IN PARTNERSHIP WITH:
CNRS

Université de Bordeaux

Activity Report 2013

Project-Team LFANT

Lithe and fast algorithmic number theory

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

RESEARCH CENTER
Bordeaux - Sud-Ouest

THEME
Algorithmics, Computer Algebra and Cryptology

Table of contents

Project-Team LFANT

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

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

1. Members

Research Scientists
Andreas Enge [Team leader, Inria, Senior Researcher, HdR]
Damien Robert [Inria, Researcher]

Faculty Members
Karim Belabas [Univ. Bordeaux I, Professor, HdR]
Jean-Paul Cerri [Univ. Bordeaux I, Associate Professor]
Henri Cohen [Univ. Bordeaux I, HdR]
Jean-Marc Couveignes [Univ. Bordeaux I, Professor, HdR]

Engineers
Hamish Ivey-Law [Inria, FP7 ERC ANTICS STG project, from Jan 2013]
Bill Allombert [CNRS]

PhD Students
Athanasios Angelakis [Universities Leiden and Bordeaux 1]
Julio Brau [Universities Leiden and Bordeaux 1]
Nicolas Mascot [Univ. Bordeaux I]
Enea Milio [Inria, FP7 ERC ANTICS STG project]
Aurel Page [Univ. Bordeaux I]

Post-Doctoral Fellow
Pierre Lezowski [Inria, FP7 ERC ANTICS STG project]

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

V. Verneuil's PhD thesis work, co-supervised by K. Belabas and carried out in the company Inside Secure, has been awarded the "Prix de thèse AMIES 2013" of AMIES, l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société. The prize recognises outstanding work securing elliptic curve cryptographic systems against side-channel attacks on smartcards and an exceptional integration into the company, see http://www.agence-maths-entreprises.fr/a/?q=fr/node/292.

After two years of development, version 2.6.0 of the Pari/GP computer algebra system has been released, incorporating numerous improvements related to the programming language and the implementation of number fields, finite fields and elliptic curves. The new release maintains Pari/GP as the world leader for number theoretic computations.

3. Research Program

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 [5]. Kummer's idea for solving Fermat's problem was to rewrite the equation as $(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y) = z^n$ for a primitive n-th root of unity ζ, which seems to imply that each factor on the left hand side is an n-th power, from which a contradiction can be derived.

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

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

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

One of the main concerns of algorithmic algebraic number theory is to explicitly compute these invariants (Cl_K and h_K, fundamental units and R_K), as well as to provide the data allowing to efficiently compute with numbers and ideals of $\mathcal{O}_K$; see [32] 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 [39], for more background material, [37]. 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 [34], [35].

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 [6]. 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 [36] 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 and Platforms

5.1. Pari/Gp

Participants: Karim Belabas [correspondent], 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: 2.5.5
- Version of `gp2c`: 0.0.8
- License: GPL v2+
- Programming language: C

5.2. GNU MPC

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

http://mpc.multiprecision.org/.

GNUMPC 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 front ends for constant folding, the evaluation of constant mathematical expressions during the compilation of a program. Since 2011, it is an official GNU project.

2012 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: 0.4.2 *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 [8].

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

5.5. AVIsogenies

Participants: Damien Robert [correspondent], 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. APIP

Participant: Jérôme Milan.

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

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

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

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

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

- Version: 2012-10-17
- License: GPL v2+
- Programming language: C with libpari

5.7. CMH

Participants: Andreas Enge, Emmanuel Thomé [INRIA project-team CARAMEL].

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

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

- Version: development snapshot
- License: GPL v3+
- Programming language: C

5.8. Cubic

Participant: Karim Belabas.

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

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

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

5.9. Euclid

Participant: Pierre Lezowski.

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

Euclid is a program to compute the Euclidean minimum of a number field. It is the practical implementation of the algorithm described in [41]. Some corresponding tables built with the algorithm are also available. Euclid is a stand-alone program depending on the PARI library.

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

5.10. 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-Paul Cerri, Pierre Lezowski.

In collaboration with E. Friedman, K. Belabas presented in [22] a new algorithm to compute the residue at $s = 1$ of the Dedekind zeta function of a number field, conditional on GRH. This improves on previous results of Eric Bach [31] by a useful constant factor. Such an estimate is one of the two key analytic ingredients to Buchmann's class group algorithm, the other being the existence (under GRH) of an explicit set of small generators [33].

In collaboration with F. Thorne, H. Cohen worked on Dirichlet series associated to cubic and quartic fields with given resolvent. In [23] they give an explicit formula for the Dirichlet series $\sum_K |\Delta(K)|^{-s}$, where the sum is over isomorphism classes of all cubic fields whose quadratic resolvent field is isomorphic to a fixed quadratic field k. This is a sequel to previous work of Cohen and Morra, where such formulæ are proved in a more general setting, in terms of sums over characters of certain groups related to ray class groups. Here, the analysis is carried further and they prove explicit formulæ for these Dirichlet series over $\mathbb{Q}$. As an application, they compute tables of the number of S_3-sextic fields K with discriminant ranging up to 10^{23}. An accompanying PARI/GP implementation is available.

In [24], they give an explicit formula for the Dirichlet series $\sum_K |\Delta(K)|^{-s}$, where this time the sum is over isomorphism classes of all quartic fields whose cubic resolvent field is isomorphic to a fixed cubic field k. This work is a sequel to an unpublished preprint of Cohen, Diaz y Diaz, and Olivier.

The papers by H. Cohen on Haberland's formula and numerical computation of Petersson scalar products and by A. Angelakis and P. Stevenhagen on imaginary quadratic fields with isomorphic abelian Galois groups, which were presented at the ANTS-X conference, were published in [17], [16].

6.2. Number and function fields

Participants: Athanasios Angelakis, Jean-Marc Couveignes, Karim Belabas.

In collaboration with Reynald Lercier, Jean-Marc Couveignes presents in [12] a randomised algorithm that on input a finite field K with q elements and a positive integer d outputs a degree d irreducible polynomial in $K[x]$. 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. In particular, the complexity is quasi-linear in the degree d.

The book of surveys "Explicit methods in number theory. Rational points and Diophantine equations" [19] edited by K. Belabas with contributions from K. Belabas, F. Beukers, P. Gaudry, W. McCallum, B. Poonen, S. Siksek, M. Stoll and M. Watkins presents the state of the art of the use of explicit methods in arithmetic geometry to solve diophantine problems.

6.3. Quaternion algebras

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

In a joint work with J. Chaubert ([11]), J.-P. Cerri and P. Lezowski have studied totally definite quaternion fields over number fields which are Euclidean, that is to say that they admit a left or right Euclidean order. In particular, they have established the complete list of totally definite and Euclidean quaternion fields over real quadratic number fields. In this list, all fields are in fact norm-Euclidean. The proofs are both theoretic and algorithmic.

A. Page uploaded a new version of his article [30] on the computation of arithmetic Kleinian groups, incorporating comments from the referee.

6.4. Complex multiplication and modularity

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

H. Ivey-Law has been implementing efficient algorithms to compute Hilbert class polynomials and modular polynomials for various modular functions, as well as various supplementary algorithms required by, or based on, these two primary components. These algorithms form an important and time-critical part of algorithms used to select elliptic curves for use in cryptographic applications.

The implementation is based on algorithms for these tasks published by A. Sutherland and his collaborators. It includes, more specifically, algorithms to compute Hilbert class polynomials for various different modular functions over $\mathbb{Z}$ or $\mathbb{Z}/M\mathbb{Z}$, modular polynomials for various different modular functions over $\mathbb{Z}$, $\mathbb{Z}/M\mathbb{Z}$, and/or pre-instantiated at a particular point. The supplementary algorithms include functionality for computing equations for isogenies between elliptic curves and equations for their codomains, for manipulating, interrogating and traversing isogeny volcanoes, for computing minimal polycyclic presentations of abstract groups, for testing supersingularity of j-invariants, for accessing optimised equations of the modular curve $X_1(N)$ for $N \leq 50$, for finding elliptic curves with a given trace or a given endomorphism ring, for calculating the endomorphism ring of a given elliptic curve, for computing the action of the torsor $\mathrm{Cl}(\mathcal{O})$ on the set of elliptic curves with endomorphism ring $\mathcal{O}$ and for enumerating the kernel of the map $\mathrm{Cl}(\mathbb{Z} + N\mathcal{O}) \to \mathrm{Cl}(\mathcal{O})$.

These algorithms are implemented in an experimental branch of PARI/GP, and will be integrated in the public version soon.

A. Enge and R. Schertz determine in [13] 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.

The paper of R. Cosset and D. Robert [25] presenting an algorithm for computing isogenies between principally polarised abelian surface has been accepted for publication in Mathematics of Computation. This paper explains, given the theta coordinates of the points of a maximal isotropic kernel of the ℓ-torsion, how to compute the corresponding isogeny. It also gives formulæ for the conversion between theta coordinates and Mumford coordinates.

The paper by K. Lauter and D. Robert on Improved CRT Algorithm for Class Polynomials in Genus 2, which was presented at the ANTS-X conference, was published in [18].

A. Enge and E. Thomé describe in [14] a quasi-linear algorithm for computing Igusa class polynomials of Jacobians of genus 2 curves via complex floating-point approximations of their roots. After providing an explicit treatment of the computations in quartic CM fields and their Galois closures, they pursue an approach due to Dupont for evaluating ϑ-constants in quasi-linear time using Newton iterations on the Borchardt mean. They report on experiments with the implementation CMH and present an example with class number 20016.

N. Mascot's article on computing modular Galois representations [15] has been published in Rendiconti del Circolo Matematico di Palermo. This article describes an algorithm to compute Galois representations attached to a newform, and to deduce the Fourier coefficients of this newform modulo a small prime.

E. Milio has implemented R. Dupont's algorithms [38] in PARI/GP. With them, he has calculated the three modular polynomials in genus 2 and level 2 defined by Streng's version of Igusa modular forms and a modular polynomial of genus 2 and level 3 coming from theta modular forms.

6.5. Elliptic curve cryptology

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

Couveignes and Lercier study in [26] the problem of parameterisations by radicals of low genus algebraic curves. They prove that for q a prime power that is large enough and prime to 6, a fixed positive proportion of all genus 2 curves over the field with q elements can be parameterised by 3-radicals. This results in the existence of a deterministic encoding into these curves when q is congruent to 2 modulo 3. Deterministic encodings into curves are useful in numerous situations, for instance in discrete logarithm cryptography. The parameterisation found by Couveignes and Lercier is in some sense the first generic one for genus 2 curves.

A software for this method is in preparation.

The survey [21], 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.

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 [40].

With D. Lubicz, D. Robert has worked on extending the algorithm to compute Weil and Tate pairings using theta functions from [42] to the ate and optimal ate pairings in [29]. The result includes how to compute the Miller functions with theta functions, but also how to generalise ate and optimal ate pairings to Kummer varieties. In contrast to preceding algorithms using Miller functions which needed a geometric interpretation of the addition law and worked with Jacobians, this new algorithm uses only the algebraic Riemann relations and works on any abelian variety (provided with a theta structure). This algorithm has been implemented using AVIsogenies.

7. Bilateral Contracts and Grants with Industry

7.1. DGA

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

- Duration: two years, 2011–2013 (ended May 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

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANRPeace – 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 at constituting 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 theoretical side, this includes an effective description of moduli spaces of curves and 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.

Meetings:

- Paris: 11/04–12/04, talks and mini-courses;
- Rennes: 02/12–03/12, talks.

8.1.2. ANRSimpatic – 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, Université de Paris 8.

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

As a participant, D. 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.

8.2. European Initiatives

8.2.1. FP7 Projects

8.2.1.1. 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. International Initiatives

8.3.1. Inria International Labs

The *MACISA* project-team (Mathematics Applied to Cryptology and Information Security in Africa) is one of the new teams of LIRIMA. Researchers from Inria and the universities of Bamenda, Bordeaux, Dakar, Franceville, Maroua, Ngaoundéré, Rennes, Yaoundé cooperate in this team.

The project is concerned with public key cryptology and more specifically the role played by algebraic maps in this context. The team focus on two themes:

- Theme 1 : Rings, primality, factoring and discrete logarithms;
- Theme 2 : Elliptic and hyperelliptic curve cryptography.

The project is managed by a team of five permanent researchers: G. Nkiet, coordinator of the project, J.-M. Couveignes, vice coordinator, T. Ezome and D. Robert, responsible for each of the two scientific working areas, A. Enge, head of the LFANT project team. The managing team organises the cooperation, schedules meetings, prepares reports, controls expenses, reports to the LIRIMA managing team and administrative staff.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Tony Ezome Mintsa, University of Franceville, Gabon, 02/2013 and 11–12/2013
- Loïc Grenie, University of Bergamo, 11–12/2013
- Matthias Waack, University of Leipzig, Germany, 10–11/2013
- Eduardo Friedman, University of Chile, 01–02/2013
- Francisco Diaz y Diaz, emeritus, 01–02/2013
- Bernadette Perrin-Riou, Université d'Orsay, 03/2013

8.4.1.1. Internships

- Fritz Hiesmayr, ÉNS Lyon, 06–07/2013
- Gregor Seiler, Technische Universität Berlin, Germany, 10/2013–03/2014

8.4.2. Visits to International Teams

D. Robert visited the cryptology team at Microsoft Research from August 06 to August 14.

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 a member of the editorial board of the *Publications mathématiques de Besançon* since 2010.

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

9.1.2. Invited talks

- J.-M. Couveignes attended the Sémestre Mathématique de Besançon in September 2013 and gave a talk on primality testing.
- J.-M. Couveignes attended GEOCRYPT 2013 in Papeete and gave a talk on genus two curves.
- A. Enge: "Class polynomials for dimension 2", Jahrestagung Computeralgebra, Konstanz, 18–22/03/2013
- A. Enge: "Class polynomials for abelian surfaces", Cryptography and Coding Theory at LIX, 20-21/06
- A. Enge: "Class polynomials for abelian surfaces", Number Theory, Geometry and Cryptography, Warwick, 01-05/07

9.1.3. Conference organisation and programme committees

The third atelier PARI/GP was held at IMB from January 14th to 18th, 2013: http://pari.math.u-bordeaux.fr/Events/PARI2013/. External speakers include Eduardo Friedman (Universidad de Chile), Xavier Roblot (Université Claude Bernard Lyon I), Jürgen Klüners (Universität Paderborn), Pascal Molin (Université Paris 7), Loïc Grenié (Università di Milano-Bicocca), Charles Boyd, Christophe Delaunay (Université de Franche-Comté), François Brunault (ENS Lyon), Philippe Elbaz-Vincent (Grenoble), Denis Simon (Caen).

A. Enge and D. Robert were programme committee members of the *Selected Area in Cryptography* 2013 conference.

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

- Friedrich Panitz (Paderborn), "An algorithm to enumerate quartic fields, after Bhargava."
- Sinai Robins (Nanyang Technological University, Singapore) "Cone theta functions and what they tell us about the irrationality of spherical polytope volumes."
- Achill Schürmann (Universität Rostock) "Exploiting Symmetries in Polyhedral Computations."
- Maike Massierer (University of Basel) "Point Compression for the Trace Zero Variety."
- Christophe Ritzenthaler (Université Aix-Marseille) "Sur la distribution des traces des courbes de genre 3 sur les corps finis."
- David Lubicz (CELAR — Rennes) "Algèbre linéaire sur $\mathbb{Z}_p[[u]]$ et application au calcul de réseaux dans les représentations galoisiennes p-adiques."
- Marie-Françoise Roy (Rennes) "Algorithme diviser pour régner pour les cartes routières."
- Sorina Ionica (ENS Paris) "Algorithms for isogeny graphs".
- Philippe Jaming (imb) "Problème de la phase dans le cadre discret"

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*.

Until October 2013, A. Enge was responsible for the international affairs of Inria–Bordeaux-Sud-Ouest. As such, he was a regular member of the COST-GTRI, the Inria body responsible for evaluating international partnerships. Since October 2013, he heads this committee.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Licence: A. Page, Fondamentaux pour les mathématiques et l'informatique, cours et TD, 18h, L1, Université Bordeaux 1, France;

Licence: A. Page, CPBx Analyse 2, TD, 43h, L2, Université Bordeaux 1, France;

Licence: A. Page, Codes et cryptographie, TD, 13h, L1, Université Bordeaux 1, France;

Master: K. Belabas, Computer Algebra, 90h, M2, Université Bordeaux 1, France;

Licence: J.-P. Cerri, Algèbre 1, cours, 22h, L1, Université Bord eaux 1, France;

Licence: J.-P. Cerri, Algèbre 2, TD, 51h, L2, Université Bordeau x 1, France;

Licence: J.-P. Cerri, Cryptographie et Arithmétique, cours, 24h, L 3, Université Bordeaux 1, France;

Licence: J.-P. Cerri, Algèbre 4, TD, 51h, L3, Université Bordeau x 1, France;

Master: J.-P. Cerri, Arithmétique, cours, 36h, M1, Université Bo rdeaux 1, France;

Master: J.-M. Couveignes, Algorithms for public key cryptograph, 40h, M2, Université Bordeaux 1, France;

Master: J.-M. Couveignes, Algorithms for number fields, 40h, M2, Université Bordeaux 1, France;

Licence: P. Lezowski, Ouverture professionnelle (help to students to look for a suitable Master), 12h, L3, Université Bordeaux 1, France;

Licence : N. Mascot, cours intégré MOSE 1003, 27h, L1, Université Bordeaux 1, France;

Licence : N. Mascot, C2I, TD, 15h, L1, Université Bordeaux 1, France;

Summer school: A. Enge, Complex multiplication of elliptic curves, 6h, PhD, Number Theory for Cryptography, Warwick, 24-28/06;

Summer school: A. Enge, Complex multiplication of elliptic curves, 1.5h, PhD, ECC 2013, Leuven, 11-13/09;

Summer school: A. Enge, Pairings on elliptic curves, 1.5h, PhD, ECC 2013, Leuven, 11-13/09.

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 was a member of the committee for

Habilitation defense (and referee) of Emmanuel Hallouin in Toulouse (November 2013).

J.-M. Couveignes was amember of the committees for

Professor position at the Université of Rennes (April 2013).

Professor position at the Université of Papeete(April 2013).

PhD defense of Jean-Gabriel Kammerer in Rennes (May 2013).

PhD defense (and referee) of Razvan Barbulescu in Nancy (december 2013).

PhD defense (and referee) of Emmanuel Fouotsa in Rennes (december 2013).

PhD defense (and referee) of Yvan Boyer in Paris (december 2013).

A. Enge was a member of the committees for

evaluation AERES LIP6, 07–09 January 2013;

evaluation AERES PRISM, 03–04 December 2013.

9.3. Popularisation

P. Lezowski has given a presentation on cryptology to high school students during “Fête de la science”.

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, pp. 1155–1168, http://www.worldscinet.com/ijnt/05/0507/S1793042109002614.html

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

[3] J. BELDING, R. BRÖKER, A. ENGE, K. LAUTER. *Computing Hilbert class polynomials*, in "Algorithmic Number Theory — ANTS-VIII", Berlin, A. VAN DER POORTEN, A. STEIN (editors), Lecture Notes in Computer Science, Springer-Verlag, 2007, vol. 5011, http://hal.inria.fr/inria-00246115

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

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

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

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

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

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

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

Publications of the year

Articles in International Peer-Reviewed Journals

[11] J.-P. CERRI, J. CHAUBERT, P. LEZOWSKI. *Euclidean totally definite quaternion fields over the rational field and over quadratic number fields*, in "International Journal of Number Theory", January 2013, vol. 9, n° 3, pp. 653-673 [*DOI :* 10.1142/S1793042112501540], http://hal.inria.fr/hal-00738164

[12] J.-M. COUVEIGNES, R. LERCIER. *Fast construction of irreducible polynomials over finite fields*, in "Israël Journal of Mathematics", 2013, vol. 194, n° 1, pp. 77-105, This text reports on a talk given at Lorentz center in Leiden during the recent workshop on it Counting points on varieties [*DOI :* 10.1007/s11856-012-0070-8], http://hal.inria.fr/hal-00456456

[13] A. ENGE, R. SCHERTZ. *Singular values of multiple eta-quotients for ramified primes*, in "LMS Journal of Computation and Mathematics", 2013, vol. 16, pp. 407-418 [*DOI :* 10.1112/S146115701300020X], http://hal.inria.fr/hal-00768375

[14] A. ENGE, E. THOMÉ. *Computing class polynomials for abelian surfaces*, in "Experimental Mathematics", 2014, Accepted for publication, http://hal.inria.fr/hal-00823745

[15] N. MASCOT. *Computing modular Galois representations*, in "Rendiconti del Circolo Matematico di Palermo", December 2013, vol. 62, n° 3, pp. 451-476 [*DOI :* 10.1007/s12215-013-0136-4], http://hal.inria.fr/hal-00776606

International Conferences with Proceedings

[16] A. ANGELAKIS, P. STEVENHAGEN. *Imaginary quadratic fields with isomorphic abelian Galois groups*, in "ANTS X - Tenth Algorithmic Number Theory Symposium", San Diego, United States, E. W. HOWE, K. S. KEDLAYA (editors), Mathematical Sciences Publisher, November 2013, vol. 1, pp. 21-39 [*DOI :* 10.2140/OBS.2013.1.21], http://hal.inria.fr/hal-00751883

[17] H. COHEN. *Haberland's formula and numerical computation of Petersson scalar products*, in "ANTS X", San Diego, United States, E. W. HOWE, K. S. KEDLAYA (editors), The Open Book Series, Mathematical Sciences Publisher, 2013, vol. 1, pp. 249-270 [*DOI :* 10.2140/OBS.2013.1.249], http://hal.inria.fr/hal-00854440

[18] K. LAUTER, D. ROBERT. *Improved CRT Algorithm for Class Polynomials in Genus 2*, in "ANTS X - Algorithmic Number Theory 2012", San Diego, United States, E. W. HOWE, K. S. KEDLAYA (editors), The Open Book Series, Mathematical Sciences Publisher, November 2013, vol. 1, pp. 437-461 [*DOI :* 10.2140/OBS.2013.1.437], http://hal.inria.fr/hal-00734450

Scientific Books (or Scientific Book chapters)

[19] K. BELABAS, F. BEUKERS, P. GAUDRY, W. MCCALLUM, B. POONEN, S. SIKSEK, M. STOLL, M. WATKINS. , *Explicit methods in number theory. Rational points and Diophantine equations*, SMF, 2013, xxi + 179 p. , http://hal.inria.fr/hal-00932377

[20] J.-M. COUVEIGNES, P. BOALCH, P. DÈBES, D. BERTRAND. , *Geometric and differential Galois theories*, Société Mathématique de France, 2013, 240 p. , http://hal.inria.fr/hal-00694296

[21] A. ENGE. *Elliptic curve cryptographic systems*, in "Handbook of Finite Fields", G. L. MULLEN, D. PANARIO (editors), Discrete Mathematics and Its Applications, Chapman and Hall/CRC, 2013, pp. 784-796, http://hal.inria.fr/hal-00764963

Other Publications

[22] K. BELABAS, E. FRIEDMAN. , *Computing the residue of the Dedekind zeta function*, 2013, 16 p. , http://hal.inria.fr/hal-00916654

[23] H. COHEN, F. THORNE. , *Dirichlet series associated to cubic fields with given quadratic resolvent*, 2013, 16 pages, submitted. Revised version: includes counts of S_3-sextic fields, http://hal.inria.fr/hal-00854662

[24] H. COHEN, F. THORNE. , *Dirichlet series associated to quartic fields with given resolvent*, 2013, 36 pages, submitted, comments welcome, http://hal.inria.fr/hal-00854664

[25] R. COSSET, D. ROBERT. , *Computing (l,l)-isogenies in polynomial time on Jacobians of genus 2 curves*, 2013, Accepté pour publication à Mathematics of Computations, http://hal.inria.fr/hal-00578991

[26] J.-M. COUVEIGNES, R. LERCIER. , *The geometry of some parameterizations and encodings*, 2013, http://hal.inria.fr/hal-00870112

[27] A. ENGE. , *Bilinear pairings on elliptic curves*, January 2013, http://hal.inria.fr/hal-00767404

[28] A. ENGE, F. MORAIN. , *Generalised Weber Functions*, 2013, http://hal.inria.fr/inria-00385608

[29] D. LUBICZ, D. ROBERT. , *A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties*, 2013, http://hal.inria.fr/hal-00806923

[30] A. PAGE. , *Computing arithmetic Kleinian groups*, 2013, Revisions according to the comments of the referee, http://hal.inria.fr/hal-00703043

References in notes

[31] E. BACH. *Improved approximations for Euler products*, in "Number theory (Halifax, NS, 1994)", Amer. Math. Soc., 1995, pp. 13–28

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

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

[34] 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/

[35] 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, pp. 49–62

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

[37] 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

[38] R. DUPONT. , *Moyenne arithmetico-geometrique, suites de Borchardt et applications*, Ecole polytechnique, Palaiseau, 2006

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

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

[41] P. LEZOWSKI. , *Computation of the Euclidean minimum of algebraic number fields*, 2011, 30 p. , To appear, http://hal.archives-ouvertes.fr/hal-00632997

[42] D. LUBICZ, D. ROBERT. *Efficient pairing computation with theta functions*, in "Algorithmic Number Theory — ANTS-IX", G. HANROT, F. MORAIN, E. THOMÉ (editors), Lecture Notes in Comput. Sci., Springer–Verlag, 07 2010, vol. 6197 [*DOI :* 10.1007/978-3-642-14518-6_21], http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf

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