IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2016

Project-Team LFANT

Lithe and fast algorithmic number theory

IN COLLABORATION WITH: Institut de Mathématiques de Bordeaux (IMB)

RESEARCH CENTER
Bordeaux - Sud-Ouest

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

1. Members **1**
2. Overall Objectives **2**
3. Research Program **2**
3.1. Number fields, class groups and other invariants 2
3.2. Function fields, algebraic curves and cryptology 3
3.3. Complex multiplication 4
4. Highlights of the Year **5**
5. New Software and Platforms **5**
5.1. APIP 5
5.2. Arb 6
5.3. AVIsogenies 6
5.4. CM 6
5.5. CMH 6
5.6. CUBIC 6
5.7. Euclid 7
5.8. FLINT 7
5.9. GNU MPC 7
5.10. KleinianGroups 7
5.11. mpmath 7
5.12. MPFRCX 8
5.13. Nemo 8
5.14. PARI/GP 8
6. New Results **8**
6.1. Class invariants in genus 2 8
6.2. Elliptic curve and Abelian varieties cryptology 9
6.3. Symbolic computation 9
6.4. Logarithmic Class Groups 10
6.5. Class groups and other invariants of number fields 10
6.6. Number and function fields 10
7. Partnerships and Cooperations **10**
7.1. National Initiatives 10
7.1.1. ANR Simpatic – SIM and PAiring Theory for Information and Communications security 10
7.1.2. ANR Alambic – AppLicAtions of MalleaBIlity in Cryptography 11
7.2. European Initiatives 11
7.3. International Initiatives 12
7.3.1. Inria International Labs 12
7.3.2. Inria International Partners 13
7.4. International Research Visitors 13
7.4.1. Visits of International Scientists 13
7.4.2. Visits to International Teams 13
8. Dissemination **13**
8.1. Promoting Scientific Activities 13
8.1.1. Scientific Events Selection 13
8.1.2. Journal 13
8.1.2.1. Member of the Editorial Boards 13
8.1.2.2. Reviewer - Reviewing Activities 14
8.1.3. Invited Talks 14
8.1.4. Scientific Expertise 14
8.1.5. Research Administration 14

8.2. Teaching - Supervision - Juries 14
8.2.1. Teaching 14
8.2.2. Supervision 14
8.2.3. Juries 15
8.3. Popularization 15
9. Bibliography **15**

Project-Team LFANT

Creation of the Team: 2009 March 01, updated into Project-Team: 2010 January 01

Keywords:

Computer Science and Digital Science:

4.3.1. - Public key cryptography
7.6. - Computer Algebra
7.7. - Number theory
7.12. - Computer arithmetic

Other Research Topics and Application Domains:

6. - IT and telecom
9.4.2. - Mathematics

1. Members

Research Scientists

Andreas Enge [Team leader, Inria, Senior Researcher, HDR]
Fredrik Johansson [Inria, Researcher]
Damien Robert [Inria, Researcher]

Faculty Members

Karim Belabas [Univ. Bordeaux, Professor, HDR]
Guilhem Castagnos [Univ. Bordeaux, Associate Professor]
Jean-Paul Cerri [Univ. Bordeaux, Associate Professor]
Jean-Marc Couveignes [Univ. Bordeaux I, Professor, HDR]

Engineers

Jared Guissmo Asuncion [Inria, from Oct 2016]
Bill Allombert [CNRS]

PhD Students

Pınar Kılıçer [Universities Leiden and Bordeaux]
Chloë Martindale [Universities Leiden and Bordeaux]
Iuliana Ciocanea-Teodorescu [Universities Leiden and Bordeaux]
Emmanouil Tzortzakis [Universities Leiden and Bordeaux]

Post-Doctoral Fellows

Cyril Bouvier [Univ. Bordeaux, until May 2016]
Enea Milio [Inria, until Mars 2016]

Visiting Scientists

Francisco Diaz Y Diaz [retraité]
Guillaume Hitsch [Univ. Blaise Pascal, Mar 2016]
Abdoulaye Maiga [Univ. Dakar, from Nov 2016]
Bernadette Perrin-Riou [Univ. Paris XI]

Administrative Assistants

Anne-Laure Gautier [Inria]
Joelle Rodrigues [Inria]

Other

Zhengying Liu [Inria, Master 1 Internship, from Mar 2016 until Jul 2016]

2. Overall Objectives

2.1. Presentation

Algorithmic number theory dates back to the dawn of mathematics itself, *cf.* Eratosthenes's sieve to enumerate consecutive prime numbers. With the arrival of computers, previously unsolvable problems have come into reach, which has boosted the development of more or less practical algorithms for essentially all number theoretic problems. The field is now mature enough for a more computer science driven approach, taking into account the theoretical complexities and practical running times of the algorithms.

Concerning the lower level multiprecision arithmetic, folklore has asserted for a long time that asymptotically fast algorithms such as SchÃ¶nhage–Strassen multiplication are impractical; nowadays, however, they are used routinely. On a higher level, symbolic computation provides numerous asymptotically fast algorithms (such as for the simultaneous evaluation of a polynomial in many arguments or linear algebra on sparse matrices), which have only partially been exploited in computational number theory. Moreover, precise complexity analyses do not always exist, nor do sound studies to choose between different algorithms (an exponential algorithm may be preferable to a polynomial one for a large range of inputs); folklore cannot be trusted in a fast moving area such as computer science.

Another problem is the reliability of the computations; many number theoretic algorithms err with a small probability, depend on unknown constants or rely on a Riemann hypothesis. The correctness of their output can either be ensured by a special design of the algorithm itself (slowing it down) or by an *a posteriori* verification. Ideally, the algorithm outputs a certificate, providing an independent *fast* correctness proof. An example is integer factorisation, where factors are hard to obtain but trivial to check; primality proofs have initiated sophisticated generalisations.

One of the long term goals of the LFANT project team is to make an inventory of the major number theoretic algorithms, with an emphasis on algebraic number theory and arithmetic geometry, and to carry out complexity analyses. So far, most of these algorithms have been designed and tested over number fields of small degree and scale badly. A complexity analysis should naturally lead to improvements by identifying bottlenecks, systematically redesigning and incorporating modern asymptotically fast methods.

Reliability of the developed algorithms is a second long term goal of our project team. Short of proving the Riemann hypothesis, this could be achieved through the design of specialised, slower algorithms not relying on any unproven assumptions. We would prefer, however, to augment the fastest unproven algorithms with the creation of independently verifiable certificates. Ideally, it should not take longer to check the certificate than to generate it.

All theoretical results are complemented by concrete reference implementations in PARI/GP, which allow to determine and tune the thresholds where the asymptotic complexity kicks in and help to evaluate practical performances on problem instances provided by the research community. Another important source for algorithmic problems treated by the LFANT project team is modern cryptology. Indeed, the security of all practically relevant public key cryptosystems relies on the difficulty of some number theoretic problem; on the other hand, implementing the systems and finding secure parameters require efficient algorithmic solutions to number theoretic problems.

3. Research Program

3.1. Number fields, class groups and other invariants

Participants: Bill Allombert, Karim Belabas, Cyril Bouvier, Jean-Paul Cerri, Iuliana Ciocanea-Teodorescu, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Pınar Kılıçer.

Modern number theory has been introduced in the second half of the 19th century by Dedekind, Kummer, Kronecker, Weber and others, motivated by Fermat's conjecture: There is no non-trivial solution in integers to the equation $x^n + y^n = z^n$ for $n \geqslant 3$. For recent textbooks, see [5]. Kummer's idea for solving Fermat's problem was to rewrite the equation as $(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y) = z^n$ for a primitive n-th root of unity ζ, which seems to imply that each factor on the left hand side is an n-th power, from which a contradiction can be derived.

The solution requires to augment the integers by *algebraic numbers*, that are roots of polynomials in $\mathbb{Z}[X]$. For instance, ζ is a root of $X^n - 1$, $\sqrt[3]{2}$ is a root of $X^3 - 2$ and $\frac{\sqrt{3}}{5}$ is a root of $25X^2 - 3$. A *number field* consists of the rationals to which have been added finitely many algebraic numbers together with their sums, differences, products and quotients. It turns out that actually one generator suffices, and any number field K is isomorphic to $\mathbb{Q}[X]/(f(X))$, where $f(X)$ is the minimal polynomial of the generator. Of special interest are *algebraic integers*, "numbers without denominators", that are roots of a monic polynomial. For instance, ζ and $\sqrt[3]{2}$ are integers, while $\frac{\sqrt{3}}{5}$ is not. The *ring of integers* of K is denoted by $\mathcal{O}_K$; it plays the same role in K as $\mathbb{Z}$ in $\mathbb{Q}$.

Unfortunately, elements in $\mathcal{O}_K$ may factor in different ways, which invalidates Kummer's argumentation. Unique factorisation may be recovered by switching to *ideals*, subsets of $\mathcal{O}_K$ that are closed under addition and under multiplication by elements of $\mathcal{O}_K$. In $\mathbb{Z}$, for instance, any ideal is *principal*, that is, generated by one element, so that ideals and numbers are essentially the same. In particular, the unique factorisation of ideals then implies the unique factorisation of numbers. In general, this is not the case, and the *class group* Cl_K of ideals of $\mathcal{O}_K$ modulo principal ideals and its *class number* $h_K = |\,\mathrm{Cl}_K\,|$ measure how far $\mathcal{O}_K$ is from behaving like $\mathbb{Z}$.

Using ideals introduces the additional difficulty of having to deal with *units*, the invertible elements of $\mathcal{O}_K$: Even when $h_K = 1$, a factorisation of ideals does not immediately yield a factorisation of numbers, since ideal generators are only defined up to units. For instance, the ideal factorisation $(6) = (2)\cdot(3)$ corresponds to the two factorisations $6 = 2\cdot 3$ and $6 = (-2)\cdot(-3)$. While in $\mathbb{Z}$, the only units are 1 and -1, the unit structure in general is that of a finitely generated $\mathbb{Z}$-module, whose generators are the *fundamental units*. The *regulator* R_K measures the "size" of the fundamental units as the volume of an associated lattice.

One of the main concerns of algorithmic algebraic number theory is to explicitly compute these invariants (Cl_K and h_K, fundamental units and R_K), as well as to provide the data allowing to efficiently compute with numbers and ideals of $\mathcal{O}_K$; see [28] for a recent account.

The *analytic class number formula* links the invariants h_K and R_K (unfortunately, only their product) to the ζ-function of K, $\zeta_K(s) := \prod_{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K} \left(1 - \mathrm{N}\,\mathfrak{p}^{-s}\right)^{-1}$, which is meaningful when $\Re(s) > 1$, but which may be extended to arbitrary complex $s \neq 1$. Introducing characters on the class group yields a generalisation of ζ- to L-functions. The *generalised Riemann hypothesis (GRH)*, which remains unproved even over the rationals, states that any such L-function does not vanish in the right half-plane $\Re(s) > 1/2$. The validity of the GRH has a dramatic impact on the performance of number theoretic algorithms. For instance, under GRH, the class group admits a system of generators of polynomial size; without GRH, only exponential bounds are known. Consequently, an algorithm to compute Cl_K via generators and relations (currently the only viable practical approach) either has to assume that GRH is true or immediately becomes exponential.

When $h_K = 1$ the number field K may be norm-Euclidean, endowing $\mathcal{O}_K$ with a Euclidean division algorithm. This question leads to the notions of the Euclidean minimum and spectrum of K, and another task in algorithmic number theory is to compute explicitly this minimum and the upper part of this spectrum, yielding for instance generalised Euclidean gcd algorithms.

3.2. Function fields, algebraic curves and cryptology

Participants: Karim Belabas, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Enea Milio, Damien Robert, Emmanouil Tzortzakis.

Algebraic curves over finite fields are used to build the currently most competitive public key cryptosystems. Such a curve is given by a bivariate equation $\mathcal{C}(X,Y)=0$ with coefficients in a finite field $\mathbb{F}_q$. The main classes of curves that are interesting from a cryptographic perspective are *elliptic curves* of equation $\mathcal{C}=Y^2-(X^3+aX+b)$ and *hyperelliptic curves* of equation $\mathcal{C}=Y^2-(X^{2g+1}+\cdots)$ with $g \geqslant 2$.

The cryptosystem is implemented in an associated finite abelian group, the *Jacobian* $\mathrm{Jac}_{\mathcal{C}}$. Using the language of function fields exhibits a close analogy to the number fields discussed in the previous section. Let $\mathbb{F}_q(X)$ (the analogue of $\mathbb{Q}$) be the *rational function field* with subring $\mathbb{F}_q[X]$ (which is principal just as $\mathbb{Z}$). The *function field* of $\mathcal{C}$ is $K_{\mathcal{C}}=\mathbb{F}_q(X)[Y]/(\mathcal{C})$; it contains the *coordinate ring* $\mathcal{O}_{\mathcal{C}}=\mathbb{F}_q[X,Y]/(\mathcal{C})$. Definitions and properties carry over from the number field case $K/\mathbb{Q}$ to the function field extension $K_{\mathcal{C}}/\mathbb{F}_q(X)$. The Jacobian $\mathrm{Jac}_{\mathcal{C}}$ is the divisor class group of $K_{\mathcal{C}}$, which is an extension of (and for the curves used in cryptography usually equals) the ideal class group of $\mathcal{O}_{\mathcal{C}}$.

The size of the Jacobian group, the main security parameter of the cryptosystem, is given by an L-function. The GRH for function fields, which has been proved by Weil, yields the Hasse–Weil bound $(\sqrt{q}-1)^{2g} \leqslant |\,\mathrm{Jac}_{\mathcal{C}}\,| \leqslant (\sqrt{q}+1)^{2g}$, or $|\,\mathrm{Jac}_{\mathcal{C}}\,| \approx q^g$, where the *genus* g is an invariant of the curve that correlates with the degree of its equation. For instance, the genus of an elliptic curve is 1, that of a hyperelliptic one is $\frac{\deg_X \mathcal{C}-1}{2}$. An important algorithmic question is to compute the exact cardinality of the Jacobian.

The security of the cryptosystem requires more precisely that the *discrete logarithm problem* (DLP) be difficult in the underlying group; that is, given elements D_1 and $D_2=xD_1$ of $\mathrm{Jac}_{\mathcal{C}}$, it must be difficult to determine x. Computing x corresponds in fact to computing $\mathrm{Jac}_{\mathcal{C}}$ explicitly with an isomorphism to an abstract product of finite cyclic groups; in this sense, the DLP amounts to computing the class group in the function field setting.

For any integer n, the *Weil pairing* e_n on $\mathcal{C}$ is a function that takes as input two elements of order n of $\mathrm{Jac}_{\mathcal{C}}$ and maps them into the multiplicative group of a finite field extension $\mathbb{F}_{q^k}$ with $k=k(n)$ depending on n. It is bilinear in both its arguments, which allows to transport the DLP from a curve into a finite field, where it is potentially easier to solve. The *Tate-Lichtenbaum pairing*, that is more difficult to define, but more efficient to implement, has similar properties. From a constructive point of view, the last few years have seen a wealth of cryptosystems with attractive novel properties relying on pairings.

For a random curve, the parameter k usually becomes so big that the result of a pairing cannot even be output any more. One of the major algorithmic problems related to pairings is thus the construction of curves with a given, smallish k.

3.3. Complex multiplication

Participants: Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Chloë Martindale, Enea Milio, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [30], for more background material, [29]. In fact, for most curves $\mathcal{C}$ over a finite field, the endomorphism ring of $\mathrm{Jac}_{\mathcal{C}}$, which determines its L-function and thus its cardinality, is an order in a special kind of number field K, called *CM field*. The CM field of an elliptic curve is an imaginary-quadratic field $\mathbb{Q}(\sqrt{D})$ with $D<0$, that of a hyperelliptic curve of genus g is an imaginary-quadratic extension of a totally real number field of degree g. Deuring's lifting theorem ensures that $\mathcal{C}$ is the reduction modulo some prime of a curve with the same endomorphism ring, but defined over the *Hilbert class field* H_K of K.

Algebraically, H_K is defined as the maximal unramified abelian extension of K; the Galois group of H_K/K is then precisely the class group Cl_K. A number field extension H/K is called *Galois* if $H \simeq K[X]/(f)$ and H contains all complex roots of f. For instance, $\mathbb{Q}(\sqrt{2})$ is Galois since it contains not only $\sqrt{2}$, but also the second root $-\sqrt{2}$ of X^2-2, whereas $\mathbb{Q}(\sqrt[3]{2})$ is not Galois, since it does not contain the root $e^{2\pi i/3}\sqrt[3]{2}$ of X^3-2. The *Galois group* $\mathrm{Gal}_{H/K}$ is the group of automorphisms of H that fix K; it permutes the roots of f. Finally, an *abelian* extension is a Galois extension with abelian Galois group.

Analytically, in the elliptic case H_K may be obtained by adjoining to K the *singular value* $j(\tau)$ for a complex valued, so-called *modular* function j in some $\tau \in \mathcal{O}_K$; the correspondence between $\mathrm{Gal}_{H/K}$ and Cl_K allows to obtain the different roots of the minimal polynomial f of $j(\tau)$ and finally f itself. A similar, more involved construction can be used for hyperelliptic curves. This direct application of complex multiplication yields algebraic curves whose L-functions are known beforehand; in particular, it is the only possible way of obtaining ordinary curves for pairing-based cryptosystems.

The same theory can be used to develop algorithms that, given an arbitrary curve over a finite field, compute its L-function.

A generalisation is provided by *ray class fields*; these are still abelian, but allow for some well-controlled ramification. The tools for explicitly constructing such class fields are similar to those used for Hilbert class fields.

4. Highlights of the Year

4.1. Highlights of the Year

Release of Pari 2.9 after two years of development. This stable releases includes three brand new modules (L-functions, Associative and Central Simple Algebras, and Modular Symbols), a major overhaul of the Elliptic Curves and Number Fields modules.

Iuliana Ciocanea-Teodorescu has defended her PhD thesis on *Algorithms for finite rings* in June 2016 http://www.theses.fr/2016BORD0121.

Pinar Kiliçer has defended her PhD thesis on *The class number one problem for genus-2 curves* in July 2016 [11].

5. New Software and Platforms

5.1. APIP

Another Pairing Implementation in PARI
SCIENTIFIC DESCRIPTION

Apip , Another Pairing Implementation in PARI, is a library for computing standard and optimised variants of most cryptographic pairings.

The following pairings are available: Weil, Tate, ate and twisted ate, optimised versions (à la Vercauteren–Hess) of ate and twisted ate for selected curve families.

The following methods to compute the Miller part are implemented: standard Miller double-and-add method, standard Miller using a non-adjacent form, Boxall et al. version, Boxall et al. version using a non-adjacent form.

The final exponentiation part can be computed using one of the following variants: naive exponentiation, interleaved method, Avanzi–Mihailescu's method, Kato et al.'s method, Scott et al.'s method.

Part of the library has been included into Pari/Gp proper.
FUNCTIONAL DESCRIPTION

APIP is a library for computing standard and optimised variants of most cryptographic pairings.

- Participant: Jérôme Milan
- Contact: Jérôme Milan
- URL: http://www.lix.polytechnique.fr/~milanj/apip/apip.xhtml

5.2. Arb

FUNCTIONAL DESCRIPTION

Arb is a C library for arbitrary-precision floating-point ball arithmetic. It supports real and complex numbers, polynomials, power series, matrices, and evaluation of many transcendental functions. All is done with automatic, rigorous error bounds. It has been accepted for inclusion in SageMath.

- Participant: Fredrik Johansson
- Contact: Fredrik Johansson
- URL: http://fredrikj.net/arb/

5.3. AVIsogenies

Abelian Varieties and Isogenies
FUNCTIONAL DESCRIPTION

AVIsogenies is a Magma package for working with abelian varieties, with a particular emphasis on explicit isogeny computation.

Its prominent feature is the computation of (l,l)-isogenies between Jacobian varieties of genus-two hyperelliptic curves over finite fields of characteristic coprime to l, practical runs have used values of l in the hundreds.

It can also be used to compute endomorphism rings of abelian surfaces, and find complete addition laws on them.

- Participants: Gaëtan Bisson, Romain Cosset and Damien Robert
- Contact: Damien Robert
- URL: http://avisogenies.gforge.inria.fr/

5.4. CM

FUNCTIONAL DESCRIPTION

The Cm software implements the construction of ring class fields of imaginary quadratic number fields and of elliptic curves with complex multiplication via floating point approximations. It consists of libraries that can be called from within a C program and of executable command line applications.

- Participant: Andreas Enge
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/index.php?prog=cm&page=home

5.5. CMH

Computation of Igusa Class Polynomials
KEYWORDS: Mathematics - Cryptography - Number theory
FUNCTIONAL DESCRIPTION

Cmh computes Igusa class polynomials, parameterising two-dimensional abelian varieties (or, equivalently, Jacobians of hyperelliptic curves of genus 2) with given complex multiplication.

- Participants: Emmanuel Thomé, Andreas Enge and Regis Dupont
- Contact: Emmanuel Thomé
- URL: http://cmh.gforge.inria.fr

5.6. CUBIC

FUNCTIONAL DESCRIPTION

Cubic is a stand-alone program that prints out generating equations for cubic fields of either signature and bounded discriminant. It depends on the Pari library. The algorithm has quasi-linear time complexity in the size of the output.

- Participant: Karim Belabas
- Contact: Karim Belabas
- URL: http://www.math.u-bordeaux.fr/~belabas/research/software/cubic-1.3.tgz

5.7. Euclid

FUNCTIONAL DESCRIPTION

Euclid is a program to compute the Euclidean minimum of a number field. It is the practical implementation of the algorithm described in [38] . Some corresponding tables built with the algorithm are also available. Euclid is a stand-alone program depending on the PARI library.

- Participants: Pierre Lezowski and Jean-Paul Cerri
- Contact: Pierre Lezowski
- URL: http://www.math.u-bordeaux1.fr/~plezowsk/euclid/index.php

5.8. FLINT

FUNCTIONAL DESCRIPTION FLINT is a C library for number theory and basic computer algebra, maintained by William Hart with code by William Hart, Sebastian Pancratz, Andy Novocin, Fredrik Johansson, Tom Bachmann, Mike Hansen, Martin Lee, David Harvey, and a large number of other authors.

FLINT is used as a back end library for polynomial arithmetic and number theory functionality in a large number of applications, including SageMath and Singular.

- Participant: Fredrik Johansson
- Contact: William Hart
- URL: http://flintlib.org/

5.9. GNU MPC

FUNCTIONAL DESCRIPTION

Mpc is a C library for the arithmetic of complex numbers with arbitrarily high precision and correct rounding of the result. It is built upon and follows the same principles as Mpfr. The library is written by Andreas Enge, Philippe Théveny and Paul Zimmermann.

- Participants: Andreas Enge, Paul Zimmermann, Philippe Theveny and Mickaël Gastineau
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/

5.10. KleinianGroups

FUNCTIONAL DESCRIPTION

KleinianGroups is a Magma package that computes fundamental domains of arithmetic Kleinian groups.

- Participant: Aurel Page
- Contact: Aurel Page
- URL: http://www.normalesup.org/~page/Recherche/Logiciels/logiciels-en.html

5.11. mpmath

FUNCTIONAL DESCRIPTION mpmath is a Python library for real and complex floating-point arithmetic with arbitrary precision. It has been developed by Fredrik Johansson since 2007, with help from many contributors.

As a dependency of the SymPy computer algebra system as well as SageMath, mpmath is a core component of the Python scientific software ecosystem.

- Participant: Fredrik Johansson
- Contact: Fredrik Johansson
- URL: http://mpmath.org/

5.12. MPFRCX

FUNCTIONAL DESCRIPTION

Mpfrcx is a library for the arithmetic of univariate polynomials over arbitrary precision real (Mpfr) or complex (Mpc) numbers, without control on the rounding. For the time being, only the few functions needed to implement the floating point approach to complex multiplication are implemented. On the other hand, these comprise asymptotically fast multiplication routines such as Toom-Cook and the FFT.

- Participant: Andreas Enge
- Contact: Andreas Enge
- URL: http://www.multiprecision.org/index.php?prog=mpfrcx

5.13. Nemo

FUNCTIONAL DESCRIPTION Nemo is a computer algebra package for the Julia programming language maintained by William Hart with code by William Hart, Tommy Hofmann, Claus Fieker, Fredrik Johansson, Oleksandr Motsak).

The features of Nemo include multiprecision integers and rationals, integers modulo n, p-adic numbers, finite fields (prime and non-prime order), number field arithmetic, maximal orders of number fields, arithmetic of ideals in maximal orders, arbitrary precision real and complex balls, generic polynomials, power series, fraction fields, residue rings and matrices.

- Participant: Fredrik Johansson
- Contact: William Hart
- URL: http://nemocas.org/

5.14. PARI/GP

FUNCTIONAL DESCRIPTION

Pari/Gp is a widely used computer algebra system designed for fast computations in number theory (factorisation, algebraic number theory, elliptic curves, ...), but it also contains a large number of other useful functions to compute with mathematical entities such as matrices, polynomials, power series, algebraic numbers, etc., and many transcendental functions.

- Participants: Karim Belabas, Bill Allombert, Henri Cohen and Andreas Enge
- Contact: Karim Belabas
- URL: http://pari.math.u-bordeaux.fr/

6. New Results

6.1. Class invariants in genus 2

Abelian surfaces, or equivalently, Jacobian varieties of genus 2 hyperelliptic curves, offer the same security as elliptic curves in a cryptographic setting and often better efficiency, and could thus be an attractive alternative. The theory of complex multiplication can be used to obtain cryptographically secure curves. Relying on Shimura reciprocity for Siegel modular forms, we have developed the necessary mathematical theory in [24]. It requires deeper algebraic reasoning than for elliptic curves: Ideals of the endomorphism rings of the abelian varieties are no more two-dimensional modules over the integers, but two-dimensional projective modules over quadratic number rings. We succeed in proving results adapted from the elliptic curve case by suitably normalising quadratic forms over number rings and using strong approximation. The result is an elegant theory that leads to clearly formulated and practical algorithms, which we illustrate by examples.

6.2. Elliptic curve and Abelian varieties cryptology

Participant: Damien Robert.

The paper [15] in which David Lubicz and Damien Robert explain how to improve the arithmetic of Abelian and Kummer varieties has been published in the journal Finite Fields and Their Applications. The speed of the arithmetic is a crucial factor in the performance of cryptosystems based on abelian varieties. Depending on the cryptographic application, the speed record holders are elliptic curves (in the Edwards model) or the Kummer surface of an hyperelliptic curves of genus 2 (in the level 2 theta model). One drawback of the Kummer surface is that only scalar multiplications are available, which may be a problem in certain cryptographic protocols. The previous known models to work on the Jacobian rather than the Kummer surface (Mumford coordinates or the theta model of level 4) are too slow and not competitive with elliptic curves. This paper explains how to use geometric properties (like projective normality) to speed up the arithmetic. In particular it introduces a novel addition algorithm on Kummer varieties (compatible addition), and uses it to speed up multi-exponentiations in Kummer varieties and to obtain new models of abelian surfaces in which the scalar multiplication is as fast as on the Kummer surface.

Theta functions, and in particular the Dedekind eta function, are at the heart of complex multiplication constructions of curves. They can be written as sparse power series with coefficients ± 1. In [23] we devise optimised addition sequences for the occurring exponents, with a proof relying on classical number theory, which help us gain a factor of 2 compared to the standard approach and which is validated in practice by our two independent implementations. Using an approach from computer algebra and a proof relying on analytic number theory, we obtain another factor of 2.

6.3. Symbolic computation

The article [27], of which F. Johansson is a coauthor, was published. The article describes SymPy, an open source computer algebra system written in pure Python. It is built with a focus on extensibility and ease of use, through both interactive and programmatic applications. These characteristics have led SymPy to become a popular symbolic library for the scientific Python ecosystem. This paper presents the architecture of SymPy, a description of its features, and a discussion of select submodules. The supplementary material provide additional examples and further outline details of the architecture and features of SymPy.

Hypergeometric functions are among the most important mathematical functions, with a wide range of applications in everything from physics to number theory. The practical computation of such functions is a challenging problem. The preprint [26]. presents an efficient implementation of hypergeometric functions in arbitrary-precision interval arithmetic. The functions ${}_0F_1$, ${}_1F_1$, ${}_2F_1$ and ${}_2F_0$ (or the Kummer U-function) are supported for unrestricted complex parameters and argument, and by extension, we cover exponential and trigonometric integrals, error functions, Fresnel integrals, incomplete gamma and beta functions, Bessel functions, Airy functions, Legendre functions, Jacobi polynomials, complete elliptic integrals, and other special functions. The output can be used directly for interval computations or to generate provably correct floating-point approximations in any format. Performance is competitive with earlier arbitrary-precision software, and sometimes orders of magnitude faster. We also partially cover the generalized hypergeometric function ${}_pF_q$ and computation of high-order parameter derivatives.

The preprint [25] is the corresponding paper for the software Arb developed by F. Johansson. Arb is a C library for arbitrary-precision interval arithmetic using the midpoint-radius representation, also known as ball arithmetic. It supports real and complex numbers, polynomials, power series, matrices, and evaluation of many special functions. The core number types are designed for versatility and speed in a range of scenarios, allowing performance that is competitive with non-interval arbitrary-precision types such as MPFR and MPC floating-point numbers. This paper discusses the low-level number representation, strategies for precision and error bounds, and the implementation of efficient polynomial arithmetic with interval coefficients.

6.4. Logarithmic Class Groups

Logarithmic class groups and units, introduced by Jaulent in 1994, are an intriguing ℓ-adic variation on the classical class and unit groups related to Iwasawa theory and the wild kernels of algebraic K-theory. These $\mathbb{Z}_\ell$-modules of finite type provide direct access to invariants studied in standard conjectures about $\mathbb{Z}_\ell$-extensions. In [12] we devised a new algorithm to explicitly compute them in subexponential time under standard conjectures (GRH and Gross-Kuz'min) and to validate unconditionaly the computed results (now in exponential time). The algorithm has been implementated in the PARI/GP system.

6.5. Class groups and other invariants of number fields

The article by H. Cohen and F. Thorne on Dirichlet series associated to quartic fields with given cubic resolvent has been published. This article gives an explicit formula for the Dirichlet series $\sum_K |\Delta(K)|^{-s}$, where the sum is over isomorphism classes of all quartic fields whose resolvent field is isomorphic to a fixed cubic field k.

The article [22] by H. Cohen and F. Thorne generalizes the work of A. Morra and the authors, on giving explicit formulas for the Dirichlet series generating function of D_ℓ extensions of odd prime degree ℓ with given quadratic resolvent. Over the course of the proof, the authors explain connections between their formulas and the Ankeny-Artin-Chowla conjecture, the Ohno-Nakagawa relation for binary cubic forms, and other topics.

In her thesis, Iuliana Ciocanea-Teodorescu describes algorithms that answer questions arising in ring and module theory. The first main result of this thesis concerns the module isomorphism problem, how to compute a set of generators of minimal cardinality, and how to construct projective covers and injective hulls. The thesis also describe tests for module simplicity, projectivity, and injectivity, and constructive tests for existence of surjective module homomorphisms between two finite modules, one of which is projective. As a negative result, the problem of testing for existence of injective module homomorphisms between two finite modules, one of which is projective, is NP-complete. The last part of the thesis is concerned with finding a good working approximation of the Jacobson radical of a finite ring, that is, a two-sided nilpotent ideal such that the corresponding quotient ring is almost semisimple. The notion used to approximate semisimplicity is that of separability.

In her thesis [11], Pinar Kiliçer determines all CM curves of genus 2 defined over the reflex field. This extends the previous CM class number one problem for elliptic curves which asked to find all elliptic curves defined over the rationals with non-trivial endomorphism ring.

6.6. Number and function fields

The article [13] written by J. Brau and J. Nathan on “Elliptic curves with 2-torsion contained in the 3-torsion field” has been published. This article study the modular curve $X'(6)$ of level 6 defined over $\mathbb{Q}$ whose $\mathbb{Q}$-rational points correspond to j-invariants of elliptic curves E over $\mathbb{Q}$ for which $\mathbb{Q}(E[2])$ is a subfield of $\mathbb{Q}(E[3])$. The authors characterize the j-invariants of elliptic curves with this property by exhibiting an explicit model of $X'(6)$. $X'(6)(\mathbb{Q})$ then gives an infinite family of examples of elliptic curves with non-abelian "entanglement fields," which is relevant to the systematic study of correction factors of various conjectural constants for elliptic curves over $\mathbb{Q}$.

7. Partnerships and Cooperations

7.1. National Initiatives

7.1.1. ANR Simpatic – SIM and PAiring Theory for Information and Communications security

Participants: Guilhem Castagnos, Damien Robert.

http://simpatic.orange-labs.fr

The SIMPATIC project is an industrial research project, formed by academic research teams and industrial partners: Orange Labs, École Normale Supérieure, INVIA, Oberthur Technologies, ST-Ericsson France, Université de Bordeaux 1, Université de Caen Basse-Normandie, Université de Paris 8.

The aim of the SIMPATIC project is to provide the most efficient and secure hardware/software implementation of a bilinear pairing in a SIM card. This implementation will then be used to improve and develop new cryptographic algorithms and protocols in the context of mobile phones and SIM cards. The project will more precisely focus on e-ticketing and e-cash, on cloud storage and on the security of contactless and of remote payment systems.

D. Robert is a participant in the Task 2 whose role is to give state of the art algorithms for pairing computations, adapted to the specific hardware requirements of the Simpatic Project.

G. Castagnos is a participant in the Task 4 whose role is to design new cryptographic primitives adapted to the specific applications of the Simpatic Project.

The SIMPATIC project has ended in August 2016. The project has shown that pairings can now efficiently be integrated into smart cards publicly deployed, by obtaining performances that outperform the state of the art. Cryptographic tools designed by the project are moreover capable of combining complex functionalities and efficiency in many areas such as digital signatures, minimization of personal data in contactless services, pay TV, or protecting data stored in an untrusted cloud.

7.1.2. ANR Alambic – AppLicAtions of MalleaBIlity in Cryptography

Participant: Guilhem Castagnos.

https://crypto.di.ens.fr/projects:alambic:main

The ALAMBIC project is a research project formed by members of the Inria Project-Team CASCADE of ENS Paris, members of the AriC Inria project-team of ENS Lyon, and members of the CRYPTIS of the university of Limoges. G. Castagnos is an external member of the team of Lyon for this project.

Non-malleability is a security notion for public key cryptographic encryption schemes that ensures that it is infeasible for an adversary to modify ciphertexts into other ciphertexts of messages which are related to the decryption of the first ones. On the other hand, it has been realized that, in specific settings, malleability in cryptographic protocols can actually be a very useful feature. For example, the notion of homomorphic encryption allows specific types of computations to be carried out on ciphertexts and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintexts. The homomorphic property can be used to create secure voting systems, collision-resistant hash functions, private information retrieval schemes, and for fully homomorphic encryption enables widespread use of cloud computing by ensuring the confidentiality of processed data.

The aim of the ALAMBIC project to investigate further theoretical and practical applications of malleability in cryptography. More precisely, this project focuses on three different aspects: secure computation outsourcing and server-aided cryptography, homomorphic encryption and applications and << paradoxical >> applications of malleability.

7.2. European Initiatives

7.2.1. FP7 & H2020 Projects

7.2.1.1. ANTICS

Title: Algorithmic Number Theory in Computer Science

Program: FP7

Duration: January 2012 - December 2016

Coordinator: Inria

Inria contact: Andreas Enge

’During the past twenty years, we have witnessed profound technological changes, summarised under the terms of digital revolution or entering the information age. It is evident that these technological changes will have a deep societal impact, and questions of privacy and security are primordial to ensure the survival of a free and open society. Cryptology is a main building block of any security solution, and at the heart of projects such as electronic identity and health cards, access control, digital content distribution or electronic voting, to mention only a few important applications. During the past decades, public-key cryptology has established itself as a research topic in computer science; tools of theoretical computer science are employed to “prove” the security of cryptographic primitives such as encryption or digital signatures and of more complex protocols. It is often forgotten, however, that all practically relevant public-key cryptosystems are rooted in pure mathematics, in particular, number theory and arithmetic geometry. In fact, the socalled security “proofs” are all conditional to the algorithmic untractability of certain number theoretic problems, such as factorisation of large integers or discrete logarithms in algebraic curves. Unfortunately, there is a large cultural gap between computer scientists using a black-box security reduction to a supposedly hard problem in algorithmic number theory and number theorists, who are often interested in solving small and easy instances of the same problem. The theoretical grounds on which current algorithmic number theory operates are actually rather shaky, and cryptologists are generally unaware of this fact. The central goal of ANTICS is to rebuild algorithmic number theory on the firm grounds of theoretical computer science.’

Title: OpenDreamKit

Program: H2020

Duration: January 2016 - December 2020

Inria contact: Karim Belabas

Description http://cordis.europa.eu/project/rcn/198334_en.html, http://opendreamkit.org

7.3. International Initiatives

7.3.1. Inria International Labs

7.3.1.1. International Laboratory for Research in Computer Science and Applied Mathematics

MACISA

Title: Mathematics Applied to Cryptology and Information Security in Africa

International Partner (Institution - Laboratory - Researcher):

> Université des Sciences et Techniques de Masuku (Gabon) - Faculté des Sciences - Dpt de Mathématiques et Informatique - Tony Ezome

Duration: 2012 - 2016

The projects aims at understanding the role played by algebraic maps in public key cryptography. Since this is a very broad topic, we will focus on objects of dimension zero (finite sets and rings) and one (algebraic curves, their differentials and jacobians). The proposed project-team consists of African and French researchers working in mathematical and statistical aspects of public-key cryptology. The French researchers work in the Inria project-team LFANT in Bordeaux, and the IRMAR (Institut de Recherche en Mathématiques et Applications de Rennes) in Rennes. The African researchers already cooperate in the project PRMAIS (Pole of Research in Mathematics and their Applications in Information Security in Sub-Saharan Africa) supported by the Simons’ foundation.

The project is managed by a team of five permanent researchers: G. Nkiet, J.-M. Couveignes, T. Ezome, D. Robert and A. Enge. Since Sep. 2014 the coordinator is T. Ezome and the vice-coordinator is D. Robert. The managing team organises the cooperation, schedules meetings, prepares reports, controls expenses, reports to the LIRIMA managing team and administrative staff.

A non-exhaustive list of activities organised or sponsored by Macisa includes

- The Summer school (EMA) in Bamenda with the International Center for Pure and Applied Mathematics (ICPAM/CIMPA), June 2016;
- The visit of Abdoulaye Maiga in Bordeaux to work with D. Robert on canonical lifts of genus 2 curves.

2016 was the last year of Macisa. A new project FAST "(Harder Better) FAster STronger cryptography" has been proposed as an associated team between LFANT and the PREMA (Pole of Research in Mathematics and Applications in Africa) Simon's foundation project.

7.3.2. Inria International Partners

7.3.2.1. Informal International Partners

The team is used to collaborate with Leiden University through the ALGANT program for PhD joint supervision.

Eduardo Friedman (U. of Chile), long term collaborator of K. Belabas and H. Cohen is a regular visitor in Bordeaux (about 1 month every year).

7.4. International Research Visitors

7.4.1. Visits of International Scientists

Researchers visiting the team to give a talk to the team seminar include Enea Milio (Inria Nancy Grand Est), Gregor Seiler (ETH Zurich), Aurélien Focqué (Industry) and Razvan Barbulescu (University Paris 6). Researchers visting the team for collaboration include Bernadette Perrin-Riou (Paris-Sud).

7.4.2. Visits to International Teams

F. Johansson visited during 1 week the PolSys team at LIP6, Pierre et Marie Curie University.

F. Johansson visited during 1 week (two times) with the Computer Algebra group, TU Kaiserslautern.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Selection

8.1.1.1. Member of the Conference Program Committees

A. Enge: 20th Workshop on Elliptic Curve Cryptography ECC 2016, İzmir

D. Robert was a member of the scientific committee for the Ecole Mathematique Africaine organised by Emmanuel Fouotsa at Bamenda.

F. Johansson organized the session: High-precision arithmetic, effective analysis and special functions. ICMS 2016, The 5th International Congress on Mathematical Software, ZIB Berlin.

8.1.2. Journal

8.1.2.1. Member of the Editorial Boards

K. Belabas acts on the editorial board of *Journal de Théorie des Nombres de Bordeaux* since 2005 and of *Archiv der Mathematik* since 2006.

H. Cohen is an editorial board member of *Journal de Théorie des Nombres de Bordeaux*; he is an editor for the Springer book series *Algorithms and Computations in Mathematics (ACM).*

J.-M. Couveignes is a member of the editorial board of the *Publications mathématiques de Besançon* since 2010.

A. Enge is an editor of *Designs, Codes and Cryptography* since 2004.

8.1.2.2. Reviewer - Reviewing Activities

F. Johansson reviewed for IEEE Transactions on Circuits and Systems I, IEEE Transactions on Computers, and ACM Transactions on Mathematical Software.

8.1.3. Invited Talks

- A. Enge: Mathematical Structures for Cryptography, Leiden: Short addition sequences for theta functions
- F. Johansson: talk at RAIM 2016, Banyuls-sur-mer on "Fast reversion of formal power series" and at FastRelax meeting, LAAS-CNRS, Toulouse on "Hypergeometric functions in Arb".

8.1.4. Scientific Expertise

J.-M. Couveignes is a member of the scientific council of the labex "Fondation Sciences Mathématiques de Paris", FSMP, Paris.

J.-M. Couveignes is a member of the ’conseil d’orientation’ of the labex "Institut de Recherche en Mathématiques, Interactions et Applications", IRMIA, Strasbourg.

8.1.5. Research Administration

A. Enge: Head of COST-GTRI, responsible for the scientific evaluation of all international cooperations of Inria

Since January 2015, K. Belabas is vice-head of the Math Institute (IMB). He also leads the computer science support service (“cellule informatique”) of IMB and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

He is an elected member of “commission de la recherche” in the academic senate of Bordeaux University.

He is a member of the “Conseil National des Université” (25th section, pure mathematics).

J.-P. Cerri is an elected member of the scientific council of the Mathematics Institute of Bordeaux (IMB) and responsible for the bachelor programme in mathematics and informatics.

Since January 2015, J.-M. Couveignes is the head of the Math Institute (IMB).

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : G. Castagnos, *Cryptanalyse*, 60h, M2, University of Bordeaux, France;

Master : G. Castagnos, *Cryptologie avancée*, 30h, M2, University of Bordeaux, France;

Master : G. Castagnos, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;

Master : D. Robert, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;

8.2.2. Supervision

Pinar Kiliçer: The class number one problem for genus-2 curves, Universities of Bordeaux and Leiden, supervised by A. Enge, M. Streng and P. Stevenhagen.

Iuliana Ciocanea-Teodorescu, Algorithms for finite rings, Universities of Bordeaux and Leiden, supervised by K. Belabas and H. Lenstra.

PhD in progress: Abdoulaye Maiga, *Computing canonical lift of genus 2 hyperelliptic curves*, University Dakar, supervised by Djiby Sow, Abdoul Aziz Ciss and D. Robert.

PhD in progress: Emmanouil Tzortzakis *Algorithms for $\mathbb{Q}$-curves*, supervised by K. Belabas and P. Bruin

PhD in progress: Pavel Solomatin *Topics on L-functions*, supervised by B. de Smit and K. Belabas

Liu Zhengying: Height of class polynomials. Ecole Polytechnique third year internship, supervised by D. Robert.

8.2.3. Juries

- PhD report by A. Enge on Loubna Ghammam: Utilisation des couplages en cryptographie asymétrique pour la micro-électronique, University of Rennes
- PhD report and jury by D. Robert on Alina Dudeanu: Computational Aspects of Jacobians of Hyperelliptic Curves, EPFL.
- D. Robert is a member of the jury of Agregations de Mathematiques. He is also the codirector with Alain Couvreur of the option "calcul formel" of the Modelisation part of the oral examination.

8.3. Popularization

D. Robert wrote with Sorina Ionica the chapter "Pairings" of the book Guide to Pairing-Based Cryptography [16] which will be published by CHAPMAN and HALL/CRC. This book aims to help Engineers understand and implement pairing based cryptography. In the Chapter Pairings D. Robert give a self contained definition and proof of the Weil and Tate pairing; including how to handle divisors with non disjoint support (this is often skipped in scientific papers but is important for practical implementations).

H. Cohen wrote a vulgarisation article [17] on Fermat's last theorem. This article explain (through the example of congruent numbers) the role of elliptic curves and algebraic number theory in the solution of Fermat's last theorem.

During the last PARIatelier four talks [19], [18], [20], [21] have been filmed and are available under a creative common licence. This will allow people from all the world to get started faster with PARI. The first two talks focus on setting up personal computers for the atelier and the new features of PARI. The next two are more technical and explain the new L-functions and modular forms features.

9. Bibliography

Major publications by the team in recent years

[1] E. Bayer-Fluckiger, J.-P. Cerri, J. Chaubert. *Euclidean minima and central division algebras*, in "International Journal of Number Theory", 2009, vol. 5, n$^{\text{o}}$ 7, pp. 1155–1168, http://www.worldscinet.com/ijnt/05/0507/S1793042109002614.html

[2] K. Belabas, M. Bhargava, C. Pomerance. *Error estimates for the Davenport-Heilbronn theorems*, in "Duke Mathematical Journal", 2010, vol. 153, n$^{\text{o}}$ 1, pp. 173–210, http://projecteuclid.org/euclid.dmj/1272480934

[3] J. Belding, R. Bröker, A. Enge, K. Lauter. *Computing Hilbert class polynomials*, in "Algorithmic Number Theory — ANTS-VIII", Berlin, A. van der Poorten, A. Stein (editors), Lecture Notes in Computer Science, Springer-Verlag, 2007, vol. 5011, http://hal.inria.fr/inria-00246115

[4] J.-P. Cerri. *Euclidean minima of totally real number fields: algorithmic determination*, in "Math. Comp.", 2007, vol. 76, n$^{\text{o}}$ 259, pp. 1547–1575, http://www.ams.org/journals/mcom/2007-76-259/S0025-5718-07-01932-1/

[5] H. Cohen. *Number Theory I: Tools and Diophantine Equations; II: Analytic and Modern Tool*, Graduate Texts in Mathematics, Springer-Verlag, New York, 2007, vol. 239/240

[6] H. COHEN, G. FREY, R. AVANZI, C. DOCHE, T. LANGE, K. NGUYEN, F. VERCAUTEREN. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete mathematics and its applications, Chapman & Hall, Boca Raton, 2006

[7] J.-M. COUVEIGNES, B. EDIXHOVEN. *Computational aspects of modular forms and Galois representations*, Princeton University Press, 2011

[8] A. ENGE. *The complexity of class polynomial computation via floating point approximations*, in "Mathematics of Computation", 2009, vol. 78, n^{o} 266, pp. 1089–1107, http://www.ams.org/mcom/2009-78-266/S0025-5718-08-02200-X/home.html

[9] A. ENGE, P. GAUDRY, E. THOMÉ. *An L(1/3) Discrete Logarithm Algorithm for Low Degree Curves*, in "Journal of Cryptology", 2011, vol. 24, n^{o} 1, pp. 24–41

[10] D. LUBICZ, D. ROBERT. *Computing isogenies between abelian varieties*, in "Compositio Mathematica", 09 2012, vol. 148, n^{o} 05, pp. 1483–1515, http://dx.doi.org/10.1112/S0010437X12000243

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] P. KILIÇER. *The CM class number one problem for curves*, Leiden University ; Inria/LFANT, July 2016, https://tel.archives-ouvertes.fr/tel-01383309

Articles in International Peer-Reviewed Journals

[12] K. BELABAS, J.-F. JAULENT. *The logarithmic class group package in PARI/GP*, in "Publications Mathématiques de Besançon : Algèbre et Théorie des Nombres", 2017, https://hal.archives-ouvertes.fr/hal-01419870

[13] J. BRAU, N. JONES. *Elliptic curves with 2-torsion contained in the 3-torsion field*, in "Proceedings of the American Mathematical Society", 2016, vol. 144, pp. 925-936, https://hal.archives-ouvertes.fr/hal-01111744

[14] M. GALAND, K. HÉRITIER, E. ODELSTAD, P. HENRI, T. BROILES, A. ALLEN, K. ALTWEGG, A. BETH, J. BURCH, M. CARR, E. CUPIDO, I. ERIKSSON, H. GLASSMEIER, F. JOHANSSON, P. LEBRETON, E. MANDT, H. NILSSON, I. RICHTER, M. RUBIN, L. SAGNIÈRES, S. SCHWARTZ, T. SÉMON, C.-Y. TZOU, X. VALLIÈRES, E. VIGREN, P. WURZ. *Ionospheric plasma of comet 67P probed by Rosetta at 3 AU from the Sun*, in "Monthly Notices of the Royal Astronomical Society", 2016, vol. 464, n^{o} 1 [*DOI :* 10.1093/MNRAS/STW2891], https://hal-insu.archives-ouvertes.fr/insu-01404142

[15] D. LUBICZ, D. ROBERT. *Arithmetic on Abelian and Kummer Varieties*, in "Finite Fields and Applications", May 2016, vol. 39, pp. 130-158 [*DOI :* 10.1016/J.FFA.2016.01.009], https://hal.archives-ouvertes.fr/hal-01057467

Research Reports

[16] S. IONICA, D. ROBERT. *Pairings*, MIS, 2016, CRC Press, to appear, https://hal.archives-ouvertes.fr/hal-01323882

Scientific Popularization

[17] H. COHEN. *Le grand théorème de Fermat*, in "Quadrature", 2016, vol. 102, pp. 10-19, https://hal.inria.fr/hal-01379484

Other Publications

[18] B. ALLOMBERT, F. BASTIEN. *Bill Allombert - "New GP features" : Atelier PARI/GP 2016*, January 2016, https://hal.archives-ouvertes.fr/medihal-01326362

[19] B. ALLOMBERT, K. BELABAS, F. BASTIEN. *B. Allombert et Karim Belabas - Start of Atelier : setting up personnal computers: Atelier PARI/GP 2016*, January 2016, https://hal.archives-ouvertes.fr/medihal-01346601

[20] K. BELABAS, F. BASTIEN. *Karim Belabas - L-functions: Atelier PARI/GP 2016*, January 2016, https://hal.archives-ouvertes.fr/medihal-01346708

[21] H. COHEN, F. BASTIEN. *Henri Cohen- Modular forms: Atelier PARI/GP 2016*, January 2016, https://hal.archives-ouvertes.fr/medihal-01346724

[22] H. COHEN, F. THORNE. *On D_ℓ extensions of odd prime degree ℓ*, 2016, working paper or preprint, https://hal.inria.fr/hal-01379473

[23] A. ENGE, W. HART, F. JOHANSSON. *Short addition sequences for theta functions*, August 2016, working paper or preprint, https://hal.inria.fr/hal-01355926

[24] A. ENGE, M. STRENG. *Schertz style class invariants for quartic CM fields*, 2016, working paper or preprint, https://hal.inria.fr/hal-01377376

[25] F. JOHANSSON. *Arb: Efficient Arbitrary-Precision Midpoint-Radius Interval Arithmetic*, November 2016, working paper or preprint, https://hal.inria.fr/hal-01394258

[26] F. JOHANSSON. *Computing hypergeometric functions rigorously*, July 2016, working paper or preprint, https://hal.inria.fr/hal-01336266

[27] A. MEURER, C. P. SMITH, M. PAPROCKI, O. ČERTÍK, S. B. KIRPICHEV, M. ROCKLIN, A. KUMAR, S. IVANOV, J. K. MOORE, S. SINGH, T. RATHNAYAKE, S. VIG, B. E. GRANGER, R. P. MULLER, F. BONAZZI, H. GUPTA, S. VATS, F. JOHANSSON, F. PEDREGOSA, M. J. CURRY, A. R. TERREL, Š. ROUČKA, A. SABOO, I. FERNANDO, S. KULAL, R. CIMRMAN, A. SCOPATZ. *SymPy: Symbolic computing in Python*, May 2016, working paper or preprint [*DOI :* 10.7287/PEERJ.PREPRINTS.2083V3], https://hal.inria.fr/hal-01404156

References in notes

[28] K. BELABAS. *L'algorithmique de la théorie algébrique des nombres*, in "Théorie algorithmique des nombres et équations diophantiennes", N. BERLINE, A. PLAGNE, C. SABBAH (editors), 2005, pp. 85–155

[29] H. COHEN, P. STEVENHAGEN. *Computational class field theory*, in "Algorithmic Number Theory — Lattices, Number Fields, Curves and Cryptography", J. BUHLER, P. STEVENHAGEN (editors), MSRI Publications, Cambridge University Press, 2008, vol. 44

[30] A. ENGE. *Courbes algébriques et cryptologie*, Université Denis Diderot, Paris 7, 2007, Habilitation à diriger des recherches, http://tel.archives-ouvertes.fr/tel-00382535/en/