ANC
(ALGORITHMS, NUMBERS, COMPUTERS)

ANU-INRIA ASSOCIATE TEAM PROPOSAL

SEPTEMBER 2007

ABSTRACT. We propose to join the research efforts of Richard Brent's team at ANU (Australian National University, Canberra, Australia) with those of the CACAO team from the "Centre de Recherche INRIA Nancy-Grand Est" (Nancy, France) into an INRIA associate team called ANC (Algorithms, Numbers, Computers). We wish to extend in such a way a long-term and successful cooperation between Richard Brent and Paul Zimmermann to all members of both teams, in particular young researchers. The support of the ANC associate team will allow to reinforce that cooperation, especially in the common scientific projects outlined in this document.

1. Composition of the Associate Team

On the ANU side, the associate team[1] composition is the following:

- **Prof. Richard P. Brent**, ARC Federation Fellow (team leader, team contact on the ANU side);
- **Paul Leopardi**, Postdoctoral Fellow;
- **Judy-anne Osborn**, Postdoctoral Fellow;
- **Joerg Arndt**, PhD student;
- **Jim White**, Visiting Fellow.

On the CACAO side, the team composition is the following:

- **Guillaume Hanrot**, Research Director (team leader);
- **Pierrick Gaudry**, Research Scientist;
- **Emmanual Thomé**, Research Scientist;
- **Paul Zimmermann**, Research Director (team contact on the CACAO side);
- **Alexander Kruppa**, PhD student;
- **Damien Robert**, PhD student;
- **Philippe Théveny**, Associate Engineer.

[1]Cf `http://www-direction.inria.fr/international/EQUIPES_ASSOCIEES/index.eng.htm` (warning: on September 17, the english version was not completely up-to-date with respect to the french version). Deadline for application is October 19, 2007; the selection will be done on November 29, with announcement of results and funding for 2008 in December. In case of selection, the team should provide each year (mid-October) (a) a brief activity report including financial and scientific data for the current year; (b) a brief description of the work program with a provisional budget for the year to come; (c) a description of previously and recently obtained co-funding. An in-depth external scientific evaluation of each Associate Team is to be scheduled after three years of operation, i.e., end of 2010.

2. Previous Collaborations

A strong collaboration started in 2000 between R. Brent — who at that time worked at OUCL (Oxford University Computing Laboratory) — and P. Zimmermann. This collaboration was reinforced thanks to regular visits, which were funded by R. Brent's grants on the Oxford and ANU sides, and by INRIA for P. Zimmermann:

- P. Zimmermann visited R. Brent in Oxford in 1999, and gave an invited talk at the workshop *Computational Number Theory* organized by R. Brent within the FoCM'99 conference (*Foundations of Computational Mathematics*);
- R. Brent visited the CACAO team (which was the SPACES team at that time) two months in August and September 2001;
- P. Zimmermann visited R. Brent in Oxford in August 2002;
- R. Brent visited the CACAO team one month in August 2003;
- R. Brent visited the CACAO team one month in September 2004;
- in July 2006, R. Brent visited INRIA-Nancy Grand Est for two weeks — including the RNC7 conference organized by the CACAO team where he gave an invited talk — before leaving together with P. Zimmermann to Berlin, where they participated to the workshop organized for the 60th birthday of R. Brent, to the ANTS 7 conference, and to the Ecrypt and Magma workshops organized after that conference (J. Arndt, G. Hanrot, and A. Kruppa also participated to some of those scientific events);
- in February 2007, P. Zimmermann visited ANU for 10 days, where he participated together with R. Brent to the 2nd Workshop on High-Dimensional Approximation (HDA07);
- in May 2007, R. Brent visited INRIA-Nancy Grand Est for 2 weeks.

Since the return of R. Brent to Australia, funding such regular visits is more expensive. Our aim is to keep alive this strong collaboration in the future, and to extend it to all researchers of the ANU and CACAO teams, in particular young researchers (PhD students, postdocs). To strenghten this collaboration, at least two or three visits per year from each side would be desirable. This is the main reason why we apply to the "associate team" funding.

2.1. **Primitive Trinomial Search.**

The search for large-degree primitive trinomials over GF(2) started in 2000, together with Samuli Larvala [13]. The main motivation was to extend the previous records [8], and to reach that goal we had to implement efficient algorithms. The first results were published in 2003 for degree 3021377 [14]. We then switched to the next candidate degree $r = 6972593$. With the algorithm we used, of complexity $O(r^3)$, this search required a huge amount of computation time (about 3,000,000 cpu hours). We therefore requested cpu time at several institutions (ANU in Australia, CINES in France). This huge effort lead to the discovery of a new record primitive trinomial [15].

Other scientific contributions are related to this search: [4] describes some random generators using primitive trinomials, and [3] introduces "almost irreducible" and "almost primitive" trinomials, which enable one to get efficient arithmetic over GF(2^r) even in the case where no irreducible (thus primitive) trinomial of degree r exists, for example when 8 divides r.

---

[8] Kumada, T., Leeb, H., Kurita, Y., and Matsumoto, M. New primitive t-nomials ($t = 3, 5$) over GF(2) whose degree is a Mersenne exponent. *Mathematics of Computation 69* (2000), 811–814.

During the visit of P. Zimmermann at ANU in February 2007, a new algorithm was invented for the search for primitive trinomials over GF(2). This algorithm, of complexity $O(r^{2+o(1)})$ — instead of $O(r^3)$ for previous algorithms —, leads to a speedup of a factor of 560 for degree $r = 24036583$. Two new primitive trinomials of that degree were found in 2007. The new algorithm was presented at the Fq8 conference (Melbourne, Australia) in July 2007, and the full details will be submitted to a special issue of *Contemporary Mathematics*.

2.2. **Integer Factorization.** Integer Factorization is another topic with a strong common interest from both the ANU and the CACAO teams. Although there was formally no common publication so far, several major contributions were made on both sides, and more importantly many discussions, most of which per e-mail, were made on that topic.

On the theoretical side, R. Brent improved Pollard's ρ algorithm [9], and proposed several nice improvements of Lenstra's Elliptic Curve Method (ECM) [10].

On the experimental side, R. Brent implemented the ECM method in the FACTOR program [11]. With his ECM program, R. Brent factored the Fermat numbers $F_{10} = 2^{2^{10}} + 1$ and $F_{11} = 2^{2^{11}} + 1$ [12]. Several years later, P. Zimmermann started another implementation of ECM which is now the reference in that domain [21].

The other currently best-known algorithm for integer factorization is the Number Field Sieve (NFS). One of the major theoretical advances for NFS in the last 10 years was done in the PhD thesis of Brian Murphy, under the supervision of R. Brent [11]. This better polynomial selection algorithm was used in the factorization of RSA-140 [17] and RSA-155 [18]. The CACAO team is involved for 2007-2010 in a project funded by the French National Research Agency (ANR), whose main goal is precisely better understand — and possibly speed up — the Number Field Sieve algorithm[2].

2.3. **Floating-Point Arithmetic.** One of the first research interests of R. Brent was the design of efficient algorithms for the numerical evaluation of mathematical functions in arbitrary precision [5, 6, 7]. In parallel, R. Brent designed the Fortran MP package [8], which is still a reference in the domain. Members of the CACAO team share the same common interests for both theoretical algorithms and their efficient implementation. For example, they initiated the development of the MPFR library (within the PolKA and SPACES project-teams) [19], which can be viewed as a modern version of the MP package.

A new result about error bounds for complex floating-point multiplication was obtained with Colin Percival, one of Brent's PhD students [2]. Although only one common publication appeared so far in that domain, several discussions have already happened, in particular related to the book "Modern Computer Arithmetic" (see below).

In October 2005, the MPFR team (Laurent Fousse, G. Hanrot, Vincent Lefèvre, Patrick Pélissier, J. White and P. Zimmermann) took part in the "Many Digits" friendly competition organized by the group of Henk Barendregt at the University of Nijmegen, Netherlands[3]. The competition consisted in 24 real values, that had to be computed with the largest possible

[2]See `http://cado.gforge.inria.fr` (in french).

[3]`http://www.cs.ru.nl/~milad/manydigits/`

[11] MURPHY, B. A. *Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm.* PhD thesis, Australian National University, 1999. 144 pages.

precision (up to one million digits) in the least possible time. The MPFR team won that competition, where commercial software like Maple or Mathematica were also represented.

2.4. **Book "Modern Computer Arithmetic".** Since 2002, R. Brent and P. Zimmermann started writing a book "Modern Computer Arithmetic". It will contain four chapters, one on integer arithmetic, one on modular arithmetic, one on basic floating-point algorithms, and one on the evaluation of special functions. The first chapter is almost in final state, the last three needing more work to be done. A preliminary version of the book is available from the authors' web page [16].

3. Common Scientific Projects

3.1. **Smooth Triangular Numbers (Størmer's Problem).** *Participants: J .White, G .Hanrot.*

We are investigating a proposed new method for the multiple-precision computation of logarithms of integers. There is already a good algorithm (Arithmetic-Geometric Mean, or AGM) for the general case of real arguments. It may be possible, however, to compute the logarithms of integers much more quickly than via the AGM. To find $\log N$, the new method involves identifying suitable integers A and B that are both smooth (composed only of small prime divisors), and which minimise $|A - BN|$. Given suitable A and B, $\log N$ can be computed very efficiently using rational power-series summation methods. The degree to which A and B can be quickly found for arbitrarily large N is the main focus of our current work in this area, as this will largely determine the wider applicability of the method. The new method presents a simple problem for which very little is known in general. Given a fixed smoothness bound, p, then for arbitrary N we wish to find p-smooth integers A and B such that $|A - BN| \leq C$. When C is very small compared to N, the values A, B and N can be combined so that $\log N$ can be obtained with highly-convergent rational power-series summations.

This appears to be a new problem, at least in these terms. The closest case of a similar problem for which a solution is known is Størmer's problem, in which we seek simply those pairs of consecutive integers $(S, S + 1)$ where both are p-smooth. Since their product must also be p-smooth, this problem is equally stated as finding the p-smooth triangular numbers. For any given p, there are only a finite number of possible solutions - this was first proved by Carl Størmer in 1897. Størmer's proof was simple and constructive, and shows that all possible solutions will be found among the set of solutions to a (much larger) finite number of Pell equations, $x^2 - Dy^2 = 1$. Solving the Størmer problem is not itself a direct concern of the new method for computing $\log N$, but the problems are very closely related. In particular, the modelling of the "smooth pair" problem using Pell equations is currently the only systematic approach. Unfortunately the complexity of the solution grows exponentially in terms of the number of primes involved, so the number of primes for which complete enumerations can be obtained in reasonable time remains very small indeed.

The original algorithm of Størmer was refined by Lehmer [9], whose 1964 paper remains as a fairly self-contained treatment of available knowledge regarding the problem. There are other methods by which the problem might be approached, however. One approach in particular is suggested by Baker's theory of linear forms, and it is this connection which

[9] Lehmer, D. H. On a problem of Størmer. *Illinois Journal of Mathematics 8* (1964), 57–79.

led to a correspondence between J. White and G. Hanrot. The practical application of a "Baker-driven" approach to the Størmer problem is suggested in theory, but has not been done in practice. A collaborative effort to explore the problem is thus proposed. This would initially address the fundamental question: can this approach provide a practical alternative to the "Pell-driven" method of Størmer/Lehmer?

3.2. **Efficient Finite-Field Arithmetic.** *Participants: R. Brent, J. Arndt, P. Gaudry, A. Kruppa, E. Thomé, P. Zimmermann.*

It is critical for cryptographic and number-theoretic applications to have very efficient arithmetic in finite fields. The field GF(2^r) is of course a key case. So far, the reference implementation was the NTL library developed by Victor Shoup [13]. However, several case studies have shown some inefficiencies of NTL, both for very small fields (corresponding to one or two machine-words) or for very large fields (where fast algorithms like the FFT should be used). This was in particular the case for primitive trinomials (§2.1), where in the latest version of our search program, although still based on NTL, we had to rewrite by ourselves all critical operations: squaring, multiplication, gcd of polynomials modulo $x^r + x^s + 1$ in GF(2).

Since 2006, P. Gaudry and E. Thomé started to develop a new library (MPFQ) for the arithmetic over finite fields. During R. Brent's visit in Nancy in May 2007, some new algorithms were found for the base-case multiplication of binary polynomials. In the short term, we will write a paper explaining those new algorithms, together with some variants of Toom-Cook's algorithm in that case. This paper will be submitted to the ANTS 8 conference.

In the medium term, we expect that several discussions will happen with Gaudry, Thomé and Arndt about efficient bit-operations, around the MPFQ library and the on-line book "Algorithms for programmers" from J. Arndt [1].

3.3. **Fast evaluation of trigonometric functions.** *Participants: R. Brent, Ph. Théveny, J. White, P. Zimmermann.*

The efficient evaluation of trigonometric functions ($\sin, \cos, \tan$) is a key problem for developers of arbitrary precision libraries like MPFR. Since the Many Digits competition, several discussions arose between the team members. Different methods are available: for the argument reduction on may use formulae like $\cos(2x) = 2\cos^2 x - 1$, or $\sin(3x) = 3\sin x - 4\sin^3 x$; one could also use an additive argument reduction, by subtracting a multiple of (an approximation of) π. For the approximation of $\cos x$ or $\sin x$ around $x = 0$, one may use a classical (naive) Taylor series, or a baby step/giant step approach [12,14], or an extension of Brent's algorithm for the exponential [6, 16].

We plan to analyze in details several algorithms, which means comparing their asymptotic complexity, their range of usage (both in terms of precision and of input domain), and implementing them carefully in the MPFR library to compare them experimentally.

---

[13] Shoup, V. NTL: A library for doing number theory. `http://www.shoup.net/ntl/`.

[12] Paterson, M. S., and Stockmeyer, L. J. On the number of nonscalar multiplications necessary to evaluate polynomials. *SIAM J. Comput. 2*, 1 (1973), 60–66.

[14] Smith, D. M. Algorithm 693. a Fortran package for floating-point multiple-precision arithmetic. *ACM Trans. Math. Softw. 17*, 2 (1991), 273–283.

3.4. **Book "Modern Computer Arithmetic".** *Participants: R. Brent, P. Zimmermann.*

This book is a long-term project. The main goal is not only to describe the best algorithms at high-level, but really to work out the nasty details that make the difference between a rough description and a detailed pseudo-code that can be readily implemented by a programmer. Consider for example the fastest known algorithm for computing the GCD of two large integers. If the multiplication of two integers of n bits costs $M(n)$, then the best-known algorithms have complexity $O(M(n) \log n)$, and one can find high-level descriptions of them in several textbooks. However, only a few authors took the risk to give a *detailed* description of such an algorithm in the integer case. Indeed, the integer case is much trickier than the polynomial case, due to the problem of carries. To our best knowledge, the only textbook description of such an algorithm has such flaws [15].

This fundamental work pushed us to ask some questions that led to new algorithmic results. A first example is the careful study of the Toom-Cook 3-way algorithm, which led to the discovery of a simpler algorithm, that was released in GMP 4.2 [6]. This work in turn made other authors have interest into Toom-Cook 3-way, see for example the work of Bodrato and Zanoni [1], and that of Chung and Hasan [4]. Another example is the discovery (together with Damien Stehlé, who was a PhD student of P. Zimmermann) of a new 2-adic recursive GCD algorithm [20].

What remains to be done is the following:

- Chapter 1 (Integer Arithmetic). It is almost in final form, but requires a full pass to check coherence between the different notations and algorithms. The "Notes and further references" section needs to be completed.
- Chapter 2 (Modular Arithmetic and Finite Fields). Several important algorithms are still missing. Also the "Exercises" and "Notes and further references" sections need to be completed. We also have to decide whether we limit ourselves to arithmetic on prime fields, or if we deal with general finite fields of the form $\mathbb{F}_q$, q a prime power.
- Chapter 3 (Floating-Point Arithmetic). This chapter is well advanced, but several algorithms need to be rewritten or improved, and some "glue" text is missing. The "Notes and further references" section needs to be completed.
- Chapter 4 (Newton's Method and Unrestricted Algorithms for Elementary and Special Function Evaluation). This chapter made good progress in 2007, however some sections are still empty, and the "Exercises" and "Notes and further references" sections need to be completed.

Due to our previous experience, we prefer not to make precise plans for the progress of our book. However we will update the on-line preliminary version regularly until the book is published. This might prove useful to the scientific community.

---

[15] Yap, C. K. *Fundamental Problems in Algorithmic Algebra*. Oxford University Press, 2000.

[6] *GNU MP: The GNU Multiple Precision Arithmetic Library*, 4.2.2 ed., 2007. `http://gmplib.org/`.

[1] Bodrato, M., and Zanoni, A. Integer and polynomial multiplication: Towards optimal Toom-Cook matrices. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ISSAC'2007, July 29-August 1st, 2007* (Waterloo, Ontario, Canada, 2007), C. W. Brown, Ed., ACM, pp. 17–24.

[4] Chung, J., and Hasan, M. A. Asymmetric squaring formulae. In *Proceedings of the 18th IEEE Symposium on Computer Arithmetic (ARITH'18)* (2007), P. Kornerup and J.-M. Muller, Eds., IEEE Computer Society, pp. 113–122.

References

[1] Arndt, J. Algorithms for programmers. http://www.jjj.de/fxt/#fxtbook. Work in progress. 910 pages as of September 16, 2007.

[2] Brent, R., Percival, C., and Zimmermann, P. Errors bounds on complex floating-point multiplication. *Mathematics of Computation 76* (2007), 1469–1481.

[3] Brent, R., and Zimmermann, P. Algorithms for finding almost irreducible and almost primitive trinomials. In *Primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams* (Banff, Canada, 2003), A. van der Poorten and A. Stein, Eds., The Fields Institute, Toronto, pp. 91–102. Invited paper. Published by the AMS, 2004.

[4] Brent, R., and Zimmermann, P. Random number generators with period divisible by a Mersenne prime. In *Proceedings of Computational Science and its Applications (ICCSA)* (2003), no. 2667 in Lecture Notes in Computer Science, Springer-Verlag, pp. 1–10. Invited paper.

[5] Brent, R. P. Multiple-precision zero-finding methods and the complexity of elementary function evaluation. In *Analytic Computational Complexity* (New York, 1975), J. F. Traub, Ed., Academic Press, pp. 151–176.

[6] Brent, R. P. The complexity of multiple-precision arithmetic. In *The Complexity of Computational Problem Solving* (1976), R. S. Anderssen and R. P. Brent, Eds., University of Queensland Press, pp. 126–165.

[7] Brent, R. P. Fast multiple-precision evaluation of elementary functions. *J. ACM 23*, 2 (1976), 242–251.

[8] Brent, R. P. A Fortran multiple-precision arithmetic package. *ACM Trans. Math. Softw. 4*, 1 (1978), 57–70.

[9] Brent, R. P. An improved Monte Carlo factorization algorithm. *BIT* (1980), 176–184.

[10] Brent, R. P. Some integer factorization algorithms using elliptic curves. *Australian Computer Science Communications 8* (1986), 149–163. http://web.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub102.html.

[11] Brent, R. P. Factor: an integer factorization program for the IBM PC. Tech. Rep. TR-CS-89-23, Australian National University, 1989. 7 pages. Available at http://wwwmaths.anu.edu.au/~brent/pub/pub117.html.

[12] Brent, R. P. Factorization of the tenth Fermat number. *Mathematics of Computation 68*, 225 (1999), 429–451.

[13] Brent, R. P., Larvala, S., and Zimmermann, P. A fast algorithm for testing irreducibility of trinomials mod 2. Tech. Rep. PRG-TR-13-00, Oxford University Computing Laboratory, 2000. 13 pages.

[14] Brent, R. P., Larvala, S., and Zimmermann, P. A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377. *Mathematics of Computation 72*, 243 (2003), 1443–1452.

[15] Brent, R. P., Larvala, S., and Zimmermann, P. A primitive trinomial of degree 6972593. *Mathematics of Computation 74*, 250 (2005), 1001–1002.

[16] Brent, R. P., and Zimmermann, P. *Modern Computer Arithmetic*. Version 0.1.1, 2006. http://www.loria.fr/~zimmerma/mca/pub226.html.

[17] Cavallar, S., Dodson, B., Lenstra, A., Leyland, P., Lioen, W., Montgomery, P., Murphy, B., te Riele, H., and Zimmermann, P. Factorization of RSA-140 using the number field sieve. In *Advances in Cryptology, Asiacrypt'99* (Berlin, 1999), L. K. Yan, E. Okamoto, and X. Chaoping, Eds., vol. 1716 of *Lecture Notes in Computer Science*, Springer, pp. 195–207.

[18] Cavallar, S., Dodson, B., Lenstra, A. K., Lioen, W., Montgomery, P. L., Murphy, B., te Riele, H., Aardal, K., Gilchrist, J., Guillerm, G., Leyland, P., Marchand, J., Morain, F., Muffett, A., Putnam, C., Putnam, C., and Zimmermann, P. Factorization of a 512–bit RSA key. In *Proceedings of Eurocrypt'2000* (Bruges, 2000).

[19] Fousse, L., Hanrot, G., Lefèvre, V., Pélissier, P., and Zimmermann, P. MPFR: A multiple-precision binary floating-point library with correct rounding. *ACM Trans. Math. Softw. 33*, 2 (June 2007).

[20] Stehlé, D., and Zimmermann, P. A binary recursive gcd algorithm. In *Proceedings of the International Symposium on Algorithmic Number Theory - ANTS VI, Burligton, US* (2004), Lecture Notes in Computer Science, pp. 411–425.

[21] Zimmermann, P., and Dodson, B. 20 years of ECM. In *Proceedings of the 7th Algorithmic Number Theory Symposium (ANTS VII)* (Berlin Heidelberg, 2006), F. Hess, S. Pauli, and M. Pohst, Eds., vol. 4076 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 525–542.

4. Financial Details

The main expenses will be visits from one team members to the other team. We take as reference cost for the travel about 1600 Euros (including the possible car or train costs to reach the airport). For the local expenses, the "official" INRIA indemnity is 260 AUD (about 160 Euros per day), but 160 AUD seems to be enough (about 100 Euros per day), especially if Liversidge Court Apartments can be booked[4]. For a one month visit, we estimate 2400 Euros will be enough for the accomodation (80 Euros per day).

On the Nancy side, nice appartements are available at "Maison des Chercheurs" near the university campus, and at about 20 minutes from the city center by tramway[5]. The price of a studio is 600 Euros per month for a researcher, and 528 Euros for two weeks.

In the following we consider two kinds of visits, with the following costs:

- two-week visit, in general by a senior researcher: 3100 Euros (travel 1600, accomodation 1500);
- one month visit, in general by a junior researcher: 4000 Euros (travel 1600, accomodation 2400).

4.1. **Workplan for 2008.** In 2008, we plan the following events in the frame of the ANC team:

- a one-month visit of two ANU team members to Nancy (8000 euros);
- a two-week visit of one ANU team member to Nancy (3100 euros);
- a one-month visit of one CACAO team member to ANU (4000 euros)
- a two-week visit of one CACAO team member to ANU (3100 euros);
- an invitation of Arjen Lenstra (EPFL, Lausanne) for three days in Nancy (500 euros). A. Lenstra is one of the key researchers in integer factorization [3,2,5,10];

[4] `http://accom.anu.edu.au/UAS/189.html`

[5] `http://www.maison-des-chercheurs-nancy.imhotel.fr/index_en.php`

[3] Cavallar, S., Dodson, B., Lenstra, A. K., Lioen, W., Montgomery, P. L., Murphy, B., te Riele, H., Aardal, K., Gilchrist, J., Guillerm, G., Leyland, P., Marchand, J., Morain, F., Muffett, A., Putnam, C., Putnam, C., and Zimmermann, P. Factorization of a 512–bit RSA key. In *Proceedings of Eurocrypt'2000* (Bruges, 2000).

[2] Cavallar, S., Dodson, B., Lenstra, A., Leyland, P., Lioen, W., Montgomery, P., Murphy, B., te Riele, H., and Zimmermann, P. Factorization of RSA-140 using the number field sieve. In *Advances in Cryptology, Asiacrypt'99* (Berlin, 1999), L. K. Yan, E. Okamoto, and X. Chaoping, Eds., vol. 1716 of *Lecture Notes in Computer Science*, Springer, pp. 195–207.

[5] Cowie, J., Dodson, B., Elkenbracht-Huizing, R.-M., Lenstra, A. K., Montgomery, P. L., and Zayer, J. A world wide number field sieve factoring record: on to 512 bits. In *Advances in Cryptology – Asiacrypt '96* (Berlin, etc., 1996), K. Kim and T. Matsumoto, Eds., vol. 1163 of *Lecture Notes in Computer Science*, Springer–Verlag, pp. 382–394.

[10] Lenstra, A. K., Lenstra, H. W., and Lovász, L. Factoring polynomials with rational coefficients. *Mathematische Annalen 261* (1982), 515–534.

- an invitation of Thorsten Kleinjung (Univ. Bonn, Germany) for three days in Nancy (500 euros). T. Kleinjung did major recent advances in polynomial selection for the Number Field Sieve [7], and is also with Bahr, Boehm and Franke the holder of the current integer factorization record (RSA-200, 200 digits);
- Total for 2008: **19200 Euros**.

The three visits of the ANU members will be planned at the same time, together with the invitation of Arjen Lenstra and Thorsten Kleinjung, to organize a three-day workshop in Nancy on "Recent Advances in Integer Factorization".

4.2. **Workplan for 2009.** In 2009, we plan the following events in the frame of the ANC team:

- a two-week visit of two senior ANU team members to Nancy (6200 euros);
- a one-month visit of one CACAO team member to ANU (4000 euros)
- a two-week visit of two CACAO team members to ANU (6200 euros);
- the invitation of two major Australian scientists of the field to ANU (2000 euros);
- Total for 2009: **18400 Euros**.

The three visits of the CACAO members, and the two invitations of Australian scientists will be planned at the same time, to organize a three-day workshop at ANU.

4.3. **Workplan for 2010.** In 2010, we plan the following events in the frame of the ANC team:

- a two-week visit of two ANU team members to Nancy (6200 euros);
- a two-week visit of two CACAO team members to ANU (6200 euros);
- Total for 2010: **12400 Euros**.

4.4. **Workplan for 2011.** In 2011, we plan the following events in the frame of the ANC team:

- a two-week visit of one ANU team member to Nancy (3100 euros);
- a two-week visit of one CACAO team member to ANU (3100 euros);
- Total for 2011: **6200 Euros**.

[7] Kleinjung, T. On polynomial selection for the general number field sieve. *Mathematics of Computation 75* (2006), 2037–2047.