INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Lfant

Lithe and Fast Algorithmic Number Theory

Bordeaux - Sud-Ouest

Theme : Algorithms, Certification, and Cryptography

Table of contents

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.*

1. Team

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, on leave from University of Toulouse II, HdR]

Technical Staff
Bill Allombert [CNRS, since 05/2010]

PhD Students
Jean-François Biasse [DGA-CNRS, until 09/2010]
Pierre Lezowski [ENS, since 09/2009]
Jérôme Milan [ANR, since 09/2009]
Pascal Molin [ENS, until 09/2010; ATER University Bordeaux 1, 10/2010–11/2010]
Vincent Verneuil [CIFRE Inside Contactless, since 2009]

Post-Doctoral Fellows
Anna Morra [ATER University Bordeaux 1, until 09/2010]
Damien Robert [INRIA, since 10/2010]
Pieter Rozenhart [INRIA, 01/2010–12/2010]

Administrative Assistant
Patricia Maleyran

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

P. Molin has defended his PhD thesis on "Intégration numérique et calculs de fonctions L" [12]. J.-F. Biasse has defended his PhD thesis on "Subexponential algorithms for number fields" [11]. In May, A. Enge has given the science talk at the ceremony awarding the Abel Prize to John Tate in Oslo. The talk, entitled "The queen of mathematics in communication security", presented links between Tate's work and cryptologic applications.

3. Scientific Foundations

3.1. Number fields, class groups and other invariants

Participants: Bill Allombert, Karim Belabas, Jean-François Biasse, Jean-Paul Cerri, Henri Cohen, Jean-Marc Couveignes, Andreas Enge, Pierre Lezowski, Pascal Molin, Anna Morra.

Modern number theory has been introduced in the second half of the 19th century by Dedekind, Kummer, Kronecker, Weber and others, motivated by Fermat's conjecture: There is no non-trivial solution in integers to the equation $x^n + y^n = z^n$ for $n \geqslant 3$. For recent textbooks, see [6]. Kummer's idea for solving Fermat's problem was to rewrite the equation as $(x+y)(x+\zeta y)(x+\zeta^2 y)\cdots(x+\zeta^{n-1}y) = z^n$ for a primitive n-th root of unity ζ, which seems to imply that each factor on the left hand side is an n-th power, from which a contradiction can be derived.

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

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

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

One of the main concerns of algorithmic algebraic number theory is to explicitly compute these invariants (Cl_K and h_K, fundamental units and R_K), as well as to provide the data allowing to efficiently compute with numbers and ideals of $\mathcal{O}_K$; see [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, Jean-François Biasse, Jean-Marc Couveignes, Andreas Enge, Jérôme Milan, Pascal Molin, Damien Robert, Pieter Rozenhart, 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, Damien Robert.

Complex multiplication provides a link between number fields and algebraic curves; for a concise introduction in the elliptic curve case, see [8], 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 [7]. For the same level of security, the latter require smaller key lengths than RSA, which results in a gain of bandwidth and (depending on the precise application) processing time. Especially in environments that are constrained with respect to space and computing power such as smart cards and embedded devices, algebraic curve cryptography has become the technology of choice. Most of the research topics of the LFANT team concern directly problems relevant for curve-based cryptology: The difficulty of the discrete logarithm problem in algebraic curves determines the security of the corresponding cryptosystems. Complex multiplication, point counting and isogenies provide, on one hand, the tools needed to create secure instances of curves. On the other hand, isogenies have been found to have direct cryptographic applications to hash functions [34] and encryption [38]. 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/

License: GPL 2+

Current stable version of PARI/GP: 2.3.5, 2010
Current testing version of PARI/GP: 2.4.3.alpha, 2010
Current version of `gp2c`: 0.0.5pl10, 2010

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.

5.2. Mpc

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

http://mpc.multiprecision.org/

License: LGPL 2.1+

Current version: 0.8.2 *Dianthus deltoides*, 2010

MPC is a C library for the arithmetic of complex numbers with arbitrarily high precision and correct rounding of the result. It is built upon and follows the same principles as MPFR. The MPC library has been registered in France by the Agence pour la Protection des Programmes on 2003-02-05 under the number IDDN FR 001 060029 000 R P 2003 000 10000.

It is a prerequisite for the release 4.5 of the GNU compiler collection GCC, 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.

5.3. Mpfrcx

Participant: Andreas Enge.

http://mpfrcx.multiprecision.org/

License: LGPL 2.1+

Current version: 0.3.1 *Banane*, 2010

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.

5.4. Cm

Participant: Andreas Enge.

http://cm.multiprecision.org/

License: GPL 2+

Initial public release: version 0.1 *Apfelkraut*, 2009

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].

5.5. Cubic

Participant: Karim Belabas.

http://www.math.u-bordeaux.fr/~belabas/research/software/cubic-1.0.tgz

License: GPL 2+

Current stable version: 1.0, 2009

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.

6. New Results

6.1. Discrete logarithms

Participant: Andreas Enge.

In [36], 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 [25], 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. The article has been accepted by *Journal of Cryptology*.

6.2. Class groups and other invariants of number fields

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

J.-F. Biasse has made practical improvements to the sieving-based algorithm of Jacobson [37] for computing the group structure of the ideal class group of an imaginary-quadratic number field [15]. These improvements, based on the use of large prime variations combined with structured Gaussian elimination, have led to the computation of the class group structure of a number field with a 110-digit discriminant (whereas older techniques were limited to 90-digit discriminants).

He has also 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 [25], cf. 6.1. The article [22] has been submitted to *Mathematics of Computation*.

In collaboration with M. Jacobson, J.-F. Biasse has described improvements to the sieving methods for ideal class group, regulator and fundamental unit computation [16]. These improvements lead to a significant speed-up over the previous state of the art, and the computation of the regulator of a number field of a 110 digit discriminant, whereas the previous record was 100 digits.

Together with M. Jacobson and A. Silvester, J.-F. Biasse has improved the algorithms for solving the discrete logarithm problem and the principal ideal problem, which are involved in the design of cryptosystems based on number fields [17]. They have assessed the impact of these improvements on the security of theses cryptosystems and provided estimates on the size of the keys required to ensure a level of security equivalent to the recommendations of the NIST.

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 [23]. 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.

The algorithms developed by J.-P. Cerri for totally real fields are currently being generalised by P. Lezowski to arbitrary number fields.

In collaboration with L. Grenié, B. Allombert and K. Belabas have considerably improved the practical efficiency of PARI/GP algorithms computing class and unit groups, in particular for number fields of large degree. They are currently working on a flexible parallelisation framework of the PARI/GP system; a first application target is to improve the relation finding part of the class group algorithms (affording in principle a linear speedup).

6.3. Number and function field enumeration

Participants: Karim Belabas, Henri Cohen, Anna Morra, Pieter Rozenhart.

In joint work with É. Fouvry (Orsay), K. Belabas has proved a new case of Malle's conjecture, a strong effective form of the inverse Galois problem [14]. They have given an asymptotic enumeration of Galois sextic fields with group S_3, ordered by discriminant, using classical Davenport-Heilbronn theory in a novel way. The same result was independently obtained by Bhargava and Wood using a different method.

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. 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. The article [30] has been submitted to *Mathematics of Computation*. 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 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. The article [24] has been accepted by *Journal of Algebra*.

6.4. L-functions

Participants: Bill Allombert, Karim Belabas, Henri Cohen, Pascal Molin.

Classical theorems of Davenport and Heilbronn enumerate cubic fields and estimate the average 3-torsion of class groups of quadratic fields. In joint work with M. Bhargava (Princeton) and C. Pomerance (Dartmouth College), K. Belabas has proved the first power-saving error terms for those results, lending support to a conjecture of Roberts [13]. As a corollary, the generating Dirichlet series associated to cubic discriminants can be analytically continued to the left of its simple pole at $s = 1$, proving a conjecture of Cohen. Since then, in the summer of 2010, Bhargava, Shankar and Tsimerman have proven Roberts's full conjecture.

As for effective computations of general L-functions, methods have been designed for ten years and programs due to T. Dokchitser and M. Rubinstein are available. In his thesis [12], P. Molin proved the complexity of such algorithms and designed improvements which led to the first fast and proven calculations. He gave explicit estimates which make it possible to experiment and investigate further on L-functions. He is currently implementating his L-function algorithms in the PARI/GP system with the help of B. Allombert.

6.5. Complex multiplication

Participant: Andreas Enge.

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 [26]. 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.

In [4], A. Enge and his coauthors have described a quasi-linear algorithm for computing generating polynomials of Hilbert class fields that rely on Chinese remaindering instead of floating point evaluations. It has been made practical and space efficient for computing reductions of the polynomials modulo large primes by A. Sutherland [39]; his implementation showed that the new algorithm was preferable for large class numbers. In [20], A. Enge and A. Sutherland have provided the one missing link to turn the algorithm into the method of choice regardless of the class number, by providing a way of applying the Chinese remainder paradigm to class invariants, smaller generators of the ring class field.

6.6. Elliptic curve cryptology

Participants: Jérôme Milan, Vincent Verneuil.

Together with C. Giraud, V. Verneuil has addressed the problem of protecting elliptic curve scalar multiplication implementations against side-channel analysis by using the atomicity principle [21]. First of all they reexamine classical assumptions made by scalar multiplication designers and point out that some of them are not relevant in the context of embedded devices. They then describe the state of the art of atomic scalar multiplication and propose an atomic pattern improvement method. Compared to the most efficient atomic scalar multiplication published so far, their technique shows an average speed improvement of up to 10.6%.

In [19], V. Verneuil and his coauthors introduce a technique of correlation analysis using only one execution power curve during an exponentiation to recover the whole secret exponent manipulated by the chip. As in Walter's Big Mac attack, longer keys facilitate this approach, and its success depends on the characteristics of the arithmetic coprocessor. Contrarily to the Big Mac attack, it applies even in the case of regular implementations such as the square-and-multiply-always or the Montgomery ladder. They also find that DSA and Diffie-Hellman exponentiations are no longer immune against CPA.

J. Milan has worked with T. Clausen and U. Herberg (Hipercom@LIX, École polytechnique) to bring some basic authentication mechanism to the OLSRv2 routing protocol in mobile ad-hoc networks by using digital signatures based on elliptic curves (ECDSA) and pairings on such curves (BSL-like signature). Such a mechanism has been developed and integrated within Hipercom@LIX's jOlsrv2 framework, which provides a Java-based implementation of the OLSRv2 protocol and interfaces with a network simulator (NS2) [18].

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. 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. Other Grants and Activities

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. PHC Ulyses: Pairing-based cryptography – implementation and security

Participants: Andreas Enge, Jérôme Milan.

The project is a collaboration with the team of Michael Scott at Dublin City University, with an emphasis on the exchange of PhD students.

Its aim is to establish the catalogue of available pairings and determine optimal parameter choices for the underlying finite fields, extension degrees and curve parameters and representations. Algorithmic improvements in the whole chain of pairing based cryptography between the finite field and the actual cryptographic primitive are attempted to be achieved.

8.3. Exterior research visitors

The following researchers have visited the LFANT team:

- Damien Robert, LORIA, February 8–12
- Eduardo Friedman, Universidad de Chile, February 1–20
- Loïc Grenié, Università di Bologna, April 5–9 and October 15–20
- Manuel Charlemagne, Dublin City University, October 11–15 and December 6–10
- David Lubicz, Rennes, December 13–17

9. Dissemination

9.1. Thesis committees

K. Belabas has been a referee for the thesis of Alexander Kruppa (Nancy, “Speeding up Integer Multiplication and Factorization”) and Alexander Rahm (Grenoble, “(Co)homologies and K-theory of Bianchi groups using computational geometric models”). He has been a committee member for the PhD defense of Tony Ezome (Toulouse, “Courbes elliptiques, cyclotomie et primalité”).

Jean-Marc Couveignes has been a committee member for Luca De Feo's PhD defense on "Algorithmes rapides pour les tours de corps finis et les isogénies" at École polytechnique.

A. Enge has taken part in the committee for Thomas Icart's PhD "Algorithms mapping into elliptic curves and applications" at Université du Luxemburg.

9.2. 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)*.

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

9.3. Invited talks

A. Enge has given a talk on "Class polynomials by Chinese remaindering" at ECC 2010 – Workshop on Elliptic Curves and Computation in Redmond.

P. Rozenhart has presented "Computing quadratic function fields with high 3-rank via cubic field tabulation" at the 11th meeting of the Canadian Number Theory Association. He has given an invited talk at Bates College in Lewiston, Maine, USA, titled "Computing quadratic function fields with high 3-rank via cubic field tabulation".

9.4. Conference organisation and programme committees

We have organised a workshop on the algorithmics of L-functions from December 6 to 10 at Bordeaux. 18 talks were programmed during the week, which left ample room for scientific exchange. In addition to the LFANT team members, the workshop was attended by a dozen of researchers. Two students from ENS Paris, who intend to pursue a PhD with the team, took also part.

The first day was dedicated to algorithmics of number fields; the second, to Iwasawa theory; the third, to theta functions and arithmetic groups; the fourth, to the search for rational points on modular curves and the algorithmics of holomorphic functions. On the last day, we have treated complex multiplication and p-adic L-functions.

The following persons have given a presentation: Bill Allombert (Bordeaux), Peter Bruin (Orsay), Julien Blondeau (Besançon), Henri Cohen (Bordeaux), Guillaume Perbet (Besançon), Christophe Delaunay (Lyon), Damien Robert (Bordeaux), Aurel Page (ENS Paris), Pierre Parent (Bordeaux), Marusia Rebolledo (Clermont-Ferrand), Jean-Marc Couveignes (Bordeaux), Pascal Molin (Nancy), Nicolas Mascot (ENS Paris), Andreas Enge (Bordeaux), Xavier Roblot (Tokyo).

H. Cohen is a member of the scientific comittee for *ANTS – Algorithmic Number Theory Symposium*, the major, biennial international conference in the field.

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

9.5. Seminar

The following external speakers have given a presentation at the LFANT seminar, see

http://www.math.u-bordeaux1.fr/~enge/lfant/index.php?category=seminar

- Damien Robert: “Calcul de pairings avec les fonctions thetas”
- Damien Robert: “Computing isogenies between abelian varieties”
- Eduardo Friedman: “Special values of Dirichlet series and Zeta integrals associated to polynomials”
- Loïc Grenié: “Comment vérifier si deux représentations galoisiennes ont la même semi-simplifiée”
- Michael Drmota: “An asymptotic analysis of Cuckoo hashing”
- Paul Zimmermann: “Peut-on calculer sur ordinateur?”
- Manuel Charlemagne: “The security of the discrete logarithm problem (DLP) in the context of pairings”
- Damien Bernard: “Petits zéros de fonctions L associées à un corps quadratique imaginaire”
- Peter Bruin: “Sur le calcul des coefficients des formes modulaires”
- David Lubicz: “Couplage avec les fonctions thêta”

9.6. Teaching

K. Belabas has taught a bachelor course in cryptology, and master courses on computer algebra, elliptic curves, and the algorithmic of public key cryptography. He has supervised master projects on cyclotomic proofs of (cases of) Fermat’s Last Theorem, optimal elliptic curve models for cryptography, factorisation of univariate polynomials over a finite field, asymptotically fast integer multiplication (from Karatsuba to Fürer), and sub-quadratic integer division algorithms.

J.-F. Biasse was a teaching assistant (“moniteur”) at the Applied Mathematics Department (CMAP) of École polytechnique. He was involved in the following courses: Introduction to C++, Numerical Analysis, Probability.

J.-P. Cerri has been in charge during two years of the course “Computational Number Theory” of the international research master programme Algant. This year, he teaches bachelor students working towards the master programme CSI on cryptology and information security. He is responsable for running the bachelor programmes in mathematics and computer science.

A. Enge is a “Chargé d’enseignement” at the Department of Informatics of École polytechnique. He has taught a master course on cryptology and a bachelor course on web programming.

9.7. 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).

A. Enge has taken part in the hiring committees for two maîtres de conférences in mathematics at the Universities of Bordeaux and Caen, and for a CNRS chair in cryptology at the department of computer science of University of Versailles.

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. 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.

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

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

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

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

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

[8] 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/.

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

[10] A. ENGE, P. GAUDRY. *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

Doctoral Dissertations and Habilitation Theses

[11] J.-F. BIASSE. *Subexponential algorithms for number fields*, École polytechnique, 2010.

[12] P. MOLIN. *Intégration numérique et calculs de fonctions L*, University of Bordeaux, 2010, http://tel.archives-ouvertes.fr/tel-00537489/fr/.

Articles in International Peer-Reviewed Journal

[13] 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.

[14] K. BELABAS, É. FOUVRY. *Discriminants cubiques et progressions arithmétiques*, in "International Journal of Number Theory", 2010, vol. 6, n° 7, p. 1491–1529, http://www.worldscinet.com/ijnt/06/0607/S1793042110003605.html.

[15] J.-F. BIASSE. *Improvements in the computation of ideal class groups of imaginary quadratic number fields*, in "Advances in Mathematics of Communications", 2010, vol. 4, n° 2, p. 141–154, http://hal.inria.fr/inria-00397408/.

International Peer-Reviewed Conference/Proceedings

[16] J.-F. BIASSE, M. JACOBSON. *Practical improvements to class group and regulator computation of real quadratic fields*, in "Algorithmic Number Theory Symposium – ANTS IX", Berlin, G. HANROT, F. MORAIN, E. THOMÉ (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6197, p. 50–65, http://hal.inria.fr/inria-00477896/.

[17] J.-F. BIASSE, M. JACOBSON, A. SILVESTER. *Security estimates for quadratic field based cryptosystems*, in "Australasian Conference in Information Security and Privacy – ACISP 2010", Berlin, P. HAWKES, R. STEINFELD (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6168, p. 233–247, http://hal.inria.fr/inria-00477949/.

[18] T. CLAUSEN, U. HERBERG, J. MILAN. *Digital Signatures for Admittance Control in the Optimized Link State Routing Protocol version 2*, in "International Conference on Internet Technology and Applications – iTAP 2010", IEEE eXpress Conference Publishing, 2010, http://hal.inria.fr/inria-00460057/.

[19] C. CLAVIER, B. FEIX, G. GAGNEROT, M. ROUSSELET, V. VERNEUIL. *Horizontal Correlation Analysis on Exponentiation*, in "Information and Communications Security – ICICS 2010", Berlin, M. SORIANO, S. QING, J. LOPEZ (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6476, p. 46–61, http://hal.inria.fr/inria-00540384/.

[20] A. ENGE, A. V. SUTHERLAND. *Class Invariants by the CRT Method*, in "Algorithmic Number Theory – ANTS-IX", Berlin, G. HANROT, F. MORAIN, E. THOMÉ (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6197, p. 142–156, http://hal.inria.fr/inria-00448729/.

[21] C. GIRAUD, V. VERNEUIL. *Atomicity Improvement for Elliptic Curve Scalar Multiplication*, in "Smart Card Research and Advanced Application – CARDIS 2010", Berlin, D. GOLLMANN, J.-L. LANET, J. IGUCHI-CARTIGNY (editors), Lecture Notes in Computer Science, Springer-Verlag, 2010, vol. 6035, p. 80–101, http://hal.inria.fr/inria-00459461/.

Research Reports

[22] J.-F. BIASSE. *An L(1/3) algorithm for ideal class group and regulator computation in certain number fields*, HAL-INRIA, 2010, n° 440223, http://hal.inria.fr/inria-00440223/.

[23] J.-P. CERRI. *Some Generalized Euclidean and 2-stage Euclidean number fields that are not norm-Euclidean*, HAL, 2010, n° 505142, To appear in Mathematics of Computation, http://hal.archives-ouvertes.fr/hal-00505142/.

[24] H. COHEN, A. MORRA. *Counting Cubic Extensions with given Quadratic Resolvent*, HAL, 2010, n° 463533, To appear in Journal of Algebra, http://dx.doi.org/10.1016/j.jalgebra.2010.08.027.

[25] A. ENGE, P. GAUDRY, E. THOMÉ. *An $L(1/3)$ Discrete Logarithm Algorithm for Low Degree Curves*, HAL-INRIA, 2010, n° 383941, To appear in Journal of Cryptology, http://dx.doi.org/10.1007/s00145-010-9057-y.

[26] A. ENGE, F. MORAIN. *Generalised Weber Functions. I*, HAL-INRIA, 2010, n° 385608, http://hal.inria.fr/inria-00385608/.

[27] J. MILAN. *Factoring Small to Medium Size Integers: An Experimental Comparison*, HAL-INRIA, 2010, n° 188645, http://hal.inria.fr/inria-00188645/.

[28] P. MOLIN. *Intégration numérique par la méthode double-exponentielle*, HAL, 2010, 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, 2010, 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, 2010, n° 477111, 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° 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, 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. 379–393, http://hal.inria.fr/inria-00135324.

[37] M. JACOBSON. *Subexponential Class Group Computation in Quadratic Orders*, Technische Universität Darmstadt, 1999.

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

[39] A. V. SUTHERLAND. *Computing Hilbert class polynomials with the Chinese remainder theorem*, 2009, To appear in Mathematics of Computation, http://arxiv.org/abs/0903.2785.