamard matrix of order np. The nice thing of his construction is that he not only allows submatrices to satisfy $X\mathrm{tr}(Y) = Y\mathrm{tr}(X)$, but also $X\mathrm{tr}(Y) = -Y\mathrm{tr}(X)$. When $m = n$, there is a link with Clifford algebras, and his framework enables one to find Williamson construction (check done during the visit for Williamson-like).

Visit of R. P. Brent and P. Leopardi at LORIA in October

Richard P. Brent visited INRIA 6-17 October 2008 in order to attend the joint CADO-ANC workshop "Recent Advances on Integer Factorization" 7-9 October and "Sage Days 10" 10-15 October. He also attended the Habilitation defense of P. Gaudry (8 October) to learn about cryptographic aspects of higher-genus curves. During the visit he discussed progress on the book "Modern Computer Arithmetic" [6] with Paul Zimmermann. They discussed the current search for high-degree primitive trinomials with Dan Bernstein (Illinois), Tanja Lange (TUE), and Emmanuel Thomé. A new version of the `gf2x` package was released to incorporate improvements and bug fixes. They also discussed irreducibility testing and the connection with modular composition and matrix multiplication over GF(2) with Martin Albrecht and Greg Bard (visitors for Sage Days).

Paul Leopardi visited LORIA from October 9 to October 15. During this visit, he attended Sage Days 10 at LORIA and there, during the "coding sprint" part, he coded an interface from Cython to the GluCat library for Clifford Algebras.

Scientific Animation

Two scientific events were organized in October 2008 in the context of the associate team:

- the CADO workshop on integer factorization (October 7-9, `http://cado.gforge.inria.fr/workshop/`) attracted at LORIA 52 participants worldwide on this quite hot topic, especially on the Number Field Sieve. The participation of Richard Brent was partially supported by the Associate Team program. During this workshop, some discussions started with Tanja Lange and Dan Bernstein about the search for primitive trinomial of degree 43112609 (see below).

- the Sage Days 10 (October 10-15, `http://wiki.sagemath.org/days10`) attracted at LORIA about 80 participants worldwide, from which about 40 stayed for the "coding sprints" (October 13-15). The participations of Paul Leopardi and Richard Brent were partially supported by the Associate Team program. During the coding sprints a collaboration started with the Sage developers about fast modular composition in GF(2)[x] (see above). Two invited speakers of Sage Days 10, namely Arne Storjohann and Éric Schost, were supported by the Associate Team.

Software and Computations

Two new versions (6.2 and 6.2.1) of GMP-ECM were released in 2008 on `http://gforge.inria.fr/projects/ecm/`. Among other new features, they implement the new P-1/P+1 algorithm from Montgomery and Kruppa.

A new version (0.3.1) of the `gf2x` library (developed by Richard Brent, Pierrick Gaudry, Emmanuel Thomé and Paul Zimmermann) was released in October 2008 (`http://wwwmaths.anu.edu.au/~brent/gf2x.html`); see reference [2] below. The `gf2x` library might be integrated in the Sage system in the future.

After the discovery of the new Mersenne prime $2^{43112609} - 1$ in September 2008, a search for primitive trinomials of degree 43112609 over GF(2) has been started, so far only on the ANU side, Grid 5000 on the french side being busy with the sieving for RSA-768. A collaboration with Eindhoven (Lange, Bernstein) started on this topic at the CADO workshop (see above).

Several numbers from the Brent-Montgomery-te Riele table were factored in 2008, with the CADO-NFS software (see `http://cado.gforge.inria.fr/news.en.html`). The largest one is a cofactor of $13^{181} + 1$, with 141 digits, with two factors of 70 and 72 digits:

$$p_{70} = 44123325908201861270818214520868675428136635037843465849680249012778 01$$

$$p_{72} = 10462879994506732346963142659182511152670525252399514258475075357979 6999$$

Publications

[1] Shi Bai and R. P. Brent, On the efficiency of Pollard's rho method for discrete logarithms, The Australasion Theory Symposium (CATS2008), Australian Computer Society, 2008, 125-131.

[2] R. P. Brent, P. Gaudry, E. Thome and P. Zimmermann, Faster multiplication in GF(2)[x], Proc. ANTS-VIII (Banff, May 17-22, 2008), Lecture Notes in Computer Science, Vol. 5011, Springer-Verlag, 2008, 153-166. Also INRIA Tech. Report RR-6359, Nov. 2007, 19 pp.

[3] R. P. Brent and P. Zimmermann, A multi-level blocking distinct-degree factorization algorithm, in Finite Fields and Applications: Contemporary Mathematics, Vol. 461, American Mathematical Society, 2008, 47-58.

[4] R. P. Brent and P. Zimmermann, Ten new primitive binary trinomials, Mathematics of Computation, to appear. Posted electronically 1 August 2008.

[5] Joerg Arndt, Testing polynomial irreducibility without GCDs, Research Report RR-6542, 9 pages, http://hal.inria.fr/inria-00281614, 2008.

[6] Modern Computer Arithmetic, Richard Brent and Paul Zimmermann, version 0.2, June 2008, http://www.loria.fr/~zimmerma/mca/mca-0.2.pdf.

[7] Algorithms for programmers, Joerg Arndt, work in progress. http://www.jjj.de/fxt/#fxtbook, 986 pages as of October 11, 2008.

2 Plans for 2009

Organization and Funding

Richard Brent will contact NICTA to see if additional support for the associate team can be obtained for 2010 and after.

In 2009, we will try to use alternate communication means like IRC meetings or videoconferences, in addition to traditional visits.

Scientific Objectives and Computational Projects

Integer Factorization. Both team 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.

Primitive Trinomial Search. We plan to continue the search for primitive trinomial of degree 43112609 over GF(2)[x]. Hopefully, this work will be finished in 2009, with additional computational resources provided by TU Eindhoven. We also plan to improve the algorithm used for that search, using fast modular composition (following discussions with Éric Schost, and in collaboration with Martin Albrecht).

Modern Computer Arithmetic. In 2009, we plan to publish a new version of the book [6], which should be ready to be published by a commercial publisher. Thus we will be looking for such a publisher.

The Hadamard Maximal Determinant problem. The Hadamard Maximal Determinant problem (that of finding maximal determinant matrices with entries drawn from the set $\{-1, +1\}$) is one with important applications in communications. This corresponds to sequence A003432 from the Encyclopedia of Integer Sequences. The so-called Hadamard orders, i.e., those which are multiples of 4, are extremely well-studied with the current smallest unknown size being 668. However amongst the non-Hadamard orders, those congruent to 1, 2 or 3 modulo 4, which are just as important in many applications, unknown orders include $19, 22, 23, 27$ and 29[2]. Even these small orders are well beyond the reach of a direct exhaustive computer search, however they are amenable to a specialized computer search based on Gram matrices. Essentially one searches first for matrices which could be the square of a max-det matrix, and then attempts to factor the candidate squares in a second computer search. The method goes back to Ehlich and Wojtas, also having been applied by Chadjipantelis, Kounias and Moissiadis. Judy-anne Osborn has previously worked on this problem with Dr Will Orrick of Indiana University, when they duplicated some of the results in the literature using Mathematica. It was clear to them at the time that there were many efficiencies that they could incorporate into their programs, as well as re-writing them in a compiled language such as C. Given their successes then, they became confident that properly optimized compiled programs would make currently unknown values accessible. We are particularly interested in the value for $n = 29$, as this is the smallest unknown order for which $n = 1 \bmod 4$, as its solution would pertain to a conjecture about the general pattern in this case. This would be an excellent project to work on in such a team, as it is achievable and draws upon the computational

[2] See `http://www.indiana.edu/~maxdet/`

and the number theory experience of the team, in particular the great expertise of Richard Brent and Paul Zimmermann. It also raises the potential for further international linkage, with Will Orrick in the USA.

Visits

Richard Brent plans to visit INRIA in March or April 2009 to continue collaboration on efficient finite-field arithmetic and applications to testing irreducibility of polynomials over finite fields. See also below about Hadamard/maximal-determinant matrices.

Joerg Arndt may visit in 2009; he is particularly interested in algorithms and finite fields.

Shi Bai may visit in 2009; his interests include elliptic curves and cryptography. He would like to consider some applications of the Edwards curve in cryptography and relevant algorithms in computation number theory. The recently introduced Edwards curve may be used to speed up the computations of some algorithms such as ECM and Schoof's algorithm for point counting. It is also interesting to consider faster invariants of cryptographic protocols based on Edwards curve.

Paul Leopardi may visit in 2009; his interests include: (1) Interfaces from Sage to GluCat (`sage-clifford`) and (with Joerg Arndt) from Sage to FXT (`sage-fxt`); (2) (with Judy-anne Osborn, Richard Brent, and members of Cacao) further development of Clifford algebra constructions for Hadamard matrices, including computer searches for such constructions; (3) (with Richard Brent and Paul Zimmermann) searches for primitive polynomials, lattices, spherical designs.

Judy-anne Osborn will probably visit at the same time as Richard Brent (March/April). She will work with Richard Brent and members of the Cacao team on a backtracking program to search for maximal-determinant matrices with ± 1 entries of order 29 (this may involve Sage).

Jim White may visit in 2009 (see what was proposed for 2008 re Størmer's Problem and Fast Evaluation of Trigonometric Functions).

Romain Cosset (PhD candidate in the Cacao team) is interested in hyperelliptic curves; in particular in genus 2 and 3. He is working on a generalisation with genus 2 curves of the algorithm ECM (elliptic curves method) for factorization and he will look at the real model.

Jérémie Detrey (new research scientist in the Cacao team) is working on the hardware implementation of arithmetic primitives, and more specifically on the use of hardware coprocessors to speed up the computation of pairings over (hyper-)elliptic curves. It might prove interesting to collaborate with Srinivas Subramanya Rao on this topic. He might also fruitfully interact with Jörg Arndt on the subject of low-level implementation and optimisation of finite-field arithmetic.