IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2012

Project-Team LFANT

Lithe and fast algorithmic number theory

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

RESEARCH CENTER
Bordeaux - Sud-Ouest

THEME
Algorithms, Certification, and Cryptography

Table of contents

Project-Team LFANT

Keywords: Algorithmic Number Theory, Complexity, Computer Algebra, Cryptology, High Performance Computing

Creation of the Project-Team: March 01, 2009 , *Updated into Project-Team:* January 01, 2010 .

1. Members

Research Scientists

Andreas Enge [Team leader, Senior Researcher, HdR]
Damien Robert [Junior Researcher]

Faculty Members

Karim Belabas [Professor, University Bordeaux 1, HdR]
Jean-Paul Cerri [Associate professor, University Bordeaux 1]
Henri Cohen [Professor emeritus, University Bordeaux 1, HdR]
Jean-Marc Couveignes [Professor, University Bordeaux 1, HdR]

Engineer

Bill Allombert [CNRS]

PhD Students

Athanasios Angelakis [Universities Leiden and Bordeaux 1]
Julio Brau [Universities Leiden and Bordeaux 1]
Pierre Lezowski [ENS]
Nicolas Mascot [ENS]
Enea Milio [ERC ANTICS]
Jérôme Milan [ANR]
Aurel Page [ENS]
Vincent Verneuil [CIFRE Inside Contactless]

Administrative Assistant

Anne-Laure Gautier [Inria]

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 Schönhage–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.

2.2. Highlights of the Year

- Vincent Verneuil has defended his PhD thesis on “Cryptographie à base de courbes elliptiques et sécurité de composants embarqués” [12] in June 2012.
- Pierre Lezowski has defended his PhD thesis on “Questions d’Euclidianité ” [11] in December 2012.
- The ERC project ANTICS of Andreas Enge started in January 2012.
- The 2nd Atelier PARI/GP was held in 2012 (after the first installment in 2004), with the aim of creating a yearly event dedicated to the development of the main software product of the LFANT team.

3. Scientific Foundations

3.1. Number fields, class groups and other invariants

Participants: Bill Allombert, Athanasios Angelakis, Karim Belabas, Julio Brau, Jean-Paul Cerri, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Pierre Lezowski, Nicolas Mascot, 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 $n \geqslant 3$. For recent textbooks, see [6]. 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 [36] 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, Julio Brau, Jean-Marc Couveignes, Andreas Enge, Nicolas Mascot, Jérôme Milan, Damien Robert, Vincent Verneuil.

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, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [41], for more background material, [40]. 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. 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 which is not a complex multiplication field and whose unit group has rank strictly greater than 1 is almost norm-Euclidean [37], [38].

Algorithms developed by the team are implemented in the free PARI/GP system for number theory maintained by K. Belabas, which is a reference and the tool of choice for the worldwide number theory community.

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 [7]. 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 smart cards and embedded devices, algebraic curve cryptography has become the technology of choice. Most of the research topics of the LFANT team concern directly problems relevant for curve-based cryptology: The difficulty of the discrete logarithm problem in algebraic curves determines the security of the corresponding cryptosystems. Complex multiplication, point counting and isogenies 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 [39] and encryption [43]. Pairings in algebraic curves have proved to be a rich source for novel cryptographic primitives. Class groups of number fields 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. Software

5.1. Pari/Gp

Participants: Karim Belabas [correspondant], Bill Allombert, Henri Cohen, Andreas Enge.

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

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.

- PARI is a C library, allowing fast computations.
- GP is an easy-to-use interactive shell giving access to the PARI functions.
- gp2c, the GP-to-C compiler, combines the best of both worlds by compiling GP scripts to the C language and transparently loading the resulting functions into GP; scripts compiled by gp2c will typically run three to four times faster.
- Version of PARI/GP: 2.5.3
- Version of gp2c: 0.0.7pl4
- License: GPL v2+
- Programming language: C

5.2. GNU MPC

Participants: Andreas Enge [correspondant], Mickaël Gastineau, Philippe Théveny, Paul Zimmermann [INRIA project-team CARAMEL].

http://mpc.multiprecision.org/.

GNU 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 GNU MPFR.

It is a prerequisite for the GNU compiler collection GCC since version 4.5, where it is used in the C and Fortran frontends for constant folding, the evaluation of constant mathematical expressions during the compilation of a program. Since 2011, it is an official GNU project.

2011 has seen the first release of the major version 1.0.

- Version: 1.0.1 *Fagus silvatica*
- License: LGPL v3+
- ACM: G.1.0 (Multiple precision arithmetic)
- AMS: 30.04 Explicit machine computation and programs
- APP: Dépôt APP le 2003-02-05 sous le numéro IDDN FR 001 060029 000 R P 2003 000 10000
- Programming language: C

5.3. MPFRCX

Participant: Andreas Enge.

http://mpfrcx.multiprecision.org/

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.

- Version: 0.4.1 *Cassava*
- License: LGPL v2.1+
- Programming language: C

5.4. CM

Participant: Andreas Enge.

http://cm.multiprecision.org/

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. For the implemented algorithms, see [9].

- Version: 0.2 *Blindhühnchen*
- License: GPL v2+
- Programming language: C

5.5. AVIsogenies

Participants: Damien Robert [correspondant], Gaëtan Bisson, Romain Cosset [INRIA project-team CARAMEL].

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

AVISOGENIES (Abelian Varieties and Isogenies) 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.

- Version: 0.6
- License: LGPL v2.1+
- Programming language: Magma

5.6. Cubic

Participant: Karim Belabas.

http://www.math.u-bordeaux1.fr/~belabas/research/software/cubic-1.2.tgz

CUBIC is a standalone 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.

- Version: 1.2
- License: GPL v2+
- Programming language: C

5.7. Euclid

Participant: Pierre Lezowski.

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

EUCLID is a C program to compute the Euclidean minimum of a number field. It uses the PARI library.

- Version: 1.0
- License: GPL v2+
- Programming language: C

5.8. KleinianGroups

Participant: Aurel Page.

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

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

- Version: 1.0
- License: GPL v3+
- Programming language: Magma

6. New Results

6.1. Class groups and other invariants of number fields

Participants: Karim Belabas, Jean-François Biasse, Jean-Paul Cerri, Pierre Lezowski.

P. Lezowski extended J.-P. Cerri's algorithm, which was restricted to totally real number fields, to decide whether a generic number field is norm-Euclidean. His procedure allowed to find principal and non norm-Euclidean number fields of various signatures and degrees up to 8, but also to give further insight about the norm-Euclideanity of some cyclotomic fields. Besides, many new examples of generalised Euclidean and 2-stage Euclidean number fields were obtained. The article [31] will appear in *Mathematics of Computation*.

In another direction, norm-Euclidean ideal classes have been studied. They generalise the notion of norm-Euclideanity to non principal number fields. Very few such number fields were known before. A modification of the algorithm provided many new examples and allowed to complete the study of pure cubic fields equipped with a norm-Euclidean ideal class [15].

J.-F.Biasse has determined a class of number fields for which the ideal class group, the regulator, and a system of fundamental units of the maximal order can be computed in subexponential time $L(1/3, O(1))$ (whereas the best previously known algorithms have complexity $L(1/2, O(1))$). This class of number fields is analogous to the class of curves described in [10]. The article [22] has been submitted to *Mathematics of Computation*.

Assuming the GRH, Bach proved that one can calculate the residue of the Dedekind zeta function of a number field K from the knowledge of the splitting of primes $p < X$, with an error bounded explicitly in terms of X and the field discriminant. This is a crucial ingredient in all algorithms used to compute class groups and unit groups in subexponential time (under GRH). Using Weil's explicit formula, K. Belabas improved on Bach's bound, speeding up by a sizable constant factor this part of the class group algorithm. The article has been submitted to *Mathematics of Computation*.

6.2. Number and function fields

Participants: Athanasios Angelakis, Karim Belabas, Pieter Rozenhart.

In joint work with R. Scheidler and M. Jacobson, P. Rozenhart has generalized Belabas's algorithm for tabulating cubic number fields to cubic function fields [17]. This generalization required function field analogues of the Davenport-Heilbronn Theorem and of the reduction theory of binary cubic and quadratic forms. As an additional application, they have modified the tabulation algorithm to compute 3-ranks of quadratic function fields by way of a generalisation of a theorem due to Hasse. The algorithm, whose complexity is quasi-linear in the number of reduced binary cubic forms up to some upper bound X, works very well in practice. A follow-up article [35] describes how to use these results to compute 3-ranks of quadratic function fields, in particular yielding examples of unusually high 3-rank.

In 1976, Onabe discovered that, in contrast to the Neukirch–Uchida results that were proved around the same time, a number field K is not completely characterised by its absolute abelian Galois group A_K. The first examples of non-isomorphic K having isomorphic A_K were obtained on the basis of a classification by Kubota of idele class character groups in terms of their infinite families of Ulm invariants, and did not yield a description of A_K. In [21], A. Angelakis and P. Stevenhagen provide a direct "computation" of the profinite group A_K for imaginary-quadratic K, and use it to obtain many different K that all have the same minimal absolute abelian Galois group.

On March 29–April 2, 2010, a meeting was organized by J.-M. Couveignes, D. Bertrand, Ph. Boalch and P. Debes, at the Luminy CIRM (France) on geometric and differential Galois theories, witnessing the close ties these theories have woven in recent years. The volume [18] collects the proceedings of this meeting. The articles gathered in this volume cover the following topics: moduli spaces of connections, differential equations and coverings in finite characteristic, liftings, monodromy groups in their various guises (tempered fundamental group, motivic groups, generalised difference Galois groups), and arithmetic applications.

Using Galois theory of extension rings, J.-M. Couveignes, R. Lercier and T. Ezome have proposed a new pseudo-primality test in [13]. For every positive integer $k \leq logn$, this test achieves the security of k Miller-Rabin tests at the cost of $k^{1/2} + o(1)$ Miller-Rabin tests. The implementation in Magma shows that this test is competitive for primes with a few thousands digits.

6.3. Quaternion algebras

Participants: Jean-Paul Cerri, Pierre Lezowski, Aurel Page.

With J. Chaubert, J.-P. Cerri and P. Lezowski have studied whether some quaternion fields over number fields are Euclidean, that is to say whether they admit a left or right Euclidean order. In particular, they have established the complete list of totally definite and Euclidean quaternion fields over the rationals or a quadratic number field. Moreover, they have proved that every field in this list is in fact norm Euclidean. The proofs are both theoretical and algorithmic. The article [23] will appear in *International Journal of Number Theory*.

Starting with an order in a suitable quaternion algebra over a number field F with exactly one complex place, one can construct discrete subgroups of $\mathrm{PSL}_2(\mathbb{C})$. These groups, called arithmetic Kleinian groups, act properly discontinuously with finite covolume on the hyperbolic 3-space. In [34], A. Page designs an efficient algorithm which computes a fundamental domain and a presentation for such a group. It is a generalization to the dimension 3 of an algorithm of J. Voight's [44] together with a new, nondeterministic, but faster enumeration procedure. A public implementation is available in KLEINIANGROUPS (see 5.8).

6.4. Complex multiplication and modularity

Participants: Jean-Marc Couveignes, Andreas Enge, Nicolas Mascot, Aurel Page, Damien Robert.

The article by D. Lubicz and D. Robert which explains how to compute an isogeny between two abelian varieties given the kernel (but with different levels of theta structures) has been published [16]. The preprint [25] with R. Cosset and D. Robert extends these method to provide an algorithm constructing the corresponding isogeny without changing the level. This give the first algorithm allowing to compute in polynomial time an isogeny between abelian varieties, and a public implementation is available in AVISOGENIES. The drawback of this algorithm is that it needs the geometric points of the kernel. To compute an isogeny of degree ℓ^g over a finite field, working with geometric points requires to take an extension of degree up to $\ell^g - 1$, and the situation is much worse over a number field. Recently, D. Lubicz and D. Robert have explained how to compute the corresponding isogeny given only the equations of the kernel. This gives a quasi-linear algorithm (in the degree ℓ^g of the isogeny) when ℓ is congruent to 1 modulo 4.

With K. Lauter, D. Robert has worked on improving the computation of class polynomials in genus 2 by the CRT method. The main improvements come from using the above isogeny computation, both to find a maximal curve from a curve in the correct isogeny class, and to find all other maximal curves from one. Further improvements are in the endomorphism ring computation to detect if the curve is maximal, a better sieving of the primes used (and a dynamic selection of them), and the use of the CRT over the real quadratic field rather than over $\mathbb{Q}$ for the case of dihedral CM fields to find factors of the class polynomials. These results have been published at the ANTS conference [30].

With C. Ritzenthaler, Damien Robert has shown how to compute explicitly the Serre obstruction for abelian varieties isogenous to a product of three elliptic curves. This allows to find genus 3 curves with many points over a finite field. The corresponding code has been implemented in an (experimental) version of AVISOGENIES.

In [24], H. Cohen studies several methods for the numerical computation of Petersson scalar products. In particular he proves a generalisation of Haberland's formula to any subgroup of finite index G of $\Gamma = \mathrm{PSl}_2(Z)$, which gives a fast method to compute these scalar products when a Hecke eigenbasis is not necessarily available.

J.-M. Couveignes and B. Edixhoven explore in [19] the relevance of numerical methods in dealing with higher genus curves and their Jacobians. Fast exponentiation is crucial in this context as a stable substitute to Newton's method and analytic continuation. Arakelov theory provides the necessary complexity estimates.

With Reynald Lercier, J.-M. Couveignes has given in [26] a quasi-linear time randomised algorithm that on input a finite field $\mathbb{F}_q$ with q elements and a positive integer d outputs a degree d irreducible polynomial in $\mathbb{F}_q[x]$. The running time is $d^{1+o(1)} \times (\log q)^{5+o(1)}$ elementary operations. The $o(1)$ in $d^{1+o(1)}$ is a function of d that tends to zero when d tends to infinity. And the $o(1)$ in $(\log q)^{5+o(1)}$ is a function of q that tends to zero when q tends to infinity. The fastest previously known algorithm for this purpose was quadratic in the degree. The algorithm relies on the geometry of elliptic curves over finite fields (complex multiplication) and on a recent algorithm by Kedlaya and Umans for fast composition of polynomials.

In [32], N. Mascot shows how to compute modular Galois representations associated with a newform f and the coefficients of f modulo a small prime ℓ. To this end, he designs a practical variant of the complex approximation method presented in the book edited by B. Edixhoven and J.-M. Couveignes [8]. Its efficiency stems from several new ingredients. For instance, he uses fast exponentiation in the modular Jacobian instead of analytic continuations, which greatly reduces the need to compute abelian integrals, since most of the computation handles divisors. Also, he introduces an efficient way to compute arithmetically well-behaved functions on Jacobians. He illustrates the method on the newform Δ, and manages to compute for the first time the associated faithful representation modulo ℓ and the values modulo ℓ of Ramanujan's τ function at huge primes for $\ell \in \{11, 13, 17, 19\}$. In particular, he gets rid of the sign ambiguity stemming from the use of a non-faithful representation as in J. Bosman's work.

A. Enge and R. Schertz determine in [29] under which conditions singular values of multiple η-quotients of square-free level, not necessarily prime to 6, yield class invariants, that is, algebraic numbers in ring class fields of imaginary-quadratic number fields. It turns out that the singular values lie in subfields of the ring class fields of index $2^{k'-1}$ when $k' \geq 2$ primes dividing the level are ramified in the imaginary-quadratic field, which leads to faster computations of elliptic curves with prescribed complex multiplication. The result is generalised to singular values of modular functions on $X_0^+(p)$ for p prime and ramified.

With F. Morain, A. Enge has determined exhaustively under which conditions "generalised Weber functions", that is, simple quotients of η functions of not necessarily prime transformation level and not necessarily of genus 1, yield class invariants [28]. The result is a new infinite family of generators for ring class fields, usable to determine complex multiplication curves. We examine in detail which lower powers of the functions are applicable, thus saving a factor of up to 12 in the size of the class polynomials, and describe the cases in which the polynomials have integral rational instead of integral quadratic coefficients.

6.5. Elliptic curve cryptology

Participants: Jean-Marc Couveignes, Andreas Enge, Damien Robert.

With J.-G. Kammerer, J.-M. Couveignes has given in [14] an appropriate geometric method for studying and classifying encodings into elliptic curves in a cryptographic context. Such encodings were first proposed by Icart in 2009, and later on by Farashahi, Kammerer, Lercier, and Renault. But it was a little bit disappointing to see that it was no more than an application of Tartaglia's result without any geometrical explanations for the existence of such "parameterisations" of elliptic curves. Couveignes and Kammerer have filled this gap by giving exactly what can be expected from geometry: a clear explanation. Moreover, they unify all the recent "parameterisations" of elliptic curves under the same geometric point of view. The approach described in this article uses dual curves with some results coming from intersection theory. The main originality of this work is that these geometrical tools are employed to explain symbolic computations used in cryptography, that is, encoding on elliptic curves.

The survey [20], to be published in the *Handbook of Finite Fields*, presents the state of the art of the use of elliptic curves in cryptography.

6.6. Pairings

Participants: Andreas Enge, Damien Robert, Jérôme Milan.

In [27], A. Enge gives an elementary and self-contained introduction to pairings on elliptic curves over finite fields. For the first time in the literature, the three different definitions of the Weil pairing are stated correctly and proved to be equivalent using Weil reciprocity. Pairings with shorter loops, such as the ate, ate$_i$, R-ate and optimal pairings, together with their twisted variants, are presented with proofs of their bilinearity and non-degeneracy. Finally, different types of pairings are reviewed in a cryptographic context. The article can be seen as an update chapter to [42].

7. Bilateral Contracts and Grants with Industry

7.1. Industrial ANR PACE

Participants: Andreas Enge, Jérôme Milan.

https://pace.rd.francetelecom.com/

The PACE project unites researchers of France Télécom, Gemalto, NXP, Cryptolog International, the INRIA project teams CASCADE and LFANT and University of Caen. It deals with electronic commerce and more precisely with electronic cash systems. Electronic cash refers to money exchanged electronically, with the aim of emulating paper money and its traditional properties and use cases, such as the anonymity of users during spending. The goal of PACE is to use the new and powerful tool of bilinear pairings on algebraic curves to solve remaining open problems in electronic cash, such as the strong unforgeability of money and the strong unlinkability of transactions, which would allow users to conveniently be anonymous and untraceable. It also studies some cryptographic tools that are useful in the design of e-cash systems.

7.2. DGA

Contract with *DGA maîtrise de l'information* about number theory and cryptography

- Duration: two years, 2011–2013
- Scientific coordinator: J.-M. Couveignes
- Topics covered: index calculus and discrete logarithms, fast arithmetic for polynomials, pairings and cryptography, algorithmics of the Langlands programme

7.3. Thèse cifre

Participants: Karim Belabas, Vincent Verneuil.

Vincent Verneuil, co-directed with B. Feix (Inside Contactless) and C. Clavier (Université de Limoges), works at Inside Contactless on elliptic curve cryptography, with an emphasis on embedded systems and side-channel attacks.

8. Partnerships and Cooperations

8.1. Regional Initiatives

8.1.1. Projet Idex CPU

The LFANT team takes part in Work package 6 of the Idex project CPU (Numerical certification and reliability). The work package concerns "Codes, Cryptology and Arithmetic Algorithms" and involves researchers from the Institut de Mathématiques de Bordeaux (Codes and Lattices team, LFANT) and Laboratoire Bordelais de Recherche en Informatique (Combinatorics and Algorithmic team).

8.2. National Initiatives

8.2.1. ANR AlgoL: Algorithmics of L-functions

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Jean-Marc Couveignes, Andreas Enge.

http://www.math.u-bordeaux1.fr/~belabas/algol/index.html

The ALGOL project comprises research teams in Bordeaux, Montpellier, Lyon, Toulouse and Besançon.

It studies the so-called L-functions in number theory from an algorithmic and experimental point of view. L-functions encode delicate arithmetic information, and crucial arithmetic conjectures revolve around them: Riemann Hypotheses, Birch and Swinnerton-Dyer conjecture, Stark conjectures, Bloch-Kato conjectures, etc.

Most of current number theory conjectures originate from (usually mechanised) computations, and have been thoroughly checked numerically. L-functions and their special values are no exception, but available tools and actual computations become increasingly scarce as one goes further away from Dirichlet L-functions. We develop theoretical algorithms and practical tools to study and experiment with (suitable classes of) complex or p-adic L-functions, their coefficients, special or general values, and zeroes. For instance, it is not known whether K-theoretic invariants conjecturally attached to special values are computable in any reasonable complexity model. On the other hand, special values are often readily computed and sometimes provide, albeit conjecturally, the only concrete handle on said invariants.

New theoretical results are translated into new or more efficient functions in the PARI/GP system.

The project lasted from 15/11/2007 to 15/02/2012, for 51 months it received an ANR funding of 200k€ for a global cost of 1M€.

8.2.2. ANR Peace – Parameter spaces for Efficient Arithmetic and Curve security Evaluation

Participants: Bill Allombert, Karim Belabas, Jean-Marc Couveignes, Andreas Enge, Nicolas Mascot, Enea Milio, Aurel Page, Damien Robert.

http://chic2.gforge.inria.fr/

The PEACE project is joint between the research teams of Institut de Recherche en Mathématiques de Rennes (IRMAR), LFANT and Institut Mathématiques de Luminy (IML).

The project aims to constitute a comprehensive and coherent approach towards a better understanding of theoretical and algorithmic aspects of the discrete logarithm problem on algebraic curves of small genus. On the theorical side, this includes an effective description of moduli spaces of curves, of abelian varieties, the maps that link these spaces and the objects they classify. The effective manipulation of moduli objects will allow us to develop a better understanding of the algorithmic difficulty of the discrete logarithm problem on curves, which may have dramatic consequences on the security and efficiency of already deployed cryptographic devices.

One of the anticipated outcomes of this proposal is a new set of general criteria for selecting and validating cryptographically secure curves (or families of curves) suitable for use in cryptography. Instead of publishing fixed curves, as is done in most standards, we aim at proposing generating rationales along with explicit theoretical and algorithmic criteria for their validation.

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

Participant: Damien Robert.

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, University of Paris 8.

The aim of the SIMPATIC project is to provide the most possible 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 efficient 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.

As a member, Damien Robert will aim to bridge the gap between the theoretical results described in the pairing module and the practical realisation of pairing-based SIM cards in an industrial setting.

8.3. European Initiatives

8.3.1. FP7 Projects

8.3.1.1. ANTICS

Title: Algorithmic Number Theory in Cryptology

Type: IDEAS

Instrument: ERC Starting Grant

Duration: January 2012 - December 2016

Coordinator: Inria (France)

Abstract: Data security and privacy protection are major challenges in the digital world. Cryptology contributes to solutions, and one of the goals of ANTICS is to develop the next generation public key cryptosystem, based on algebraic curves and abelian varieties. Challenges to be tackled are the complexity of computations, certification of the computed results and parallelisation, addressed by introducing more informatics into algorithmic number theory.

8.3.2. Collaborations in European Programs, except FP7

Program: Erasmus Mundus

Project acronym: ALGANT

Project title: ALgebra, Geometry and Number Theory

Duration: 09/2004–

Coordinator: University Bordeaux 1

Other partners: University Leiden (Netherlands), University Milano (Italy), University Padova (Italy), University Paris-Sud (France), Chennai Mathematical Institute (India), Concordia University (Canada), Stellenbosch University (South Africa)

Abstract: Joint master and doctoral programme; the PhD theses of Athanasios Angelakis and Julio Brau are co-supervised by P. Stevenhagen (Leiden) and K. Belabas

8.4. Research Visitors

- Atelier PARI/GP (23–27/01)
  - Charles Boyd (Amherst)
  - Pierre Castel (Caen)
  - Jeroen Demeyer (Ghent)
  - Tony Ezome (Franceville)
  - Vincent Fleckinger (Besançon)
  - Jean-Pierre Flori (Télécom Paristech)
  - Eduardo Friedman (Santiago de Chile)
  - Loic Grenié (Bergamo)
  - Bernadette Perrin-Riou (Orsay)
  - Firmin Varescon (Besançon)
- Damien Stehlé, Lyon (06–09/03)
- Bernadette Perrin-Riou, Orsay (24–27/01, 09–23/03)
- Vasily Golyshev, Bonn and Moscow (12/03)
- Marco Streng, Warwick (27–30/03)
- Gaëtan Bisson, Sydney (10–13/04)
- David Lubicz, Rennes (10–13/04, 03–07/09, 17–21/12)
- Bruno Salvy, Inria Paris (14/06)
- Workshop MPFR/MPC (25–27/06)
  - Benjamin Dadoun (Nancy)
  - Mickaël Gastineau (Paris)
  - Vincent Lefèvre (Lyon)
  - Patrick Pélissier (Toulouse)
  - Philippe Théveny (Lyon)
  - Paul Zimmermann (Nancy)
- Bernhard Schmidt, Singapore (02/07)
- Fernando Mario, Berlin (09/10)
- Luca De Feo, Versailles (30/10)

8.4.1. Visits to International Teams

J.-M. Couveignes: Tsinghua University, Beijing, 02/04–08/05

A. Enge: Tsinghua University, Beijing, 20/04–02/06

9. Dissemination

9.1. Scientific Animation

9.1.1. Editorships

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 associate editor of *Séminaires et Congrès* since 2008, of *Mathematics of Computation* since 2008, of *London Mathematical Society Journal for Computation and Mathematics* since 2009 and of *Publications mathématiques de Besançon* since 2010.

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

9.1.2. Invited talks

- A. Enge: "Class polynomials for abelian surfaces by complex approximations" at *Number Theory, Discrete Mathematics and Their Applications*, Tsinghua University, China, 25–27/05

9.1.3. Conference organisation and programme committees

A. Enge acts on the scientific advisory board of the *Journées Nationales de Calcul Formel.*

9.1.4. Seminar

The following external speakers have given a presentation at the LFANT seminar, see
http://lfant.math.u-bordeaux1.fr/index.php?category=seminar

- Charles Boyd (Amherst): "Paridroid"
- Loïc Grenié (Bergamo): "A modular HNF", "bnfinit ()"
- Vassily Golyshev (Bonn): "Searching for congruences of Galois representations "
- Marco Streng (Warwick): "Smaller class invariants for quartic CM-fields"
- Gaëtan Bisson (Sydney): "Un algorithme à la Pollard pour le problème du sac à dos"
- Bruno Salvy: "Itération de Newton: du numérique à la combinatoire, et réciproquement"
- Bernhardt Schmidt (Singapore): "Values and ideals in combinatorial problems"
- Fernando Mario (Berlin): "Packings of bodies in Euclidean space"
- Luca De Feo (Versailles): "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

9.1.5. Research administration

K. Belabas is the head of the mathematics department of University Bordeaux 1. He also leads the computer science support service ("cellule informatique") of the Institute of Mathematics of Bordeaux and coordinates the participation of the institute in the regional computation cluster PlaFRIM.

He is a permanent invited member of the councils of both the math and computer science department (UFR) and the Math Institute (IMB).

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 2011, J.-M. Couveignes is involved in the *GDR mathématiques et entreprises* and in the *Agence pour les mathématiques en interaction avec l'entreprise et la société*.

A. Enge is responsible for the international affairs of Inria–Bordeaux-Sud-Ouest and a member of the COST-GTRI, the Inria body responsible for evaluating international partnerships.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- K. Belabas

  Algèbre et Calcul Formel, 100h, M2, Université Bordeaux 1, France

- J.-P. Cerri

  Cryptographie et Arithmétique, 24h, L3, Université Bordeaux 1, France

  Arithmétique, 36h, M1, Université Bordeaux 1, France

  Algorithmic Number Theory, 70h, M2, Université Bordeaux 1, France

- J.-M. Couveignes

  Algorithms for public key cryptograph, 40h, M2, Université Bordeaux 1, France

  Algorithms for number fields, 40h, M2, Université Bordeaux 1, France

  Algorithms for Modular Curves, Jacobians and Forms, 16h, Tsinghua University, Beijing, China

- A. Enge:

  Elliptic Curves in Cryptologie, 14h, L2–PhD, Tsinghua University, Beijing, China

- P. Lezowski: Moniteur and ATER at Université Bordeaux 1

  MHT411: Groupes, anneaux, corps, TD, 40h, L2, Université Bordeaux 1, France

  M1MI1002: Fondamentaux pour les Mathématiques et l'Informatique, cours–TD, 80h, L1, Université Bordeaux 1, France

- N. Mascot: Moniteur at Université Bordeaux 1

  MOSE1003: Analyse et algèbre, cours–TD, 36h h, L1, Université Bordeaux 1, France

  M1MI1001: Bases de l'analyse, cours–TD, 37.5h, L1, Université Bordeaux 1, France

- A. Page: Moniteur at Université Bordeaux 1

  M1CP3022:Maths analyse II, TD, 42h, L2, Université Bordeaux 1, France

  M1mi2012:Algèbre 1, TD, 18h, L1, Université Bordeaux 1, France

9.2.2. Supervision

- K. Belabas, A. Enge

  PhD Aurel Page, *Méthodes explicites pour les groupes arithmétiques*, University Bordeaux

- K. Belabas, J.-M. Couveignes

  PhD Nicolas Mascot, *Calcul de représentations galoisiennes modulaires*, University Bordeaux

- K. Belabas, P. Stevenhagen

  PhD Athanasios Angelakis, *Number fields sharing the same abelianized Galois group*, ALGANT, University Bordeaux and University Leiden

  K. Belabas, T. Dokchitser, P. Stevenhagen

  PhD Julio Brau, *Computing Galois representations attached to elliptic curves*, ALGANT, University Bordeaux and University Leiden

- A. Enge, D. Robert

  PhD Enea Milio, *Isogénies entre surfaces abéliennes*, University Bordeaux

9.2.3. Juries

- K. Belabas

  PhD Pierre Lezowski, *Questions d'Euclidianité*, University Bordeaux, 07/12 (committee).

  HdR Emmanuel Thomé *Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques*, University Nancy-Lorraine, 13/12 (referee, committee).

- A. Enge

  PhD Jean-Pierre Flori, *Fonctions booléennes, courbes algébriques et multiplication complexe*, Télécom Paristech, 03/02 (president)

  PhD Aurélien Bajolet, *Aspects numériques de l'analyse diophantienne*, University Bordeaux, 07/12 (committee)

9.3. Popularization

N. Mascot and A. Page have given a presentation “Cryptologie” for the Fête de la Science.

J.-M. Couveignes has given a presentation at the seminar “Unithé ou café” of INRIA Bordeaux–Sud-Ouest on “Vous trouvez ça complexe? Tant mieux!”.

A. Enge has contributed to the Inria exhibition around Turing, computing machines and cryptology for the Fête de la Science.

A. Enge has given a presentation “Petit théorème de Fermat et courbes elliptiques, les mathématiques au service du secret” for the yearly meeting of Association des professeurs de mathématiques de l'enseignement public.

10. 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^{o} 7, p. 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^{o} 1, p. 173–210, http://projecteuclid.org/euclid.dmj/1272480934.

[3] K. BELABAS, F. DIAZ Y DIAZ, E. FRIEDMAN. *Small generators of the ideal class group*, in "Mathematics of Computation", 2008, vol. 77, n^{o} 262, p. 1185–1197, http://www.ams.org/journals/mcom/2008-77-262/S0025-5718-07-02003-0/home.html.

[4] 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.

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

[6] 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.

[7] 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.

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

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

[10] 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, p. 24–41.

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] P. Lezowski. *Questions d'Euclidianité*, University of Bordeaux, 2012, http://tel.archives-ouvertes.fr/tel-00765252/.

[12] V. Verneuil. *Cryptographie à base de courbes elliptiques et sécurité de composants embarqués*, University of Bordeaux, 2012, http://tel.archives-ouvertes.fr/tel-00733004/.

Articles in International Peer-Reviewed Journals

[13] J.-M. Couveignes, T. Ezome, R. Lercier. *A faster pseudo-primality test*, in "Rendiconti del circolo matematico di Palermo", 2012, vol. 61, n^{o} 2, p. 261–278.

[14] J.-M. Couveignes, J.-G. Kammerer. *The geometry of flex tangents to a cubic curve and its parameterizations*, in "Journal of Symbolic Computation", 2012, vol. 47, n^{o} 3, p. 266–281.

[15] P. Lezowski. *Examples of norm-Euclidean ideal classes*, in "International Journal of Number Theory", 2012, vol. 8, n^{o} 5, p. 1315–1333.

[16] D. Lubicz, D. Robert. *Computing isogenies between abelian varieties*, in "Compositio Mathematica", 2012, vol. 148, n^{o} 5, p. 1483–1515.

[17] P. Rozenhart, M. Jacobson, R. Scheidler. *Tabulation of Cubic Function Fields Via Polynomial Binary Cubic Forms*, in "Mathematics of Computation", 2012, vol. 81, n^{o} 280, p. 2335–2359.

Scientific Books (or Scientific Book chapters)

[18] D. Bertrand, P. Boalch, J.-M. Couveignes, P. Dèbes. *Geometric and differential Galois theories*, Séminaires et Congrès, Société Mathématique de France, 2012, vol. 27, http://smf4.emath.fr/en/Publications/SeminairesCongres/2012/27/html/smf_sem-cong_27.php.

[19] J.-M. Couveignes, B. Edixhoven. *Approximate computations with modular curves*, in "Geometry and Arithmetic", C. Faber, G. Farkas, R. de Jong (editors), EMS Series of Congress Reports, European Mathematical Society, Zürich, 2012, vol. 7, p. 91–112.

[20] A. Enge. *Elliptic curve cryptographic systems*, in "Handbook of Finite Fields", Boca Raton, G. L. Mullen, D. Panario (editors), Discrete Mathematics and Its Applications, Chapman and Hall/CRC, Boca Raton, 2012.

Research Reports

[21] A. Angelakis, P. Stevenhagen. *Imaginary quadratic fields with isomorphic abelian Galois groups*, ArXiv, 2012, n^o 1209.6005, To appear in Proceedings of Algorithmic Number Theory Symposium — ANTS X.

[22] J.-F. Biasse. *An L(1/3) algorithm for ideal class group and regulator computation in certain number fields*, HAL-Inria, 2012, n^o 440223, To appear in Mathematics of Computation.

[23] J.-P. Cerri, J. Chaubert, P. Lezowski. *Euclidean totally definite quaternion fields over the rational field and over quadratic number fields*, HAL, 2012, n^o 738164, To appear in International Journal of Number Theory.

[24] H. Cohen. *Haberland's formula and numerical computation of Petersson scalar products*, HAL, 2012, To appear in Proceedings of Algorithmic Number Theory Symposium — ANTS X, http://math.ucsd.edu/%7Ekedlaya/ants10/cohen/paper.pdf.

[25] R. Cosset, D. Robert. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, HAL-Inria, 2012, n^o 578991.

[26] J.-M. Couveignes, R. Lercier. *Fast construction of irreducible polynomials over finite fields*, HAL, 2012, n^o 456456, To appear in Israel Journal of Mathematics.

[27] A. Enge. *Bilinear pairings on elliptic curves*, HAL-Inria, 2012, n^o 767404.

[28] A. Enge, F. Morain. *Generalised Weber Functions. I*, HAL-Inria, 2012, n^o 385608.

[29] A. Enge, R. Schertz. *Singular values of multiple eta-quotients for ramified primes*, HAL-Inria, 2012, n^o 768375.

[30] K. Lauter, D. Robert. *Improved CRT Algorithm for Class Polynomials in Genus 2*, HAL, 2012, n^o 734450, To appear in Proceedings of Algorithmic Number Theory Symposium — ANTS X.

[31] P. Lezowski. *Computation of the Euclidean minimum of algebraic number fields*, HAL, 2012, n^o 632997, To appear in Mathematics of Computation.

[32] N. Mascot. *Computing modular Galois representations*, ArXiv, 2012, n^o 1211.1635.

[33] P. Molin. *Intégration numérique par la méthode double-exponentielle*, HAL, 2012, n^o 491561.

[34] A. PAGE. *Computing arithmetic Kleinian groups*, HAL, 2012, n^{o} 703043.

[35] P. ROZENHART, M. JACOBSON, R. SCHEIDLER. *Computing quadratic function fields with high 3-rank via cubic field tabulation*, HAL-Inria, 2012, n^{o} 462008.

References in notes

[36] 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, p. 85–155.

[37] J.-P. CERRI. *Spectres euclidiens et inhomogènes des corps de nombres*, IECN, Université Henri Poincaré, Nancy, 2005, http://tel.archives-ouvertes.fr/tel-00011151/en/.

[38] J.-P. CERRI. *Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1*, in "J. Reine Angew. Math.", 2006, vol. 592, p. 49–62.

[39] D. X. CHARLES, E. Z. GOREN, K. E. LAUTER. *Cryptographic Hash Functions from Expander Graphs*, in "Journal of Cryptology", 2009, vol. 22, n^{o} 1, p. 93–113.

[40] 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.

[41] 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/.

[42] A. ENGE. *Elliptic Curves and Their Applications to Cryptography — An Introduction*, Kluwer Academic Publishers, 1999.

[43] A. ROSTOVTSEV, A. STOLBUNOV. *Public-key cryptosystem based on isogenies*, 2006, Preprint, Cryptology ePrint Archive 2006/145, http://eprint.iacr.org/2006/145/.

[44] J. VOIGHT. *Computing fundamental domains for Fuchsian groups*, in "J. Théor. Nombres Bordeaux", 2009, vol. 21, n^{o} 2, p. 469–491, http://www.cems.uvm.edu/~jvoight/articles/funddom-jntb-galley.pdf.