

**The Final Report**  
**GTEM Research Training Network**  
**Galois Theory and Explicit Methods in Arithmetic**  
**Contract Number: HPRN-CT-2000-00114**  
**Contract beginning October 1, 2000, lasting 48 months**  
**Reporting Period = Year 4**

**Network Coordinator:**

Dr. Leila Schneps  
Equipe Analyse Algébrique  
Université de Paris 6  
175 rue du Chevaleret  
75013 Paris  
FRANCE  
Tel: 33 1 44 27 37 63  
Fax: 33 1 44 27 85 51  
Email: leila@math.jussieu.fr

**Network Home Page:** <http://www.math.jussieu.fr/~leila/gtem/gtem.html>

## Part A: Research Results

### A.1. Research highlights

#### A.1.1. Fourth reporting period

In this section we give a brief indication of the main new results from the fourth year of the network, organised by theme. Some of them are explained at more length in the context of the final report of network research given in **A.1.2**. For the relation with the tasks and milestones established in the network contract, see **B.3**.

#### *Dessins d'enfants over $p$ -adic fields*

The study of the reduction mod  $p$  of characteristic curve covers has made significant progress. This situation was classically understood completely in the case where  $p$  does not divide the order of the monodromy group of the cover: in other words, the corresponding extension of moduli fields of the cover is unramified at  $p$  if  $p$  does not divide  $G$ . Within the last year, the case where  $p$  divides the order but  $p^2$  does not has been completely clarified in the case of a curve cover of  $\mathbb{P}^1 - \{0, 1, \infty\}$  (i.e. a dessin d'enfant) with bad reduction at  $p$  (S. Wewers). He shows that the prime  $p$  is at most tamely ramified in this case. Using  $p$ -adic theta functions, L. Zapponi has been able to treat the case where any power of  $p$  divides the monodromy group for a particular family of genus 1 dessins with bad reduction. He determines in this case that the moduli field extension explicitly and finds that it is a tamely ramified extension of a cyclotomic extension.

#### *Explicit comparison between $G_{\mathbb{Q}}$ and $GT$*

This task, commonly known as Grothendieck-Teichmüller theory, draws on original ideas by Grothendieck and Drinfeld to give a combinatorial definition of a certain group called  $GT$  which has many arithmetic properties; above all it contains the absolute Galois group  $G_{\mathbb{Q}}$ . One aspect of the comparison of these two groups  $G_{\mathbb{Q}}$  and  $\widehat{GT}$  which has been developed within this last year is that of linear representations. In other words, instead of asking whether  $G_{\mathbb{Q}} = \widehat{GT}$ , one can ask the weaker question of whether the pro-algebraic envelope of  $\widehat{GT}$  is the pro-algebraic envelope of  $G_{\mathbb{Q}}$ , in other words, whether these two groups share the same linear representations. Until now there was no information on linear representations of  $\widehat{GT}$ . However recent work by I. Marin (former postdoc of Heidelberg) has exhibited the first family of linear representations.

The Lie analogue of this theory has also made progress this year. One can compare the Deligne-Ihara Lie algebra associated to  $G_{\mathbb{Q}}$  with the graded Lie algebra  $\mathfrak{grt}$  associated to  $\widehat{GT}$ . Although progress has not been made on the the main structure conjecture on the graded Lie algebra  $\mathfrak{grt}$  associated to the group  $\widehat{GT}$ , namely that it is free on one generator in each odd degree, interesting discoveries have been made on the number theory appearing in the Lie algebra. An example is the following theorem:

**Theorem.** For each even  $k \geq 12$ , there is a vector subspace of  $\mathfrak{grt}$  canonically isomorphic to  $S_k(\mathrm{SL}_2(\mathbb{Z}))$ , the space of modular cusp forms on  $\mathrm{SL}_2(\mathbb{Z})$  of weight  $k$ .

Progress has also been made on another fundamental conjecture concerning  $\mathfrak{grt}$ , namely that it is isomorphic to the dual Lie algebra of the Lie co-algebra of formal new multizeta values. All the topics concerning  $\mathfrak{grt}$  employ methods of computational arithmetic.

*Arithmetic of covers and fundamental groups.*

Another milestone which has been achieved in the last year of the network concerns the dihedral case of Oort's conjecture (Task 8, see **B.3**). Oort's conjecture is about lifting cyclic covers from characteristic  $p > 0$  to characteristic 0. I. Bouw (Essen) and S. Wewers (Bonn) were able to show that every smooth curve in characteristic  $p > 0$  together with an action of a dihedral group  $D_p$  lifts equivariantly to characteristic 0. For more progress in the direction of Oort's conjecture, see **A.1.2**.

Progress has also been made in finding rational points or rational subvarieties on moduli spaces, especially considering profinite groups and infinite towers of Hurwitz spaces (milestone of task 8). Given any projective system  $(G_n)_{n \geq 0}$  of finite groups, network research has provided infinite towers  $(\mathcal{H}_n)_{n \geq 0}$  of moduli spaces, geometrically irreducible and defined over  $\mathbf{Q}$ , with rational points over any henselian field (of residue characteristic not dividing the  $|G_n|$ s and with sufficiently many roots of 1). Strong irreducibility results for the varieties deduced from the  $\mathcal{H}_n$ s by fixing some of the branch points have been obtained, leading to analogous results in smaller dimension, yielding new results and examples on real,  $p$ -adic, totally real and totally  $p$ -adic points of Hurwitz spaces. Over number fields, rational points are conjectured by M. Fried to disappear beyond a certain level, in the situation of *modular* towers. A recent important network theorem in this domain states that projective systems of rational points cannot exist on modular towers.

*Elliptic and higher genus curves: explicit computation*

Progress has been made on the major milestone of this task, namely explicit determination of the Tate-Shafarevitch groups. Flynn and Bruin have developed a theory of "visualisation" via number fields and product varieties. This allows widely applicable techniques for the computation of ranks of Jacobians of higher genus curves, even when the 2-Selmer bound is not attained; this was previously only possible for a few special cases. They also demonstrate a connection with degree 4 del Pezzo surfaces, and show how the Brauer-Manin obstruction on these surfaces can be used to compute members of the Shafarevich-Tate group of Jacobians.

The quintuplet Cremona, Stoll, Simon, Fisher and O'Neil (all but the last from GTEM) have made significant progress towards explicit  $m$ -descent on elliptic curves over number fields for  $m \geq 2$ . For  $m=3$  this work is complete and implemented in Magma, allowing for explicit models for the elements of the 2-Selmer group to be determined. For  $m=5$  and  $m=8$ , the first explicit models of nontrivial elements of order  $m$  in the Weil-Chatelet group of an elliptic curve over  $\mathbf{Q}$  have been constructed. Network support has enabled a number of meetings between the five collaborators in Nottingham, Caen, Dagstuhl and Oberwolfach. A series of three preprints by the five authors are in preparation.

*Effective computation of coefficients of modular forms*

J-M. Couveignes (Bordeaux-Toulouse) and B. Edixhoven (Leiden) have made striking progress on the problem of computing the coefficients  $a_p$  (for primes  $p$ ) of cusp forms for congruence subgroups  $f = \sum_n a_n q^n$ , in an attempt to answer the question originally posed by R. Schoof of whether these coefficients can be computed in a time which is polynomial in  $\log p$ . The progress uses new algorithms developed by Couveignes for computing in Jacobians of modular curves. See **A.1.2** for a more complete description of this research.

### A.1.2. Major research results over the whole duration of the network

We first present five main themes corresponding to the five articles chosen for section **A.2.2**, and then add a discussion of other important themes and milestones on which progress was made by network research.

#### *Differential inverse Galois theory.* (B.H.Matzat, M. van der Put)

During the network duration, M. van der Put and B. H. Matzat developed a new approach to differential Galois theory in characteristic  $p > 0$ , called *iterative differential Galois theory*, based on Hasse and Witt's iterative derivations. Not only did they prove an analogue of the Abhyankar conjecture for connected linear groups, but *they solved the differential inverse Galois problem*, liquidating one of the main milestones set up to evaluate network accomplishments, the two articles cited below in **A.2.2**. Let us describe their results.

They begin with a constructive foundation of the Picard-Vessiot in characteristic zero, leading to a smallest differential field extension containing a full system of solutions of a linear differential equation with a linear algebraic group as Galois group. They explain the Galois correspondence between the intermediate differential fields of a Picard-Vessiot extension and the Zariski closed subgroups of the differential Galois group. They then develop the link between the differential Galois group and the monodromy group over the complex numbers generalizing the effective version of the Riemann Existence Theorem used in ordinary inverse Galois theory. After recalling past solutions of the inverse differential Galois problem over  $\mathbb{C}$  and subsequently for connected groups over general algebraically closed fields of characteristic zero, they turn to the characteristic  $p$  case.

It is first necessary to re-develop the Picard-Vessiot theory in this situation. Ordinary derivations, which no longer suffice, are generalized to a family of higher "iterative" derivations (originally defined by Hasse and Schmidt), which allow them to construct iterative Picard-Vessiot extensions in the same formal way as in characteristic zero. They again reduced linear algebraic groups defined over the field of constants as differential (ID) Galois groups, and establish a Galois correspondence between the intermediate ID-fields of a Picard-Vessiot extension and the reduced closed subgroups of the corresponding ID Galois groups. Finally, they determine the structure of all ID modules and ID Galois groups over local fields, determining that *they are all trigonalizable extensions of connected solvable groups by finite local Galois groups*. This allows them to solve the differential inverse Galois problem for these groups in the case of local fields. They were then able to extend the proof to a complete solution of the differential Galois problem in the case of global fields of characteristic  $p > 0$ .

#### *Geometric Galois theory.* (Y. André)

One of the major questions in the comparison theory of  $\widehat{GT}$  and  $G_{\mathbb{Q}}$ , a question which has been raised by experts for over 10 years, since the very beginnings of Grothendieck-Teichmüller theory, can be phrased as follows: if  $\widehat{GT}$  is to be like  $G_{\mathbb{Q}}$ , then where are the primes? network. I. Marin (former young postdoc in Heidelberg) has developed In other words, where are the "local subgroups at primes" corresponding to the local subgroups  $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$  of  $G_{\mathbb{Q}}$ ? As  $\widehat{GT}$  is defined a priori by its geometric action on the fundamental

groups of moduli spaces, which extends that of  $G_{\mathbb{Q}}$ , the primes appeared to be invisible.

The breakthrough in this direction was made by Yves André (Paris), who actually came up with the idea of how to define a “temperate” or  $p$ -adic fundamental group of a scheme  $X$  defined over  $\mathbb{Q}$ , by explicitly describing which covers should be classified by such a fundamental group. He then proved that the  $p$ -adic fundamental group is naturally a subgroup of the profinite (algebraic) fundamental group of  $X$  classifying all étale covers of  $X$ . Since  $\widehat{GT}$  acts on the algebraic fundamental groups of certain schemes, in particular  $X = \mathbb{P}^1 - \{0, 1, \infty\}$ , this made it natural to define a “local” subgroup  $\widehat{GT}_p$  as the subgroup of  $\widehat{GT}$  preserving the  $p$ -adic fundamental group of  $X$  viewed as a subgroup of the algebraic fundamental group of  $X$ .

Fixing an embedding of  $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$  identifies a local subgroup  $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$  inside  $G_{\mathbb{Q}}$  (which otherwise is defined only up to conjugation). If the definition of  $\widehat{GT}_p$  proposed by André seems to be the “right generalization” of the local subgroup of  $G_{\mathbb{Q}}$ , it is because André was able to prove that  $\widehat{GT}_p \cap G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ , where here  $G_{\mathbb{Q}}$  is considered as a subgroup of  $\widehat{GT}$ . This proof uses the theory of  $\widehat{GT}$  only to explicitly describe the action of  $G_{\mathbb{Q}}$  on the algebraic fundamental group of  $X$ . André then proves that an element of  $G_{\mathbb{Q}}$  preserves the  $p$ -adic subgroup (i.e. lies in  $\widehat{GT}_p$ ) if and only if it satisfies a classical property of elements of  $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$  on algebraic numbers, namely  $\sigma \in G_{\mathbb{Q}}$  belongs to  $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$  if and only if for all  $j \in \overline{\mathbb{Q}}$  such that  $|j|_p \leq 1$ , we also have  $|\sigma(j)|_p \leq 1$ .

This discovery gives a totally new direction to research on the relation between  $G_{\mathbb{Q}}$  and  $\widehat{GT}$ . It should also give rise to interesting computational possibilities for the image of the local subgroups of  $\widehat{GT}$  in the Lie algebra  $\mathfrak{grt}$ .

In this task, we also point out the remarkable work of L. Dieulefait (Barcelona, former postdoc in Paris), who works extensively on images of Galois representations geometric or automorphic having consequences in the inverse Galois theory over  $\mathbb{Q}$ . Dieulefait has a number of more recent papers concerning modularity, leading to proofs of new cases of the Fontaine-Mazur conjecture and of Serre’s conjecture for level 1 and weight 2 (now submitted for publication, see **A.2.1**).

*Dessins d’enfants, covers of curves* (S. Wewers, I. Bouw, P. Dèbes, L. Zapponi, M. Saïdi, M. Matignon)

*Topic 1. Dessins d’enfants over local fields.* This paragraph is concerned with the recent achievements in studying stable models of curve covers over  $p$ -adic fields. The GTEM nodes involved are essentially Bonn (M. Romagny, S. Wewers), Essen (I. Bouw, S. Flon), Nottingham (M. Saïdi) Bordeaux (C. Lehr and M. Matignon) and Bonn/Lausanne (L. Zapponi).

The new results are all related to a celebrated series of papers of M. Raynaud. The problem is the following: given a three point cover (i.e. a finite cover of the projective line unramified outside the points 0, 1 and  $\infty$ , in other words, a *dessin d’enfant*) defined over a  $p$ -adic field  $K$ , one would like to construct a stable model of it defined over the ring of integers  $R$  of  $K$ . It is known that, after extending the base field, such a model exists and is unique (in fact, if the cover is Galois then there exists a minimal extension  $L/K$  over which the stable model is defined, the so-called finite monodromy). However, the stable

model is not understood, i.e. in general it cannot be described explicitly.

Before the work of Raynaud, only the 'prime-to- $p$ ' case was completely understood. If the residue characteristic  $p$  of  $K$  does not divide the order of the (geometric) monodromy group then the cover has a smooth model; this is essentially the geometric part of Beckmann's works. As an arithmetic implication, one deduces that the field of moduli of the cover, which is a number field, is unramified outside the primes dividing the order of the group.

The difficulty is dealing with the case where  $p$  does divide the order of the monodromy group. This is where significant progress has been made by network research. We cite in particular the work by S. Wewers, C. Lehr and M. Matignon, and L. Zapponi described below, noting that although Wewers and Zapponi publish separately, their discussions during Zapponi's postdoctoral visits to Bonn were vital to the results described here.

There is still no complete description in the general case, but the the results of S. Wewers (among others) allow to treat the case where  $p$  simply divides the order of the monodromy group (i.e.  $p$  divides the order but  $p^2$  does not). The goal is to completely describe the stable model of the cover, and then deduce the arithmetic consequences of ramification at  $p$  of the extension of the associated moduli fields. One of the main results in this direction can be summarized as follows (cf. S. Wewers, Stable reduction of three-point covers, **A.2.2**).

**Theorem.** *Let  $f : X \rightarrow \mathbb{P}^1$  be a Galois three point cover of group  $G$  (a dessin d'enfant) with field of moduli  $K$  and bad reduction at  $p$ . If  $p$  simply divides the order of  $G$ , then the stable model of the cover can be explicitly described. In particular, the prime  $p$  is at most tamely ramified in  $K$ .*

There are other partial results, applying to specific families of covers. For example, C. Lehr and M. Matignon (cf. Lehr-Matignon, Wild monodromy..., **A.2.1**) are able to explicitly describe the finite monodromy in the  $p$ -cyclic case. In another context, L. Zapponi is able to predict the bad reduction of an infinite family of three point covers of genus one (with a different approach, based on the study of  $p$ -adic theta series) but with no restriction on the power of  $p$  which divides the order of the monodromy group. He is able to determine for this family the complete behaviour of the ramification at  $p$  of the moduli field extension and shows that both tame and wild ramification can occur. This aspect of the theory uses computational methods.

*Topic 2. Fields of definition of covers.* Finding the fields of definition of algebraic covers given by their topological invariants is a central problem. The regular inverse Galois problem is an obvious motivation. On Hurwitz moduli spaces of covers, this amounts to the following question:

*Milestone:* finding rational points or rational subvarieties on moduli spaces.

For the most recent network research on this topic, see **A.1.1**. Network research contained considerable foundational work on Hurwitz spaces, most notably about their compactification and their construction in finite characteristic dividing the order of the group (the wild case).

*Topic 3. Reduction and lifting of covers.* Knowledge of fundamental groups in characteristic  $p > 0$  is one motivation for these two basic issues. Another one is that arithmetic information on reduced covers generally provides arithmetic information on the initial covers.

*Milestone:* describing the stable reduction of curves and of covers.

An important project is to make “effective” Raynaud’s work on semi-stable reduction of Galois nilpotent covers of a  $p$ -adic curve that are ramified above an étale divisor: for example, to determine minimal extensions where a semi-stable model exists. This extension can now be explicitly described (even algorithmically) in the case that the curve is a  $p$ -cyclic cover of the affine line. This research has raised some questions about the automorphisms groups of  $p$ -cyclic covers of the affine line. Some classification is under way.

On moduli spaces it is the boundary of moduli spaces that is generally relevant for these questions. Some work in this direction has provided some refined versions of Beckmann’s theorem about the connection between the reduction of a cover and the ramification of the prime  $p$  in question in the field of moduli of the cover.

*Milestone:* Oort’s conjecture about lifting cyclic covers from characteristic  $p > 0$  to characteristic 0.

Since the first results for cyclic  $p$ -groups of order  $\leq p^2$ , this problem was one of the ongoing concerns of network research. It is now known that every smooth curve in characteristic  $p > 0$  together with an action of a dihedral group  $D_p$  lifts equivariantly to characteristic 0. New obstructions to lifting actions of  $\mathbf{Z}/p\mathbf{Z}^n$ -torsors on a curve have been obtained, which turn out to vanish for  $n = 2$  and  $p = 2$ , thus providing an interesting situation where such actions can always be lifted. Using some refinement of the equivariant  $K$ -theory, some results of Nakajima about the modular representation of global sections of invertible  $G$ -sheaves on a curve in characteristic  $p > 0$ , have been extended from the case “ $G$  cyclic of order  $p$ ” to the general case “ $G$  cyclic”; these modules constitute an obstruction to lifting wildly ramified  $G$ -covers to the Witt vector ring.

*Effective methods in curves and modular forms* (J-M. Couveignes, B. Edixhoven, R. Schoof)

Very important progress has been made in Task 6 (fast algorithms). One of the most striking domains of progress is in answering the following questions, due to R. Schoof:

**Question.** *Let  $f = \sum_n a_n q^n$  be a modular form. Can one compute the coefficient  $a_p$ , for a prime  $p$ , in a time that is polynomial in  $\log p$ ?*

Schoof (Rome) began work on this question, and B. Edixhoven (Leiden) developed a program to lead to the complete answer. He noted that it is enough to consider cusp forms with integral weight  $k$ . The main idea, as in Schoof’s original algorithm, is to use the fact that  $a_p$  is the trace of a Frobenius element at  $p$ , and compute it modulo  $\ell$  for sufficiently many small  $\ell$ . The algorithms in the case  $k = 1, 2$  are already well understood. For  $k \leq 3$ , the classical method imitating the  $k = 1, 2$  case is not practicable because of the appearance of algebraic curves which are too large to compute. The new significant idea due to Edixhoven and Couveignes in this case is to use numerical computations in the Jacobians of modular curves. Let  $J_1(N\ell)$  denote the Jacobian of the modular curve  $X_1(N\ell)$  and let  $E_f = \mathbb{Q}(\{a_n\})$  be the number field obtained by adjoining the coefficients of  $f$  to  $\mathbb{Q}$ . Suppose (for  $k \leq \ell + 1$ ) that we have a surjection of the ring of integers  $\mathcal{O}_{E_f} \twoheadrightarrow \mathbb{F}_\ell$ . Then the trace operators  $T_r - a_r$  cut out a 2-dimensional subspace  $V_{f,\ell}$  of  $J_1(N\ell)(\overline{\mathbb{Q}})[\ell]$  for  $r \leq N^2\ell^2$ . But the system is too large to solve directly.

Couveignes’ suggestion is to do numerical computations in

$$J_1(N\ell)(\mathbb{C}) = H_1(X_1(N\ell)(\mathbb{C}), \mathbb{R})/H_1(X_1(N\ell)(\mathbb{C}), \mathbb{Z}) \supset V_{f,\ell}.$$

For some  $x \neq 0$  in  $V_{f,\ell}$ , he suggests approximating  $F(x) \in \mathbb{C}$  for some rational function  $F$  on  $J_1(N\ell)$ , defined over  $\mathbb{Q}$ , such that  $\mathbb{Q}(x) = \mathbb{Q}(F(x))$ , and bounding the height and the

degree of  $F(x)$ , so as to compute this algebraic number by its minimal polynomial. Here the degree no longer causes a problem because  $V_{f,\ell}$  is a 2-dimensional  $\mathbb{F}_\ell$  vector space, so has only  $\ell^2$  elements, one of which is zero, so the degree is  $\leq \ell^2 - 1$ . So the goal is to approximate  $F$  and bound its height. Edixhoven and Couveignes have developed a series of algorithmic methods to accomplish this task. The main tools for the computational algorithm in Jacobians, together with the study of their complexity and stability, are given in the article by Couveignes cited in **A.2.2**.

*Absolute Galois groups and field arithmetic.* (M. Jarden, D. Haran, G. Frey, W-D. Geyer, F. Pop)

Let us cover some of the most important work done by this group of researchers. See **A.2.1** for references to the four articles discussed here, and **A.2.2** for the reference to the one chosen to figure among the five most important publications of the network.

Geyer and Jarden have now proved a large part of a conjecture they made 1979 on  $\ell$ -torsion points of abelian varieties. More details are given in [4] of **A.2.2**.

In a series of two joint articles (cf. **A.2.1**), D. Haran, M. Jarden, and F. Pop contribute to the classification of absolute Galois groups among all profinite groups. In the first article, they give a far-reaching generalization of a (now) classical result of Ax-Haran-Lubotzky-v.d.-Dries that a profinite group  $G$  is projective if and only if  $G$  is the absolute Galois group of a PAC field. The generalization contained in the present work states that a profinite group structure  $\mathbf{G}$  is projective if and only if  $\mathbf{G}$  is the absolute Galois group of a proper field-valuation structure with block approximation. In the second article, they give an application of this result, considering a finite set  $\mathcal{F}$  of fields, each of which is a finite extension of  $\mathbb{Q}_p$  for some  $p$  or of  $\mathbb{R}$ . They show that a profinite group  $G$  is  $\mathcal{F}$ -projective if and only if  $G$  is isomorphic to the absolute Galois group of a PFC field.

In a joint paper by W-D. Geyer and M. Jarden studying the rank of abelian varieties over large algebraic fields (cf. **A.2.1**, the authors strengthen a result of G. Frey and the second author from 1974. Let  $K$  be a finitely generated field over its prime field and  $A$  an abelian variety over  $K$ . The main result says that for almost all  $(\sigma_1, \dots, \sigma_e) \in \text{Gal}(K)^e$  the rank of the abelian group  $A(K_s[\sigma_1, \dots, \sigma_e])$  is infinite. Here  $K_s$  is the separable closure of  $K$ , for  $\sigma_1, \dots, \sigma_e \in \text{Gal}(K)$  the symbol  $K_s(\sigma_1, \dots, \sigma_e)$  stands for the fixed field of  $(\sigma_1, \dots, \sigma_e)$  in  $K_s$ , and  $K_s[\sigma_1, \dots, \sigma_e]$  is the maximal Galois extension of  $K$  in  $K_s(\sigma_1, \dots, \sigma_e)$ .

Finally, a joint article by G. Frey and M. Jarden (cf. **A.2.1**) improves on earlier results on properties of almost all fields  $K_s(\sigma_1, \dots, \sigma_e)$  (with  $K$  finitely generated field), which were proved for all  $e$  or made a distinction between the cases  $e = 1$  and  $e \geq 2$ . The main result of the present work reveals a situation distinguishing between  $e \leq 2$  and  $e \geq 3$ .

**Theorem:** *The following holds for almost all  $\sigma_1, \dots, \sigma_e \in \text{Gal}(\mathbb{Q})^e$ :*

**Condition (a):** *If  $e \leq 2$ , then there are infinitely many elliptic curves  $E$  (up to  $\mathbb{C}$ -isomorphism) with CM over  $\overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_e)$  such that  $\text{End}(E) \subset \overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_e)$ .*

**Condition (b):** *If  $e \geq 3$ , then there are only finitely many elliptic curves  $E$  (up to  $\mathbb{C}$ -isomorphism) with CM over  $\overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_e)$  such that  $\text{End}(E) \subset \overline{\mathbb{Q}}(\sigma_1, \dots, \sigma_e)$ .*

Further results about elliptic curves with CM distinguishes between the situations  $e \leq 3$  and  $e \geq 4$ .

## A.2. Joint research and YR research

As usual the network as a whole has produced dozens of articles this year. To give an idea, since the inception of the GTEM preprint archive shortly after the Midterm Review Meeting, 123 preprints have been uploaded. We give here only publications resulting either from a joint inter-team collaboration or signed by a young researcher.

The authorship of a postdoc of the network is signaled by bold type. Authorship by inter-team collaboration is signaled by indicating the team in parentheses. Note that several articles have been co-authored by former young researchers of the network who now may have other jobs, but whose collaborations were formed during their network stay.

### A.2.1. Joint inter-team and YR publications in the fourth reporting period

I. Bouw (Essen) and S. Wewers (Bonn), The local lifting problem for dihedral groups, preprint.

**David Brink**, On alternating and symmetric groups as Galois groups, preprint.

N. Bruin, E.V.Flynn, Visualising Sha[2] in Higher Genus, preprint.

**M. Dettweiler** and S. Wewers, Variation of local systems and parabolic cohomology, preprint.

**L. Dieulefait**, Nuria Vila, On the images of modular and geometric three-dimensional Galois representations. *Amer. J. Math.* 126 (2004), no. 2, 335–361.

**L. Dieulefait**, On the images of the Galois representations attached to genus 2 Siegel modular forms. *J. Reine Angew. Math.* 553 (2002), 183–200.

**L. Dieulefait**, Explicit determination of the images of the Galois representations attached to abelian surfaces with  $\text{End}(A) = \mathbb{Z}$ . *Experiment. Math.* 11 (2002), no. 4, 503–512,

**L. Dieulefait**, Existence of families of Galois representations and new cases of the Fontaine-Mazur conjecture, to appear in *J. Crelle*.

**Julio Fernandez**, A moduli approach to quadratic Q-curves realizing mod  $p$  projective Galois representations, preprint.

**Julio Fernandez**, J-C. Lario, Anna Rio, On twists of the modular curves  $X(p)$ , to appear in *Bull. London Math. Soc.*

G. Frey (Essen) and M. Jarden (Tel Aviv), On the number of elliptic curves with CM over large algebraic fields, preprint.

W-D. Geyer (Essen) and M. Jarden (Tel Aviv), The rank of Abelian varieties over large algebraic fields, preprint.

D. Haran (Tel Aviv), M. Jarden (Tel Aviv) and F. Pop (Bonn), Projective group structures as absolute Galois structures with block approximation, preprint.

D. Haran (Tel Aviv), M. Jarden (Tel Aviv) and F. Pop (Bonn), P-adically projective groups as absolute Galois groups, preprint.

- Claus Lehr** and M. Matignon, Automorphisms groups for  $p$ -cyclic covers of the affine line, to appear in *Compositio Math.*
- C. Lehr** and M. Matignon, Wild monodromy and automorphisms of curves, to appear in *Workshop on the Cryptography and Theory of Algebraic Curves supporting it*, /Chuo Univ. Tokyo/ 2003.
- C. Lehr**, Effective methods for vanishing cycles of  $p$ -cyclic covers of the  $p$ -adic line, *J. Algebra*, 271 (2004), no. 1, 407–425
- C. Lehr**, An analog to Deuring’s criterion for good reduction of elliptic curve, submitted.
- R. Litcanu** and **L. Zapponi**, Arithmetic properties of Lamé operators with finite monodromy, to appear in *Proceedings of the conference Groupes de Galois arithmétiques et différentiels*, Luminy 8-12 mars 2004.
- Ivan Marin**, Caractère de rigidité du groupe de Grothendieck-Teichmüller, preprint 2004.
- Martin Möller**, Shimura- and Teichmüller curves, preprint math.AG/0501333, 2004.
- F. Pop (Bonn) and M. Saïdi (Nottingham), On the specialization homomorphism of fundamental groups of curves in positive characteristic, in *Galois groups and Fundamental groups* (ed. Schneps), MSRI Pub. Series 41, 2003, 107–118.
- M. Romagny**, Group actions on stacks and applications, to appear in *Mich. Math. J.*
- M. Romagny** and S. Wewers, Hurwitz spaces, to appear in *Proceedings of the conference Groupes de Galois arithmétiques et différentiels*, Luminy 8-12 mars 2004.
- M. Romagny** and J. Bertin, Champs de Hurwitz, submitted.
- J. Stix**, A logarithmic view towards semistable reduction, *J. of Algebraic Geometry* **14** (2005), 119-136.
- J. Stix**, A monodromy criterion for extending curves, to appear in *Int. Math. Research Notices*.
- L. Zapponi**, Some arithmetic properties of Lamé operators with dihedral monodromy, to appear in *Rivista di Mat. di Parma*.
- L. Zapponi**, Specialization of polynomial covers of prime degree, *Pacific Math. J.* **214** (2004), 161-183.

A.2.2. Five major articles produced by the network

The following five works represent some of the key scientific advances of the network over its entire duration. The specific results are described in **A.1.2**. Here, we indicate their relevance with respect to tasks and milestones corresponding to the complete work plan given in **B.3**.

**Please observe that although three of the five articles are authored by a single researcher, they form parts of joint inter-team research collaborations, although the members of these collaborations (mentioned in the commentaries following each article) may choose to publish their contributions separately.**

[1] B. H. Matzat (Heidelberg) and M. van der Put (Leiden), Iterative differential equations and the Abhyankar conjecture, *J. reine angew. Math.* **557** (2003), 1-52.

See also

B. H. Matzat (Heidelberg) and M. van der Put (Leiden), Constructive Differential Galois Theory, in *Galois groups and Fundamental Groups*, L. Schneps, ed. MSRI Publications, Cambridge U. Press, 2003.

*These breakthrough articles completely settled the problem of inverse differential Galois theory in characteristic  $p$ , solving it via the development of a theory called iterative differential Galois theory (cf. Task 7, 3rd milestone of **B.3**).*

[2] Y. André (Paris), On a geometric description of  $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$  and a  $p$ -adic avatar of  $\widehat{GT}$ , *Duke Math. J.* **119** No. 1 (2003), 1-39.

*This article brought an answer to one of the most longstanding questions on the Grothendieck-Teichmüller group  $\widehat{GT}$ : in comparing this group to the absolute Galois group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , one must be able to identify the local groups at primes, corresponding to the local Galois groups  $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$  inside  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . André's theory of the  $p$ -adic fundamental group of a variety allowed him to define such  $p$ -adic subgroups  $\widehat{GT}_p$ , thus accomplishing one of the milestones of Task 4, **B.3**.*

[3] S. Wewers (Bonn), Stable reduction of 3-point covers, *J. Amer. Math. Soc.* **16** No. 4 (2003), 991-1032.

*This article forms part of the ongoing research project of the group S. Wewers (Bonn), L. Zapponi (Lausanne/Paris), I. Bouw (Essen), M. Matignon (Bordeaux), M. Saïdi (Nottingham) and young researchers) on the study of stable models and ramification of moduli field extension of curve covers over  $p$ -adic fields. This particular article contains a breakthrough in the case where  $p$  divides the order of the monodromy group. This situation, which up to now was understood only for isolated examples, is dealt with here for all bad reduction dessins d'enfants. It represents a milestone of Task 3, **B.3**.*

[4] J-M. Couveignes, Jacobiens, jacobiennes et stabilité numérique, preprint 2004.

*This article contains a seminal contribution, giving fast algorithms for computing in Jacobians of modular curves (task 6, cf **B.3**), to the ongoing program involving R. Schoof*

(Rome) and B. Edixhoven (Leiden) of computing coefficients of modular forms. See **A.1.1** and **A.1.2** for further description.

[5] W.-D. Geyer, Moshe Jarden, Torsion of Abelian varieties over large algebraic fields, to appear in *Finite Field Theory and its Applications*.

*Comments:* This article contains the following major contribution to a conjecture made by the authors in 1979.

**Theorem:** Let  $A$  be an abelian variety over a number field  $K$ . Then there exists a finite Galois extension  $L$  of  $K$  such that for almost all  $\sigma \in \text{Gal}(\bar{L}/L)$ , there are infinitely many prime numbers  $l$  such that the group  $A_l(\bar{L}(\sigma))$  has a point of order  $l$ , where  $\bar{L}(\sigma)$  denotes the fixed field of  $\sigma$ .

The above-mentioned conjecture predicts that one may take  $L = K$  in the Theorem. This is actually achieved in some cases, for example when  $A$  is an elliptic curve or  $\text{End}(A) = \mathbb{Z}$  and  $\dim(A)$  is 2, 6, or an odd number. The proof uses published and unpublished results of J.-P. Serre on representations of  $\text{Gal}(K)$  acting on  $A_l(\bar{K})$ .

## Part B: Comparison with the Project Programme

### B.1: RESEARCH OBJECTIVES

The research objectives of the network remained as stated in the contract. Progress was made on many of the objectives originally stated (see part **A**).

- *The differential inverse Galois problem* has been completely solved, thanks to inter-team network collaboration (Matzat-van der Put) in the characteristic  $p$  case and subsequent work by young researcher Julia Hartmann (Heidelberg) in the characteristic zero case.
- A new theme developed within the context of the original research objectives: *comparison between the Lie algebras associated to  $G_{\mathbb{Q}}$  (Deligne-Ihara algebra), to  $GT$  and the new zeta space* (see part A, paragraph 4). This has led to a new domain of application of effective methods to Galois theory.

### B.2: RESEARCH METHOD

The research method remains as described in the contract. A summary:

There are eight specific tasks and a “miscellaneous” task (9). The list is given in the next section **B.3**. The table showing which teams were involved in which tasks is as follows. Each team made significant discoveries during the network duration (see part **A**).

Team	Task	1	2	3	4	5	6	7	8	9
Paris		•		•	•	•		•	•	•
Barcelona		•				•		•	•	•
Bonn			•	•	•	•			•	•
Bordeaux		•				•	•	•	•	•
Essen			•			•				•
Heidelberg		•	•				•	•	•	•
Leiden						•	•	•		•
Lille			•					•	•	•
Nottingham						•	•			•
Besançon			•	•	•	•				•
Rome						•	•			•
Tel Aviv		•	•						•	•
Lausanne				•						•

### B.3: WORK PLAN

In this section we recall the original work plan of the network, with its division into tasks and milestones. This work plan is referred to in the descriptions of scientific highlights in part **A** of this report. The division of tasks and milestones was finalized after the Midterm Review Meeting and has not changed since then.

Task 1: Explicit realisation of new finite groups as Galois groups

Milestone: Explicit realisation of new Galois groups

Task 2: Inverse Galois Theory

Milestone: Shafarevitch conjecture on the structure of  $G_Q$

Task 3: Geometric Galois Actions (dessins d'enfants etc.)

Milestone: Determination of Galois invariants of dessins d'enfants

Task 4: Comparison of  $G_Q$  and  $GT$  and their Lie algebra versions

Milestone: Explicit comparison features of  $G_Q$  and  $GT$  or their Lie algebra versions

Task 5: Elliptic curves and curves of higher genus: arithmetic and explicit computation

Milestones: Galois representations arising from the action on the torsion points of abelian varieties: how to distinguish and compute these,

Task 6: Fast algorithms in class field theory

Milestone: Improving methods for decomposing integers into two primes

Task 7: Differential Galois groups in positive characteristic, differential inverse Galois problem

Milestones: Effective computation of differential Galois groups for families of equations,  
Determination of the finite quotients of fundamental groups of curves  
Differential inverse Galois problem

Task 8: Arithmetic of covers and fundamental groups

Milestones: Finding rational points or rational subvarieties on moduli spaces,  
Describing the stable reduction of curves and of covers  
Oort's conjecture on lifting cyclic covers from char.  $p$  to char.  $0$

Task 9: Miscellaneous topics

#### *Assessment for the final report*

The work plan **B.3** and the involvement of teams **B.2** remained essentially the same throughout the network. Major scientific accomplishments of the network were carried out in the tasks 2, 3, 4 and 7, steady progress was made in task 8 and certain excellent results were discovered which do not belong to the above specific categories, so belong to task 9. The explicit description of five main results is given in **A.1.2**, with the references given in **A.2.2**.

## **B.4: ORGANISATION AND MANAGEMENT**

### **B.4.1. Organisation**

The overall organisation and management of the network was handled by the main coordinator. All information concerning the network was kept fully up to date on the GTEM web page

<http://www.math.jussieu.fr/~leila/gtem/gtem.html>.

Frequent messages concerning the entire network were forward to all team leaders, to be disseminated among their team members. Active discussions were thus able to be held among all participants, for instance on the subject of the possible continuation of what was felt to be a very positive and fruitful network.

The following organisational tasks were delegated to specific people:

- (i) to the main coordinator: upkeep of the web page, and in particular a page concerning all upcoming conferences thematically relevant to the network. In this way, many requests were made by network members to attend conferences outside the network and even outside the EU.
- (ii) to team leaders: collection of financial information for annual reports, details of hiring postdocs on their team, dissemination of information about the network within their university;
- (iii) to task/project leaders: collection of information on the progress on the various research themes of the network and exchanges and collaborations;
- (iv) to certain members of the network: organisation of network conferences.
- (v) to the Leiden team: creation and upkeep of the network's preprint server.

Members and young researchers who published papers and attended conferences invariably cited the Network as their source of support. Some members attended international non-network conferences (with prior permission from the Commission). The most important of these (most relevant to network themes) are listed here:

**Algorithmic Number Theory Symposium (ANTS-V)**, Sydney, Australia, July 7-12, 2002

**Arithmetic of Fundamental Groups**, BIRS-Banff, Canada, September 6-20, 2003

**Algorithmic Number Theory Symposium (ANTS-VI)**, University of Vermont, Vermont, USA, June 13-19, 2004

**Arithmetic Geometry**, St. Petersburg, Russia, June 20-26, 2004

### B.4.2. Network meetings

We list here all the large-scale conferences and workshops organised by GTEM, attended by members of all network teams and also outside participants and invited external experts.

*Théorie de Galois et géométrie*

CIRM-Luminy, France, June 4-8 2001

Organisers: Pierre Dèbes, Florian Pop

External experts: Abhyankar, Chinburg, Harbater, Ihara, Tamagawa...

*Explicit methods in Galois theory and arithmetic (plus Midterm Evaluation Conference)*

Lorentz Center, Netherlands, June 10-14, 2002

Organisers: Bart de Smit, Martine Girard

External Experts: Alan Lauder (Oxford), Noriko Yui (Cambridge)

This conference doubled as the mid-term evaluation conference and a full-fledged mathematical network conference with all teams represented.

*Noncommutative aspects of arithmetic algebraic geometry*

Durham, England, August 28-September 5, 2002

Organisers: Ivan Fesenko, Martin Taylor, Michael Spiess

External Experts: J. Ellenberg (Princeton), Hidekazu Furusho (Kyoto), D. Whitehouse (Pasadena), C. Soulé (IHES), J. Koenigsmann (Basel)...

This was a large conference uniting two networks and many outside participants, aiming at a maximal dissemination of network themes and results.

*Differential and general Galois theory*

CIRM-Luminy, March 8-13, 2004

Organisers: Daniel Bertrand, Pierre Dèbes, B.H. Matzat

External Experts: Alexandru Buium (New Mexico), Michael Fried (Irvine), David Harbater (U Penn), Andy Magid (U Oklahoma)

*Iwasawa 2004: Théorie de Galois et méthodes effectives en Arithmétique*

Besançon, France, July 5-9, 2004

Organisers: J-R. Belliard, T. Nguyen Quang Do, H. Oukhaba, Michel Vérant

External experts: K. Rubin (Stanford), A. Huber (Leipzig)

*From Arithmetic to Cryptology (Frey Birthday Celebration)*

Essen, Germany, July 8-10, 2004

Organiser: Claus Diem

External Experts: Nigel Boston (Wisconsin), Kumar Murty (Toronto), Alexey Nesterenko (Moscow), Ki-Seng Tan (Taiwan), Alev Topuzoglu (Istanbul)

### B.4.3. Networking

**List of GTEM-organised learning workshops, schools and conferences.** These meetings, specifically aimed at young researchers, have been organised by individual or associated teams of the network.

Ecole en théorie algébrique des nombres et géométrie arithmétique (TANGA), Lille, March 26-30, 2001

Organisers: Bordeaux-Lille-Valenciennes

Galois Theory and Fundamental Groups Workshop Bonn, Germany, May 25-June 2, 2001

Organiser: Florian Pop

Arbeitsgemeinschaft Bonn Bonn, Germany, June 24-28, 2002

Organiser: Bonn team

Explicit methods in number theory Leiden, Netherlands, September 13-October 2, 2002

Organiser: H.W. Lenstra, P. Stevenhagen

Explicit algebraic number theory Oberwolfach, Germany, November 10-16, 2002

Organiser: H.W. Lenstra, P. Stevenhagen

GTEM Seminar in Lille Lille, France, 2002-2003

Organiser: Lille team

Explicit Methods in Number Theory Oberwolfach, Germany, July 20-26, 2003

Organiser: H. Cohen, H.W. Lenstra, D. Zagier

Differential Galois Theory (in planning) Heidelberg, Germany, spring 2003

Organiser: B.H. Matzat

**Inter-team visits leading to active collaborations** (see diagram below).

Heidelberg-Paris: collaboration on differential Galois theory.

Bonn-Paris: collaboration on moduli spaces and multizeta values.

Barcelona-Rome: collaboration on elliptic curves.

Barcelona-Heidelberg-Paris: collaboration on 3-dimensional Galois representations.

Bordeaux-Heidelberg: collaboration on field discriminants.

Heidelberg-Tel Aviv: collaboration on differential Galois groups.

Heidelberg-Leiden: collaboration on differential inverse Galois problem.

Lille-Tel Aviv: collaboration on the regular inverse Galois problem over “small” fields.

Nottingham-Bordeaux-Essen: collaboration on 3-descent.

Nottingham-Barcelona: collaboration on elliptic curves.

The inter-team collaborations and the exchange of postdocs between countries are represented in the two diagrams below.

Diagram 1: Collaborations between the teams

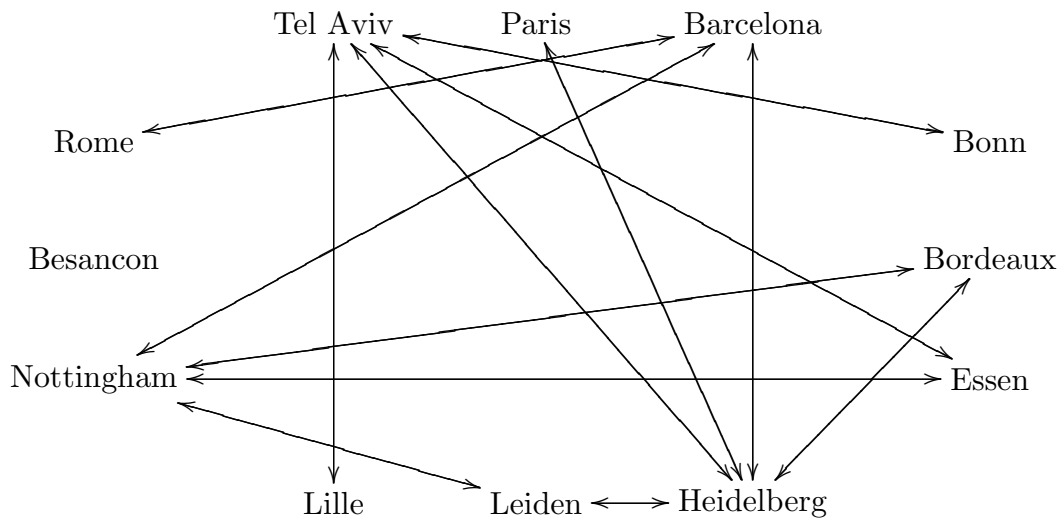
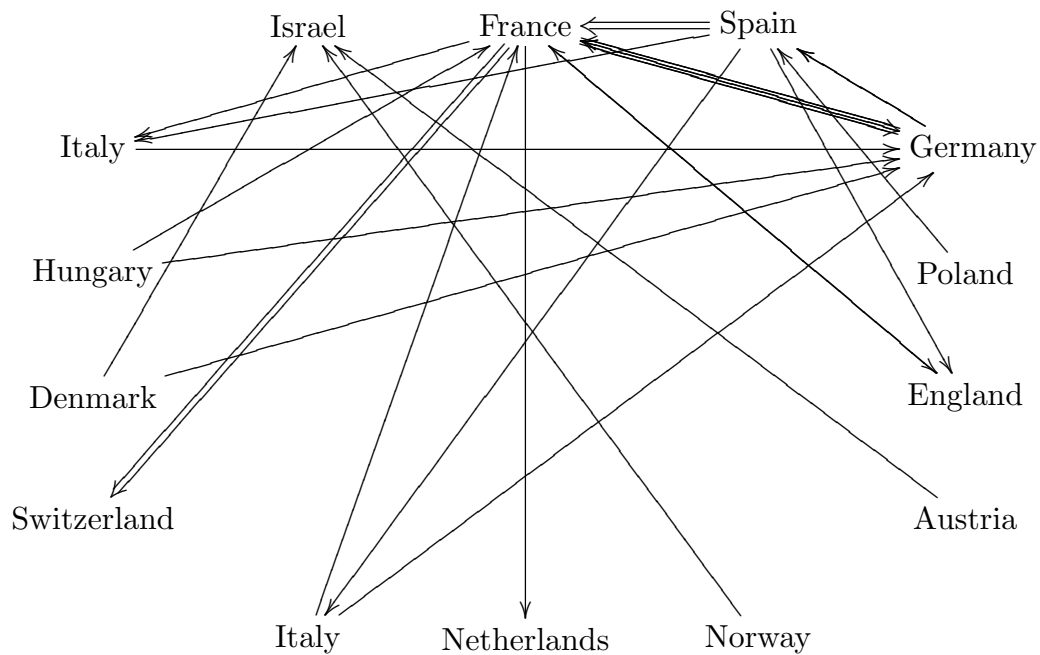


Diagram 2: Hiring of young researchers



*Assessment for the final report:* The above information and diagrams give sufficient commentary as to the usefulness and plenitude of international networking, both from conferences and visits. The network enabled researchers and above all young researchers to greatly multiply their international contacts, and there was strong benefit to research. The value and advantage for nearly 50 young researchers in terms of help, learning, good research conditions and further job searching was incalculable. It would be an excellent thing if such contacts could be multiplied on the international level throughout the world and not just within the European community.

## B.5: TRAINING

### B.5.1. Appointing young researchers

Vacancies were published on the GTEM web site and the EC networks site. These methods attracted a few applications. But the majority of applications came from contacts between team members and various young researchers who already belonged to network teams, or who were encountered during visits and conferences to other universities.

The following tables show how much each of the twelve EC financed teams spent on personnel/training.

**Table 1: Overall Network Spending**

Team	Budget	Spent	Personnel	Networking	Overheads
1	145000	132473	100641	9733	22099
2	100000	100723	59498	24439	16786
3	100000	101303	63093	20947	17263
4	150000	156232	99570	30624	26038
5	125000	118301	72778	27718	17805
6	125000	116457	80392	15142	15779
7	140000	132498	86069	24037	22392
8	125000	129074	86673	21687	20714
9	120000	102224	62108	23105	17011
10	145000	139919	90251	33778	15890
11	100000	91022	48691	27363	14986
12	125000	120269	71098	29126	20045
Totals:	1500000	1440495	920862	287699	231934

**Table 2: Network spending as percentages**

Team	Personnel	Networking	Overheads
1	76%	7%	17%
2	59%	24%	17%
3	62%	21%	17%
4	64%	20%	16%
5	62%	23%	15%
6	69%	13%	18%
7	65%	18%	17%
8	67%	17%	16%
9	61%	22%	17%
10	65%	24%	11%
11	53%	30%	17%
12	59%	24%	17%
Totals:	64%	20%	16%

### B.5.2. Recruitment of young researchers

The following table shows the hiring progress of the four years of the network as a whole. The twelve EC-financed teams are listed first, then the Swiss team as an extra line.

The three first columns of the table represent the total person-months to be delivered by the network according to the contract. The next three columns represent the actual person-months delivered by the end of the contract.

**Table 1: Young Researcher Months**

Team	Contract deliverable			Actually hired		
	Pre-doc	Postdoc	Total	Pre-doc	Postdoc	Total
1	0	24	24	2	26	28
2	2	16	18	1	19	20
3	2	12	14	9	21	30
4	4	21	25	0	28	28
5	6	12	18	6	21	27
6	4	14	18	11	27	38
7	3	17	20	2	25	27
8	4	20	24	0	24	24
9	4	20	24	0	22	22
10	0	24	24	15	13	28
11	0	18	18	0	21	21
12	4	16	20	11	22	33
EC funded:	33	214	247	57	269	326
13	0	20	20	2	18	20
Totals:	33	224	267	59	287	346

*Assessment for the final report:* The network as a whole provided a total of 346 young researcher months, 326 financed by the EC, as opposed to the 247 originally undertaken in the contract.

Thus, the network was able to provide many more young researcher months than stipulated in the original contract. There are two reasons for this. One is that certain teams spent most of their budget on young researchers, and the other is that certain teams were able to pay a lower salary than that recommended by the Commission, either because the salary was paid as a stipend, thereby reducing government charges, or because it was comparable to the university's practice with other postdocs. The total number of young researcher months shown above were divided among a total of **49** young researchers.

The training aspect of the network was highly successful, with several pre-docs obtaining their Ph.D.'s, and postdocs spending time in multiple teams, going to conferences, publishing articles, and often obtaining good positions after their postdoc period.

### **B.5.3. Integration into the network programme**

Young researchers furthered their research training by working with team members, participating in seminars and attending conferences. They were exceptionally fertile, producing dozens of publications during the four-years duration of the network, mostly alone, occasionally together with network members and (rarely) together with collaborators from outside the network. All publications of network members were freely available from the network's archive. All of the pre-doctoral students made significant progress on their theses; at least two of them finished their theses during their network stay.

See section **A.1.** for the list of publications signed by postdocs of the network.

### **B.5.4. Training through conferences and meetings**

Every young researcher was sent to at least one international conference in his subject, if not more. All were encouraged to present their work in this context. Furthermore, young researchers were regularly invited to lecture on their research within their team, in seminars and local colloquia. A long list of full-fledged network conferences and subsidiary workshops was organised with the strong participation of young researchers. They were also sent to network-linked conferences, i.e. conferences organised outside of the network but attended by a significant number of network participants, as well as occasionally to international conferences outside of the EU. *See section B.4.2 for the full list of conferences and workshops.*

### **B.5.5. Equal opportunities**

The network succeeded in attracting 6 women young researchers out of the total of 49, a total of 12% which is very reasonable compared with the percentage of women graduate students in math.

### **B.5.6. Multidisciplinarity**

The very nature of the network is multidisciplinary in that there are teams which specialise in computational work (Bordeaux, Leiden, Heidelberg, Nottingham), teams which specialise in theoretical work (Bonn, Besançon, Lille, Tel Aviv) and several teams which

combine these two aspects (Paris, Barcelona, Essen, Rome). The multidisciplinary aspect of the training within this network was particularly enhanced by the fact that at least one quarter of the young researchers spent time in more than one team.

### **B.5.7. Connections to industry**

Only one young researcher from the network asserted that his training provided him with skills relevant to industry. This was a postdoc interested in cryptography, who met with cryptography experts (not members of GTEM) during his postdoc stay in Tel Aviv. Cryptography would be a useful and relevant addition to the network themes in the event of a renewal.

*Assessment for the final report:* The training programme went well beyond what was initially planned for the network, providing a total of 346 young-researcher months instead of the originally planned 247. The planned balance of pre- and postdocs was essentially respected, with advantage to postdocs, although there were some exceptional and beneficial events such as pre-docs passing their doctoral theses while in the network, and thus changing status. Every single young researcher and all of their employers expressed great satisfaction with the postdoctoral programme. The best aspect was that the research experience gained by young researchers during their postdoc positions led in numerous cases to further appointments either as postdocs or as permanent members of a department.

The only difficulty with recruitment was the late start, which meant that a few teams were unable to recruit as much as they would have been able to financially (although all teams fulfilled their contract deliverables). There is no real difficulty with recruiting postdocs, because of the large number of young European Ph.D.'s without permanent positions, but it must be taken care of sufficiently in advance.

## **B.6: DIFFICULTIES**

There were very few difficulties with the network, except that it was quite large and therefore it tended to be difficult to gather all the paperwork for all the different teams. Recruitment of postdocs by certain teams began rather late. Reimbursements and financial statements also tended to be late, however all went smoothly in the end. EC personnel were extremely helpful at all times.

### **Part C: Young Researcher Reports for the fourth reporting period**

We include the young researcher reports of the following young researchers. Most are from the fourth year of GTEM, but a few come from earlier young researchers who had not previously filled out a report. (Most young researchers did not choose to enclose their report in a sealed envelope, although they were invited to do so.)

Fabrizio Andreatta (*Italian, postdoc in Bonn*)

Marco Boggi (*Italian, postdoc in Paris*)

David Brink (*Danish, predoc in Essen and Tel Aviv*)

Michael Dettweiler (*German, predoc in Tel Aviv*)

Stéphane Flon (*French, postdoc in Bonn and Essen*)

Alexander Gurevich (*Russian but resident in Germany, postdoc in Beer Sheva (part of Tel Aviv node)*)

Razvan Litcanu (*Romanian, postdoc in Lille, Barcelona and Bonn*)

Christophe Ritzenthaler (*French, postdoc in Essen and Leiden*), 2 separate reports

Matthieu Romagny (*French, postdoc in Bonn*)

Alexander Stasinski (*Swedish, postdoc in Bonn*)

Jakob Stix (*German, postdoc in Nottingham and Tel Aviv*)

Tamàs Szamuely (*Hungarian, postdoc in Besancon and Bonn*)

Xavier Taixés i Ventosa (*Spanish, predoc in Essen*)

Ilia Toli (*Albanian but resident in Italy, postdoc in Tel Aviv*)