RESEARCH CENTRE

Bordeaux - Sud-Ouest

IN PARTNERSHIP WITH:

CNRS, Université de Bordeaux

2020

ACTIVITY REPORT

Project-Team

LFANT

Lithe and fast algorithmic number theory

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team LFANT

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

Keywords

Computer sciences and digital sciences

A4.3.1. – Public key cryptography

A8.4. – Computer Algebra

A8.5. – Number theory

A8.10. – Computer arithmetic

Other research topics and application domains

B6. – IT and telecom

B9.5.2. – Mathematics

1 Team members, visitors, external collaborators

Research Scientists

- Andreas Enge [Team leader, Inria, Senior Researcher, HDR]
- Razvan Barbaud [CNRS, Researcher]
- Xavier Caruso [CNRS, Senior Researcher, HDR]
- Fredrik Johansson [Inria, Researcher]
- Aurel Page [Inria, Researcher]
- Damien Robert [Inria, Researcher]
- Benjamin Wesolowski [CNRS, Researcher]

Faculty Members

- Karim Belabas [Univ de Bordeaux, Professor, HDR]
- Guilhem Castagnos [Univ de Bordeaux, Associate Professor, HDR]
- Jean-Paul Cerri [Univ de Bordeaux, Associate Professor]
- Henri Cohen [Univ de Bordeaux, Emeritus, HDR]
- Jean-Marc Couveignes [Univ de Bordeaux, Professor, HDR]

PhD Students

- Jared Guissmo Asuncion [Univ de Bordeaux]
- Amaury Durand [Univ de Bordeaux]
- Elie Eid [Univ de Rennes I]
- Jean Kieffer [École Normale Supérieure de Paris]
- Abdoulaye Maiga [Université Cheikh Anta Diop, Dakar, Sénégal]
- Pavel Solomatin [Université de Leiden - Pays-Bas]
- Ida Tucker [École Normale Supérieure de Lyon, until Sep 2020]
- Anne Edgar Wilke [Inria]

Technical Staff

- Bill Allombert [CNRS, Engineer]

Interns and Apprentices

- Pierre Briaud [Inria, Intern, from Mar 2020 until Jun 2020]
- Oren Nezer [Inria, Intern, from Mar 2020 until Jul 2020]

Administrative Assistant

- Sabrina Duthil [Inria]

External Collaborator

- Tony Ezome Mintsa [Université des Sciences et Techniques de Masuku - Gabon]

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, Jared Guissmo Asuncion, Karim Belabas, Xavier Caruso, Jean-Paul Cerri, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Aurel Page.

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 $n \geqslant 3$. 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 [54] 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, $\zeta_K(s) := \prod_{\mathfrak{p} \text{ prime ideal of } \mathcal{O}_K} (1 - \mathrm{N}\mathfrak{p}^{-s})^{-1}$, 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 Razvan Barbulescu, Karim Belabas, Guilhem Castagnos, Jean-Marc Couveignes, Andreas Enge, Damien Robert, Benjamin Wesolowski, Jean Kieffer.

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 $\mathscr{C}(X,Y)=0$ 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 $\mathscr{C}=Y^2-(X^3+aX+b)$ and *hyperelliptic curves* of equation $\mathscr{C}=Y^2-(X^{2g+1}+\cdots)$ with $g\geqslant 2$.

The cryptosystem is implemented in an associated finite abelian group, the *Jacobian* $\mathrm{Jac}_{\mathscr{C}}$. 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 $\mathscr{C}$ is $K_{\mathscr{C}}=\mathbb{F}_q(X)[Y]/(\mathscr{C})$; it contains the *coordinate ring* $\mathscr{O}_{\mathscr{C}}=\mathbb{F}_q[X,Y]/(\mathscr{C})$. Definitions and properties carry over from the number field case $K/\mathbb{Q}$ to the function field extension $K_{\mathscr{C}}/\mathbb{F}_q(X)$. The Jacobian $\mathrm{Jac}_{\mathscr{C}}$ is the divisor class group of $K_{\mathscr{C}}$, which is an extension of (and for the curves used in cryptography usually equals) the ideal class group of $\mathscr{O}_{\mathscr{C}}$.

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 $(\sqrt{q}-1)^{2g}\leqslant|\mathrm{Jac}_{\mathscr{C}}|\leqslant(\sqrt{q}+1)^{2g}$, or $|\mathrm{Jac}_{\mathscr{C}}|\approx q^g$, 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 $\frac{\deg_X\mathscr{C}-1}{2}$. 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 $\mathrm{Jac}_{\mathscr{C}}$, it must be difficult to determine x. Computing x corresponds in fact to computing $\mathrm{Jac}_{\mathscr{C}}$ 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 $\mathscr{C}$ is a function that takes as input two elements of order n of $\mathrm{Jac}_{\mathscr{C}}$ 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 Jared Guissmo Asuncion, Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Fredrik Johansson, Damien Robert, Anne-Edgar Wilke.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [60, Sect. 1.1], for more background material, [59]. In fact, for most curves $\mathscr{C}$ over a finite field, the endomorphism ring of $\mathrm{Jac}_{\mathscr{C}}$, 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 $\mathscr{C}$ 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 Application domains

4.1 Number theory

Being able to compute quickly and reliably algebraic invariants is an invaluable aid to mathematicians: It fosters new conjectures, and often shoots down the too optimistic ones. Moreover, a large body of theoretical results in algebraic number theory has an asymptotic nature and only applies for large enough inputs; mechanised computations (preferably producing independently verifiable certificates) are often necessary to finish proofs.

For instance, many Diophantine problems reduce to a set of Thue equations of the form $P(x,y)=a$ for an irreducible, homogeneous $P \in \mathbb{Z}[x,y]$, $a \in \mathbb{Z}$, in unknown integers x, y. In principle, there is an algorithm to solve the latter, provided the class group and units of a rupture field of P are known. Since there is no other way to prove that the full set of solutions is obtained, these algebraic invariants must be computed and certified, preferably without using the GRH.

Deeper invariants such as the Euclidean spectrum are related to more theoretical concerns, e.g., determining new examples of principal, but not norm-Euclidean number fields, but could also yield practical new algorithms: Even if a number field has class number larger than 1 (in particular, it is not norm-Euclidean), knowing the upper part of the spectrum should give a *partial* gcd algorithm, succeeding for almost all pairs of elements of $\mathcal{O}_K$. As a matter of fact, every number field whose unit group has rank strictly greater than 1 is almost norm-Euclidean [57, 56].

Algorithms developed by the team are implemented in the free PARI/GP system for number theory maintained by K. Belabas (see §6.1 for details). They will thus have a high impact on the worldwide number theory community, for which PARI/GP is a reference and the tool of choice.

4.2 Cryptology

Public key cryptology has become a major application domain for algorithmic number theory. This is already true for the ubiquitous RSA system, but even more so for cryptosystems relying on the discrete logarithm problem in algebraic curves over finite fields. For the same level of security, the latter require smaller key lengths than RSA, which results in a gain of bandwidth and (depending on the precise application) processing time. Especially in environments that are constrained with respect to space and computing power such as smrt cards and embedded devices, algebraic curve cryptography has become the technology of choice. Most of the research topics of the LFANT team detailed in §3 concern directly problems relevant for curve-based cryptology: The difficulty of the discrete logarithm problem in algebraic curves (§3.2) determines the security of the corresponding cryptosystems. Complex multiplication, point counting and isogenies (§3.3) provide, on one hand, the tools needed to create secure instances of curves. On the other hand, isogenies have been found to have direct cryptographic applications to hash functions [58] and encryption [61]. Pairings in algebraic curves (§3.2) have proved to be a a rich source for novel cryptographic primitives. Class groups of number fields (§3.1) also enter the game as candidates for algebraic groups in which cryptosystems can be implemented. However, breaking these systems by computing discrete logarithms has proved to be easier than in algebraic curves; we intend to pursue this cryptanalytic strand of research.

Apart from solving specific problems related to cryptology, number theoretic expertise is vital to provide cryptologic advice to industrial partners in joint projects. It is to be expected that continuing pervasiveness and ubiquity of very low power computing devices will render the need for algebraic curve cryptography more pressing in coming years.

5 Highlights of the year

5.1 Awards

B. Allombert has been awarded the Cristal medal of CNRS for outstanding contributions to the advancement of knowledge and the excellence of French research, as the main developer of the PARI/GP computer algebra system.[1]

I. Tucker has received the 2020 Prix Jeunes Talents France L'Oréal–UNESCO pour les femmes et la science.[2]

B. Wesolowski and his coauthors have been awarded the Best Paper Award at ASIACRYPT 2020 for their article [23].

5.2 Defenses

I. Tucker has defended her doctoral thesis *Functional encryption and distributed signatures based on projective hash functions, the benefit of class groups* [26].

Sudarshan Shinde has defended his doctoral thesis *Cryptographic applications of modular curves* [25].

5.3 Major software releases

The PARI Group released a new version of PARI/GP (2.13) featuring many bug fixes and optimizations, including a better MPQS integer factorization engine, a complete rewrite of algebraic number theory modules to use "compact units" representations throughout (represent algebraic numbers as formal products of small S-units) and new tricks to avoid tough discrete logarithms by working in appropriate quotients, a new algorithm to compute subfields, and a rewrite of the Bernoulli numbers cache generation (inspired by ARB).

ARB has had two new releases, 2.18 and 2.19. These releases mainly feature a large number of bug fixes and optimizations.

The year 2020 has seen the release 1.2 *Hyacinthus orientalis* of GNU MPC. The release features the new functions `mpc_sum` and `mpc_dot` and several bug fixes, in particular to make functions more robust if the user reduces the exponent range. It also contains the tool `mpcheck` for easier comparison with computations by the C library on standard precision floating-point numbers.

5.4 Special events

The year 2020 was marked by the covid crisis and its impact on society and its overall activity. The world of research was also greatly affected: Faculty members have seen their teaching load increase significantly; PhD students and post-docs have often had to deal with a worsening of their working conditions, as well as with reduced interactions with their supervisors and colleagues; most scientific collaborations have been greatly affected, with many international activities cancelled or postponed to dates still to be defined.

The LFANT team was able, however, to organise a physical PARI/GP workshop in Grenoble in January 2020, right before the pandemic struck, with videos of some presentations made available[51, 49, 48, 50].

[1] https://www.insmi.cnrs.fr/fr/cnrsinfo/propos-de-la-medaille-de-cristal-de-bill-allombert

[2] https://www.inria.fr/fr/ida-tucker-jeune-talent-loreal-unesco

6 New software and platforms

6.1 New software

6.1.1 PARI/GP

Keyword: Computational number theory

Functional Description: Pari/Gp is a widely used computer algebra system designed for fast computations in number theory (factorisation, algebraic number theory, elliptic curves, modular forms ...), 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.

URL: `http://pari.math.u-bordeaux.fr/`

Contacts: Andreas Enge, Karim Belabas

Participants: Andreas Enge, Hamish Ivey-Law, Henri Cohen, Karim Belabas

Partner: CNRS

6.1.2 Arb

Name: Arb

Keywords: Multiple-Precision, Interval arithmetic, Interval analysis, Computational number theory, Numerical algorithm

Functional Description: C library for arbitrary-precision ball arithmetic

URL: `http://arblib.org`

Contact: Fredrik Johansson

6.1.3 GNU MPC

Keyword: Arithmetic

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.

Release Contributions: Bug fixes: - Fix an incompatibility problem with GMP 6.0 and before. - Fix an intermediate overflow in asin.

URL: `http://www.multiprecision.org/`

Authors: Andreas Enge, Philippe Théveny, Paul Zimmermann, Mickaël Gastineau

Contacts: Andreas Enge, Paul Zimmermann

Participants: Andreas Enge, Mickaël Gastineau, Paul Zimmermann, Philippe Théveny

6.1.4 abelianbnf

Keyword: Computational number theory

Functional Description: abelianbnf is a gp script computing class groups of abelian fields using norm relations in the Galois group. Requires Pari/gp, development version or stable version v2.13+.

URL: `https://hal.inria.fr/hal-02961482`

Publication: hal-02497890

Contact: Aurel Page

6.1.5 APIP

Name: Another Pairing Implementation in PARI

Keywords: Cryptography, Computational number theory

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.

URL: http://www.lix.polytechnique.fr/~milanj/apip/apip.xhtml

Author: Jérôme Milan

Contact: Andreas Enge

Participant: Jérôme Milan

6.1.6 AVIsogenies

Name: Abelian Varieties and Isogenies

Keywords: Computational number theory, Cryptography

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.

URL: http://avisogenies.gforge.inria.fr/

Contact: Damien Robert

Participants: Damien Robert, Gaëtan Bisson, Romain Cosset

6.1.7 CM

Keyword: Arithmetic

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.

Release Contributions: Changes in version 0.3.1 ("Wurstebrei"): - increase minimal version number for mpfrcx to 0.5 and for pari to 2.9. - many internal rewrites - bug fixes

URL: http://www.multiprecision.org/cm/home.html

Author: Andreas Enge

Contact: Andreas Enge

Participant: Andreas Enge

6.1.8 CMH

Name: 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.

URL: http://cmh.gforge.inria.fr

Authors: Andreas Enge, Emmanuel Thomé, Regis Dupont

Contacts: Emmanuel Thomé, Andreas Enge

Participants: Andreas Enge, Emmanuel Thomé, Regis Dupont

6.1.9 CUBIC

Keyword: Number theory

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.

URL: http://www.math.u-bordeaux.fr/~belabas/research/software/cubic-1.2.tgz

Contact: Karim Belabas

Participant: Karim Belabas

6.1.10 Euclid

Keyword: Number theory

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.

URL: http://www.math.u-bordeaux1.fr/~plezowsk/euclid/index.php

Contact: Jean-Paul Cerri

Participants: Jean-Paul Cerri, Pierre Lezowski

6.1.11 FromLatticesToModularForms

Keyword: Cryptography

Functional Description: FromLatticesToModularForms is a magma package which allows to

- span the isogeny class (of principally polarised abelian varieties) of a power of an elliptic curve by enumerating unimodular hermitian lattices - compute the abelian variety A corresponding to a given lattice by exhibiting a kernel and an isogeny from Eĝ to A - A is represented by its theta null point (of level 2 or 4) in such a way that we give an affine lift of the theta null point corresponding to the pushforward of the standard diagonal differential dx/y on Eĝ - in particular one can evaluate rational modular forms on A - in dimension 2 or 3 we also provide code to recognize when A is a Jacobian and if so to find the corresponding curve.

URL: https://gitlab.inria.fr/roberdam/fromlatticestomodularforms

Contact: Damien Robert

6.1.12 KleinianGroups

Keywords: Computational geometry, Computational number theory

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

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

Publication: hal-00703043

Contact: Aurel Page

6.1.13 MPFRCX

Keyword: Arithmetic

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.

Release Contributions: Changes in version 0.6: - new functions mpfrx_eval and mpcx_eval for evaluating polynomials in a single argument using a Horner scheme, this complements the existing functions mpcx_multieval and mpfrx_multieval - new convenience functions * mpcx_mul_c, mpcx_mul_fr, mpcx_mul_si, mpcx_mul_ui, mpfrx_mul_fr, mpfrx_mul_si, mpfrx_mul_ui for multiplying polynomials by constants of various types * mpcx_mul_x, mpfrx_mul_x for multiplying by powers of the variable - bug: make multieval work for polynomials of degree <= 1

URL: http://www.multiprecision.org/mpfrcx/home.html

Author: Andreas Enge

Contact: Andreas Enge

Participant: Andreas Enge

6.1.14 Nemo

Name: Nemo

Keywords: Computer algebra system (CAS), Symbolic computation

Functional Description: A computer algebra package for the Julia programming language

URL: http://nemocas.org

Contact: Fredrik Johansson

Partner: Technische Universität Kaiserslautern (UniKL), Allemagne

6.2 New platforms

6.2.1 Tate algebras

Following the article [30], Xavier Caruso and Thibaut Verron implemented the *PoTe* and the *VaPoTe* algorithm for computing Gröbner bases in Tate algebras; their implementation is part of the standard distribution of SageMath since version 9.1.

6.2.2 Ore polynomials

Xavier Caruso wrote a package on Ore polynomials, which has been accepted for inclusion in SageMath, version 9.2. Beyond basic operations, this implementation includes capabilities for working in the field of fractions of Ore algebras and an optimized factorization algorithm for skew polynomials over finite fields.

6.2.3 From Lattices To Modular Forms

A code implementing the article [46] for spanning the isogeny class of products of elliptic curves and computing modular forms (and related obstruction) on them is available as a MAGMA package called FromLatticesToModularForm.

6.2.4 Modular polynomials

The paper [19] was the first paper for the reproducibility pilot of the *Journal of Number Theory*. The reproducibility archive is available at https://data.mendeley.com/datasets/yy3bty5ktk/1.

7 New results

7.1 Cryptography

Participants Razvan Barbulescu, Guilhem Castagnos, Ida Tucker, Benjamin Wesolowski.

Classical public-key cryptography. The security of pairing-based cryptography requires discrete logarithms in finite fields of degree larger than 1 to be difficult to compute. After having proposed several improvements which reduced the security of the proposed pairings in the literature, R. Barbulescu together with Sylvain Duquesne suggested in 2019 a model to evaluate the security of pairings [53]. In a subsequent work Nadia El Mrabet pointed out that exotic pairings, not studied in the literature before might be interesting, and this led to a joint study with Loubna Ghammam and R. Barbulescu of over 200 curve families [27], providing very precise security estimates.

The presumed hardness of the discrete logarithm problem (DLP) in finite fields (or other families of groups) is a foundation of classical public-key cryptography. It has recently been discovered that the DLP is much easier than previously believed in an important family: finite fields of *small characteristic*.

Algorithms of quasi-polynomial complexity have been discovered. In [37], R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski and J. Zumbrägel demonstrate the practicality of these new methods through the computation of a discrete logarithm in $\mathbb{F}_{2^{30750}}$, breaking by a large margin the previous record, which was set in January 2014 by a computation in $\mathbb{F}_{2^{9234}}$.

In [21], G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker propose a new cryptographic protocol to compute threshold EC-DSA signatures with two parties. EC-DSA (Elliptic Curves Digital Signature Algorithm) is a widely adopted standard for electronic signatures. For instance, it is used in the TLS (Transport Layer Security) protocol and in many cryptocurrencies such as Bitcoin. Threshold Signatures allow n parties to share the power of issuing digital signatures so that any coalition of size at least $t+1$ can sign, whereas groups of t or less players cannot. Over the last few years many schemes addressed the question of realizing efficient threshold variants for the specific case of EC-DSA signatures. In this work they present new solutions to the problem that aim at reducing the overall bandwidth consumption. The main contribution is a new variant of the Gennaro and Goldfeder protocol from ACM CCS 2018 using cryptography based of class groups of quadratic fields that avoids all the required range proofs, while retaining provable security against malicious adversaries in the dishonest majority setting. The experiments show that – for all levels of security – the new signing protocol reduces the bandwidth consumption of best previously known secure protocols for factors varying between 4.4 and 9, while key generation is consistently two times less expensive. Furthermore compared to these same protocols, signature generation is faster for 192-bits of security and beyond.

Post-quantum cryptography. It has been known since the work of Shor in 1994 that a functional, large-scale quantum computer would be able to break most classical public-key cryptosystems deployed today. The cryptographic community has since then investigated new families of *post-quantum* cryptosystems, meant to resist the advance of quantum computing. *Lattice-based cryptography*, one of the leading post-quantum candidates, relies on the presumed hardness of certain computational problems in euclidean lattices. There is strong confidence in the hardness of these problems in general, but the use of algebraic lattices (necessary for efficiency or advanced functionalities) opens new angles of attack. In [14], R. Cramer, L. Ducas and B. Wesolowski expose an unexpected quantum hardness gap between generic lattices and an important family of algebraic lattices, so-called *cyclotomic ideal lattices*. This journal article expands upon preliminary results presented at Eurocrypt 2017.

An ideal lattice is essentially an ideal in the ring on integers of a number field that is stable by multiplication, with a geometry induced by the Minkowski embedding. Fixing a number field, the space of all ideal lattices, up to isometry, is naturally an abelian group called the *Arakelov class group*. In [22], K. De Boer, L. Ducas, A. Pellet-Mary and B. Wesolowski study the relative hardness of computational problems within the Arakelov class group. More precisely, it is shown that the worst-case of the Shortest Vector Problem (*Ideal-SVP*) reduces to its average-case (up to an approximation factor that depends on the field). In other words, "random" instances of Ideal-SVP are as hard as the hardest ones, an essential property for building cryptography. This result assumes the Riemann Hypothesis for Hecke L-functions, which allows to prove that certain random walks in Arakelov class groups have rapid mixing properties.

Isogeny-based cryptography is another popular candidate for post-quantum cryptography. Their main asset: they allow for smaller keys than other post-quantum candidates, and more confident key-size selection. For a while, is was unknown whether one could build an isogeny-based digital signature scheme (besides the immediate but inefficient construction from the Jao–De Feo–Plût identification protocol). In [23], L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski introduce the signature scheme *SQISign*. Its most notable feature is its compactness: the signature and public key sizes combined are an order of magnitude smaller than all other post-quantum signature schemes. It is however less efficient than its competitors: on a modern workstation, the proof-of-concept C implementation takes 2.5s for signing, and 50ms for verification.

Verifiable delay functions. In [20], B. Wesolowski constructs the first practical verifiable delay function (VDF). A VDF is a function whose evaluation requires running a given number of sequential steps, yet the result can be efficiently verified. They have applications in decentralised systems, such as the generation of trustworthy public randomness in a trustless environment, or resource-efficient blockchains. This journal article expands upon preliminary results presented at Eurocrypt 2019.

The construction is based on groups of unknown order such as an RSA group or the class group of an imaginary quadratic field. The “delaying” property relies on the assumption that in groups of unknown order, exponentiating a random element by 2^t essentially requires to perform t squarings sequentially, and parallelisation does not allow to go faster. It is then important to understand precisely how quickly a single modular squaring operation can be computed, even in parallel on dedicated hardware. To this end, in [47], B. Wesolowski and R. Williams devise lower bounds for the depth of circuits computing modular squaring.

7.2 Number fields

Participants Razvan Barbulescu, Henri Cohen, Jean-Marc Couveignes, Aurel Page.

In [12], H. Cohen and F. Thorne give explicit formulæ for the Dirichlet series generating function of D_ℓ-extensions of odd prime degree ℓ with given quadratic resolvent.

In [11], Razvan Barbulescu in a joint work with Jishnu Ray (University of British Columbia, Vancouver) brings elements to support Greenberg’s p-rationality conjecture. On the theoretical side, they propose a new family proven to be p-rational. On the algorithmic side, they compare the tools to enumerate number fields of given abelian Galois group and of computing class numbers, and extend the experiments on the Cohen–Lenstra–Martinet conjectures.

In [13] and [34], Jean-Marc Couveignes constructs small models of number fields and functions fields. One option is to look for local equations rather than a full set of generators of the ideal of these models. Another option is to provide approximations of a small collection of algebraic numbers or functions in the field of interest, that are sharp enough to recover the ideal of relations. A consequence for number fields is a better bound for the number of number fields of given degree n and discriminant bounded by H.

In [29], A. Page and his coauthors analyse in detail the subfield method to accelerate the computation of S-units and class groups, in the Galois case. They introduce a new group-theoretic notion of norm relation that extends classical ones and give criteria for the existence of such relations. They provide subfield-based algorithms for the computation of invariants of number fields in the presence of a norm relation and prove a polynomial-time reduction to the subfields. They compute class groups of number fields of large degree that go far beyond previous records, both under GRH (degree 1728) and unconditionally (degree 576).

7.3 Modular forms and L-functions

Participants Razvan Barbulescu, Damien Robert.

The best algorithms for integer factorisation use a non-negligible proportion of the time to enumerate smaller integers and to test if all their prime factors are below a given bound. A lot of effort has been spent in the literature to improve the best algorithm for this task, the elliptic curve method (ECM). In [28], R. Barbulescu and his doctoral student Sudarshan Shinde have given a simple method which allows to find rapidly, in a unified manner, all the previously known families of elliptic curves for ECM. They proved that there are precisely 1525 ECM-friendly families using the theory of modular forms.

In [46], M. Kirschmer, F. Narbonne, C. Ritzenthaler and D. Robert give an algorithm to span the isomorphism classes of principally polarized abelian varieties in the isogeny class of E^g, where E is an elliptic curve. The varieties are first described as hermitian lattices over (not necessarily maximal) quadratic orders and then geometrically in terms of their algebraic theta null point. They also show how to algebraically compute Siegel modular forms of even weight given as polynomials in the theta constants by a careful choice of an affine lift of the theta null point. They then use these results to give an algebraic computation of Serre’s obstruction for principally polarized abelian threefolds isogenous to E^3 and of the Igusa modular form in dimension 4. They illustrate these algorithms with examples of curves with many rational points over finite fields.

7.4 p-adic rings and geometry

Participants Xavier Caruso.

In [32], Xavier Caruso, Tristan Vaccon and Thibaut Verron continued to develop the theory of Gröbner bases over Tate algebras: they designed two F5-like algorithms, called *PoTe* (**Po**sition over **Te**rm) and *VaPoTe* (**Va**luation over **Po**sition over **Te**rm) respectively and implemented them in the software SageMath.

In the note [30], Xavier Caruso studied the localisation of roots in an algebraic closure of random polynomials with coefficients in $\mathbb{Z}_p$ (the ring of p-adic numbers). He proved, in particular, that a polynomial of degree d over $\mathbb{Z}_p$ has 1 root in $\mathbb{Q}_p$ on average, and $d - O(1/p)$ roots on average in the maximal unramified extension of $\mathbb{Q}_p$.

7.5 Complex multiplication and isogenies of abelian varieties

Participants Xavier Caruso, Elie Eid, Sorina Ionica, Jean Kieffer, Abdoulaye Maiga, Chloe Martindale, Enea Milio, Aurel Page, Damien Robert.

In [18], Chloe Martindale, former doctoral student in the team, presents an algorithm to compute higher dimensional Hilbert modular polynomials. She also explains applications of this algorithm to point counting, walking on isogeny graphs, and computing class polynomials.

The paper by E. Milio, former doctoral student in the team, and D. Robert [19] on computing cyclic modular polynomials has been published. This was the first paper of the Journal of Number Theory with a reproducible archive for computations.

J. Kieffer, A. Page and D. Robert have updated their article [45] on computing isogenies between abelian surfaces using modular polynomials. They added a purely algebraic description of the deformation map and gave precise geometric conditions for the algorithm to work.

A. Maiga and D. Robert examine in [24] modular polynomials for abelian surfaces with good reduction modulo 2, which enables them to compute canonical lifts of such surfaces over a finite field of characteristic 2 and to ultimately deduce their cardinality, the main security parameter for hyperelliptic curve cryptosystems.

In [42], J. Kieffer gives degree and height bounds for modular equations on PEL Shimura varieties in terms of their level. In particular, this result answers previous questions about Hilbert and Siegel modular polynomials and the complexity of algorithms manipulating them.

In [44], J. Kieffer shows that the sign choices made in Dupont's algorithm to evaluate genus 2 theta constants in quasi-linear time in the precision are indeed correct. This gives a positive answer to a question raised by Dupont in his 2006 thesis, and lifts one of the heuristic that Dupont's algorithm uses.

In [43], J. Kieffer designs an algorithm to evaluate Siegel and Hilbert modular polynomials over number fields, based on complex approximations and fast computations of theta functions in genus 2. Analyzing the possible precision losses and using interval arithmetic makes the output provably correct. In many situations, using this algorithm to evaluate modular equations on the fly is more efficient than precomputing and storing them.

In [16], Sorina Ionica, former postdoc of the team, and Emmanuel Thomé look at the structure of isogeny graphs of genus 2 Jacobians with maximal real multiplication. They generalise a result of Kohel's describing the structure of the endomorphism rings of the isogeny graph of elliptic curves. Their setting considers genus 2 jacobians with complex multiplication, with the assumptions that the real multiplication subring is maximal and has class number 1. Over finite fields, they derive a depth first search algorithm for computing endomorphism rings locally at prime numbers, if the real multiplication is maximal.

In [31], X. Caruso, E. Eid and Reynald Lercier designed a new algorithm for computing isogenies between elliptic curves over an extension of the field of 2-adic numbers. Their methods rely on a highly efficient and numerically stable algorithm for solving certain types of nonlinear singular 2-adic differential equations. From this work, they deduced fast algorithms for computing isogenies between elliptic curves in characteristic 2 and generating irreducible polynomials of large degrees over $\mathbb{F}_2$.

In [35], E. Eid extended the above strategy to the case of isogenies between Jacobians of hyperelliptic curves in odd characteristic. The obtained algorithm has quasi-linear complexity with respect to the degree of the isogeny.

7.6 Multiprecision arithmetic

Participants Henri Cohen, Fredrik Johansson.

H. Cohen in [33] examines the branches of the complex Lambert W-function, branch identities and series developments.

In [38], F. Johansson describes Calcium, a new library for exact real and complex arithmetic with the ability to prove equalities for a large class of numbers.

In [36], E. Friedman, F. Johansson and G. Ramirez-Raposo prove a conjecture from 2014 by Katok, Katok and Rodriguez Hertz, rigorously establishing the minimal value of the Fried average entropy for higher-rank Cartan actions.

In [41], F. Johansson reviews the Preparata-Sarwate algorithm for computing the characteristic polynomial and determinant of matrices, finding that it outperforms more widely used algorithms in some applications.

In [40], F. Johansson describes FunGrim, a semantic database of special function identities.[3]

In [17], F. Johansson gives an algorithm for computing all the complex branches of the Lambert W function in arbitrary-precision arithmetic with rigorous error bounds.

In [39], F. Johansson describes a new algorithm for computing coefficients of the j-function and finds the first prime numbers in this sequence.

7.7 Miscellanea

Participants Andreas Enge.

With his contribution [15] to the Ten Years Reproducibility Challenge[4], A. Enge has endeavoured to reproduce the results of his 20 year old article on volume computation for convex polytopes [55]. While the content is not related to number theory, the success of the reproduction confirms the choice of the LFANT team to provide software mainly as portable and standard C code.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

G. Castagnos has a three years contract with Orange (Orange Labs Cesson-Sévigné) for the supervision of the PhD of Élie Bouscatié (Thèse CIFRE) from November 2020 to November 2023.

9 Partnerships and cooperations

9.1 International Initiatives

9.1.1 Visits of International Scientists

A. Bartel visited the team for two weeks in February.

[3] https://fungrim.org/

[4] https://rescience.github.io/ten-years/

9.2 National Initiatives

9.2.1 ANR ALAMBIC – AppLicAtions of MalleaBIlity in Cryptography

Participants 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.

9.2.2 ANR CLAP–CLAP – The p-adicr Langlands correspondence: a constructive and algorithmical approach

Participants Xavier Caruso, Jean-Marc Couveignes.

The p-adic Langlands correspondence has become nowadays one of the deepest and the most stimulating research programs in number theory. It was initiated in France in the early 2000's by Breuil and aims at understanding the relationships between the p-adic representations of p-adic absolute Galois groups on the one hand and the p-adic representations of p-adic reductive groups on the other hand. Beyond the case of $\mathrm{GL}_2(\mathbb{Q}_p)$ which is now well established, the p-adic Langlands correspondence remains quite obscure and mysterious new phenomena enter the scene; for instance, on the $\mathrm{GL}_n(F)$-side one encounters a vast zoology of representations which seems extremely difficult to organize.

The CLap–CLap ANR project aims at accelerating the expansion of the p-adic Langlands program beyond the well-established case of $\mathrm{GL}_2(\mathbb{Q}_p)$. Its main originality consists in its very constructive approach mostly based on algorithmics and calculations with computers at all stages of the research process. We shall pursue three different objectives closely related to our general aim:

1. draw a conjectural picture of the (still hypothetical) p-adic Langlands correspondence in the case of GL_n,
2. compute many deformation spaces of Galois representations and make the bridge with deformation spaces of representations of reductive groups,
3. design new algorithms for computations with Hilbert and Siegel modular forms and their associated Galois representations.

This project will also be the opportunity to contribute to the development of the mathematical software SAGEMATH and to the expansion of computational methodologies.

9.2.3 ANR CIAO – Cryptography, Isogenies and Abelian varieties Overwhelming

Participants Jean-Marc Couveignes, Jean Kieffer, Aurel Page, Damien Robert.

The CIAO ANR project is a young researcher ANR project led by Damien Robert October 2019.

The aim of the CIAO project is to study the security and improve the efficiency of the SIDH (supersingular isogenies Diffie Helmann) protocol, which is one of the post-quantum cryptographic project submitted to NIST, which passed the first round selection.

The project include all aspects of SIDH, from theoretical ones (computing the endomorphism ring of supersingular elliptic curves, generalisation of SIDH to abelian surfaces) to more practical aspects like arithmetic efficiency and fast implementations, and also extending SIDH to more protocols than just key exchange.

Applications of this project is to improve the security of communications in a context where the currently used cryptosystems are vulnerable to quantum computers. Beyond post-quantum cryptography, isogeny based cryptosystems also allow to construct new interesting cryptographic tools, like Verifiable Delay Functions, used in block chains.

10 Dissemination

10.1 Promoting Scientific Activities

10.1.1 Journal

Member of Editorial Boards X. Caruso is an editor and one of the founders of the journal *Annales Henri Lebesgue*.

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

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

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

10.1.2 Scientific Expertise

K. Belabas is a member of the “conseil scientifique” of the Société Mathématique de France.

A. Enge has acted as an evaluator for the German National Research Data Infrastructure[5] on the panel on mathematics, particle physics and astrophysics.

10.1.3 Research Administration

Since January 2015, K. Belabas is vice-head of the Mathematics 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.

Between January 2017 and June 2020, A. Enge was “délégué scientifique” of the Bordeaux-Sud-Ouest Inria Research Centre. As such, he was also a designated member of the “commission d’évaluation” of INRIA.

He is a member of the administrative council of the Société Arithmétique de Bordeaux, which edits the *Journal de théorie des nombres de Bordeaux* and supports number theoretic conferences.

G. Castagnos is responsible for the bachelor programme in mathematics and informatics.

[5] https://www.nfdi.de/en-gb/

10.2 Teaching - Supervision - Juries

10.2.1 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*, 30h, M2, University of Bordeaux, France;
- Licence: G. Castagnos, *Arithmétique et Cryptologie*, 24h, L3, Université de Bordeaux, France
- Master : D. Robert, *Courbes elliptiques*, 60h, M2, University of Bordeaux, France;
- Master: X. Caruso and J.-M. Couveignes, *Algorithmique arithmétique, introduction à l'algorithmique quantique*, 60h, M2, University of Bordeaux, France;
- Master : K. Belabas, *Algèbre et calcul formel 1 et 2*, 91h, M2, University of Bordeaux, France;
- Licence: K. Belabas, *Algorithmique mathématique 2*, TD, 35h, L3, University of Bordeaux, France;
- Licence: K. Belabas, *Structures algébriques 1*, TD, 51h, L2, University of Bordeaux, France;
- Master: J.-M. Couveignes, *Modules, espaces quadratiques*, 30h, M1, University of Bordeaux, France;
- Licence : J.-P. Cerri, *Arithmétique et Cryptologie*, TD, 36h, L3, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Algèbre linéaire*, TD, 51h, L2, Université de Bordeaux, France;
- Licence : J.-P. Cerri, *Topologie*, TD, 35h, L3, Université de Bordeaux, France;
- Master : J.-P. Cerri, *Cryptologie*, Cours-TD, 60h, M1, Université de Bordeaux, France;
- Licence: J. Kieffer, *Algorithmique Mathématique 2*, 32h, L3, Université de Bordeaux, France;
- Master: R. Barbulescu, *Arithmetic algorithms for cryptology*, M2, Master Parisien de Recherche Informatique;
- Licence, Master : J.-P. Cerri, 2 TER (L3, M1), 1 Projet (M2), Université de Bordeaux, France;
- Master : J. Asuncion, *Elliptic curves*, TD, 16h, M1, Universiteit Utrecht (Mastermath), Pays-Bas;
- Master: D. Robert, *Courbes elliptiques*, 30h, M2, University of Bordeaux, France;
- Licence : A.-E. Wilke, *Outils mathématiques pour la biologie*, TD, 32h, Université de Bordeaux, France;
- Licence : A.-E. Wilke, *Coloration mathématique*, TD, 32h, Université de Bordeaux, France.

10.2.2 Supervision

- Master thesis: Reem Chaalan, *Gabidulin Codes and Skew Polynomials*, supervised by Xavier Caruso
- Master thesis: William Dallaporta, *Parametrization of ideals and other algebraic structures by quadratic forms*, supervised by Karim Belabas
- Master thesis: Raoul Hallopeau, *From Euler's formula to derived categories*, supervised by Xavier Caruso
- Master thesis: Raphaël Pagès, *Étude d'algèbres d'opérateurs différentiels, techniques de calcul rapide de factorielles et applications au calcul de la p-courbure*, supervised by Alin Bostan and Xavier Caruso
- PhD in progress: Élie Bouscatié, *Conception d'algorithmes de chiffrement cherchable*, since November 2020, supervised by Guilhem Castagnos

- 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: Jared Asuncion, *Class fields of complex multiplication fields*, since September 2017, supervised by A. Enge and Marco Streng (Universiteit Leiden).
- PhD in progress: Elie Eid, *Computing isogenies between elliptic curves and curves of higher genus*, since September 2018, supervised by Xavier Caruso and Reynald Lercier
- PhD in progress: Amaury Durand, *Geometric Gabidulin codes*, since September 2019, supervised by Xavier Caruso
- PhD in progress: Jean Kieffer, *Computing isogenies between abelian surfaces*, since September 2018, supervised by Damien Robert and Aurel Page
- PhD in progress: Raphaël Pagès, *Factorisation des opérateurs différentiels en caractéristique p*, since September 2020, supervised by Alin Bostan and Xavier Caruso
- PhD in progress: Pavel Solomatin *Topics on L-functions*, since September 2018, supervised by B. de Smit and K. Belabas
- PhD in progress: Anne-Edgar Wilke *Enumerating integral orbits of prehomogeneous representations*, since September 2019, supervised by K. Belabas.
- PhD defended in 2020: I. Tucker *Functional encryption and distributed signatures based on projective hash functions, the benefit of class groups* [26], supervised by G. Castagnos with F. Laguillaumie, Université de Lyon
- PhD defended in 2020: Sudarshan Shinde *Cryptographic applications of modular curves* since October 2016, supervised by R. Barbulescu with Pierre-Vincent Koseleff (Sorbonne Université) [25]

10.2.3 Juries

- A. Enge has written a report for the doctoral dissertation by Simon Masson, Université de Lorraine: *Algorithmique des courbes destinées au contexte de la cryptographie bilinéaire et post-quantique.*
- X. Caruso and J.-M. Couveignes were part of the selection committee for a position of full professor in ENS Rennes.
- X. Caruso was part of the selection committee for a position of full professor in the University of Versailles.
- X. Caruso has written a report for the doctoral dissertation by Joelle Saade, Université de Limoges: *Méthodes symboliques pour les systèmes différentiels linéaires à singularité irrégulière.*
- K. Belabas was part of the selection committee for a position of full professor in Versailles Saint-Quentin-en-Yvelines University.
- R. Barbulescu was part of the three members jury of the oral examination in mathematics for math-info, the admission examination for ENS de Lyon.
- R. Barbulescu was a member of the jury for a lecturer position (maître de conférence) in the number theory team (mathematics) at University of Paris (former Paris 7).
- X. Caruso was part of the selection committee for a position of associate professor in the University of Limoges.
- D. Robert is a member of the jury of Agrégations de Mathématiques. He is also the director of the option “calcul formel” of the Modélisation part of the oral examination.

10.3 Popularization

X. Caruso and C. Ménini are leaders of the popularisation group at IMB (Institut de Mathématiques de Bordeaux).

R. Barbulescu, X. Caruso, A. Enge and B. Wesolowski have taken part as evaluators in the Tournois Français des Jeunes Mathématiciennes et Mathématiciens[6], a competition between high school classes on mathematical research questions.

R. Barbulescu is one of the organizers of Concours Alkindi[7], an online cryptography competition for middle and high school classes of French 4e, 3e and 2nde with 65000 participants in the 2019/2020 edition. Romania, Tunisia and Cameroun created national editions in which they use the same content as the French contest and had a few hundred participants.

10.3.1 Articles and contents

X. Caruso wrote several small webpages/apps in order to present interesting mathematical objects and highlight their more striking properties:

- a 2048-like game, based on the properties of the Fibonacci sequence `https://diffusion.math.u-bordeaux.fr/embed/987/`
- a walk on the flat surface of genus 2 `https://diffusion.math.u-bordeaux.fr/embed/walks/genus2.html`
- a dialog about the tilings of the hexagone `https://diffusion.math.u-bordeaux.fr/tilehexa/`

An ongoing collaboration with the PIRVI platform[8] has started; its main objective is to realise a 3D rendering engine in hyperbolic geometry.

10.3.2 Interventions

X. Caruso gave a talk and animated a workshop on continued fractions and their applications to the construction of musical scales.

11 Scientific production

11.1 Major publications

[1] E. Bayer-Fluckiger, J.-P. Cerri and J. Chaubert. ‘Euclidean minima and central division algebras’. In: *International Journal of Number Theory* 5.7 (2009), pp. 1155–1168. URL: `http://www.worldscinet.com/ijnt/05/0507/S1793042109002614.html`.

[2] K. Belabas, M. Bhargava and C. Pomerance. ‘Error estimates for the Davenport-Heilbronn theorems’. In: *Duke Mathematical Journal* 153.1 (2010), pp. 173–210. URL: `http://projecteuclid.org/euclid.dmj/1272480934`.

[3] X. Caruso and J. L. Borgne. ‘A new faster algorithm for factoring skew polynomials over finite fields’. In: *J. Symbolic Comput.* 79 (2018), pp. 411–443.

[4] X. Caruso, D. Roe and T. Vaccon. ‘Tracking p-adic precision’. In: *LMS J. Comput. Math.* 17 (2014), pp. 274–294.

[5] G. Castagnos, F. Laguillaumie and I. Tucker. ‘Practical Fully Secure Unrestricted Inner Product Functional Encryption modulo p’. In: *Advances in Cryptology – ASIACRYPT 2018, Part II*. Ed. by T. Peyrin and S. Galbraith. Vol. 11273. Lecture Notes in Computer Science. International Association for Cryptologic Research, 2018, pp. 733–764.

[6] `https://tfjm.org/`

[7] `https://www.concours-alkindi.fr/`

[8] `http://cristal.univ-lille.fr/pirvi/`

[6] H. Cohen and F. Strömberg. *Modular Forms: A Classical Approach.* Vol. 179. Graduate Studies in Mathematics. American Mathematical Society, 2017. URL: http://bookstore.ams.org/gsm-179/.

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

[8] A. Enge, P. Gaudry and E. Thomé. 'An L(1/3) Discrete Logarithm Algorithm for Low Degree Curves'. In: *Journal of Cryptology* 24.1 (2011), pp. 24–41.

[9] A. Enge, W. Hart and F. Johansson. 'Short addition sequences for theta functions'. In: *Journal of Integer Sequences* 18.2 (2018), pp. 1–34.

[10] D. Lubicz and D. Robert. 'Computing isogenies between abelian varieties'. In: *Compositio Mathematica* 148.05 (Sept. 2012), pp. 1483–1515. DOI: 10.1112/S0010437X12000243. URL: http://dx.doi.org/10.1112/S0010437X12000243.

11.2 Publications of the year

International journals

[11] R. Barbulescu and J. Ray. 'Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture'. In: *Journal de Théorie des Nombres de Bordeaux* 32.1 (2020), pp. 159–177. URL: https://hal.archives-ouvertes.fr/hal-01534050.

[12] H. Cohen and F. Thorne. 'On D_ℓ extensions of odd prime degree ℓ'. In: *Proceedings of the London Mathematical Society* 121.5 (2020), pp. 1171–1206. DOI: 10.1112/plms.12339. URL: https://hal.inria.fr/hal-01379473.

[13] J.-M. Couveignes. 'Enumerating number fields'. In: *Annals of Mathematics* 192.2 (2020), pp. 487–497. DOI: 10.4007/annals.2020.192.2.4. URL: https://hal.archives-ouvertes.fr/hal-02375397.

[14] R. Cramer, L. Ducas and B. Wesolowski. 'Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time'. In: *Journal of the ACM (JACM)* 68.2 (6th Jan. 2021), pp. 1–26. DOI: 10.1145/3431725. URL: https://hal.archives-ouvertes.fr/hal-03102234.

[15] A. Enge. '[Re] Volume computation for polytopes: Vingt ans après'. In: *The ReScience journal* 6.1 (4th Dec. 2020), #17. DOI: 10.5281/zenodo.4242972. URL: https://hal.inria.fr/hal-03053781.

[16] S. Ionica and E. Thomé. 'Isogeny graphs with maximal real multiplication'. In: *Journal of Number Theory* 207 (Feb. 2020), pp. 385–422. DOI: 10.1016/j.jnt.2019.06.019. URL: https://hal.archives-ouvertes.fr/hal-00967742.

[17] F. Johansson. 'Computing the Lambert W function in arbitrary-precision complex interval arithmetic'. In: *Numerical Algorithms* 83.1 (Jan. 2020), pp. 221–242. DOI: 10.1007/s11075-019-00678-x. URL: https://hal.inria.fr/hal-01519823.

[18] C. Martindale. 'Hilbert Modular Polynomials'. In: *Journal of Number Theory* 213 (2020), pp. 464–498. DOI: 10.1016/j.jnt.2019.11.019. URL: https://hal.inria.fr/hal-01990298.

[19] E. Milio and D. Robert. 'Modular polynomials on Hilbert surfaces'. In: *Journal of Number Theory* (May 2020). DOI: 10.1016/j.jnt.2020.04.014. URL: https://hal.archives-ouvertes.fr/hal-01520262.

[20] B. Wesolowski. 'Efficient Verifiable Delay Functions (extended version)'. In: *Journal of Cryptology* (9th Sept. 2020). DOI: 10.1007/s00145-020-09364-x. URL: https://hal.archives-ouvertes.fr/hal-02945371.

International peer-reviewed conferences

[21] G. Castagnos, D. Catalano, F. Laguillaumie, F. Savasta and I. Tucker. 'Bandwidth-Efficient Threshold EC-DSA'. In: PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography. Public-Key Cryptography – PKC 2020. Edinburgh / Virtual, United Kingdom, 29th Apr. 2020, pp. 266–296. DOI: 10.1007/978-3-030-45388-6_10. URL: https://hal.archives-ouvertes.fr/hal-02944825.

[22] K. De Boer, L. Ducas, A. Pellet-Mary and B. Wesolowski. 'Random Self-reducibility of Ideal-SVP via Arakelov Random Walks'. In: CRYPTO 2020. Santa Barbara, United States, 17th Aug. 2020. DOI: 10.1007/978-3-030-56880-1_9. URL: https://hal.archives-ouvertes.fr/hal-02513308.

[23] L. De Feo, D. Kohel, A. Leroux, C. Petit and B. Wesolowski. 'SQISign: compact post-quantum signatures from quaternions and isogenies'. In: ASIACRYPT 2020 - 26th Annual International Conference on the Theory and Application of Cryptology and Information Security. Daejeon (virtual), South Korea, 7th Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03038004.

[24] A. Maiga and D. Robert. 'Computing the 2-adic Canonical Lift of Genus 2 Curves'. In: ICMC 2021 - 7th International Conference on Mathematics and Computing. Shibpur / Virtual, India, 2nd Mar. 2021. URL: https://hal.inria.fr/hal-03119147.

Doctoral dissertations and habilitation theses

[25] S. Shinde. 'Cryptographic applications of modular curves'. Sorbonne Université, 10th July 2020. URL: https://tel.archives-ouvertes.fr/tel-03146424.

[26] I. Tucker. 'Functional encryption and distributed signatures based on projective hash functions, the benefit of class groups'. Université de Lyon, 19th Oct. 2020. URL: https://tel.archives-ouvertes.fr/tel-03021689.

Reports & preprints

[27] R. Barbulescu, N. El Mrabet and L. Ghammam. *A taxonomy of pairings, their security, their complexity*. 31st Aug. 2020. URL: https://hal.archives-ouvertes.fr/hal-02129868.

[28] R. Barbulescu and S. Shinde. *A classification of ECM-friendly families using modular curves: intégré à la thèse de doctorat de Sudarshan Shinde, Sorbonne Université, 10 juillet 2020*. 10th July 2020. URL: https://hal.archives-ouvertes.fr/hal-01822144.

[29] J.-F. Biasse, C. Fieker, T. Hofmann and A. Page. *Norm relations and computational problems in number fields*. 28th Feb. 2020. URL: https://hal.inria.fr/hal-02497890.

[30] X. Caruso. *Where are the zeroes of a random p-adic polynomial?* 28th Apr. 2020. URL: https://hal.archives-ouvertes.fr/hal-02557280.

[31] X. Caruso, E. Eid and R. Lercier. *Fast computation of elliptic curve isogenies in characteristic two*. 16th Mar. 2020. URL: https://hal.archives-ouvertes.fr/hal-02508825.

[32] X. Caruso, T. Vaccon and T. Verron. *Signature-based algorithms for Gröbner bases over Tate algebras*. 2020. URL: https://hal.archives-ouvertes.fr/hal-02473665.

[33] H. Cohen. *Lambert W-Function Branch Identities*. 23rd Dec. 2020. URL: https://hal.inria.fr/hal-03087491.

[34] J.-M. Couveignes. *Short models of global fields*. 4th Nov. 2020. URL: https://hal.archives-ouvertes.fr/hal-02989008.

[35] E. Eid. *Fast computation of hyperelliptic curve isogenies in odd characteristic*. 24th Sept. 2020. URL: https://hal.archives-ouvertes.fr/hal-02948514.

[36] E. Friedman, F. Johansson and G. Ramirez-Raposo. *The minimal Fried average entropy for higher-rank Cartan actions*. 22nd July 2020. URL: https://hal.inria.fr/hal-02904336.

[37] R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski and J. Zumbrägel. *Computation of a 30 750-Bit Binary Field Discrete Logarithm.* 22nd Sept. 2020. URL: https://hal.archives-ouvertes.fr/hal-02945361.

[38] F. Johansson. *Calcium: computing in exact real and complex fields.* 3rd Nov. 2020. URL: https://hal.inria.fr/hal-02986375.

[39] F. Johansson. *Computing isolated coefficients of the j-function.* 29th Nov. 2020. URL: https://hal.inria.fr/hal-03030172.

[40] F. Johansson. *FunGrim: a symbolic library for special functions.* 12th Mar. 2020. URL: https://hal.inria.fr/hal-02506816.

[41] F. Johansson. *On a fast and nearly division-free algorithm for the characteristic polynomial.* 24th Nov. 2020. URL: https://hal.inria.fr/hal-03016034.

[42] J. Kieffer. *Degree and height estimates for modular equations on PEL Shimura varieties.* 12th Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02436057.

[43] J. Kieffer. *Evaluating modular polynomials in genus 2.* 19th Oct. 2020. URL: https://hal.archives-ouvertes.fr/hal-02971326.

[44] J. Kieffer. *Sign choices in the AGM for genus two theta constants.* 14th Oct. 2020. URL: https://hal.archives-ouvertes.fr/hal-02967220.

[45] J. Kieffer, A. Page and D. Robert. *Computing isogenies from modular equations in genus two.* 12th Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02436133.

[46] M. Kirschmer, F. Narbonne, C. Ritzenthaler and D. Robert. *Spanning the isogeny class of a power of an ordinary elliptic curve over a finite field. Application to the number of rational points of curves of genus* ≤ 4. 26th Apr. 2020. URL: https://hal.inria.fr/hal-02554714.

[47] B. Wesolowski and R. Williams. *Lower bounds for the depth of modular squaring.* 3rd Dec. 2020. URL: https://hal.archives-ouvertes.fr/hal-03038044.

Other scientific publications

[48] B. Allombert and F. Bastien. *Bill Allombert - New GP features: Atelier PARI/GP 2020.* 20th Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02524550.

[49] B. Allombert and F. Bastien. *Bill Allombert - Start of Atelier (setting up personal computers): Atelier PARI/GP 2020.* 20th Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02514157.

[50] K. Belabas and F. Bastien. *Karim Belabas - S-units and compact representations in number fields: Atelier PARI/GP 2020.* 22nd Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02530400.

[51] A. Page and F. Bastien. *Aurel Page - Construction of subfields and abelian overfields: Atelier PARI/GP 2020.* 21st Jan. 2020. URL: https://hal.archives-ouvertes.fr/hal-02530402.

11.3 Other

Softwares

[52] [SW] A. Page, *abelianbnf* version 1.0, Sept. 2020. HAL: ⟨hal-02961482⟩, URL: https://hal.inria.fr/hal-02961482, SWHID: ⟨swh:1:dir:2028b86e77e21a66f522a8d0e2bcf6c341f6a4b4;origin=https://hal.archives-ouvertes.fr/hal-02961482;visit=swh:1:snp:fcf14abf20c8f027f2e290c472ea9ca7710b4dee;anchor=swh:1:rev:9235b295296670186eeace394da3cbd1abb1f53b;path=/⟩.

11.4 Cited publications

[53] R. Barbulescu and S. Duquesne. 'Updating key size estimations for pairings'. In: *Journal of Cryptology* 32.4 (2019), pp. 1298–1336. DOI: 10.1007/s00145-018-9280-5. URL: https://hal.archives-ouvertes.fr/hal-01534101.

[54] K. Belabas. 'L'algorithmique de la théorie algébrique des nombres'. In: *Théorie algorithmique des nombres et équations diophantiennes*. Ed. by N. Berline, A. Plagne and C. Sabbah. 2005, pp. 85–155.

[55] B. Büeler, A. Enge and K. Fukuda. 'Exact Volume Computation for Polytopes: A Practical Study'. In: *Polytopes — Combinatorics and Computation*. Ed. by G. Kalai and G. M. Ziegler. Vol. 29. DMV Seminar. Basel: Birkhäuser Verlag, 2000, pp. 131–154.

[56] J.-P. Cerri. 'Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1'. In: *J. Reine Angew. Math.* 592 (2006), pp. 49–62.

[57] J.-P. Cerri. 'Spectres euclidiens et inhomogènes des corps de nombres'. Thèse de doctorat. IECN, Université Henri Poincaré, Nancy, 2005. URL: http://tel.archives-ouvertes.fr/tel-00011151/en/.

[58] D. Charles, E. Goren and K. Lauter. 'Cryptographic Hash Functions from Expander Graphs'. In: *Journal of Cryptology* 22.1 (2009), pp. 93–113.

[59] H. Cohen and P. Stevenhagen. 'Computational class field theory'. In: *Algorithmic Number Theory — Lattices, Number Fields, Curves and Cryptography*. Ed. by J. Buhler and P. Stevenhagen. Vol. 44. MSRI Publications. Cambridge University Press, 2008.

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

[61] A. Rostovtsev and A. Stolbunov. 'Public-key cryptosystem based on isogenies'. Preprint, Cryptology ePrint Archive 2006/145. 2006. URL: http://eprint.iacr.org/2006/145/.