

Curriculum Vitae

Identification

First name : SEDJELMACI
Last name : Sidi Mohamed
Date and place of birth : 1955, May 14th, Tlemcen (Algeria)
Email : sms@lipn.univ-paris13.fr
Web page: <http://www-lipn.univ-paris13.fr/~sedjelmaci>

Education

- 1999 **Ph.D in Computer science.**
Thesis about " The parallel computation of the greatest common divisor of two integers".
Advisor : Christian Lavault, University of Paris 13, France.
- 1982 **Ph.D in Mathematics.**
Thesis about "A solution of hyperbolic partial differential equations systems".
Advisor : Jean Claude De Paris, University of Lille 1, France.
- 1978 **M.sc. in Mathematics**, University of Lille 1, France.

Employment

2010/–: Teaching mathematics at ESILV high school, Paris (France)
2008/2009: Reseach Assistant, LIPN, Université of Paris 13 (France)
2005/08: Teaching mathematics at Cours Legendre, Paris, (France)
2004/05: Teaching Assistant, at INSIA high school, Paris, (France)
2003/04: Teaching Assistant, Comp. Sc., Université of Créteil (France)
2002/03: Post-Doc, Comp. Sc., Université of Paris 13 (France)
2001/02: Post-Doc, Comp. Sc., Université of Cergy (France)
2000/01: Post-Doc, Comp. Sc., Université of Paris 13 (France)
1999/00: Post-Doc, Comp. Sc., Université of UTC, Compiègne (France)
1982/96: Assistant professor, Math. & Comp. Sc., Université of Oran (Algeria).

Teaching

I have more than 15 years teaching experience including pure and applied mathematics, numerical analysis, and in computer science as well.

Computer science: '99–

- Graduate level in several French universities: Cergy, Compiègne and Paris 13 as post-doc:

Parallel and sequential algorithms, programming, complexity analysis, architectures, networks, mathematics for computer science, computer algebra.

Mathematics '82–

Assistant professor in:

- Graduate level:

'2010- : University of Léonard de Vinci, ESILV, Paris, France: Mathematics for Physics.

'92-'93: University of Oran, Algeria: Numerical analysis, algebra, number theory, statistics, differential equations, geometry and functional analysis.

- Post-graduate level:

'92-'93: Scientific computing, DEA de Génie Spatial. Université des Sciences et Techniques d'Oran, Algeria.

'93: Partial differential equations, University of Annaba, Algeria.

Adviser

Five (5) graduate students got their computer science engineers under our direction, at university of Es-Sénia, Algeria.

Research

Keywords: Parallel algorithms, complexity analysis, scientific computing, computer arithmetic, computer algebra, greatest common divisor (gcd).

Main Results

- The algorithm “A Fast Parallel GCD of Many Integers” presented as a poster to ISSAC’2013 computes the GCD of n integers of $O(n)$ bits in $O(n/\log n)$ time with $O(n^{2+\epsilon})$ processors on CRCW PRAM model. To our knowledge, it is the first deterministic algorithm which computes the GCD of many integers with this parallel performance and polynomial work.
- We have improved the complexity bounds previously known to the fast GCD of two polynomials in the paper “New Fast Euclidean Algorithms“, J. of Symbolic Comp., 50 (2013) 208-226 (with M.F Roy).
- The ILE algorithm presented at ISSAC’01 is considered as one of the fastest parallel algorithms computing the GCD of two integers in $O(n/\log n)$ time with $O(n^{1+\epsilon})$ processors on CRCW PRAM model (see for example the article of K. Weber et al., “A Modular integer GCD algorithm”, Journal of Algorithms 54 (2005), 152-167, page 154, ligne 8). More precisely, our GCD algorithm shares the best parallel performance with Sorenson and Chor & Goldreich.
- Moreover the ILE algorithm is the only one, with this parallel performance, which is also an extended GCD, i.e.: an algorithm which gives the Bézout coefficients (JDA journal paper).
- The poster presented in ANTS’08 described the **first** SLP (Straight Line Program) on GF_2 , which computes the greatest common divisor of two integers.
- The Accelerated Euclidean Algorithm presented (poster at ISSAC’04) reach the best sequential complexity, see **mathworld** encyclopedia, <http://mathworld.com/Half-GCD.html>.

Publications

Thesis

Ph.D Thesis in Computer Science

Contribution au calcul parallèle du plus grand commun diviseur de deux entiers, thèse de doctorat, Université de Paris-Nord (Paris XIII), France, 1999, September 30th.

Ph.D Thesis in Mathematics

Solutions nulles pour un opérateur différentiel matriciel analytique relativement à une hypersurface caractéristique triple, 2ième cas avec condition de bonne décomposition pour un opérateur scalaire associé, thèse de doctorat 3ième cycle, Université des Sciences et Techniques de Lille (Lille I), France, 1982, March 23th.

Book

AN INTRODUCTION TO GCD ALGORITHMS, work in progress.

Journal papers

- M.F. Roy, S.M. Sedjelmaci. *New Fast Euclidean Algorithm*, Journal of Symbolic Computation, 50 (2013) 208-226.
- S.M. Sedjelmaci. *Some Related Functions to Integer GCD and Coprimality*, Electronic Notes in Discrete Mathematics, 37 (2011), 135-140.
- S.M. Sedjelmaci. *The Mixed Binary GCD Algorithm*, in Electronic Notes in Discrete Mathematics, 35 (2009) 169-176.
- S.M. Sedjelmaci. *A Parallel Extended GCD Algorithm*, Journal of Discrete Algorithms, (6), Issue 3, (2008) 526-538.
- S.M. Sedjelmaci. *Jebelean-Weber's Algorithm without Spurious Factors*, Information Processing Letters, vol. 102, 6, North-Holland, (2007) 247-252.
- S.M. Sedjelmaci. *A Modular Reduction for GCD Computation*. Journal of Computational and Applied Mathematics 162-I, (2004) 17-31.
- S.M. Sedjelmaci, C. Lavault. *Worst-case analysis of Weber's Algorithm*. Information Processing Letters 72, (1999) 125-130.
- S.M. Sedjelmaci, C. Lavault. *Improvements on the accelerated integer GCD algorithm*. Information Processing Letters 61, (1997) 31-36.

Reviewing papers

- Journal of Discrete Algorithms (JDA), Information Processing Letters (IPL).

Refereed conference proceedings papers

- S.M. Sedjelmaci. *A Fast Parallel GCD of Many Integers*, Poster Talk at ISSAC'2013, June 26-29, (Boston) USA, ACM Communications in Computer Algebra, Vol. 47, No. 3, Issue 185, (2013).
- S.M. Sedjelmaci. *Some Related Functions to Integer GCD and Coprimality*, accepted in the Latin- American Graphs, Optimization Symposium (LAGOS'2011), Bariloche, Argentina, 2011, pre-print available at <http://www-lipn.univ-paris13.fr/~sms>.
- S.M. Sedjelmaci, *The Mixed Binary GCD Algorithm*, in Proc. of the Latin- American Graphs, Optimization Symposium (LAGOS'09), Gramado, Brazil, 2009.
- S.M. Sedjelmaci. *A Straight Line Program for Computing Integer GCD*, Poster Talk at ANTS'08, May 17-22, (Alberta) Canada, ACM Communications in Computer Algebra, 42 (1-2), (2008) 62-64.
- S.M. Sedjelmaci. *The Accelerated Euclidean Algorithm*, in Proc. of EACA, Laureano Gonzales-Vega and Thomas Recio Eds., 283-287, July 1-3, 2004, Santander, Spain, accepted as Poster in ISSAC'04, July 3-7, Santander, Spain.
- S.M. Sedjelmaci. *On a Parallel Lehmer-Euclid GCD Algorithm*, in Proc. of the 15th International Symposium on Symbolic and Algebraic Computation ISSAC'01. ACM Press, 303-308, July 22-25, 2001, London, Canada.
- S.M. Sedjelmaci. *On a Parallel Extended Euclidean Algorithm*, in ACS/IEEE International Conference on Computer Systems and Applications AICCSA'2001 235-241, June 26-29, 2001, Beyrouth, Libanon.
- S.M. Sedjelmaci, C. Lavault. *A new modular division algorithm and applications*, in Proc. ICTCS'98, World Scientific, 65-76, Nov. 1998, Prato, Italy.
- M.N. Senhadji, S.M. Sedjelmaci. *Convergence acceleration of monotone sequences using synchronous subsequences*, in Colloque sur les mathématiques appliquées. Avril 1993, Oujda, Marocco.
- S.M. Sedjelmaci, Y. Slimani. *Expérimentation d'un noyau graphique basée sur une arithmétique exacte*, in Proceedings des 11^{èmes} journées de mathématiques appliquées, Vol. 2, Juillet 1992, Rabat, Marocco.
- S.M. Sedjelmaci, *Expériences numériques sur diverses arithmétiques*, in Colloque national sur les Micro-ordinateurs et Systèmes. Février 1988, Arzew, Algeria.

Others papers

- S.M. Sedjelmaci, Y. Slimani, L. Sekhri, M.N. Senhadji, M.D. Kateb, *Semantics of programs: A Matrix Approach*, in AMSE periodicals: Advances in Modelling & Analysis, A, Vol. 31, (1995) 39-48.
- S.M. Sedjelmaci, Y. Slimani, M.N. Senhadji, *Fault-tolerant numerical programs using the Arithmetic GFP*, in AMSE periodicals: Advances in Modelling & Analysis, A, Vol. 31, (1995) 55-60.
- S.M. Sedjelmaci, Y. Slimani, *How to Program with Matrix*, in AMSE periodicals: Advances in Modelling & Analysis, A, Vol. 31, (1995) 49-54.

Talks

- Talk in honor of Prof. Christian Lavault's retirement (in French), July 5th, 2011, Villetaneuse, France.
- S.M. Sedjelmaci, C. Lavault. *Sur un Algorithme de Division Modulaire et applications*, in Colloque de l'arithmétique des ordinateurs et géométrie algorithmique. Janvier 1998, Luminy, France.
- S.M. Sedjelmaci, M.N. Senhadji. *Accélération de convergence et conditionnement*, in 1^{er} Congrès national de mathématique. Novembre 1994, Tizi-Ouzou, Algeria.
- M.N. Senhadji, S.M. Sedjelmaci. *Convergence acceleration of fixed point by intercalation method*, in 1^{er} Congrès national de mathématique. Novembre 1994, Tizi-Ouzou, Algeria.
- S.M. Sedjelmaci. *On the Conditioning of fixed point sequences*, in 2ième Congrès Jordanien de mathématique. Août 1994, Mùtah University, Mùtah, Jordan.

Technical reports

- S.M. Sedjelmaci. *Complexity Analysis of the Accelerated Euclidean Algorithm*. Publication du LIPN, UMR CNRS 7030, 2004/02, mars 2004. Laboratoire d'informatique de Paris Nord, France.
- S.M. Sedjelmaci. *The Accelerated Euclidean Algorithm*. Publication du LIPN, UMR CNRS 7030, 2003/04, juin 2003. Laboratoire d'informatique de Paris Nord, France.
- S.M. Sedjelmaci. *A Redundant Equivalent of Hensel code for b-ary system*. Publication interne ERSIG, 02/92. Université d'Ès-Sénia Oran, Algeria, juin 1992.

- S.M. Sedjelmaci, A. Mili. *On a precise computer arithmetic for rationals: the choice of radix*. UT-ERPAH-89-RR-002. Université de Tunis, Tunisia, janvier 1989.

Papers in preparation

- S.M. Sedjelmaci, *Fast parallel GCD algorithm for many integers*, April (2013).
- S.M. Sedjelmaci, *Note on 0-1 Linear Diophantine equation and applications*, May (2013).

Seminars Talks and Invitations

- **Computer Algebra Workshop EACA**, "Accelerated Euclidean Algorithm and Applications to Subresultants and Cauchy Index" (with M.F. Roy), Santander, Spain, 3-7 july 2004.
- **CRYPTOGRAPHIE** Team, University of Rennes 1, **Invited**: March 8-20, 2004, with the talk: "Algorithme d'euclide rapide pour polynômes", France.
- **SPACE** Team, university de Paris 6, Jussieu: "Sur un algorithme d'Euclide rapide", January 22, 2004, France.
- **IRMAR** Team, university of Rennes 1: "Algorithmes du PGCD rapides appliqués aux polynômes", **Invited** November 28, 2003.
- **GREYC** Team, university of Caen: "Algorithmes de Lehmer accéléré", October 22, 2003, France.

Scientific activities

- Chairman session at the 10th IEEE International Symposium on Computer Arithmetic, ARITH'10, June 1991, Grenoble, France.
- Organizing Committee member of the Premier Symposium International sur le Génie Logiciel, November 1988, université d'És-Sénia, Oran, Algeria.

Head of research projects

'93-'98 Scientific computing, under grant N° B 3101/02/12/93, Ministère de l'Enseignement et de la Recherche d'Algérie.

'90-'92 Computer Arithmetics, under grant N° B 3101/04/02/90, Ministère de l'Enseignement et de la Recherche d'Algérie.

Spoken languages

French - English - Arabic.

Professional activities

- '84 Head of the mathematic and computer science institute at the university of Es-Sénia, Oran, Algeria.

Contact References

Marie-Francoise Roy, Professor at University of Rennes 1, France.
marie-francoise.roy@univ-rennes1.fr, Tel.: +(33) 02 23 23 60 20

Nelson Maculan, Professor at Federal University of Rio de Janeiro, Brazil, maculan@cos.ufrj.br, or nelsonmaculan@mec.gov.br.

Jonathan Sorenson, Professor and Head of Computer Science & Software Engineering at Butler University, USA, sorenson@butler.edu, Tel.: 317 940 9765.

Christian Lavault, Professor at University of Paris 13, France.
lavault@lipn.univ-paris13.fr, Tel.: +(33) 01 49 40 35 95.