GTEM Research Program

This document contains the research plan of the GTEM proposal, and the list of tasks and deliverables agreed with the European Commission.

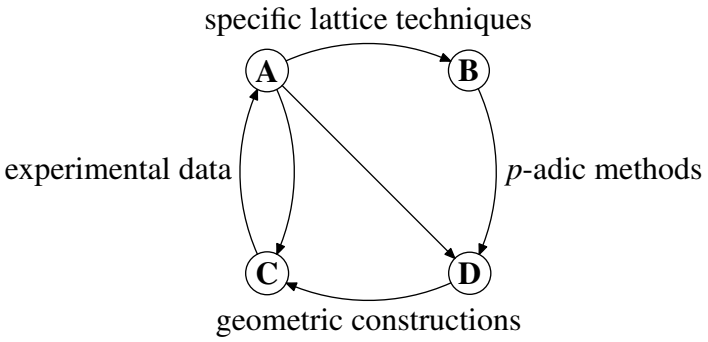
1. PROPOSAL DESCRIPTION

The research project is divided into four **work packages**, described in detail below, and the **dissemination work package** described in the next section. Each of the four work packages will employ 3 ESRs of 36 months each. Each partner will contribute one ESR in a specified work package (Table 1 below). In addition, each partner will contribute several researchers from the permanent staff who will guide and supervise the ESR research (Table 2, p. 3). Details about the work packages are given below.

Table 1: Work packages

A.	Lattices and Arakelov theory (9 fte years)	Leader: Bayer ESR at: Lausanne, Rome, Leiden
B.	Galois representations (9 fte years)	Leader: Schneps ESR at: Paris, Barcelona, Tel Aviv
C.	Constructive Galois theory (9 fte years)	Leader: Matzat ESR at: Bordeaux, Lille, Heidelberg
D.	Effective cohomology computations (9 fte years)	Leader: Cremona ESR at: Essen, Leuven, Nottingham

While the exact interrelations between work packages will only be determined by the work package coordinators in the course of the project, one can say in advance that a continuous flow of ideas and techniques will go between work packages, as illustrated below. In order to facilitate and encourage this process, each partner will serve one or two other packages in a supporting role (Table 2, p. 3). All ESRs will spend an estimated 25% of their time in secondment at other partners. These periods will be a combination of work within the same work package, and work in support of another package.



1.1. Package A: Lattices and Arakelov theory

The study of Euclidean lattices is important in its own right and by its many applications, in mathematics and in the other sciences (computer science, communication systems, material sciences, physics). Precisely for this reason, this topic suffers from fragmentation: the scientists working on lattices with a certain application in mind are not always aware of work being done from another point of view or with a different aim. To overcome this, work package A will contribute expertise and specific lattice techniques to the other packages. Very fruitful cooperation is expected, with breakthroughs both in theory and applications of lattices.

The research will focus particularly on Euclidean lattices defined over number fields and central simple algebras. We will develop new computational techniques for the Arakelov class group, an abstract object classifying such lattices, which plays a central role in modern thinking about computational number theory [**?**]. One milestone is the analysis and implementation of Lenstra's new "scanning" algorithm, which will yield data to gain new fundamental insights in Arakelov class groups.

In addition we will pursue the classification of modular lattices, construction of extremal lattices and sphere packings, and construction of codes for fading channels. Two breakthroughs we expect are important progress, due to the collaborative effort, towards Minkowski's 19th century conjecture concerning the inhomogeneous minimum of lattices, and construction of optimal space–time codes.

1.2. Package B: Galois representations

Much of the network research is devoted to developing and applying computational techniques to determining the structure of Galois groups. One important aspect, which is central in the major results in number theory of the last 10 years, is the topic of Galois representations, i.e., analysis of Galois actions on certain geometric objects. Little has been done in this area in the direction of an algorithmic treatment, but there are new ideas and promising partial results. The goal in this work package is to gain computational control over the Galois action on the two most promising and widely applied geometric objects: abelian varieties (giving linear Galois representations) and fundamental groups of moduli spaces of curves (non-linear representations).

An important class of abelian varieties is that of Jacobians of modular curves. For them, the mod p Galois representations can be constructed from modular forms. Our first specific goal concerning linear Galois representations is to determine the exact image of this representation for given modular forms. This will enable explicit geometric constructions of number fields with Galois groups of

Table 2: Work package participation by partner. The symbol E denotes the employment of a 36 month ESR; the symbol s denotes a supporting role.

Partner	Key scientists	Specific contributed expertise	A	B	C	D
Leiden	de Smit, Edixhoven, Lenstra, Stevenhagen	class field theory, arithmetical theory of modular forms, lattice reduction	E	s		s
Barcelona	Crespo, P. Bayer, Lario, Quer, Vila	Galois representations; inverse Galois problems		E	s	s
Bordeaux	Matignon, Bachoc, Belabas, Cohen, Couveignes	computational number theory: theory and software; p-adic methods; lattices; coding theory	s		E	s
Essen	Frey, Geyer, Nebe, Stoll, Völklein	arithmetic geometry with applications in cryptology	s			E
Heidelberg	Matzat, Malle, Klüners, Dettweiler	inverse Galois problem, enumerative Galois theory		s	E	
Lausanne	E. Bayer	theory and applications of lattices	E		s	s
Leuven	Denef, Vercauteren	p-adic methods for point counting and applications in cryptology		s		E
Lille	Dèbes, Emsalem, Ramero	Geometry and arithmetic of moduli spaces, p-adic methods			E	s
Nottingham	Cremona, Fesenko	computations with automorphic forms, point finding		s		E
Paris	Schneps, André, Soulé, Bertrand, Lochak	Geometry of moduli spaces, Arakelov theory.		E	s	
Rome	Schoof, Gasbarri	l-adic point counting, Arakelov theory, coding theory	E	s		
Tel Aviv	Jarden, Haran, Sonn, Efrat, Vishne	Infinite Galois theory and field arithmetic		E	s	

linear type, together with an explicit determination of their arithmetic invariants such as conductor and decomposition laws for primes, which will be used in work package C. The second goal is to generalise Serre's results about mod p representations of the Galois group acting on torsion points of an abelian variety over a number field to the case of finitely generated fields, and then apply this to generalise a result of Geyer-Jarden about torsion of abelian varieties over large algebraic fields.

The objective for the research in non-linear representations concerns the combinatorial description of the Galois action on algebraic geometric fundamental groups of moduli spaces of curves. This Galois action gives rise to elements of a combinatorial nature in the profinite free group on two generators. The key open problem is: which elements occur in this way? The specific goal is to answer this question by a special purpose computer algebra application. Initial results in this direction are the very first examples of computer algorithms applied to fundamental groups of moduli spaces (Schmithüsen 2004).

1.3. Package C: Constructive Galois theory

The general goal of this theme is the determination of which finite groups occur as Galois groups of number fields (possibly with additional local restrictions), and to understand the asymptotics of how often they occur for number fields with a given bound on the discriminant. We will pursue two specific objectives.

The first goal is to gain insight into a far-reaching conjecture of G. Malle concerning the asymptotics. For nilpotent groups a weak form of Malle's conjecture was proved recently by J. Klüners and G. Malle. For the general conjecture a specific aim is to find the constant leading term in the conjectured asymptotic. We will pursue the gathering experimental evidence from tables of number fields. For this, efficient algorithms and programs for computing very large tables of number fields or discriminants have to be devised. This interdisciplinary project will require state of the art programming and storage and retrieval techniques. The data will be vital for the study of algebraic lattices in work package A.

The second objective is the construction of exceptional motives, predicted by a conjecture of J.-P. Serre (1990), and the construction of modular forms associated to Galois motives appearing in the convolution process. This would lead to considerable progress in Serre's modularity conjecture. For both questions techniques developed in the recent Habilitation thesis of M. Dettweiler should prove essential.

1.4. Package D: Effective cohomology computations

Cohomological methods are powerful tools that are ubiquitous in abstract number theory and arithmetic geometry. By their abstract nature, the objects involved are quite difficult to do actual computations with. In this work package we pursue the development and applications of new methods to get computational grip on two kinds of cohomology groups: Monsky-Washnitzer cohomology and Brauer groups of local and global fields. In addition to their inherent mathematical interest, both have clear cryptographic implications. The first yields point counting algorithms in small characteristic, which is an essential part of hyper-elliptic curve cryptography. The second gives rise to bilinear structures on class groups related to curves, which become increasingly important in public key cryptography; cf. [**?**].

In the last five years new p-adic methods have been employed with striking success: we can now calculate the number of rational points on an elliptic curve over a field with 2^n elements, for n around 150, in less than a tenth of a second (Harley 2002). Very recently the team in Leuven obtained an algorithm with cubic time complexity for random curves with a given Newton polygon. The algorithm is based on calculating the Frobenius action on the p-adic cohomology of Monsky-Washnitzer, using toric geometry. The first goal is to obtain quadratic time complexity. A second goal is to find a practical algorithm that works for arbitrary curves in small characteristic. For this, one wants to calculate in Monsky-Washnitzer cohomology in cases where it does not equal the algebraic de Rham cohomology.

The p-adic methods are also becoming important in the determination of rational points on curves and varieties over global fields. This approach has been proposed by Elkies, and independently in a special case by Heath-Brown. To date the method has proved very successful in some special cases, and the time is ripe to apply it to more general systems of equations (including higher-dimensional varieties), to equations defined over number fields, and over function fields. The resulting point finding methods will be used in work package C.

We intend to obtain effective control of the arithmetic of Brauer groups of local and global fields by using the Hasse-Noether-Brauer sequence. This will also lead to an index-calculus algorithm for local invariants and the discrete logarithm in finite fields by constructing "nice" elements with the Tate-Lichtenbaum pairing. The new insights obtained this way are interesting from the theoretical point of view and most important for the security and efficiency of public key cryptography.

2. RESEARCH TASKS AND MILESTONES

The research project is divided into four **work packages**, described in detail below. Each partner will appoint a single ESR for the duration of 36 months. In addition, each partner will contribute several researchers from the permanent staff who will help, guide and supervise the ESR research. Partners have a primary task in a single work package, and secondary tasks in support of other work packages.

Below, the work plan for each Work Package is given as a list of tasks, followed by a table of milestones, and a schedule.

Work package A: Lattices and Arakelov theory

Leader: Partner 6

Task A1. Generalized lattices: theory and computations • Partner 1: Development of a new theory of generalized lattice structures. • Partners 1,6: Applications to classical lattices and to number theory Milestones: MA1, MA2
Task A2. Applications of geometry of numbers, particularly to coding theory • Partner 6,4: Investigation of optimal space-time codes, and codes for fading channels • Partner 1: Applied generalized lattice techniques Milestones MA2, MA3
Task A3. Algorithms of Arakelov class groups: analysis and implementation • Partner 11: Analysis of Lenstra's scanning algorithm • Partner 10: Arakelov theory • Partner 3: Specific computer algebra techniques Milestones MA4, MA5
Task A4. Development of new techniques in the geometry of numbers for number fields • Partner 6: Investigation of Euclidean lattices and central simple algebras • Partner 1, 11: Applications of generalized lattices and Arakelov techniques Milestones MA5

Work package B: Galois representations

Leader: Partner 10

Task B1. Galois representations mod l associated to l-torsion of abelian varieties. • Partner 2: expertise in abelian varieties • Partner 12: expertise on the image of Galois Milestone: MB1
Task B2: Development of a new theory of combinatorial geometry of moduli spaces • Partner 4, 8: necessary techniques on moduli spaces of curves • Partner 10: analysis of curve complexes Milestones: MB2, MB3
Task B3: Explicit computation with cohomology associated to moduli spaces • Partner 4: expertise in Hodge structures • Partner 10: moduli space algorithms Milestone: MB4
Task B4: Explicit study of Shimura curves and geometric Galois representations • Partner 2: explicit computation on Shimura curves • Partner 10: study of images of geometric Galois representations Milestones: MB5, MB6

Work package C: Constructive galois Theory

Leader: Partner 5

Task C1: Enumerative Galois Theory and Malle's conjecture • Partner 3: Analysis of number field counting algorithms • Partner 3, 5: Inverse Galois problems, enumerative Galois theory Milestones: MC1, MC2
Task C2: Inverse Galois theory • Partner 8: Braid group actions and Hurwitz spaces • Partner 2: Galois realizations with ramification conditions • Partner 5: Applications of motivic Galois representations Milestones: MC1, MC3
Task C3: Generation of experimental data for Galois realizations in classical and differential setting with database access • Partner 3: Specific computational techniques, Number field algorithms • Partner 5: Algorithmic Galois theory techniques (classical and differential) Milestone: MC4
Task C4: Arithmetic Differential Galois Theory • Partner 5: Differential Galois representations and Grothendiecks p-curvature conjecture • Partner 10: Parametrized differential Galois groups and moduli problems • Partner 2: Explicit inverse problems in differential Galois theory Milestones: MC4, MC5

Work package D: Effective cohomology computations

Leader: Partner 9

Task D1: Real and complex multiplication, Hecke operators and low genus curves • Partners 4, 9: Hecke operator characteristic polynomial computation • Partner 4: construction and arithmetic on curves with RM • Partner 4, 7: testing index calculus attacks Milestones: MD1, MD2
Task D2: Pairings on curves and applications to cryptography • Partners 4, 7: High genus curve Tate pairings • Partners 4, 9: Divisor class group addition algorithms Milestone: MD2
Task D3: Arithmetic of Brauer groups and applications to cryptography • Partner 4, 9: Brauer group Index calculus • Partner 4: Cryptographic application Milestone: MD3
Task D4: Monsky-Washnitzer Cohomology for curves (small characteristic). • Partner 4, 7: Calculation of Frobenius by p-adic deformation theory. • Partner 7: Calculation of Frobenius using special lifts of Frobenius. Milestones: MD4, MD5, MD6
Task D5: p-adic lattice methods for point-finding over global fields • Partner 9: Point-finding over number fields and function fields • Partner 1, 11: lattices over number fields Milestones: MD7, MD8

Scientific milestones and deliverables

Milestone	Month	Resp.	Description	Comment
MA1	12	1	Preliminary report on generalized lattice theory and LLL algorithms	Result of task A1, required for A2 and A4
MA2	24	1	Report: new results on reduction theory of generalized lattices, and exploration of applications	Result of task A1 and A2, required for A4
MA3	48	6	Report: new results on lattices techniques and applications in coding theory	Result of task A2
MA4	36	11	Report on Arakelov class group techniques, and algorithmic advances.	Theoretical results of task A3.
MA5	48	11	Summary report on new techniques in geometry of numbers over number fields	Joint result of tasks A3, A4
MB1	48	12	Report on new results on Galois image on l-torsion	Result of TB1
MB2	12	10	Report main results concerning curved complexes of moduli spaces	Intermediate result of TB2
MB3	36	10	Report on determination of automorphism groups of fundamental groups of moduli spaces	Result of TB2
MB4	48	10	Report on Hodge decomposition of cohomology of moduli spaces	Result of TB3
MB5	24	2	Elaboration of tables of Q-curves	Intermediate result of TB4
MB6	48	2	Report on design and implementation of new algorithms for Shimura curve computations	Result of TB4
MC1	12	3	Analysis of requirements for new asymptotic and effective Galois realizations	Intermediate result of TC1 and TC2, required for TC3
MC2	36	3	Report: new results, proven and conjectural, on the Malle conjecture	Result of TC1
MC3	48	8	Report: applications of Hurwitz spaces to inverse Galois problems.	Result of TC2
MC4	24	3	Database launch for Galois groups and differential Galois groups.	Initial result of TC3, TC4
MC5	48	5	Report: Local-global principles and algorithms for differential Galois problems	Result of TC4; contributes to TC3

Milestone	Month	Resp	Description	Comment
MD1	12	4	Report: construction of curves suitable for cryptography with discrete logarithms, index calculus and pairings	Result of task D1
MD2	24	4	Report: construction of curves with RM and CM curves of genus 2; pairing-friendly curves of genus 2; resistance against side-channel attacks	Result of tasks D1 and D2
MD3	36	4	Report: use of Quadratic sieve in Brauer group index calculus; application of Brauer group methods to discrete logs	Result of task D3
MD4	12	7	Report: implementation of fast algorithm to construct generic curves of genus 2 suitable for use in cryptography	Result of task D4
MD5	24	7	Report: improvement of Castryck-Denef-Vercauteren algorithm for zeta function of nondegenerate curves	Result of task D4
MD6	48	7	Report: faster construction of generic C_{ab}-curves suitable for cryptographic use with p-adic deformations.	Depends on MD4, MD5
MD7	12	9	Report: Applications of polynomial lattices to point-finding over rational function fields	Result of Task D5
MD8	48	9	Report: Lattice-based methods for point-finding over number fields and function fields	Depends on MA1, MA2; result of tasks D5

Scheduling of tasks and deliverables