IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2011

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 Numbers Theory, Complexity, Computer Algebra, Cryptology

LFANT *is an INRIA project-team joint with University of Bordeaux and CNRS (IMB, UMR 5251). The team was created on March 1st, 2009, and has become a project-team on January 1st, 2010.*

Beginning of the Team: 01/01/2010.

1. Members

Research Scientist
Andreas Enge [Team leader, INRIA Research Director, HdR]

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]

Engineers
Bill Allombert [CNRS]
Franck Labat [INRIA]

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

Post-Doctoral Fellow
Damien Robert [INRIA]

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

- With PARI/GP 2.5.0, the first major stable release of the software since 2007 has been made in June 2011.
- In March 2011, the MPC software has become an official GNU package with Andreas Enge as its maintainer.

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 [7]. 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 [31] 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 $\left(\sqrt{q} - 1\right)^{2g} \leqslant |\,\mathrm{Jac}_\mathcal{C}\,| \leqslant \left(\sqrt{q} + 1\right)^{2g}$, 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, 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 [36], for more background material, [35]. 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 [32], [33].

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 [8]. 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 [34] and encryption [37]. 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.

2011 has seen the release of the next major stable version, 2.5, ending the 2.3 release series started in 2007.

- Version of PARI/GP: 2.5.0
- Version of `gp2c`: 0.0.7pl11
- License: GPL v2+
- Programming language: C

5.2. MPC

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

http://mpc.multiprecision.org/.

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.

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.

- Version: 0.9 *Epilobium montanum*
- License: LGPL v2.1+
- 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: 0.3.1 *Banane*
- 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: 0.1 *Apfelkraut*
- License: LGPL 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: 0.4
- 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

6. New Results

6.1. Discrete logarithms

Participant: Andreas Enge.

In [10], we presented for the first time an algorithm for the discrete logarithm problem in certain algebraic curves that runs in subexponential time less than $L(1/2)$, namely, $L(1/3+\varepsilon)$ for any $\varepsilon > 0$. In [13], we lower this complexity to $L(1/3)$, showing that the corresponding algebraic curves (essentially C_{ab} curves of genus g growing at least quadratically with the logarithmic size of the finite field of definition, $\log q$) result in cryptosystems that are as easily attacked as RSA or tradtional cryptosystems based on discrete logarithms in finite fields. We provide a complete classification of all the curves to which the attack applies.

6.2. Class groups and other invariants of number fields

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

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 [13], cf. ref ssec:dlog. The article [18] has been submitted to *Mathematics of Computation*.

Using new theoretical ideas and his novel algorithmic approach, J.-P. Cerri has discovered examples of generalised Euclidean number fields and of 2-stage norm-Euclidean number fields in degree greater than 2 [11]. These notions, extending the link between usual Euclideanity and principality of the ring of integers of a number field had already received much attention before; however, examples were only known for quadratic fields.

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 [25] has been submitted to *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. The article [26] has been submitted to *International Journal of Number Theory*.

With E. Hallouin, J.-M. Couveignes has studied descent obstructions for varieties [21]. Such obstructions play an important role when one studies families of varieties (e.g. curves of a given genus). Obstructions are often measured by elements in groups like class groups. The theory of stacks provides a more general treatment for these obstructions. Couveignes and Hallouin give the first example of a global obstruction for a variety (that is an obstruction that vanishes locally at every place).

6.3. Number and function field enumeration

Participants: Henri Cohen, Anna Morra, 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 [30]. 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 [29] describes how to use these results to compute 3-ranks of quadratic function fields, in particular yielding examples of unusually high 3-rank.

H. Cohen and A. Morra [12] have obtained an explicit expression for the Dirichlet generating function associated to cubic extensions of an arbitrary number field with a fixed quadratic resolvent. As a corollary, they have proved refinements of Malle's conjecture in this context.

6.4. Complex multiplication and modularity

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

The book [16] edited by J.-M. Couveignes and B. Edixhoven, with contributions by J.-M. Couveignes, B. Edixhoven, R. de Jong, F. Merkl and J. Bosman, describes the first polynomial time algorithms for computing Galois representations and coefficients of modular forms. Modular forms are tremendously important in various areas of mathematics, from number theory and algebraic geometry to combinatorics and lattices. Their Fourier coefficients, with Ramanujan's τ-function as a typical example, have deep arithmetic significance. Prior to this book, the fastest known algorithms for computing these Fourier coefficients took exponential time, except in some special cases. The case of elliptic curves (Schoof's algorithm) was at the birth of elliptic curve cryptography around 1985. This book gives an algorithm for computing coefficients of modular forms of level one in polynomial time. For example, Ramanujan's τ of a prime number p can be computed in time bounded by a fixed power of the logarithm of p. Such fast computation of Fourier coefficients is itself based on the main result of the book: the computation, in polynomial time, of Galois representations over finite fields attached to modular forms by the Langlands programme. Because these Galois representations typically have a nonsolvable image, this result is a major step forward from explicit class field theory, and it could be described as the start of the explicit Langlands programme.

The computation of the Galois representations uses their realisation, following Shimura and Deligne, in the torsion subgroup of Jacobian varieties of modular curves. The main challenge is then to perform the necessary computations in time polynomial in the dimension of these highly nonlinear algebraic varieties. Exact computations involving systems of polynomial equations in many variables take exponential time. This is avoided by numerical approximations with a precision that suffices to derive exact results from them. Bounds for the required precision – in other words, bounds for the height of the rational numbers that describe the Galois representation to be computed – are obtained from Arakelov theory. Two types of approximations are treated: one using complex uniformisation and another one using geometry over finite fields.

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 [24]. 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.

With J.-C. Faugère and D. Lubicz, D. Robert has given an explicit construction for a modular correspondance between abelian varieties [14]. This correspondance describes the algebraic relations of ThetaNullWerte of different levels on isogenous abelian varieties. With R. Cosset, D. Robert has then given an algorithm explaining how to construct the corresponding isogeny, when we are given its (maximally isotropic) kernel [20]. This usse a formula by Koizumi for changing the level of the ThetaNullWerte. This is the first algorithm allowing to compute in polynomial time an isogeny between abelian varieties, and a public implementation is available in AVIsogenies.

With K. Lauter, D. Robert has worked on improving the computation of class polynomials in genus 2 by the CRT method. This involves some improvements to detect if the curve is maximal, a better sieving of the primes used, and the use of the CRT over the real quadratic field rather than over $\mathbb{Q}$ for the case of dihedral CM fields. The main improvements comes from using the above isogeny computation, both in order to be able to find a maximal curve from a curve in the correct isogeny class, and in order to find all others maximal curves from one. A preprint describing these improvements is being written, some details are described in the talk http://www.normalesup.org/~robert/pro/publications/slides/2011-04-C2.pdf.

With Reynald Lercier, J.-M. Couveignes has given in [23] 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.

6.5. Elliptic curve cryptology

Participants: Jean-Marc Couveignes, Vincent Verneuil.

In joint work with C. Clavier, B. Feix, G. Gagnerot and M. Roussellet, V. Verneuil has presented in [15] new side-channel analysis results on the AES. They propose improvements on collision-correlation attacks which require less power traces than classical second-order power analysis techniques. In particular, two new methods are presented and are shown to be efficient in practice on two first-order protected AES implementations. They also mention that other symmetric embedded algorithms can be targeted by these new techniques.

With the same coauthors, V. Verneuil has presented new exponentiation algorithms for embedded implementations in [19]. Embedded exponentiation techniques have become a key concern for security and efficiency in hardware devices using public key cryptography. An exponentiation is basically a sequence of multiplications and squarings, but this sequence may reveal exponent bits to an attacker on an unprotected implementation. Although this subject has been covered for years, they present new exponentiation algorithms based on trading multiplications for squarings. This method circumvents attacks aimed at distinguishing squarings from multiplications at a lower cost than other countermeasures. Finally, they present new algorithms using two parallel squaring blocks which provide one of the fastest exponentiation algorithms.

Together with D. Lubicz, D. Robert has extended their algorithm to compute pairings on abelian varieties using theta functions (published at ANTS 2010) to the case of the ate and optimal ate pairings. This involves a description of the Miller functions in term of theta coordinates and an extension of the addition law using more general Riemann relations in order to compute them. The case of theta functions of level 2 has been optimised by introducing a way to compute "compatible" additions without the need for a square roots. A preprint describing these results is being written, and some details can be found in the talk http://www.normalesup.org/~robert/pro/publications/slides/2011-06-Geocrypt.pdf.

With J.-G. Kammerer, J.-M. Couveignes has given in [22] 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.

7. 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, 2011–2012
- Scientific coordinator: K. Balabas
- 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. National Initiatives

8.1.1. ANR AlgoL: Algorithmics of L-functions

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

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.

8.2. European Initiatives

8.2.1. 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

8.3. International Initiatives

8.3.1. Visits of International Scientists

The following researchers have visited the LFANT team:

- Christophe Ritzenthaler, Luminy, Marseille, February 23–25
- Bernadette Perrin-Riou, Université d'Orsay, March 4–18 and June 10–17
- Vanessa Vitse, Universié de Versailles–St.-Quentin-en-Yvelines, April 13–14
- Jérémy Le Borgne, University of Rennes, April 27–28
- Andy Novocin, ÉNS Lyon and INRIA project-team ARÉNAIRE, May 4–5
- Lassina Dembelé, University of Warwick, May 18–19
- Jean-François Biasse, University of Calgary, May 25–26
- David Lubicz, Université de Rennes, July 18–22
- Eduardo Friedman, Universidad de Chile, October 3–21
- Michael Rubinstein, University of Waterloo, October 3–7
- Tony Ezome, Université de Franceville, Gabon, December 2011–January 2012

9. Dissemination

9.1. Animation of the scientific community

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

- K, Belabas: "Théorie algébrique des nombres et calcul formel" at *Journées Nationales de Calcul Formel*, Luminy, November 2011
- J.-M. Couveignes: "The geometry of flex tangents to a cubic curve and its parameterizations" at *Elliptic Curve Cryptography – ECC 2011*, Nancy, September 2011
- A. Enge: "Algorithms for complex multiplication of elliptic curves" at *Coding, Cryptology and Combinatoric Designs*, Singapore,, 23rd to 26th May

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

- Christophe Ritzenthaler (Marseilles): "Couplages sur les courbes d'Edwards et formules d'addition complètes"
- Martin Weimann: "Factorisation torique des polynômes bivariés"
- Vanessa Vitse (Versailles): "Attaques par recouvrement et décomposition du logarithme discret sur courbes elliptiques"
- Jérémie Le Borgne (Rennes): "Algorithmique des phi-modules pour les représentations galoisiennes p-adiques"
- Andy Novocin (Lyon): "L1 a new quasi-linear LLL algorithm"
- Lassina Dembelé (Warwick): "Sur la conjecture de Gross"
- Jean-François Biasse (Calgary): "Calcul du groupe de classes et des unités dans les corps de nombres"
- Peter Stevenhagen (Leiden): "Radical extensions and primitive roots"
- Michael Rubinstein (Waterloo): "Conjectures, experiments, and algorithms concerning the moments of $L(1/2, \chi_d)$

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 an elected 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

9.2.1. University courses

- K. Belabas

  Algèbre et Calcul Formel, 75h, M2, Université Bordeaux 1, France
- J.-P. Cerri

  Algorithmique Algébrique 1, 26h, L3, Université Bordeaux 1, France

  Arithmétique, 40h, M1, 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
- A. Enge: Chargé d'enseignement at École polytechnique

  Cryptologie, 38.25h, M1, École polytechnique, France

  Modex Programmation Web, 37.125h, L3, École polytechnique, France

- P. Lezowski: Moniteur at Université Bordeaux 1

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

  MOSE1003: Analyse et algèbre, cours–TD, 27h, L1, Université Bordeaux 1, France
- N. Mascot: Moniteur at Université Bordeaux 1

  MOSE1003: Analyse et algèbre, cours–TD, 29h h, L1, Université Bordeaux 1, France

  M1MI1001: Bases de l'analyse, cours–TD, 20h, L1, Université Bordeaux 1, France
- A. Page: Moniteur at Université Bordeaux 1

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

9.2.2. Thesis committees and supervision

- K. Belabas

  PhD Claire Bourbon, *Propagation de la 2-birationalité*, Bordeaux, 2011 (committee), Jean-François Jaulent.

  PhD Jérémy Berthomieu, *Contributions à la résolution des systèmes algébriques: réduction, localisation, traitement des singularités; implantations*, Polytechnique, 2011 (committee), Marc Giusti and Grégoire Lecerf.

  HdR Damien Stehlé, *Réseaux Euclidiens: Algorithmes et Cryptographie*, ENS Lyon, 2011 (committee).
- J.-M. Couveignes

  PhD Jean Lancrenon, *Authentification d'objets à distance*, Grenoble, 2011 (committee)

  PhD Safia Haloui, *Sur le nombre de points rationnels des variétés abéliennes sur les corps finis*, Marseille, 2011 (committee)
- A. Enge

  PhD Ezekiel Kachisa, *Constructing Suitable Ordinary Pairing-friendly Hyperelliptic Curves*, Dublin City University, 2011-05-08 (report)

  PhD Amandine Jambert, *Outils cryptographiques pour la protection des contenus et de la vie privé des utilisateurs*, Université Bordeaux 1, 2011-03-15 (committee)

  PhD Pierre Castel, *Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation*, Université de Caen, 2011-08-06 (committee)

  PhD Vanessa Vitse, *Attaques algébriques du problème du logarithme discret sur courbes elliptiques*, Université de Versailles–Saint-Quentin-en-Yvelines, 2011-10-20 (committee)

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, M. VAN HOEIJ, J. KLÜNERS, A. STEEL. *Factoring polynomials over global fields*, in "Journal de Théorie des Nombres de Bordeaux", 2009, vol. 21, n^{o} 1, p. 15–39, http://jtnb.cedram.org/item?id=JTNB_2009__21_1_15_0.

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

[5] 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.

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

[7] 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.

[8] 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.

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

[10] A. ENGE, P. GAUDRY. *An $L(1/3+\varepsilon)$ algorithm for the discrete logarithm problem for low degree curves*, in "Advances in Cryptology — Eurocrypt 2007", Berlin, M. NAOR (editor), Lecture Notes in Computer Science, Springer-Verlag, 2007, vol. 4515, p. 367–382, http://hal.inria.fr/inria-00135324/.

Publications of the year

Articles in International Peer-Reviewed Journal

[11] J.-P. CERRI. *Some Generalized Euclidean and 2-stage Euclidean number fields that are not norm-Euclidean*, in "Mathematics of Computation", 2011, vol. 80, n° 276, p. 2289–2298, http://hal.archives-ouvertes.fr/hal-00505142/.

[12] H. COHEN, A. MORRA. *Counting Cubic Extensions with given Quadratic Resolvent*, in "Journal of Algebra", 2011, vol. 325, n° 1, p. 461–478, http://hal.archives-ouvertes.fr/hal-00463533/.

[13] 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° 1, p. 24–41, http://hal.inria.fr/inria-00383941/.

[14] J.-C. FAUGÈRE, D. LUBICZ, D. ROBERT. *Computing modular correspondences for abelian varieties*, in "Journal of Algebra", 2011, vol. 343, n° 1, p. 248–277, http://hal.inria.fr/hal-00426338/.

International Conferences with Proceedings

[15] C. CLAVIER, B. FEIX, G. GANEROT, M. ROUSSELLET, V. VERNEUIL. *Improved Collision-Correlation Power Analysis on First Order Protected AES*, in "Cryptographic Hardware and Embedded Systems — CHES 2011", Berlin, B. PRENEEL, T. TAKAGI (editors), Lecture Notes in Computer Science, Springer-Verlag, 2011, vol. 6917, p. 49–62, http://hal.inria.fr/inria-00633527/.

Scientific Books (or Scientific Book chapters)

[16] J.-M. COUVEIGNES, B. EDIXHOVEN. *Computational aspects of modular forms and Galois representations*, Princeton University Press, 2011, http://arxiv.org/abs/math/0605244/.

Research Reports

[17] K. BELABAS. *Théorie algébrique des nombres et calcul formel*, Cours du CIRM series, 2011, Notes for a series of invited lectures at "Journées Nationales de Calcul Formel 2011". To appear, http://www.cedram.org/article.php3?id_article=212.

[18] J.-F. BIASSE. *An L(1/3) algorithm for ideal class group and regulator computation in certain number fields*, HAL-INRIA, 2011, n° 440223, http://hal.inria.fr/inria-00440223/.

[19] C. CLAVIER, B. FEIX, G. GANEROT, M. ROUSSELLET, V. VERNEUIL. *Square Always Exponentiation*, HAL-INRIA, 2011, n° 633545, To appear in Proceedings of Indocrypt 2011, http://hal.inria.fr/inria-00633545/.

[20] R. COSSET, D. ROBERT. *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, HAL-INRIA, 2011, n° 578991, http://hal.inria.fr/hal-00578991/.

[21] J.-M. COUVEIGNES, E. HALLOUIN. *Global descent obstructions for varieties*, HAL, 2011, n° 630393, To appear in Algebra and Number Theory, http://hal.archives-ouvertes.fr/hal-00630393/.

[22] J.-M. COUVEIGNES, J.-G. KAMMERER. *The Geometry of Flex Tangents to a Cubic Curve and its Parameterizations*, HAL, 2011, n° 630392, http://hal.archives-ouvertes.fr/hal-00630392/.

[23] J.-M. COUVEIGNES, R. LERCIER. *Fast construction of irreducible polynomials over finite fields*, HAL, 2011, n° 456456, To appear in Israel Journal of Mathematics, http://hal.archives-ouvertes.fr/hal-00456456/.

[24] A. ENGE, F. MORAIN. *Generalised Weber Functions. I*, HAL-INRIA, 2011, n° 385608, http://hal.inria.fr/inria-00385608/.

[25] P. LEZOWSKI. *Computation of the Euclidean minimum of algebraic number fields*, HAL, 2011, n° 632997, http://hal.archives-ouvertes.fr/hal-00632997/.

[26] P. LEZOWSKI. *Examples of norm-Euclidean ideal classes*, HAL, 2011, n° 634643, http://hal.archives-ouvertes.fr/hal-00634643/.

[27] J. MILAN. *Factoring Small to Medium Size Integers: An Experimental Comparison*, HAL-INRIA, 2011, n° 188645, http://hal.inria.fr/inria-00188645/.

[28] P. MOLIN. *Intégration numérique par la méthode double-exponentielle*, HAL, 2011, n° 491561, http://hal.archives-ouvertes.fr/hal-00491561/.

[29] P. ROZENHART, M. JACOBSON, R. SCHEIDLER. *Computing quadratic function fields with high 3-rank via cubic field tabulation*, HAL-INRIA, 2011, n° 462008, http://hal.inria.fr/inria-00462008/.

[30] P. ROZENHART, M. JACOBSON, R. SCHEIDLER. *Tabulation of Cubic Function Fields Via Polynomial Binary Cubic Forms*, HAL-INRIA, 2011, n^{o} 477111, To appear in Mathematics of Computation, http://hal.inria.fr/inria-00477111/.

References in notes

[31] 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.

[32] 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/.

[33] 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.

[34] 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.

[35] 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.

[36] 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/.

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