CONTRIBUTIONS to SCIENCE, **1** (2): 125-145 (1999)
Institut d'Estudis Catalans, Barcelona

Arithmetical problems in number fields, abelian varieties and modular forms*

P. Bayer et al.**

Abstract

Number theory, a fascinating area in mathematics and one of the oldest, has experienced spectacular progress in recent years. The development of a deep theoretical background and the implementation of algorithms have led to new and interesting interrelations with mathematics in general which have paved the way for the emergence of major theorems in the area.

This report summarizes the contribution to number theory made by the members of the *Seminari de Teoria de Nombres (UB-UAB-UPC)* in Barcelona. These results are presented in connection with the state of certain arithmetical problems, and so this monograph seeks to provide readers with a glimpse of some specific lines of current mathematical research.

Key words: Number field, L-function, Galois group, quadratic form, modular form, modular curve, elliptic curve, Galois representation, abelian variety, Fermat curve, arithmetic variety, scheme, cycle, motive.

Resum

La teoria de nombres, una àrea de la matemàtica fascinant i de les més antigues, ha experimentat un progrés espectacular durant els darrers anys. El desenvolupament d'una base teòrica profunda i la implementació d'algoritmes han conduït a noves interrelacions matemàtiques interessants que han fet palesos teoremes importants en aquesta àrea.

Aquest informe resumeix les contribucions a la teoria de nombres dutes a terme per les persones del *Seminari de Teoria de Nombres (UB-UAB-UPC)* de Barcelona. Els seus resultats són citats en connexió amb l'estat actual d'alguns problemes aritmètics, de manera que aquesta monografia cerca proporcionar al públic lector una ullada sobre algunes línies específiques de la recerca matemàtica actual.

Number theory, or arithmetic, is a fascinating area in mathematics, and one of the oldest. It has changed dramatically since the 17th century, when Fermat was essentially working in isolation in his careful study of Diophantus' *Arithmetica* or, needless to say, since the Babylonian period when an arithmetician sculpted a stone tablet containing fifteen «pythagorean» triangles [Plimpton 322, ca. 1800 B.C.]. Diophantus' *Arithmetica* [ca. III A.C.] and Gauss' *Disquisitiones Arithmeticae* [1801] are milestones of the past which never became as popular as Euclid's *Elementa* [ca. IV-III B.C.] or Newton's *Principia* [1686]. Nevertheless, from a set of arithmetical problems proposed by Diophantus, Fermat, and Gauss a mathematical treasure emerged: number theory as it is understood today.

Number theory covers a wide range of subjects: integer numbers, diophantine equations, number fields, arithmetical aspects of algebraic varieties, arithmetical functions, zeta and *L*-functions, automorphic forms, and much more besides. A detailed outline of its advances is beyond the scope of this article; suffice it to say that the progress made in the arithmetic of elliptic curves, modular curves and modular forms, combined with specific methods developed by G. Frey, B. Mazur, K. Ribet, and J-P. Serre, among others, made possible the momentous study of A. Wiles [1995] on Fermat's Last Theorem.

In Barcelona, in the mid-1970s, an appreciation at the inherent beauty of arithmetic began to emerge; since then, an increasing number of mathematicians have shared the plea-

*Dedicated to Albert, Carles, Carlos and Enrique, Elisabet, Pau and Mireia, Gabriel, Maria del Mar, Carolina, Javier, Maria dels Àngels, Antoni, Josep Maria and Joaquim, Marcel·lí, Enric, Judit, Sara, and Mireia.

**Autor for correspondence: Pilar Bayer, Departament d'Àlgebra i Geometria. Universitat de Barcelona. Gran Via de les Corts Catalanes, 585. 08007 Barcelona, Catalonia (Spain). Tel. 34 93 402 16 16. Email: bayer@cerber.mat.ub.es

sure and pain of its unsolved problems, achievements, and methods, drawing on tools from many different fields in mathematics. The *Seminari de Teoria de Nombres (UB-UAB-UPC)* began as an independent research group in 1986 and has organized activities every year since. Henceforth, for brevity's sake, we will refer to this group as STNB.

Research group

The STNB is made up of scientific personnel from three universities: Universitat de Barcelona (UB), Universitat Autònoma de Barcelona (UAB), and Universitat Politècnica de Catalunya (UPC). They are listed below.

UB-team: A. Arenas, P. Bayer, T. Crespo, J. Guàrdia, G. Pascual, A. Travesa, M. Vela, N. Vila; UAB-team: F. Bars, S. Comalada, J. Montes, E. Nart, X. Xarles; UPC-team: M. Alsina, G. Cardona, J. Gonzàlez, J.-C. Lario, J. Quer, A. Rio; as well as several graduate students writing their Ph. D. theses under the direction of one of the doctors in the group.

Research area

Classification codes will be given according to the Mathematics Subject Classification, 1991 revision.

The research interests of the STNB lie mainly in: algebraic number theory (11R, 11S), field extensions (12F), quadratic forms (11E), automorphic forms (11F), diophantine geometry (11G, 14G), and computational number theory (11Y).

All aspects included in these interests are closely interrelated, and so those primarily engaged in one are inevitably involved in the others. In addition, most of the researchers of the STNB have worked together for a number of years on joint projects supported by the DGICYT or the European Union.

Research method

The activities of the STNB can be divided into two broad groups: research and training. Research activities are normally conducted via individual studies, interaction with colleagues, and the exchange of scientific ideas with other specialists. Training activities, for their part, tend to take the form of lectures and since 1986 have been organized into 60-hour blocks of lectures per year. The STNB lectures are open to all faculty members and graduate students, and serve to disseminate some of the major findings in current research. The subject matter of the lectures is decided on by the STNB each academic year. To date, the following subjects have been addressed:

Rational points on algebraic curves (1986-87); Serre's conjecture on modular Galois representations (1987-88); Modular curves and the Eisenstein ideal (1988-89); Galois structures of Hodge-Tate type (1989-90); Algorithms in modular curves (1990-91); Arithmetic surfaces (1991-92); Galois representations of dimension 2 (1992-93); Chow motives (1992-93); Preliminaries to Fermat-Wiles theorem (1993-94); Modular forms and Galois groups (1994-95); Torsion points of elliptic curves (1994-95); Modular elliptic curves (1995-96); Automorphic representations of GL(2) (1996-97); Embedding problems over large fields (1998-99); Birch and Swinnerton-Dyer conjecture (1998-99); Abelian varieties with complex muliplication (1999-00); Introduction to crystalline cohomology (1999-00).

Among the universities or research institutes where members of the STNB have spent substantial periods of time are: Berkeley, Bonn, Essen, Freiburg, Harvard, Kraków, La Habana, Luminy, Mar del Plata, McGill, Oberwolfach, Princeton, Regensburg, Santander, Tokyo-Chuo, and Tokyo-Waseda.

The *Journées Arithmétiques* are an international meeting with a long tradition. They take place every two years, held alternately in France and in other countries in Europe, and are recognized as the most important meeting devoted to number theory. The STNB organized the 19*èmes Journées Arithmétiques*, with the support of the Generalitat de Catalunya, the Ministerio de Educación y Ciencia, and other official institutions, in the summer of 1995. From July 16 to 20, over 300 participants engaged in a forum for the presentation and discussion of recent number-theoretical developments against a Mediterranean backdrop; cf. [e7: Ba-Cr 97].

This article is organized as follows: in the following pages we present an up-to-date overview of the main contributions made by members of the STNB. This is divided in short sections which include many references to pioneering studies. A list of research publications is enclosed. In the main these are quoted in the text, though additional references precede the main list. They include: textbooks, monographs, survey articles, software packages and, in general, publications supporting research and providing necessary background. References are numbered in inverse chronological order, and so the lowest numbers correspond to the most recent items. Further details are available on request.

Co-authors of this report

A. Arenas, T. Crespo, J. Guàrdia, J.-C. Lario, E. Nart, J. Quer, A. Rio, A. Travesa, N. Vila, X. Xarles.

1. Algebraic number theory: global and local fields (11R, 11S)

The arithmetical analysis of algebraic equations consists in solving the equations taking into account the minimum field or ring to which solutions belong. Solutions lie in extensions of finite degree of the field containing the coefficients of the equations. Assuming this ground field to be the field $\mathbb{Q}$ of the rational numbers leads us to the study of their finite extensions, which are called number fields.

The ring of integers O_K of a number field K is a subring which is able to support, at the level of ideals, arithmetical properties analogous to those of the ring of integers $\mathbb{Z}$. These arithmetical properties are essential for the arithmetical analysis of equations.

Among the fundamental challenges concerning the arithmetical structure of these rings or fields we find:

(1) determining how the rational primes decompose as products of prime ideals in O_K; (2) computing the discrimi-

nant –an invariant taking into account the ramified primes; (3) computing an integral basis –a basis of O_K as a free $\mathbb{Z}$-module; (4) determining generators of the group of units of O_K; (5) computing the ideal class group H of O_K –ideals modulo principal ideals– or, at least, computing its order h, called the class number of K.

After the pioneering work of K. Hensel at the end of the last century, centring attention on the arithmetical properties concerning one single prime p is well reflected by the process of completion of number fields with respect to p-adic topologies. In this way one obtains the so-called p-adic fields, which possess a simpler arithmetical structure (stronger properties), allowing a much more rigorous analysis. Iwasawa theory of $\mathbb{Z}_p$-extensions is a masterpiece among the many developments stressing the power of the p-adic techniques.

Among the main tools for the study of the arithmetical properties of number fields are zeta functions and L-functions. These analytical objects play an essential role in the complex process of gathering global information from the local data given by p-adic analysis of equations at different primes p. The Riemann zeta function is the simplest example of a zeta function. It originated in a proof of L. Euler [1737] of the infinitude of rational primes; cf. for instance [c11: Ba 84]. Let us mention, by way of illustration, that a close control of the zeros of the Riemann zeta function –the Riemann hypothesis– furnishes valuable information about the distribution of rational primes among the integers.

1.1. Quadratic extensions and cubic extensions

Let K be a quadratic number field and H its ideal class group. Given a prime p, let $\mathbb{F}_p$ denote the field of p elements. The p-rank of K is, by definition, the dimension of the $\mathbb{F}_p$-vector space H/H^p. If K is imaginary with discriminant $-d$, let us denote by r the 3-rank of K, and by s the 3-rank of the real quadratic field with discriminant $d' = 3d/(3,d)^2$ associated to K. A theorem of A. Scholz [1932] established the inequalities $s'' \le r'' \le s+1$.

In collaboration with F. Díaz y Díaz, P. Llorente and Quer [50: Di-Llo-Qu 88] obtained a criterion for the equality $r = s$ in terms of the existence of cubic fields with a certain prescribed discriminant. They applied this criterion to the 1824 imaginary quadratic fields with $r = 4$ computed in [52: Llo-Qu 88-1], [b11: Qu 87], and found exactly 17 cases in which $r = s = 4$.

P. Llorente and Quer [51: Llo-Qu 88-2] also developed a refined method to obtain all totally real cubic fields with discriminant $D < 10^7$. They considered the fields $K(a, b)$ generated by irreducible polynomials $f(a,b,X) = X^3 - aX + b$, where a and b are positive integers. The discriminant D of the field is a divisor of the discriminant $D(a, b)$ of $f(a, b, X)$. Namely, $D(a, b) = 4a^3 - 27b^2 = Ds^2$. A quadratic form $F(a, b)$ is associated with the pair (a, b); it represents exactly those integers a' for which there exists an integer b' such that the two fields $K(a, b)$ and $K(a', b')$ are isomorphic. By applying Gauss' theory of reduction of quadratic forms (cf. section 2), a bound for s as a function of a was obtained.

As a consequence, a table of all totally real non-cyclic cubic fields as above could be constructed from a finite number of pairs (a, b), by carrying out the following steps:

(i) eliminating the reducible polynomials f; (ii) computing D from $D(a, b)$ by use of the bound on s; (iii) eliminating isomorphic fields by studying the associated quadratic form. P. Llorente and Quer used their table to obtain the empirical value of the density of each type of decomposition of a rational prime in cubic fields. They compared this value to the asymptotic value of this density which had been given by H. Davenport and H. Heilbronn [1971].

Previously, P. Llorente and Nart [64: Llo-Na 83] had found explicit effective conditions to determine the prime ideal decomposition of a rational prime in a cubic field in terms of a defining equation of the field. These explicit conditions were also used to find an explicit computation of the discriminant and the index of the cubic field (cf. 1.2).

1.2. Ramification and extension theory

P. Llorente, Nart, and Vila contributed to the analysis of arithmetical properties of number fields in terms of a specific defining equation. The articles [33: Llo-Na-Vi 91], [63: Llo-Na-Vi 84] are mainly devoted to obtaining an explicit computation of the discriminant and the prime ideal decomposition of the rational primes when the number field defining equation is a trinomial. An old method developed by O. Öre [1928], based on Newton polygon techniques, was one of the ingredients. This method was refined by Montes and Nart [27: Mo-Na 92] and has been developed further by Montes, who invented higher polygons and designed a new algorithm to compute prime ideal decomposition in terms of an arbitrary defining equation. This algorithm has been implemented by Guàrdia (cf. 9.3), and has proved to be much more efficient and faster than other known algorithms.

Nart [60: Na 85], [b14: Na 82] studied an invariant $i(K)$ of a number field K, called its index. This invariant is defined as the gcd of all indices $i(\theta)$ of algebraic integer generators θ of K over $\mathbb{Q}$. An explicit formula for $i(K)$ in terms of certain local invariants was found; for each prime p, the highest power of p dividing $i(K)$ depends on the family $(K_P)_{P|p}$ of P-adic completions of K at the primes P dividing p. If $K|\mathbb{Q}$ is a Galois extension, all these p-adic fields are isomorphic, and Nart conjectured that $i(K)$ should depend in this case only on the higher ramification numbers of K_P. This conjecture is still open and deserves the attention of specialists.

Given a finite non-empty set S of rational primes, a family $(e_p)_{p\in S}$, of positive integers, and a fixed integer n, Travesa [41: Tr 90-1], [b10: Tr 88] found a formula for the number of abelian extensions of $\mathbb{Q}$ of degree n which are unramified outside S and have ramification index e_p at each $p \in S$. The formula is based on the author's algorithm for finding all these fields.

In the local case, Travesa [40: Tr 90-2], [b10: Tr 88] found explicit formulae for the number of abelian extensions of a p-adic field, with prescribed ramification. Moreover, the generating function of these numbers was computed in terms of the zeta function of a Grassmannian variety, and showed

that this function can be extended meromorphically to the entire plane.

In many arithmetical problems, local computations at $p = 2$ are rather involved and require special treatment, as we will shortly see.

Let us consider the group $\tilde{S}_4$, the double cover of the symmetric group S_4 in which transpositions lift to involutions; it has as a matrix model the general linear group $GL(2, \mathbb{F}_3)$. Galois extensions of S_4-type provide some of the first examples of solvable non-abelian extensions. They are suitable for testing conjectures and play a crucial role in the proof of some recent theorems (cf. 5.3, 8.1, 8.2).

A. Weil [1974] determined eight Galois extensions of the field $\mathbb{Q}_2$, of the 2-adic numbers, whose Galois group is isomorphic to $\tilde{S}_4$. The number of Galois extensions of $\mathbb{Q}_2$ whose Galois group is a non-trivial subgroup of $\tilde{S}_4$ totals 130. Bayer and Rio [1: Ba-Ri 98], [b3: Ri 96] have determined all these extensions. Most of them have been obtained through the resolution of successive local Galois embedding problems (cf. 3.3). In each case, an irreducible equation and the discriminant of the field have been given.

The above articles have been referred to in [G. Cornell; J. H. Silverman; G. Stevens, 1997], [S. D. C. Cohen; A. Movahhedi; A. Salinier, 1997], [L. C. Washington, 1997], [A. Movahhedi; A. Salinier, 1996], [H. Cohen, 1993; 1995], [W. Narkiewicz, 1990], [H. Osada, 1987], and [K. S. Williams, 1986].

1.3. Iwasawa theory and zeta functions

A prime p is called regular if it does not divide the class number of the cyclotomic field of the p-roots of unity; otherwise it is called irregular. E. Kummer [1847], in a strenuous *tour de force*, discovered a proof of Fermat's Last Theorem (FLT) for regular prime exponents; cf. [c13: Ba 76]. Kummer's work on the arithmetic of cyclotomic fields was taken up again by K. Iwasawa and H. W. Leopoldt in the 1960s, when they investigated the arithmetic of towers of cyclotomic fields.

Given a prime p, let $p^{e(n)}$ denote the highest power of p dividing the class number of the p^n-th cyclotomic field, obtained by adjoining to $\mathbb{Q}$ all p^{n+1}-roots of unity. After [K. Iwasawa, 1964] and [B. Ferrero; L. C. Washington, 1979], we know of the existence of constants λ, ν, independent of n, such that $e(n) = \lambda n + \nu$.

There are two sorts of p-adic L-functions attached to a totally real number field: those constructed in the abelian case in [T. Kubota; H. W. Leopoldt, 1964] and those arising from Iwasawa modules [K. Iwasawa, 1964]. Kubota-Leopoldt p-adic L-functions are of an analytical nature, since they interpolate special values of Dedekind zeta functions. Iwasawa L-functions are arithmetically defined, since they take Galois actions into account. The main conjecture of Iwasawa theory asserts that both functions have the same singularities.

A prime p is regular if and only if $\lambda = \nu = 0$. A pair (p, m) is said to be irregular if p divides the numerator of the Bernoulli number B_{2m}. The index of irregularity, δ, of a prime p is defined as the number of irregular pairs (p, m) for $1 \leq m \leq (p-3)/2$. By a criterion of E. Kummer, a prime p is irregular if and only if $\delta \uparrow 0$. Numerical evidence suggests the equality $\lambda = \delta$. T. Metsänkylä [1975] found a criterion for the fulfilment of this equality in terms of congruences of Bernoulli numbers and Bayer [f7: Ba 79] reobtained this criterion as a consequence of some explicit formulae for p-adic L-functions of Kubota-Leopoldt type.

The values of the zeta function $\zeta_K(s)$ of a totally real number field K at the negative integers $s = -n$ are, by a theorem of Siegel [1969], rational numbers; they are zero if and only if n is even. S. Lichtenbaum [1972] conjectured that the p-adic absolute values $|\zeta_K(-n)|_p$ might be expressed as étale Euler characteristics of the scheme $\chi = \mathrm{Spec}\, O_K[1/p]$, for every odd integer n and $p \uparrow 2$.

Bayer and Neukirch [68: Ba-Ne 78] developed a theory in which Lichtenbaum's conjecture is a natural consequence of the main conjecture of Iwasawa theory. First of all, they proved a formula, analogous to Lichtenbaum's formula, for the zeta function of an algebraic scheme over a finite field, inspired in A. Grothendieck's cohomological interpretation of the zeta function in terms of characteristic polynomials of the Frobenius. Then, in the number field case, they introduced the so-called Iwasawa L-functions as characteristic polynomials of certain Galois actions in the theory of $\mathbb{Z}_p$-extensions and which are –according to the main conjecture– related to p-adic L-functions. For these p-adic Iwasawa L-functions they proved Lichtenbaum's formula in much the same way as they did for schemes over finite fields.

Assume that K is a real abelian number field. Bayer [67: Ba 79] compared the value at $s = 1$ of the above mentioned Iwasawa L-functions with the Kubota-Leopoldt p-adic L-functions, independently of any conjecture. The quotients of the respective p-adic absolute values, which conjecturally are equal to one, were expressed as quantities h_ϕ/m_ϕ, where numerator and denominator come from a p-adic decomposition of the class group and the group of units of K, respectively, which takes into account their Galois structure. In some cases, essentially given by cyclicity conditions of some class group, the expected equality $h_\phi = m_\phi$ was obtained. This equality is in agreement with a conjecture of G. Grass [1977].

The above results have been quoted in the following publications, among others: [L. C. Washington, 1982; 1997], [P. Schneider, 1982; 1983], [B. Mazur; A. Wiles, 1984], [J. S. Milne, 1986], [A. Wiles, 1990], [S. Turner, 1990], [S. Bentzen; I. Madsen, 1990], and [J. Neukirch, 1992].

Kummer's criterion for irregular primes was strengthened by K. Ribet [1976]. Ribet established the converse to a Kummer-Herbrand theorem by using modular curves and p-adic modular forms. The interplay between modular curves and the arithmetic of cyclotomic fields shown in Ribet's beautiful article was the starting point for a refined theory developed by Mazur and Wiles. In [B. Mazur; A. Wiles, 1984], the authors succeeded in proving the main conjecture of the Iwasawa theory when the ground field is $K = \mathbb{Q}$. Their theory is based in the behaviour of the so-called Eisenstein ideal. As a consequence, the conjectures of Lichtenbaum and Grass were proven in this case.

2. Quadratic forms (11E)

The ubiquity of quadratic forms is well known among mathematicians working in number theory, lattice theory, and coding theory. Integral quadratic forms were studied by L. Euler, J. L. Lagrange and A. M. Legendre but the first coherent exposition of the theory of binary quadratic forms is that of C. F. Gauss in his *Disquisitiones arithmeticae* [1801]. The greatness of Gauss lies in having written a book that with fairly modest prerequisites inaugurated a whole new era in number theory. Today, this fundamental book is available in Catalan, thanks to the translation by G. Pascual [a3: Pa 96]. This Catalan edition of *Disquisitiones* was prepared by Pascual and Travesa, together with the philologists M. Otero and M. T. Sucarrats.

2.1. Binary quadratic forms

C. F. Gauss [1801; 1996] showed that the equivalence classes of primitive binary quadratic forms with given discriminant d have a natural structure of abelian group which we will denote by $H(d)$. In modern language, the group $H(d)$ is isomorphic to the ideal class group of an order of the quadratic field $K = \mathbb{Q}(\sqrt{d})$. Gauss also introduced the concept of genus for binary forms and expressed it in terms of characters.

Let K be a quadratic number field and let H be the ideal class group of its ring of integers –or maximal order. A classical question, originally posed by Gauss, is that of proving the existence of quadratic fields with arbitrarily large p-rank (cf. 1.1). P. Llorente and Quer [52: Llo-Qu 88-1], [b11: Qu 87] obtained the first known examples of imaginary quadratic fields with 3-rank $r = 5$. For all these fields the 3-rank of the associated real quadratic field is $s = 4$. Although these real fields were not the first ones to be known with this 3-rank, they do have the advantage of having a sufficiently small discriminant that one can calculate the regulator and determine the structure of its class group. To find these examples, the authors made use of some elliptic curves studied by J. F. Mestre [1983]. They also compared the frequency of the fields obtained, for a given rank, with the conjectural estimates established by H. Cohen and H. W. Lenstra [1983]. The construction of quadratic fields of large 3-rank allowed Quer [58: Qu 87], [b11: Qu 87] to obtain three elliptic curves of the form $Y^2 = X^3 + d$, defined over $\mathbb{Q}$, whose Mordell-Weil group over $\mathbb{Q}$ has rank equal to 12. This record was referred to in [M. Stoll, 1998], [H. G. Zimmer, 1998], [J. Gebel, 1996], and [H. Cohen, 1993; 1995].

2.2. Ternary quadratic forms

A. M. Legendre [1878] proved that a positive integer n can be expressed as a sum of three integral squares, $n = x^2 + y^2 + z^2$, if and only if $n \uparrow 4^a(8m+7)$. However, very little is known about the summands x, y, z. Gauss's algorithm for counting the number of primitive representations of positive integers by positive ternary quadratic forms essentially reduces the problem to that of representing binary quadratic forms by ternary quadratic forms. The algorithm was detailed in [e9: Ar 95-2].

The concept of genus of binary quadratic forms introduced by Gauss was subsequently generalized by G. Eisenstein [1852] to the case of ternary quadratic forms. Eisenstein himself conjectured that two quadratic forms in any number of variables would belong to the same genus if and only if they were rationally equivalent; but this is not true in general.

To decide the solvability of some Galois embedding problems whose study was started in [b13: Vi 83] (cf. 3.2), it is necessary to characterize those integers n that admit a representation as a sum of three integral squares with at least one summand prime to n. This characterization was attained in [b12: Ar 85]. For this purpose, the level $l(n)$ is defined as the maximum integer l such that n can be written as a sum of three squares with l summands prime to n, so that $0 \leq l(n) \leq 3$. The concept and the first properties of the level for positive integers were introduced in [f4: Ar 86], [f5: Ar 84]. Arenas and Bayer [56: Ar-Ba 87] proved that $l(n) = 3$ if $\gcd(n, 10) = 1$, and $l(n) = 2$ if $\gcd(n, 10) \uparrow 1$, when n increases keeping its radical fixed. The levels are evaluated analytically. The main term in the evaluation of $l(n)$ is related to the genus of several ternary forms. To obtain the main term, p-adic densities corresponding to rational primes which divide the determinant of the ternary quadratic forms involved are explicitly calculated by means of Gauss-Weber sums; the rest of the densities are covered by a theorem of Minkowski-Siegel [1935]; cf. [e19: Ar 89], [e21: Ar 87]. The error term in the evaluation of $l(n)$ is related to Fourier coefficients of cusp forms of weight 3/2. Since all integers with a given radical fall into finitely many quadratic families, Shimura's lifting, applied and combined with growth conditions on the coefficients of weight 2 cusp forms, makes it possible to obtain the quoted result. Clearly, the case n square free is not covered by quadratic families. For this reason, this case was handled separately in Arenas [49: Ar 88].

A new result on the number of representations of any odd positive integer by integral ternary quadratic forms of Tunnell's type was presented in [28: Ar 91-2]. These ternary forms intervene in the ancient congruent numbers problem (cf. section 5).

2.3. n-ary quadratic forms

The rational classification of quadratic forms over local and global number fields is a classical result due to H. Minkowski and H. Hasse. Given a number field K and a finite set P of primes of K, the quadratic forms over the totally P-adic field K_P were classified in [f9: Ba 76], [b15: Ba 75]. The Witt ring $W(K_P)$ was studied by using invariants afforded by Clifford algebras.

Arenas [55: Ar 87-1] gave an algorithm for counting the number of primitive representations of positive integers by quadratic forms in any number of variables which generalizes that given by C. F. Gauss [1801]. A key role is played by a square root of $-\det(f)g^{adj}$, modulo $\det(g)$, attached to every primitive representation of a quadratic form g in $(n-1)$ variables by a quadratic form f in n variables. Moreover, formulae were obtained for the number of primitive representa-

tions of an integer by f, and for the number of primitive representations of g by f.

The study of the genus of integral quadratic forms becomes more difficult if the forms involved are indefinite. Bayer and Nart [44: Ba-Na 89] proved that two forms, definite or indefinite, with the same average in the genus theta series belong to the same genus if they have the same signature and the same 2-type. This is an answer to a conjecture of Y. Kitaoka [1971]. The result had been announced by C. L. Siegel [1935] for definite n-ary forms and $n \geq 5$. The proof given in [44: Ba-Na 89] deals simultaneously with the definite case, $n \geq 3$, and the indefinite case, $n \geq 4$. Examples were produced to show that neither the signature nor the 2-type condition can be relaxed. From this result it was also proved that two forms, as above, with the same representation masses must also have the same average in the genus masses.

Arenas [13: Ar 95] gave explicit formulae for the number of rational and p-adic integral classes of n-ary integral quadratic forms, for $n \geq 3$ and definite or indefinite; the case $p = 2$ being particularly delicate. Moreover, it was proved under which necessary and sufficient conditions Eisenstein's conjecture on the genus of quadratic forms is true. The case $n = 2$ was treated in [29: Ar 91-1], [43: Ar 89]. Exact formulae for the number of genera of primitive integral positive definite ternary quadratic forms were given in [e10: Ar 95-1].

3. Inverse Galois theory (12F12)

The inverse Galois theory deals with the question of which finite groups G can occur as Galois groups over a ground field K. The theory presents a number of interesting aspects:

(1) the existence of polynomials or extensions with a given Galois group; (2) the effective construction of these polynomials; (3) the existence of extensions with some additional conditions; (4) the solvability of Galois embedding problems; and so on.

Many results have been obtained for special types of groups, but as yet no general techniques are available. In any case, the results and techniques differ widely depending on the nature of the field K.

There is a general feeling that any finite group G should occur as a Galois group over the rational field $\mathbb{Q}$. This is the main problem of the inverse Galois theory. At present, it is far from being completely solved. Its current situation, and the most significant methods developed in connection with it, were explained in [c5: Vi 92].

One major result in inverse Galois theory is due to I. Šhafarevič [1954], who managed to prove that every finite solvable group occurs as a Galois group over any number field. Šhafarevič's technique is based on the solution of successive Galois embedding problems (cf. 3.2) together with deep insights in the reciprocity laws afforded by class field theory. However, Šhafarevič's proof of this theorem is long and difficult, and is still being revised. For solvable groups of odd order, Šhafarevič's proof was made more accessible by J. Neukirch [1979]. An updated proof of Šhafarevič's theorem, which also corrects a mistake in the original article, has been submitted [A. Schmidt; K. Wingberg, 1998, preprint].

As for constructive Galois theory, or rigidity methods, the first results were obtained in the work of G. V. Belyi [1979], B. H. Matzat [1984] and J. G. Thompson [1984]. By these methods, it has been proved that many simple groups occur as Galois groups of regular extensions of the rational function field $\mathbb{Q}(T)$.

3.1. Galois realizations of S_n and A_n

Over one hundred years ago, in a seminal article, D. Hilbert [1892] proved that any symmetric group S_n and any alternating group A_n occur as Galois groups over the field $\mathbb{Q}(T)$. In the same article, Hilbert stated his famous irreducibility theorem. Putting both together, we know that S_n and A_n occur as Galois groups as well over $\mathbb{Q}$.

Nart and Vila [c12: Na-Vi 79] presented Hilbert's construction of polynomials with Galois group S_n and A_n over $\mathbb{Q}(T)$ in an algebraic and modern language. A simplified proof of Hilbert's irreducibility theorem was given in [c9: Vi 86]. Nevertheless, it should be pointed out that Hilbert's results over $\mathbb{Q}$ are non-effective.

As far as effective constructions of polynomials over $\mathbb{Q}$ with Galois group S_n or A_n are concerned, I. Schur [1930] obtained partial results by using Hermite and Laguerre polynomials. Nart and Vila [f8: Na-Vi 79] studied explicit conditions for polynomials to have Galois group over $\mathbb{Q}$ isomorphic to S_n or A_n. Two criteria for trinomials of the type $X^n + aX + b$ to have Galois group over $\mathbb{Q}$ isomorphic to S_n were given. Infinite families of polynomials of this type with S_n as Galois group over $\mathbb{Q}$ were constructed. In [65: Na-Vi 83], criteria to ensure that polynomials of the type $X^n + aX^3 + bx^2 + cX + d$ have Galois group A_n over any number field were given and infinitely many polynomials with absolute Galois group A_n were constructed, for every value of n. The case n even, not divisible by 4, for which explicit equations were still unknown, was covered in this way. A primitivity criterion given in [f6: Na-Vi 80], which generalizes one due to [Ph. Furtwängler, 1922], was used in the process.

These results have been considered in the following articles, among others: [G. Karpilovski, 1989], [S. D. C. Cohen, 1989], [B. H. Matzat, 1988; 1987], [H. Osada, 1987], and [E. Maus, 1984].

3.2. Galois embedding problems over A_n, S_n, and M_{12}

The data of a Galois embedding problem are a Galois extension $L|K$ with finite Galois group G, and a group extension E of G with kernel A. An embedding problem given by these data can be denoted by $E \to G \simeq \mathrm{Gal}(L|K)$. A solution to the embedding problem is a field or an algebra $\tilde{L}$ such that $\tilde{L}$ is a Galois extension of L with Galois group A and a Galois extension of K with Galois group E such that the restriction epimorphism $\mathrm{Gal}(\tilde{L}|K) \to \mathrm{Gal}(L|K)$ is the given epimorphism $E \to G$.

If the kernel A of the embedding problem is an abelian group, and $\varepsilon \in H^2(G, A)$ is the element corresponding to E, then the embedding problem is solvable if and only if the el-

ement $\varphi^*\varepsilon \in H^2(G_K, A)$ vanishes, in which G_K is the absolute Galois group of the field K, $\varphi: G_K \to G$ is the epimorphism corresponding to the extension $L|K$ and φ^* is the morphism induced on the cohomology groups.

We note that the cohomology class $\varphi^*\varepsilon \in H^2(G_K, A)$ giving the obstruction to the solvability of an embedding problem is in general not directly computable. Two important aspects of the Galois embedding problem are the explicit determination of this cohomology class and the explicit construction of its set of solutions, when the obstruction is trivial.

Vila [b13: Vi 83] considered the realization of some non-solvable groups as Galois groups over the rational field. The aim was to realize the central extensions of the alternating group A_n as Galois groups over Q. Since rigidity methods require, in fact, a trivial centre, the central extensions are on the opposite side. The problem was handled as a Galois embedding problem.

Let $\widetilde{A}_n$ be the non-trivial double cover of A_n which is the universal central extension of A_n. The Galois realization of central extensions of A_n reduces to the realization of $\widetilde{A}_n$. Looking at local behaviour at infinity, criteria were given in order to make a first trial of extensions having as Galois group A_n and which could be embedded in a $\widetilde{A}_n$-Galois extension [e24: Vi 84-1]. The obstruction to the Galois embedding problem attached to the particular case of $\widetilde{A}_n$ lies in the 2-component of the Brauer group of the ground field K. At about the same time, J-P. Serre [1984] characterized this obstruction in terms of the Hasse-Witt invariant of the quadratic trace form attached to the field of definition of the A_n-extension. By using Serre's formula, Vila [61: Vi 85-2] computed the obstruction for the A_n-polynomials previously constructed in [65: Na-Vi 83]. The result was that the corresponding fields can be embedded in a Galois extension with Galois group $\widetilde{A}_n$ if and only if $n \equiv 2 \pmod 8$ and n sum of two squares, or $n \equiv 0 \pmod 8$. Thus, for these values of n, every central extension of A_n occurs as Galois group over Q.

In order to cover more values of n, Vila [62: Vi 85-1], [b13: Vi 83] constructed new families of equations with Galois group A_n over $\mathrm{Q}(T)$, using rigidity methods that were new at that time. The obstruction to the Galois embedding problem in $\widetilde{A}_n$ attached to them was computed by means of Serre's formula. The new answers to the problem were that every central extension of A_n appears as Galois group over Q if $n \equiv 0, 1 \pmod 8$; $n \equiv 2 \pmod 8$ and n sum of two squares; $n \equiv 3 \pmod 8$ and n sum of three squares $n = x_1^2 + x_2^2 + x_3^2$ and $(x_1, n) = 1$ (cf. 2.2). Moreover, by means of the same families of polynomials, it was also proved that every central extension of A_n appears as Galois group over $\mathrm{Q}(i)$, for every n, $n \uparrow 6, 7$.

Bayer, P. Llorente, and Vila [59: Ba-Llo-Vi 86] showed that every central extension of the Mathieu group M_{12} occurs as Galois group over Q. The polynomials used on this occasion were those defining the M_{12}-Galois extensions of $\mathrm{Q}(T)$ constructed by B. H. Matzat and A. Zeh [1986]. Shortly afterwards, the result was generalized by J. F. Mestre to $\mathrm{Q}(T)$.

A systematic study of the obstruction to the Galois embedding problem over $\mathrm{Q}(T)$ in $\widetilde{A}_n$ for the rigid Galois realizations of A_n, obtained from rigid triples of conjugacy classes of S_n of genus zero, was done in [48: Tu-Vi 89]. These results did not lead to any new realization of $\widetilde{A}_n$ as Galois group over $\mathrm{Q}(T)$. However, it was proved that either the central product of a cyclic group of order 4 and $\widetilde{A}_n$ or the central product of the dihedral group of order 8 and $\widetilde{A}_n$ are Galois groups over every number field.

The symmetric group S_n has four double covers, two of which are stem covers: $\widetilde{S}_n$ and $\hat{S}_n$. Vila [53: Vi 88] showed that every finite stem extension of S_n occurs as Galois group over every number field if $n \equiv 0, 1, 2$ or $3 \pmod 8$. Moreover, if the number field K contains $\sqrt{-1}$, then every finite stem extension of S_n, for every value of n, occurs as Galois group over K. The Artin polynomials over $\mathrm{Q}(T)$ were those obtained in [e24: Vi 84-1].

The local Artin root numbers of the Galois representation defining the zeta function of an algebraic number field have an explicit connection with the Hasse-Witt invariant of the quadratic trace form attached to it. In [42: Vi 90], the local Artin root numbers associated to Hilbert's polynomials realizing A_n, and to the exponential Taylor polynomials with Galois groups A_n or S_n, were determined. So Weil's additive characters of the attached Witt classes could be computed.

The above articles caught the attention of specialists, such as [P. E. Conner; R. Perlis, 1984], [J-P. Serre, 1984; 1988; 1989; 1992], [M. Schacher; J. Sonn, 1986], [W. Feit, 1986; 1989], [B. H. Matzat, 1987; 1988; 1991], [J. Sonn, 1988; 1989; 1991], [P. E. Conner; N. Yui, 1988], [G. Karpilovski, 1989], [J. F. Mestre, 1990; 1994], [A. Turull, 1992], [H. Völklein, 1992], [E. Bayer-Fluckiger, 1994], [J. R. Swallow, 1994], and [M. Epkenhans, 1994; 1997].

It should be mentioned in closing this item that J. F. Mestre [1990] succeeded in proving that $\widetilde{A}_n$ occurs as Galois group over $\mathrm{Q}(T)$ for any n. To overcome the obstacles to making the proof run inconditionally on n, Mestre combines the above mentioned techniques with ideas due to G. Henniart, J. Oesterlé, and J-P. Serre.

Another aspect of the Galois embedding problem is the study of the existence of solutions with particular conditions. In the case of number fields, an interesting point is the control of the ramification set of the solutions. Crespo [45: Cr 89-2], [b9: Cr 88] studied the case in which an embedding problem with abelian kernel over number fields has a solution field $\widetilde{L}_n$ such that the extension $\widetilde{L}_n|\mathrm{K}$ has a reduced ramification set.

3.3. Explicit solutions to Galois embedding problems

Crespo obtained a method for computing explicit solutions to embedding problems given by double covers and to embedding problems given by central extensions of alternating and symmetric groups with a cyclic kernel of order a power of 2.

The articles [46: Cr 89-1], [b9: Cr 88] contain the case of the non-split double cover of an alternating group. The method is based on the fact that the solvability of this kind of embedding problems is equivalent to the existence of a certain isomorphism between Clifford algebras. This result was

explained in [e20: Ba 89]. For embedding problems given by double covers of symmetric groups, [38: Cr 90-1] yields two different methods of reduction to the alternating case.

The explicit resolution of embedding problems given by double covers of symmetric and alternating groups can be used to compute modular forms of weight one; cf. 8.2, as well as [e8: Cr 97] and [e15: Cr 93]. It has also been used by A. Ash and M. McConnell [1992] to check experimentally the Langlands conjecture by attaching a three-dimensional Galois representation to any Hecke eigenclass in the mod p cohomology of a congruence subgroup of the special linear group SL(3, $\mathbb{Z}$). L. Schneps [1992] and J. R. Swallow [1994] used Crespo's result in the case of regular extensions of $\mathbb{Q}(T)$. This result is referred to by J-P. Serre [1992], among others.

J-P. Serre's formula [1984] mentioned above relates the element $\varphi^*\varepsilon$ with Hasse-Witt invariants and allows its computation. Not long afterwards, this formula was generalized by [A. Fröhlich, 1985] to the wider context of embedding problems associated to orthogonal representations. For these embedding problems, a formula expressing the obstruction to solvability in terms of Hilbert symbols was given.

Within Fröhlich's general framework, Crespo [37: Cr 90-2] obtained a generalization of the above methods which can be applied to an embedding problem given by an orthogonal representation. This result was partially generalized by J. R. Swallow [1995].

The resolution of embedding problems given by central extensions of alternating or symmetric groups with a cyclic kernel can be reduced to the case when the kernel has order a power of 2. For this kind of embedding problems, Crespo [4: Cr 98], [14: Cr 95-2], [15: Cr 95-1], [21: Cr 94], [26: Cr 92] gives a criterion for the solvability and a method of computation of the solutions by reducing to the case of an embedding problem with kernel of order 2.

As regards the explicit resolution of Galois embedding problems with a cyclic kernel of order bigger than 2, Crespo [31: Cr 91] suggested a method of resolution for problems associated to representations in the group of automorphisms of a central simple algebra using reduced norms. Unfortunately, the number of examples obtained in this way is very limited. Another attempt to solve explicitly these kinds of embedding problem was made by J. R. Swallow [1996].

Recently, embedding problems with a cyclic kernel of order bigger than two have been studied by Vela [b1: Ve 98], by using representations in the group of automorphisms of generalized Clifford algebras. A formula giving the obstruction to these embedding problems in terms of Galois symbols, and a method of explicit resolution, have been obtained. Several examples have been completed. Vela had previously obtained structure theorems for $\mathbb{Z}/n\mathbb{Z}$-graded central simple algebras and generalized Clifford algebras. The structure of the automorphism groups for classical and generalized Clifford algebras has been studied in [f2: Ve 98].

3.4. Arithmetico-geometric constructions of Galois groups

The action of the absolute Galois group over the rationals $G_{\mathbb{Q}}$ on certain arithmetico-geometric objects and the mod p Galois representation attached led H. Weber [1908] and K.-Y. Shih [1974] to the realization of certain linear and projective linear groups as Galois groups over $\mathbb{Q}$ (cf. sections 4 and 5 for tools used in this item).

Reverter [b4: Re 95] studied the images associated to the Galois action on p-torsion points of elliptic curves and to modular forms in order to obtain Galois realizations of finite groups as Galois groups over $\mathbb{Q}$.

The first aspects of Galois representations attached to p-torsion points of elliptic curves to be studied were the relation between the images of mod p Galois representations and the existence of isogenies of degree p. The images were determined for a large family of elliptic curves having a p-isogeny. The purpose of the study in [b4: Re 95] was to determine the images for every elliptic curve $E/\mathbb{Q}$ with conductor $N \leq 200$, without complex multiplication, and for every prime p, i.e. the computation of the Galois groups $\mathrm{Gal}(\mathbb{Q}(E[p])|\mathbb{Q})$ as a subgroup of GL(2, $\mathbb{F}_p$). Moreover, explicit polynomials were given for each subgroup of GL(2, $\mathbb{F}_3$) and GL(2, $\mathbb{F}_5$) that appears as images.

The images of the mod p Galois representations attached to modular forms led to new solutions to the inverse Galois problem over $\mathbb{Q}$ concerning realizations of projective linear groups over finite fields as Galois groups. K. Ribet [1975] had studied the images of mod p Galois representation attached to eigenforms of S_k, the space of cusp forms of weight k for SL(2, $\mathbb{Z}$). In [e13: Re-Vi 95], [b4: Re 95] a sufficient condition was given to assert that the groups PSL(2, $\mathbb{F}_q$), $q = p^{2n}$, *and* $q = p^{2n+1}$, appear as Galois groups over $\mathbb{Q}$, for infinitely many prime values of p. The computation of the characteristic polynomial of the Hecke operator T_2 acting on S_k made it possible to obtain an algorithm to find primes p such that these groups appear as Galois groups over $\mathbb{Q}$. In particular, the groups PSL(2, $\mathbb{F}_q$), for $q = p^{2r}$, $1 \leq r \leq 5$, and $q = p^{2r+1}$, $1 \leq r \leq 4$, are Galois groups over $\mathbb{Q}$, for infinitely many values of p. Moreover, using mod p Galois representations attached to eigenforms of weight 2, prime level $N = 29, 31$, and trivial character, it was shown that PSL(2, $\mathbb{F}_q$), $q = p^2$, occurs as Galois group over $\mathbb{Q}$, for every prime $p \geq 2069$.

4. Modular forms and modular curves (11F11, 11G18, 14G35)

The theory of automorphic forms is a subject where many diverse branches of mathematics such as complex analysis, hyperbolic geometry, arithmetic algebraic geometry, and representation theory come together. The concept of automorphic function –automorphic form of weight zero– generalizes that of periodic function. Automorphic forms present very strong symmetries with respect to an arithmetic group; when this group is contained in the modular group SL(2, $\mathbb{Z}$), automorphic forms are called modular forms. Although the origin of the theory dates back to the 19th century, one of its most attractive aspects has been its surprising adaptability to recent powerful computing tools.

At the centre of the theory of modular forms is the STW-conjecture, named after G. Shimura, Y. Taniyama, and A. Weil. It asserts that any elliptic curve E defined over $\mathbb{Q}$ can be uniformized by modular functions. The interest in the STW-conjecture grew considerably after the work of G. Frey [1986], who first suggested that STW might imply FLT. A careful proof that STW implies FLT was given in [J-P. Serre, 1987] together with [K. Ribet, 1990]. As is well known, A. Wiles [1995] chose to prove the STW-conjecture –for semi-stable elliptic curves– as the strategy to prove FLT.

The outlines of that program, and some background for the proof, were supplied in [c6: Ba 88], and in [c1: Ar 99], [c3: Ba 98-1], respectively. For additional information, the reader should consult [G. Cornell; J. H. Silverman; G. Stevens, 1997], which contains a series of expanded versions of lectures given on the subject of FLT.

4.1. Automorphic forms

The study of the periods of Γ-automorphic forms, for $\Gamma \subseteq \mathrm{SL}(2, \mathbb{R})$ a fuchsian group of the first kind, led L. Eichler [1957] and G. Shimura [1971] to establish an isomorphism $S(\Gamma, k+2) \simeq H^1_P(\Gamma, V^k_{\mathbb{R}})$ between the space of cusp forms with respect to Γ of weight $k+2$ and the first parabolic Eichler cohomology group for a certain constructible sheaf $V^k_{\mathbb{R}}$ which arises from the k-th symmetric power of the standard representation of the group $\mathrm{SL}(2, \mathbb{R})$ on $\mathbb{R}^2$. A direct proof of this isomorphism in the spirit of Hodge theory with degenerating coefficients was given by Bayer and J. Neukirch [66: Ba-Ne 81]. The proof also makes explicit the equality of the natural polarization of the Hodge structure and the Petersson inner product on $S(\Gamma, k+2)$. This correspondence between cusp forms and cohomology classes had been the starting point of the derivation of the Ramanujan-Petersson conjecture from Weil's conjectures [P. Deligne, 1971].

A discussion of Ramanujan's τ-function, the justification of recurrence formulae for calculating it, and the steps to prove Ramanujan's conjecture $\tau(n) = O(n^{11/2+\varepsilon})$ can be found in [c8: Ba 87-1].

Modular forms provide one of the most powerful tools to deal with quantitative aspects on the theory of quadratic forms (cf. 2.2). The sum of the singular series is just the average number $r(n,\ \mathrm{gen}\ I_k)$ of representations of a positive integer n by the genus of the identity quadratic form in k variables. Arenas [54: Ar 87-2] obtained a formula for $r(n, \mathrm{gen}\ I_k)$ in some special cases, which cover the case $k = 24$, as well as other cases previously considered by P. T. Bateman [1951]. Therefore, Ramanujan's celebrated formula on the number of representations of an integer as sum of 24 squares was reobtained as an application of the sum of the singular series.

Hodge-Tate structures should provide a p-adic analogue for classical Hodge theory. The relationship between cusp forms, associated p-adic Galois representations, and Hodge-Tate structures coming from the action of the inertia group at p was studied in [G. Faltings, 1987]. A resumé of this work was presented in [e18: Ba 91].

4.2. Modular forms and Galois representations

The relevant article [J-P. Serre, 1987], already quoted, contains two precise conjectures on the modularity of some mod p Galois representations. The equivalence of the two conjectures for representations arising from torsion points of elliptic curves of certain reduction type was proved by Lario [b7: La 91]; cf. also 5.3. Many other mathematicians have worked on the equivalence of these two conjectures in other situations: [F. Diamond, 1995], [A. Wiles, 1995], [B. Edixhoven, 1992], [B. Gross, 1990], [K. Ribet, 1990; 1994], and [H. Carayol, 1989]. This is a difficult topic, which plays an important role in Wiles' proof of FLT. Dealing with it requires a deep understanding of the arithmetic of modular curves and, more generally, of Shimura curves attached to quaternion algebras. An introduction to these subjects in connection with Langlands' program is worked out in [a2: Ba-Tr 97].

4.3. Modular curves

One of the most interesting families of curves are those consisting of the modular curves $X_0(N)$ and $X_1(N)$. The curves $X_0(N)$ parametrize elliptic curves with cyclic subgroups of order N. The curves $X_1(N)$ parametrize elliptic curves with points of order N. Modular curves allow a geometric and arithmetical interpretation of modular forms, since these can be seen as higher differentials on those curves. Very often, the behaviour of the Fourier coefficients of a modular form mirrors the arithmetic of the modular curve involved.

The handbook [a5: Ba-Tr 92] contains numerical tables for modular forms and modular curves. It was prepared jointly by all the members of the STNB; cf. also [d7: STNB 92]. These numerical data have been widely used –cf. for instance [T. Ekedal; J-P. Serre, 1993].

A. P. Ogg [1974] determined all modular hyperelliptic curves $X_0(N)$ of genus $g > 1$, but only in a few cases were the equations of the curves known. Equations of all these hyperelliptic curves of genus $g > 1$ were obtained by Gonzàlez [b5: Go 94], [32: Go 91]. These equations have been used by [H. Weber, 1997] and [F. Leprévost, 1993], among others.

Let $E/\mathbb{Q}$ be an elliptic curve –an abelian variety of dimension one– defined over the rational field. For a given prime p, an important local invariant of the curve is its Hasse-Witt invariant $r_p(E)$ (cf. section 7). Classically, the curve $E/\mathbb{Q}$ is called supersingular at p if and only if $r_p(E)$ is equal to zero. If the elliptic curve E has complex multiplication, the set of supersingular primes for $E/\mathbb{Q}$ has density equal to 1/2 [M. Deuring, 1941]. S. Lang and H. Trotter [1976] formulated a conjectural law on the asymptotic behaviour of the number $P_E(x)$ of supersingular primes for $E/\mathbb{Q}$ that are $'' x$. It is known that if E does not have complex multiplication, the set of supersingular primes for $E/\mathbb{Q}$ has density equal to zero in the set of all primes [J-P. Serre, 1981]. N. Elkies [1991] proved that $P_E(x) = O(x^{3/4})$. Both results are still far from the assertion in the Lang-Trotter conjecture. Given an abelian variety $A/\mathbb{Q}$ of dimension ≥ 2, the behaviour of the Hasse-Witt invariant for its geometric fibres is less well known, even conjecturally. Let Γ denote a congruence subgroup, f a newform of weight

two for Γ without complex multiplication, and $A_f/\mathbb{Q}$ the abelian variety attached to f by G. Shimura [1971]. A higher-dimensional analogue of the Lang-Trotter conjecture was formulated by Bayer and Gonzàlez [9: Ba-Go 97]. The conjecture is supported by the construction of a probabilistic model and by numerical evidence compiled for modular curves of level up to one hundred and primes $p'' 10^4$.

5. Elliptic Curves over global, local, and finite fields (11G05, 11G07)

Abelian varieties constitute a cross-roads where algebra, analysis, geometry, topology, statistics, and computational methods meet. From the viewpoint of number theory, the specific case of elliptic curves is of particular significance given their great flexibility to interact with many other arithmetical problems. To exemplify this, we will briefly mention two longstanding problems: the congruent numbers problem, and FLT.

Congruent numbers are defined as those positive integers that are the area of right triangles with rational sides. The Babylonians already knew some congruent numbers; the medieval Arabs verified them and found some more; and Fermat proved that 1 is not a congruent number –equivalently, that Fermat's equation of exponent 4 has no non-trivial integer solutions. Recently, elliptic curves have appeared on the scene and have almost helped to obtain a final solution for the ancient question of characterizing these numbers; cf. for instance [c7: Ba 87-2].

The second problem in which elliptic curves have proved to play a decisive role is FLT. The beginning of the end came when G. Frey was astute enough to associate an appropriate elliptic curve, namely $Y^2 = X(X - a^p)(X + b^p)$, to a hypothetical solution (a, b, c) of the Fermat equation $X^p + Y^p = Z^p$, where $p \geq 5$ is a prime.

As we have mentioned, elliptic curves can be studied *per se* or as a tool to broach arithmetical applications but, in either case, the Hasse-Weil zeta functions attached to them become essential. They play an important role, as do Dedekind zeta functions in the case of number fields. Dedekind zeta functions were intensively studied during the 19th century, proving to be excellent objects for storing the arithmetical properties of number fields. Likewise, one expects adapted phenomena to be true in the case of elliptic curves. However, much remains to be understood in the case of elliptic curves –such as analytical continuation or STW-conjecture, special values or the Birch and Swinnerton-Dyer conjecture. The main contributions made by members of the STNB to this subject can be summarized as follows:

(1) a new characterization of modular elliptic curves (cf. 5.1); (2) research on the reduction properties of fibres of the Néron models of elliptic curves defined over number fields (cf. 5.2); (3) deriving methods to find elliptic curves over $\mathbb{Q}$ with large rank (cf. 1.1, 2.1); and (4) studies on the Galois modules of p-torsion points of elliptic curves over $\mathbb{Q}$ (cf. 3.4, 5.3).

5.1. Formal version of the STW-conjecture

Nart [22: Na 93] took advantage of the study of formal group laws for certain formal groups arising from modular curves to reformulate the STW-conjecture as follows. Let N be a positive, odd, square-free integer. Let $J_0(N)$ be the jacobian of the modular curve $X_0(N)$ over $\mathbb{Q}$, $J_0(N)^{new}$ its new quotient, and $\mathcal{J}^{new}$ the Néron model over $\mathbb{Z}$ of $J_0(N)^{new}$. The logarithm of the formal group $(\mathcal{J}^{new})^\wedge$ was expressed in terms of the action of Hecke operators on the new part of the $\mathbb{Z}$-module of cusp forms over $\mathbb{Z}$ of level N and weight 2. As an application, it was shown that an elliptic curve $E/\mathbb{Q}$ of conductor N satisfies STW-conjecture if there exists a non-zero homomorphism of formal groups over $\mathbb{Z}$ from $(\mathcal{J}^{new})^\wedge$ to $\mathcal{E}^\wedge$, where $\mathcal{E}$ is the Néron model of E.

For related topics on formal groups, we refer the reader to [f3: Na 91] and [39: De-Na 90] where, in particular, some theorems of P. Cartier and T. Honda on elliptic curves are generalized to the case of abelian varieties.

5.2. Global minimal models and fibres of Néron models

Let K be a number field and v a finite place of K. Let E be an elliptic curve defined over K, χ a quadratic character of K, and E^χ the corresponding twisted curve. J. H. Silverman [1984] had shown that when χ is unramified at the primes of K over 2 and at the primes of bad reduction of E, the formula relating the discriminants of E, χ and E^χ is simply $D(E^\chi|K) = D(\chi)^6 D(E|K)$. For general χ, Comalada [20: Co 94-1], [b8: Co 91] defined a correcting local factor h_v and then computed it explicitly together with the type of the special fibre of the v-minimal, v-regular model of E^χ. The problem of finding the exact relation between the geometric conductors of E and E^χ was also addressed.

J. H. Silverman [1984] had proved that there exists a quadratic twist of E admitting a global minimal Weierstrass equation. Comalada [19: Co 94-2], [b8: Co 91] considered a quadratic field K and a semistable elliptic curve E over K. A necessary and sufficient condition, in terms of the Weierstrass class of E relative to K, for the existence of a semistable twist of E with a global minimal Weierstrass equation was given. If E has trivial conductor, a criterion for the existence of a twist of E with trivial conductor and a global minimal model was deduced.

Let $J(v)$ denote the set of $j \in K$ such that there exists an elliptic curve defined over K with modular invariant j and good reduction at v. In the first part of [25: Co-Na 92], Comalada and Nart gave an explicit description of $J(v)$. When the residual characteristic of v is different from 2 or 3 the result is well known and easy ($j \in J(v)$ if and only if $v(j) \geq 0$, $v(j) \equiv 0$ [mod 3], and $v(j - 1728) \equiv 0$ [mod 2]). When the residual characteristic of v is equal to 2 or 3, their result describes $J(v)$ assuming v is absolutely unramified. Let S be a finite set of finite places of K; in the second part of the article, Comalada and Nart compute the obstruction to the existence of an elliptic curve defined over K with modular invariant $j \in \cap_{v \notin S} J(v)$ and good reduction outside S. As an application, they give a criterion for deciding whether a given $j \in K$ is the modular invariant of an elliptic curve defined over K with good reduction

everywhere and modular invariant *j*; cf. also [36: Co 90-1].

Comalada [b8: Co 91], [35: Co 90-2] continued the classification of elliptic curves with good reduction everywhere. J. Tate [1983] had shown that there are no such curves over $\mathbb{Q}$. R. J. Stroeker [1983] had proved that there are no such curves over imaginary quadratic fields having a global minimal Weierstrass equation. C. B. Setzer [1978; 1981] had found all elliptic curves over a quadratic imaginary field with good reduction everywhere and having a rational 2-torsion point, and also all such curves over any quadratic field whose *j*-invariant is in $\mathbb{Q}$. Later, Comalada described all elliptic curves over real quadratic fields which have a rational 2-torsion point and which admit a global minimal Weierstrass equation. Some partial results were given in the case that there is no minimal equation. For example, it was proved that there are exactly eight elliptic curves defined over a quadratic field having good reduction everywhere and full level 2 structure; cf. also [57: Co-Na 87].

5.3. Residual Galois representations

Let ρ: $G_{\mathbb{Q}} \to$ GL(2, k) be a continuous, irreducible, and odd representation, where k denotes an algebraic closure of $\mathbb{F}_p$. J-P. Serre [1987] attached a conductor $N(\rho)$, a weight $k(\rho)$, and a character $\varepsilon(\rho)$ to such a representation and conjectured that ρ is associated to a cuspidal eigenform mod p of type $(N(\rho), k(\rho), \varepsilon(\rho))$. An interpretation for this conjecture is that the Frobenius distribution law for the splitting field of ρ depends heavily on its ramified primes.

Bayer and Lario [24: Ba-La 92], [b7: La 91] took ρ to be given by the Galois action on the p-division points of an elliptic curve $E/\mathbb{Q}$. They showed that Serre's conjecture is true when ρ is irreducible and E is modular with potentially ordinary reduction at $p > 7$ or semistable reduction at $p \geq 5$. To do this they manipulated the weight-2 newform attached to E to obtain the desired eigenform. This process was suggested by computer experimentation.

Lario [e16: La 93], [b7: La 91] considered Serre's conjecture over the cyclotomic twists $\rho(n)$ of a given general ρ. The twist with the lowest weight is called the minimal twist. The main achievement was the demonstration that the conjecture for the minimal $\rho(n)$ implies the conjecture for ρ. Then, the results in [24: Ba-La 92] were applied to verify the conjecture for $\rho(n)$ in the potentially ordinary case. Lario [e17: La 92] suggested a strategy for verifying Serre's conjecture in the potentially supersingular case. Some numerical examples were given.

Lario and Rio [12: La-Ri 96], [17: La-Ri 95] showed that if the representation ρ:$G_{\mathbb{Q}} \to$ GL(2, $\mathbb{F}_3$) has determinant equal to the cyclotomic character and splitting field of degree at least 16, then there exists a modular elliptic curve $E/\mathbb{Q}$ such that ρ arises on the 3-division points of E. To do this they made an explicit analysis of the moduli space of elliptic curves which realize some twist of ρ on their 3-division points. This space is in fact rational. The authors produced a point on this moduli space corresponding to an elliptic curve with semistable reduction at 3 and applied the main theorem of F. Diamond [1996].

6. Abelian varieties of dimension >1 (11G10)

Abelian varieties are excellent territory for a number theorist. They emerged in the study of certain integrals related to length of arcs and physical phenomena, though they had already been present in some particular diophantine equations. Many questions about the arithmetic of abelian varieties are still unanswered and are the focus of attention for many mathematicians.

6.1. Abelian varieties of GL(2)-type

In his survey *Number Theory as a Gadfly* [1991], B. Mazur raised the question of how STW-conjecture can be generalized to elliptic curves defined over number fields. K. Ribet [1992] came up with a conjectural answer to that question: the modular elliptic curves over number fields should coincide with those which are isogenous to their Galois conjugates. By means of Weil's functor of the restriction of scalars, the study of the arithmetic of abelian varieties of GL(2)-type and their building blocks aroused great interest; the $\mathbb{Q}$-curves turned out to be the one dimensional building blocks.

Besides some recent articles by Y. Hasegawa, K. Hashimoto, and B. Roberts on explicit examples of $\mathbb{Q}$-curves of low degree, several members of the STNB have begun to develop a systematic study of the arithmetic of $\mathbb{Q}$-curves. Quer [e2: Qu 98-2], [e3: Qu 98-1] has clarified the set of abelian varieties of GL(2)-type that contain a given $\mathbb{Q}$-curve as a building block. This represents a thorough study of the different cohomogical groups related to classes of 2-cocycles attached to $\mathbb{Q}$-curves. In particular, Quer obtains specific results on inner-twist theory by exploring the endomorphism algebras of the abelian varieties involved; cf. also [8: Qu 98], [e1: Qu 98-3].

Another subject that has been analyzed along the same route is the study of the possible main degrees of the isogenies for $\mathbb{Q}$-curves. This has been partially accomplished by Gonzàlez and Lario [7: Go-La 98], in which quadratic, triquadratic, and tetraquadratic families of $\mathbb{Q}$-curves have been obtained from the study of rational points of the modular curves $X^*(N)$ for those values of N such that the corresponding curve has genus 0 or 1. According to standard conjectures on rational points, it seems very likely that [7: Go-La 98] exhausts all the isogeny classes of $\mathbb{Q}$-curves except for a finite number of exotic cases. As for the field of definition of $\mathbb{Q}$-curves, Gonzàlez [5: Go 98-2] has proved that they are forced by several restrictions. Moreover, some properties of the bad reduction fibres and behaviour of the *j*-invariants of $\mathbb{Q}$-curves that reveal the complex multiplication case have been determined.

The results of J. M. Brunat and Lario [2: Br-La 98] can be thought of as a complement of [N. Elkies 1993, preprint] on $\mathbb{Q}$-curves. The aim of their article was to begin with the study of Galois graphs, emphasizing the particular case of graphs associated to $\mathbb{Q}$-curves. Lastly, further investigations on modularity of algebraic curves of genus 2 have been performed in [3: CGLR 98]. More precisely, if C is a hyperelliptic

curve of genus 2 with non-abelian automorphism group, then explicit criteria are given to decide whether its jacobian variety $J(C)$ is of GL(2)-type.

6.2. p-ranks and endomorphism algebras

Let A be an abelian variety defined over a finite field of characteristic p. Gonzàlez [f1: Go 98], [b5: Go 94] has discussed the relationship between the p-rank of A, $r(A)$, and its endomorphism algebra, $\mathrm{End}^0(A)$. As is well known, $\mathrm{End}^0(A)$ determines $r(A)$ when A is an elliptic curve. It has been shown that, under some conditions, the value of $r(A)$ and the structure of $\mathrm{End}^0(A)$ are related. For example, if the centre of $\mathrm{End}^0(A)$ is an abelian extension of $\mathbb{Q}$, then A is ordinary if and only if $\mathrm{End}^0(A)$ is a commutative field. Nevertheless, an example is provided of two abelian varieties of dimension 3 which have $\mathbb{Q}$-isomorphic endomorphism algebras but show different p-ranks. One of these is the jacobian of the modular curve $X_0(41)/\mathbb{F}_3$.

6.3. Rigidity p-adic methods

The aim of S. Bosch and Xarles [11: Bo-Xa 96] was to study some local arithmetical properties of abelian varieties. Let R be a complete discrete valuation ring with field of fractions K and let A_K be an abelian variety. The first result in this article is to prove the existence of a rigid uniformization of A_K: there exists a semi-abelian group scheme E_K, extension of an abelian variety B_K with potentially good reduction by a torus, and a not necessarily split lattice $M_K \subseteq E_K$ such that, in terms of rigid K-groups, A_K is isomorphic to the quotient E_K/M_K. This result is the rigid-analytical version of the usual complex uniformization of abelian varieties and it was introduced in the case of semistable reduction by M. Raynaud.

This uniformization was then used to study the group of components ϕ_A of the Néron model of A_K. This is a finite abelian group with an action of the absolute Galois group of K that contains important arithmetical information of A_K. It has been known since the work of A. Grothendieck, D. Lorenzini and others that there exists a canonical filtration in four steps of the prime-to-p part of ϕ_A, where p is the characteristic of the residue field of R, and with graduate quotients bounded in some sense. Bosch and Xarles [11: Bo-Xa 96] have constructed a similar filtration for the whole ϕ_A: $\Sigma_3 \subseteq \Sigma_2 \subseteq \Sigma_1 \subseteq \phi_A$, which coincides with the previous filtration when restricted to the prime-to-p part. It verifies that ϕ_A/Σ_1 and Σ_2/Σ_3 have orders bounded by an explicit constant depending only on the unipotent rank u of the reduction of A, while the group Σ_3 has minimum number of generators less than or equal to the toric rank of the reduction of A. The remaining quotient Σ_1/Σ_2 has prime-to-p part bounded by an explicit constant depending also on u.

These results have been applied in [e5: Xa 98] to study the number of torsion points of an abelian variety A_K over a finite extension K of $\mathbb{Q}_p$. Suppose that the reduction of the Néron model of A_K does not contain the multiplicative group scheme $\mathbb{G}_m$. The aim of that article is to show the existence of an explicit bound for the number of torsion elements in $A_K(K)$ depending only on the dimension of A_K, the degree of K over $\mathbb{Q}_p$ and the prime p. This result was obtained in the case of dimension 1 by M. Flexor, J. Oesterlé, and others, and it was also studied previously for the prime-to-p torsion points by F. Oort, A. Silverberg, and D. Lorenzini.

7. Curves over finite, local, and global fields (11G20, 11G30)

Given a non-singular projective curve C/k of genus $g > 0$ defined over an algebraically closed field of characteristic $p > 0$, its Hasse-Witt invariant $r(C)$ is defined as the maximum number of cyclic unramified independent extensions of degree p of the function field $k(C)$. It is known that $r(C)$ is the p-rank of the absolute Frobenius F^* acting on the first cohomology group of the curve: $r(C) = \dim_{\mathbb{F}_p} H^1(C,O)^{F^*}$. From this, one sees that $0 \leq r(C) \leq g$. The Hasse-Witt invariant is also equal to the p-rank of the kernel $J(C)[p]$ of the multiplication by p on the jacobian $J(C)$.

Gonzàlez [10: Go 97], [b5: Go 94] computed the Hasse-Witt invariants for a certain class of curves, which include hyperelliptic curves and Fermat curves of prime degree. The curves of the family C_l are defined by the equations $Y^l = F(X)$, where l is a prime and $F(X) \in k[X]$ a separable polynomial of degree n. If $l = 2$ and $n > 2$, one obtains hyperelliptic curves; if $F(X) = X^l + 1$, Fermat curves. Hasse-Witt matrices were explicitly computed for this family of curves. A formula for the Hasse-Witt invariant of the Fermat curve at each prime $p \uparrow l$ was obtained, and the Hasse-Witt invariant was shown to depend only on the residue degree. It was previously known that the triviality of the p-rank was not sufficient for the Fermat jacobian to be isogenous to a power of a supersingular elliptic curve. Here, the density question of the set of primes p such that the Fermat jacobians have the above property is addressed. For instance, if $l \geq 11$ and $l \equiv 3 \pmod 4$, then the density of the set of primes p such that $r_p(C) = 0$ and the jacobian $J(C_l/k)$, where l denotes an algebraic closure of $\mathbb{F}_p$, is not isogenous to a power of a supersingular elliptic curve is $\geq \varphi((l-1)/2)/(l-1)$, where φ denotes the function of Euler.

In [6: Go 98-1], [b5: Go 94], Gonzàlez considers the splitting of Fermat jacobians of prime degree l over an algebraic closure of a finite field of characteristic p not equal to l. Gonzàlez proved that their decomposition is determined by the residue degree of p in the cyclotomic field of the l-th roots of unity, and gave some results about the Hasse-Witt invariants of these curves. They are used to provide a numerical criterion that allows computation of the absolutely simple subvarieties and their multiplicity in the Fermat jacobian.

8. Galois properties of automorphic forms (11F80)

8.1. Galois representations

The absolute Galois group of a number field K is a profinite topological group with its natural Krull topology, where a base of open subgroups is given by the fixers of finite extensions of K. This group G_K is countably generated as a topo-

logical group. The study of representations of the absolute Galois group of the rational field, or any number field, or a local field, is a strategy used to obtain all the arithmetical information stored in that group.

Nowadays it is generally understood that the outstanding structure to study in connection with arithmetical problems is not merely the topological group but also a rather more elaborate structure which takes into account local data at each prime and is essentially determined by the conjugacy classes of Frobenius elements.

We have a reasonably satisfactory understanding of the abelianization of this structure; this is the principal achievement of class field theory. To extend the study of the structure of the Galois group beyond describing its abelianization, one unavoidable obstacle to contend with is that the group is non-abelian and therefore it is difficult to state precise results more intrinsically than «up to conjugation».

A standard tactic for such situations –which we might call the Tannakian approach– is to try to study representations of G_K, because the study of representations is insensitive to the fact that we know the group only up to inner automorphisms.

From this perspective, class field theory has provided an adequate theory of 1-dimensional representations, i.e., representations in GL(1, $\mathbb{C}$), the multiplicative group of $\mathbb{C}$, or in the multiplicative group of any commutative ring.

We are led, then, to think of Galois representations, namely continuous homomorphisms $\rho : G_K \to \mathrm{GL}(n, A)$ for A some topological ring, and any n = 1, 2, ... To understand the structure mentioned above we must understand such representations as well as their local behaviour.

Galois representations arise in a natural way when we consider elliptic curves or, more generally, abelian varieties. The action on torsion points provides residual and l-adic representations where many of the arithmetical properties of the variety can be read; cf. 5.3. Due to the work of L. Eichler and G. Shimura [G. Shimura, 1971; 1994], to a modular form one can attach an abelian variety and therefore a Galois representation. In this way, a Galois representation becomes an algebraic object in which significant geometric and analytical objects meet.

In higher dimensions, in order to have a description of the Galois representations as satisfactory as that obtained for the 1-dimensional case, one should establish reciprocity laws. In the 2-dimensional case, although the theory is not yet complete, some partial results have proved sufficient, for example, to conquer the FLT at long last.

In this 2-dimensional case, the analogues of reciprocity laws of class field theory are formulated in terms of associated modular forms. The existence of an associated modular form is predicted by M. Artin's conjecture for representations in characteristic zero and by Serre's conjecture for representations in positive characteristic; cf. 4.2 and 5.3. Serre's conjecture was formulated in [J-P. Serre, 1987], motivated by G. Frey's work [1986]. Frey had shown that by attaching an elliptic curve to a hypothetical solution of the Fermat equation and then considering an associated Galois representation, the expected behaviour of this representation would provide the desired contradiction –an idea which actually led to the proof of the theorem! More than three centuries had passed before an accepted mathematical proof of the enigma was found; cf. [A. Wiles; R. Taylor-A. Wiles, 1995].

8.2. Artin's conjecture and STW-conjecture

The 2-dimensional representations are classified by types, according to the group which appears as the image of the corresponding projective representation. The dihedral case is the easier one to deal with, since attached newforms can be obtained as linear combinations of theta series of binary quadratic forms. The remaining types are the tetrahedral (A_4), the octahedral (S_4), and the icosahedral (A_5). For results about the icosahedral case see J. Buhler, 1978] and [G. Frey, 1994]. It is known, by a theorem of R.P. Langlands [1980] and J. Tunnell [1981], that the representations of octahedral type are modular. This means that the reciprocity law is true in this case. Background material is supplied in [a2: Ba-Tr 97].

When we consider the Galois action on 3-torsion points of an elliptic curve, we almost always obtain an octahedral Galois representation, which is modular. Then, for a semistable elliptic curve, A. Wiles managed to carry the modularity up to the 3-adic representation, to the elliptic curve. For this purpose, Wiles combined arrangement of constants, [K. Ribet, 1990] and [F. Diamond, 1995], with the deformation theory of Galois representations, [B. Mazur, 1989]. In this way the STW-conjecture is proved in [A. Wiles, 1995].

Since, in the conditions required for a modular form to be attached, there exist no linear representations with an image isomorphic either to A_4, S_4 or A_5, we must consider representations with an image isomorphic to a non-trivial extension of the corresponding group. The case of index two is the first to be studied. At this point, results about the solvability of embedding problems become necessary (cf. section 3).

In the article of Bayer and G. Frey [30: Ba-Fr 91], Galois representations of octahedral type and index two with odd determinant were described in terms of 2-coverings of elliptic curves. An algorithm which computes the Fourier coefficients of the Artin L-series for representations in characteristic zero was obtained. The algorithm combines techniques of Galois representations with the knowledge of the obstruction to embedding problems and their explicit solutions presented in 3.3. The algorithm was implemented by Quer [d6: Qu 93]. The results in [30: Ba-Fr 91] have been used by [A. Antoniadis; M. Bungert; G. Frey, 1990], [M. Bungert, 1993], [I. Kiming, 1993; 1994], [E. Bayer-Fluckiger, 1994], [A. Jehanne, 1995] and [P. C. Cassou-Noguès; A. Jehanne, 1996; 1997], among others.

This work was continued in Rio [b3: Ri 96], where the contribution of the wildly ramified primes to the level of the attached modular form was calculated. To characterize and classify the possibilities for the ramification of the prime 2, the most intricate one, all the corresponding dyadic extensions were described completely. In this work, octahedral representations ρ in positive characteristic are considered and Serre's constants ($N(\rho)$, $k(\rho)$, $\varepsilon(\rho)$) are explicitly com-

puted. In particular, the minimal space where one should look for the associated newform is shown to be effectively computable in terms of the corresponding projective representation, i.e., in terms of a quartic polynomial. Further results directly connected with this subject were developed in [17: La-Ri 95] and [12: La-Ri 96]. Citation of [b3: Ri 96] and [12: La-Ri 96] can be found in Wiles' collaborators [F. Diamond; K. Kramer, 1997].

In positive characteristic there are many more cases for the types of the Galois representations. This was comprehensively studied by Quer [18: Qu 95]. Liftings of 2-dimensional projective representations of the absolute Galois group of a field were related to solution of certain Galois embedding problems, computing the obstruction to the existence of a lifting of index 2, and, in the case of the field Q, obtaining an easily computable criterion for the existence of a lifting of any given index.

9. Arithmetic varieties and schemes
(14L15, 14C25, 14G40)

Our work in arithmetic algebraic geometry centres mainly on three topics: (1) the arithmetic of algebraic tori; (2) the study of algebraic cycles and motivic cohomology; and (3) Arakelov geometry.

9.1. Algebraic tori

An algebraic group T over a field is an algebraic torus if there exists a finite separable extension such that the extension of scalars of T is isomorphic to a finite product of copies of the multiplicative group G_m. These algebraic groups are commutative, affine, smooth, and of finite type. Furthermore, every smooth commutative algebraic group contains a maximal sub-torus and its quotient is unipotent. An algebraic torus is totally determined by its character group $X(T)$, the group of homomorphisms over a separable closure from T to G_m; it is a torsion-free abelian group with rank equal to the dimension d of T with a continuous action of the absolute Galois group G_K of the field; or, equivalently, a continuous representation ρ of G_K to the group of integral invertible matrices $\mathrm{GL}(d, \mathrm{Z})$.

As for the case of abelian varieties, if K is the quotient field of a discrete valuation ring R with residue field K, for every algebraic torus T over K there exists a canonical model $\mathcal{T}$ over R, which is a smooth group scheme of finite type and satisfies a certain universal property. Thus, the reduction of this model to the residue field is a smooth algebraic group of finite type and its identity component is an extension of an algebraic torus $\bar{T}$ by a unipotent algebraic group U. The main aim of Nart and Xarles [34: Na-Xa 91] was to find a sufficient condition for U to be isomorphic to a power of the additive group G_a, in the case that the residue field is perfect. This condition is, expressed in terms of the associated integral representation ρ, that the fixed field of the kernel of ρ has a ramification index less than the characteristic of the residue field. It was also shown that the character group of $\bar{T}$ is equal to the maximal quotient of $X(T)$ which is torsion free and fixed by the inertia group. Xarles [b6: Xa 94], [23: Xa 93] studied, when the residue field K is perfect, the component group ϕ of the reduction of the Néron model of T, which is a finitely generated group with an action of the absolute Galois group G_K of K. The main idea is that, since T is totally determined by X, it should be possible to compute ϕ in terms of X. M. Raynaud, A. Grothendieck, and L. Begueri obtained some results in this direction, but no complete description of ϕ was known. The article characterized first of all the structure of the torsion and torsion-free parts of ϕ in terms of the cohomology groups of the inertia acting on the character group X of T. This result is not sufficient to determine ϕ, as was shown in the article by means of computing some examples. A complete characterization of ϕ was finally obtained by using the language of derived categories. Some of these results were used in [11: Bo-Xa 96] to study the Néron models of abelian varieties (cf. 6.3).

9.2. Algebraic cycles and motivic cohomology

The –still conjectural– motivic or absolute cohomology should be a cohomology theory from which all the other good, or Weil, cohomology theories that are known in algebraic geometry can be deduced. In an attempt to show the Weil conjectures for varieties over finite fields –whose proof was completed by P. Deligne [1974]– Grothendieck together with M. Artin developed étale cohomology in the sixties, which affords a suitable Weil cohomology theory provided one considers cohomology with finite coefficients and relatively prime to residue characteristics. S. Lichtenbaum [1983] formulated a general conjecture on the existence of an integer-valued arithmetic cohomology theory which induces étale cohomology after passing to torsion coefficients, and which should be related to algebraic K-theory. Specifically, he conjectured for a regular scheme X the existence of complexes $\mathrm{Z}(r)$, r a non-negative integer, of étale sheaves, such that the cohomology of the complex cone of the morphism multiplication by n, n prime to the characteristics, should be the étale cohomology with coefficients in $\mathrm{Z}/n\mathrm{Z}(r)$. These complexes should provide the right hypercohomology coefficients in order to express the values of the zeta function of X at negative integers as Euler-Poincaré characteristics. As pointed out by Lichtenbaum himself, the axioms imply also that these complexes play the role of a dualizing object in a very general theorem extending Artin-Verdier duality to higher dimensional regular schemes. A candidate for $\mathrm{Z}(r)$ was given in [S. Bloch, 1986] by means of certain relative cycles of codimension r on X. He proved, in particular, that $\mathrm{Z}(1) = \mathrm{G}_m[-1]$. In the same article, Bloch constructed the so-called Bloch higher Chow groups $\mathrm{CH}^n(X,i)$, which can be considered as kinds of absolute motivic cohomology groups.

Nart [47: Na 89] is concerned primarily with the study of the Bloch complex $\mathrm{Z}(1)$. It was proved in the article that, for any noetherian scheme X, the complex $\mathrm{Z}(1)$ is quasi-isomorphic to the complex used in [C. Deninger, 1987] to extend Artin-Verdier duality to a proper, perhaps singular, scheme of dimension one, thus giving evidence that Bloch complex-

es could be the right dualizing object even in the non-regular case. The proof depends on an explicit description of the boundary maps of $\mathbb{Z}(1)$, which is also given with a detailed proof in the article. It is also proved that the Bloch higher Chow groups $CH^1(X,n)$ vanish for $n > 1$.

One of the most useful tools when studying algebraic cycles of codimension 1 or divisors over a smooth projective variety X is its Jacobian variety; it is an abelian variety $J(X)$ together with a map, the Abel-Jacobi map, from the divisors of degree zero to $J(X)$. In the case that X is defined over the complex number field $\mathbb{C}$, in 1969 P. Griffiths used Hodge theory to define some complex tori, the intermediate jacobians $J^i(X)$, which generalize the jacobian variety to algebraic cycles of codimension i. He also defined an Abel-Jacobi map between the subgroup of the i-th Chow group consisting of cycles homologically equivalent to zero and the complex torus $J^i(X)$. The tori $J^i(X)$ have many good properties, but they have several shortcomings from an algebro-geometric point of view. For example, if X is considered over an arbitrary field, then there is at present no theory of $J^i(X)$; there are as yet no «abstract intermediate jacobians». Now, if K is a finite extension of the p-adic field $\mathbb{Q}_p$, we have there a notion of analytic geometry, the rigid analytic geometry, so we can hope to construct some kind of intermediate jacobians by using analytic tools. In [e4: Ra-Xa 98], W. Raskind and Xarles introduced a theory of intermediate jacobians for smooth projective varieties X defined over K, subject to restrictions on the special fibre of a suitable regular proper model of X over the ring of integers of K. Analytic tori $J^i(X)$ over K, not necessarily abelian varieties, are introduced, together with an Abel-Jacobi map from the group of cycles of codimension i homologically equivalent to zero, modulo rational equivalence, to $J^i(X)$. The construction of these analytic tori uses some cohomological results on the étale cohomology of these types of varieties, and especially the comparison theorem between p-adic cohomology and logarithmic crystalline cohomology due to M. Fontaine, G. Faltings, T. Tsuji, and others.

9.3. Arakelov theory

Arakelov theory combines tools from algebraic geometry, analysis, and arithmetic. Following the undertaking of a general study during the STNB course «Arithmetic Surfaces» (1991-92), specific research into certain Arakelov invariants was conducted. Specifically, the objects studied are Faltings' δ invariant and the self-intersection of the dualizing sheaf. These invariants appear in most of the main conjectures in Arakelov theory, but they are not simple to compute, and are only known in a few cases: modular curves [A. Abbes; E. Ullmo, 1997] and some genus 2 curves [J. B. Bost; J. F. Mestre; L. Moret-Bailly, 1990].

Guàrdia [b2: Gu 98] has performed a comprehensive study of a family of genus 3 curves, aimed at to the determining these invariants. The geometric study of these curves contains the determination of the automorphism group, the period matrix and the relation between the bitangent lines and the odd 2-torsion points of their Jacobians. The analytical study provides, through the invariance of the Green function under isometries, a simplified formula of Faltings' δ-invariant. The arithmetical study of the curves contains the determination of their stable models over the bad reduction primes. Combining all this information, one can estimate Faltings'modular height of the curves and give lower bounds for the self-intersection of the dualizing sheaf. Performing these estimations required the development of the package `Newton` [d2: Gu-Mo 96-2] based on an algorithm of Montes, to determine the type of decomposition of primes in number fields of very high degree.

Finally, the article [16: De-Na 95] contains an attempt, in a specific situation, to linearize Arakelov theory –in view of the conjectural theory of absolute motives. For a number field one can define the category of mixed motives by using for example the ideas of P. Deligne and U. Jannsen. From the point of view of Arakelov geometry its ring of integers defines an affine arithmetic curve and hence its compactification Y defines the analog of a complete curve. A. J. Scholl [1994] defined a category of mixed motives over this ring of integers by imposing a local condition at every finite place, and he interpreted Beilinson-Deligne's conjectures on values of L-functions in terms of the annihilation of the group of 2-extensions between $\mathbb{Q}(0)$ and $\mathbb{Q}(1)$. This article extends Scholl's local condition to the infinite primes to define what should be the category of mixed motives over the compactification Y. By analogy with the étale cohomology $H^2(X, \mathbb{Z}/n\mathbb{Z}(1))$ of a projective curve over a field X, the group of 2-extensions over this category between $\mathbb{Q}(0)$ and $\mathbb{Q}(1)$ should be non-trivial. This is what is shown in the article by constructing a non-trivial trace map from this group with values in $\mathbb{R}$. As an application a canonical construction of a motivic height pairing with values in $\mathbb{R}$ is obtained.

Some of the reasons for studying Arakelov theory are related to other ways of understanding FLT. But this is another story which, unfortunately, *hanc marginis exiguitas non caperet*.

10. Instructional expositions: textbooks

(11-01, 12-01)

[a1: Tr 98] Travesa, A.: *Aritmètica,* Edicions de la Universitat de Barcelona, UB 25, Barcelona, 1998. ISBN: 84-8338-031-5.

[a2: Ba-Tr 97] Bayer, P.; Travesa, A., eds.: *Representacions automorfes de* GL(2), vol. I, II, STNB, Barcelona, 1997. ISBN: 84-923250-2-X.

[a3: Pa 96] Pascual, G.: *Disquisicions Aritmètiques,* Societat Catalana de Matemàtiques; Institut d'Estudis Catalans, Barcelona, 1996. Preface and Catalan translation of C. F. Gauss' *Disquisitiones Arithmeticae*, Leipzig, 1801. ISBN: 84-7283-313-5.

[a4: Gu-Vi 96] Guàrdia, J.; Vila, N.: *Àlgebra I: de la pràctica a la teoria,* Publicacions de la UB, Textos docents, n. 53, 1996. ISBN: 84-475-1337-8.

[a5: Ba-Tr 92] Bayer, P.; Travesa, A., eds.: *Corbes modulars: taules,* STNB, Barcelona, 1992. ISBN: 84-604-3577-6.

[a6: Al-Mi-Ri 91] Alsina, M.; Miret, J. M.; Rio, A.: *Càlcul i Àlgebra: resums i problemes*, 1991. D. L. B-42031-91.

[a7: Al-Bu-Ve 90] Alsina, M.; Busqué, C.; Ventura, E.: 500 *Problemes d'Àlgebra,* 1990. D. L. B-4492-90.

[a8: Ba-Mo-Tr 90] Bayer, P.; Montes, J.; Travesa, A.: *Problemes d'Àlgebra*, Publicacions de la UB, Materials Docents, n. 7, 1990. ISBN: 84-7875-361-3; MR# 92a: 00014.

11. Research expositions: monographs
(11-02, 12-02)

[b1: Ve 98] Vela, M.: *Álgebras* $\mathbb{Z}/n\mathbb{Z}$*-graduadas y problema de inmersión galoisiano,* UB, 1998. Thesis (September 18, 1998). Thesis advisor: T. Crespo.

[b2: Gu 98] Guàrdia, J.: *Geometria aritmètica en una família de corbes de gènere tres.* UB, 1998. Thesis (March 5, 1998). Thesis advisor: P. Bayer.

[b3: Ri 96] Rio, A.: *Representacions de Galois octaèdriques, UB,* 1996. Thesis (March 26, 1996). Thesis advisor: P. Bayer.

[b4: Re 95] Reverter A.: *Construccions aritmètico-geomètriques de grups de Galois,* UB, 1995. Thesis (July 12, 1995) in microfilm n. 2826, ISBN: 84-475-1326-2. Thesis advisor: N. Vila.

[b5: Go 94] Gonzàlez J.: *Invariants diferencials de corbes algebraiques sobre cossos de característica positiva,* UB, 1993. Thesis (February 4, 1994). D. L.: 36515-93. Thesis advisor: P. Bayer.

[b6: Xa 94] Xarles, F.-X.: *Teoremes de dualitat per a models de Néron de varietats semiabelianes,* UAB, 1994. Thesis (September 23, 1993) in microfilm; ISBN: 84-7929-968-X. Thesis advisor: E. Nart.

[b7: La 91] Lario, J.-C.: *Representacions de Galois i corbes el·líptiques,* Publicaciones EUEE, 1991. Thesis (September 17, 1991). D. L.: B-44929-90. Thesis advisor: P. Bayer.

[b8: Co 91] Comalada, S.: *Reducció dels torcements de corbes el·líptiques sobre cossos de nombres,* UAB, 1991. Thesis (Juny 12, 1991) in microfilm, ISBN: 84-7929-222-9. Thesis advisor: E. Nart.

[b9: Cr 88] Crespo, T.: *Sobre el problema de inmersión de la Teoría de Galois,* UB, 1987. Thesis (February 25, 1988) in microfilm n. 339, ISBN: 84-7528-545-7. Thesis advisor: P. Bayer.

[b10: Tr 88] Travesa, A.: *Nombres d'extensions abelianes i les seves funcions generatrius,* UB, 1987. Thesis (February 25, 1988) in microfilm n. 341, CDU 51, ISBN: 84-7528-547-3. Thesis advisor: P. Bayer.

[b11: Qu 87] Quer, J.: *Sobre el* 3*-rang dels cossos quadràtics i la corba el·líptica* $Y^2 = X^3 + M$*,* UAB, 1987. Thesis (July 14, 1987). Thesis advisor: P. Llorente.

[b12: Ar 85] Arenas, A.: *Un problema aritmético sobre las sumas de tres cuadrados,* UB, 1985. Thesis (July 8, 1985). D. L.: B-997-1986. Thesis advisor: P. Bayer.

[b13: Vi 83] Vila, N.: Sobre la realització de les extensions centrals del grup alternat com a grup de Galois sobre el cos dels racionals*, Publicacions Matemàtiques UAB*, 27 (1983), *p.* 43-143. MR# 86h: 12005. Thesis (July 19, 1983). Thesis advisor: P. Bayer.

[b14: Na 82] Nart, E.: Sobre l'índex d'un cos de nombres, *Publicacions Matemàtiques UAB,* 27, *p.* 579-583 (1983). Thesis (November 16, 1982). Thesis advisor: P. Llorente.

[b15: Ba 75] Bayer, P.: *Extensiones maximales de un cuerpo global en las que un divisor primo descompone completamente,* Publicaciones UB, 1975. Thesis (April 1, 1975). D. L. B-9463-1976. Thesis advisor: R. Mallol.

[b16: Pa 75] Pascual, G.: *Contribución al estudio de las extensiones galoisianas de grupo diedral,* Publicaciones UB, 1975. Thesis (April 1, 1975). D. L. B-46672-1977. Thesis advisor: E. Linés.

12. Research expositions: survey articles
(11-02, 12-02)

[c1: Ar 99] Arenas, A.: Formas modulares, 400 *años de Matemáticas alrededor del Teorema de Fermat,* (1999) p. 81-100. Publicaciones de la UCM, El Escorial, 1996.

[c2: Ba 98-2] Bayer, P.: Monstres, cordes, fantasmes i clars de lluna, *Butlletí de la Societat Catalana de Matemàtiques,* 14, n. 1 (1999), p. 9-30.

[c3: Ba 98-1] Bayer, P.: Conjeturas modulares, 400 *años de Matemáticas alrededor del Teorema de Fermat,* (1999) p. 101-116. Publicaciones de la UCM. El Escorial, 1996.

[c4: Ba 96] Bayer, P.: *Els sòlids platònics,* Reial Acadèmia de Doctors, 1996. D. Legal: B-4122-1996.

[c5: Vi 92] Vila, N.: On the inverse problem of Galois theory, *Publicacions Matemàtiques UAB,* 36, n. 2B (1992), p. 1053-1073. MR# 94a: 12006.

[c6: Ba 88] Bayer, P.: Weil versus Fermat. Presented in the XIII Jornadas Hispano-Lusas de Matemàticas. Universidad de Valladolid, 1988.

[c7: Ba 87-2] Bayer, P.: Triangles rectangles de costats racionals, *Butlletí de la Societat Catalana de Matemàtiques,* 1 (1987) p. 22-32. MR# 89f: 11085.

[c8: Ba 87-1] Bayer, P.: Sobre una llibreta d'apunts (Ramanujan), *Butlletí de la Societat Catalana de Matemàtiques,* 1 (1987) p. 7-13. MR# 88i: 01061.

[c9: Vi 86] Vila, N.: Sobre el teorema d'irreductibilitat de Hilbert, *Publicacions Matemàtiques UAB,* 30, n. 2-3 (1986), p. 83-88. MR# 88c: 12004.

[c10: Vi 85] Vila, N.: Liouville i els nombres transcendents, *Butlletí de la Secció de Matemàtiques,* 18, n. 2B (1985), p. 32-43. MR# 87i: 01308.

[c11: Ba 84] Bayer, P.: Variae observationes circa series infinitas, *Butlletí de la Societat Catalana de Ciències,* 2 (1984), p. 429-481.

[c12: Na-Vi 79] Nart, E.; Vila, N.: Sobre l'existència d'equacions que realitzen S_n, A_n com a grups de Galois d'un cos de nombres, *Publicacions Matemàtiques UAB,* 13 (1979), p. 79-87.

[c13: Ba 76] Bayer, P.: El Teorema de Fermat, *Publicacions Matemàtiques UAB,* 2 (1976), p. 49-100.

13. Explicit machine computations and programs (11-04)

[d1: Ve 98] Vela, M.: `N-Clifford`. Software package to deal with products and powers in Kummer fields $K(\sqrt[n]{\alpha})$ and Clifford algebras of type *n*. Implemented in Mathematica for PC-DOS and Windows systems. 1998.

[d2: Gu-Mo 96-2] Guàrdia, J.; Montes, J.: `Newton`. Software package to deal with decomposition of rational primes in number fields, following Montes' algorithm. Implemented in Mathematica for PC-DOS and Windows systems. 1996.

[d3: Gu-Mo 96-1] Guàrdia, J.; Montes, J.: FF (Finite Fields). Software package to deal with arithmetic in finite fields. Implemented in Mathematica for PC-DOS and Windows systems. 1996.

[d4: Gu-Vi 95] Guàrdia, J.; Vila, N.: `Galois`. To compute in Galois theory. Instructional package for a first course in Algebra. Implemented in Mathematica for PC-DOS and Windows systems. 1995.

[d5: Qu 94] Quer, J.: `MS` (Modular Systems). Software package to compute the action of Hecke operators on modular symbols associated to $\Gamma_1(N)$, and Fourier coefficients of the corresponding weight 2 modular forms. Implemented in Mathematica for PC-DOS and Windows systems. 1994.

[d6: Qu 93] Quer, J.: `Gamma`. Explicit computation of solutions to embedding problems over A_4, S_4 and A_5 fields, and coefficients of the corresponding modular forms. Implemented in Mathematica for PC-DOS systems. 1993.

[d7: STNB 92] Alsina, M.; Arenas, A.; Bayer, P.; Cases, E.; Comalada, S.; Crespo, T.; Dexeus, J.; Gonzàlez, J.; Guàrdia, J.; Lario, J.-C.; Magret, D.; Maureso, M.; Montes, J.; Nart, E.; Pascual, G.; Quer, J.; Reverter, A.; Rio, A.; Ruiz, J.-L.; Travesa, A.; Vila, J.; Vila, N.; Xarles, X.: Modular. Over 20 computer programs, most for PC-DOS system, to compute in modular curves and modular forms. 1991.

[d8: Qu 87] Quer, J.: `CLASS`. Software package to compute the ideal class group of quadratic fields. Implemented both in Assembler and Fortran, for the VAX-VMS system. 1987.

14. Proceedings, conferences, preprints, etc. (11-06)

[e1: Qu 98-3] Quer, J.: Embedding Problems over Abelian Groups and Application to $\mathbb{Q}$-curves. Preprint, 1998

[e2: Qu 98-2] Quer, J.: On $\mathbb{Q}$-curves, to appear in *Proceedings of the Conference on Number Theory and Algebraic Geometry.* Sant Feliu de Guíxols. 1997. Preprint IEM-Essen, n. 14; 8-12, 1998.

[e3: Qu 98-1] Quer, J.: $\mathbb{Q}$-curves and Abelian varieties of GL_2-type. Pre-print IEM-Essen, n. 9, 1998.

[e4: Ra-Xa 98] Raskind, W.; Xarles, X.: On *p*-adic intermediate jacobians. Preprint, 1998.

[e5: Xa 98] Xarles, X.: On torsion points of abelian varieties over *p*-adic fields. Preprint, 1998.

[e6: Al 97] Alsina, M.: Fundamental domains of upper half plane by the action of matrix groups, EAMA-97. Cobos, F. J.; Gómez, J. R.; Mateos, F., eds. (1997), p. 10-17. Sevilla. ISBN: 84-605-6586-6.

[e7: Ba-Cr 97] Bayer, P.; Crespo, T., eds.: Proceedings of the 19èmes Journées Arithmétiques, Barcelona 1995. *Collectanea Mathematica*, v. XLVIII, n. 1, 2, Barcelona, 1997. MR# 98b: 11002.

[e8: Cr 97] Crespo, T.: Galois representations, embedding problems and modular forms, *Collectanea Mathematica,* 48 (1997), p. 63-83. Proceedings of the 19èmes Journées Arithmétiques, Barcelona 1995. MR# 98j: 11101.

[e9: Ar 95-2] Arenas, A.: Sums of three squares, from Gauss to modular forms, in *Symposia Gaussiana,* Behara; Fritsch; Lintz, eds., Walter de Gruyter, Berlin, 1995, p. 241-248. MR# 96j: 11047.

[e10: Ar 95-1] Arenas, A.: On the number of genera of positive-definite integral ternary quadratic forms, *Conference Proceedings Canadian Mathematical Society,* AMS, 15 (1995), p. 1-11. MR# 96h: 11027.

[e11: Cr 95] Crespo, T.: Explicit Galois realization of C_{16}-extensions of A_n and S_n, *Recent Developments in the Inverse Galois Problem,* American Mathematical Society, Fried, M. et al., eds., Contemporary Mathematics, 186 (1995), p. 3-13. MR# 96g: 12004.

[e12: Gu-Vi 95] Guàrdia, J.; Vila, N.: Galois, prácticas de álgebra con Mathematica, *Actas de las Jornadas sobre Nuevas Tecnologías en la Enseñanza de las Matemáticas en la Universidad,* TEMU'95, Barcelona, 1995.

[e13: Re-Vi 95] Reverter, A.; Vila, N.: Some projective linear groups over finite fields as Galois groups over $\mathbb{Q}$, *Recent Developments in the Inverse Galois Problem,* American Mathematical Society, Fried, M. et al., eds., Contemporary Mathematics, 186 (1995), p. 51-63. MR# 96g: 12006.

[e14: Al 94] Alsina, M.: Álgebras de cuaterniones: álgebras de matrices y álgebras de división, *EAMA-94,* Diputación Foral de Álava, 1994, p. 14-14. ISBN: 84-7821-187-X.

[e15: Cr 93] Crespo, T.: Construction of $\widetilde{S}_4$-fields and modular forms of weight 1, *Proceedings of the Third Conference of the Canadian Number Theory Association,* Oxford University Press (1993). MR# 96j: 11070.

[e16: La 93] Lario, J.-C.: On Serre's conjecture ($3.2.4_?$) and vertical Weil curves, *Advances in number theory* (*Kingston, ON, 1991*), Gouvea, F. Q.; Yui, N., eds., Clarendon Press, Oxford, 1993, p. 281-291. Proceedings of the Third Conference of the Canadian Number Theory Association, 1991. MR# 96j: 11075.

[e17: La 92] Lario, J.-C.: Serre's conjecture on Galois representations attached to Weil curves with additive reduction, *Astérisque* 15, n. 209 (1992), p. 247-255. MR# 94f: 11034.

[e18: Ba 91] Bayer, P.: The Eichler-Shimura theorem and its non-archimedian analogues, *Mathematical Contributions to the Memory of V. Onieva* (1991), p. 27-34, Universidad de Cantabria. MR# 92f: 11074.

[e19: Ar 89] Arenas, A.: Quantitative aspects of the representations of integers by quadratic forms, *Number Theory,* J.-M. de Koninck; C. Levesque, eds., Walter de Gruyter (1989), p. 7-14. MR# 90k: 11037.

[e20: Ba 89] Bayer, P.: Embedding problems with kernel of order two, *Séminaire de Théorie des Nombres, Paris 1986-87,* Progress in Mathematics, 75, Birkhäuser (1989), p. 27-34. MR# 90e: 12004.

[e21: Ar 87] Arenas, A.: On positive integers representable as a sum of three squares, *Astérisque,* 147-148 (1987), p. 259-263, SMF. Proceedings of the 14èmes Journées Arithmétiques, Besançon 1985. MR# 89a: 11034.

[e22: Tr 86] Travesa, A.: Sobre el número de extensiones de grado dado de un cuerpo local, *Actas de las X Jornadas Hispano-Lusas de Matemáticas*, Murcia, Instituto Jorge Juan de Matemáticas (1986), p. 235-247. MR# 87h: 11117.

[e23: Vi 84-2] Vila, N.: Sur la résolution d'un problème de plongement, *Proceedings of the* 13*èmes Journées Arithmétiques,* Noordwijkerhout 1983, Springer, Lecture Notes in Mathematics 1068 (1984), p. 243-253. MR# 86c: 11098.

[e24: Vi 84-1] Vila, N.: Sur la réalisation des extensions centrales du groupe alterné comme groupe de Galois sur $\mathbb{Q}$, *Séminaire de Théorie des Nombres de Bordeaux,* (1983-84), p. 1801-1809. MR# 784 067.

[e25: Ba 73] Bayer, P.: Propiedades cohomológicas del anillo de los enteros de un cuerpo de números, *Actas de las Primeras Jornadas Matemáticas Hispano-Lusitanas,* Instituto Jorge Juan de Matemáticas, 1973, p. 284-290. Madrid. MR# 49 #7047.

15. Research articles published in Spanish journals

[f1: Go 98] Gonzàlez, J.: On the *p*-rank of an abelian variety and its endomorphism algebra, *Publicacions Matemàtiques UAB,* 42 (1998), p. 119-130.

[f2: Ve 98] Vela, M.: Graded algebra automorphisms, *Collectanea Mathematica,* 49, n. 2, 3 (1998), p. 549-564.

[f3: Na 91] Nart, E.: The formal completion of the Néron model of $J_0(p)$, *Publicacions Matemàtiques UAB,* 35 n. 2 (1991), p. 537-542. MR# 94f: 11053.

[f4: Ar 86] Arenas, A.: The concept of *K*-level for positive integers, *Publicacions Matemàtiques UAB,* 30, n. 1 (1986), p. 41– 48. MR# 89c: 11149.

[f5: Ar 84] Arenas, A.: On a certain type of primitive representations of rational integers as sum of squares, *Publicacions Matemàtiques UAB,* 28 (1984), p. 75-80. MR# 87g: 11044.

[f6: Na-Vi 80] Nart, E.; Vila, N.: A primitivity criterion, *Publicacions Matemàtiques UAB,* 20 (1980), p. 185-187. MR# 86h: 12003.

[f7: Ba 79] Bayer, P.: Sobre el índice de irregularidad de los números primos, *Collectanea Mathematica,* 30, n. 1 (1979), p. 11-20. MR# 81h: 12003.

[f8: Na-Vi 79] Nart, E.; Vila, N.: Equations of the type $X^n + aX + b$ with absolute Galois group S_n, *Revista de la Universidad de Santander,* 2, n. II (1979), p. 821-828. MR# 754 788.

[f9: Ba 76] Bayer, P.: Formas cuadráticas sobre cuerpos totalmente *p*-ádicos, *Publicacions Matemàtiques UAB,* 3 (1976), p. 1-15.

16. Recent contributions

This section contains references added in proof. They are not quoted in the text.

[a-2: Qu-99] Quer, J., ed.: *La conjectura de Birch i Swinnerton-Dyer,* STNB, Barcelona, 1999. ISBN: 84-923250-4-6.

[a-1: Ve-Vi 99] Vela, M.; Vila, N., eds.: *Problemes d'immersió sobre cossos grans*, STNB, Barcelona, 1999. ISNB: 84-923250-3-8.

[b-2: Al-00] Alsina, M.: *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura,* UB, 2000. Thesis (February 7, 2000). Thesis advisor: P. Bayer.

[b-1: Mo 00] Montes, J.: *Polígonos de Newton de orden superior y aplicaciones aritméticas,* UB, 2000. Thesis (February 7, 2000). Thesis advisor: E. Nart.

[d-1: Al 00] Alsina, M.: `Poincare.` Software package to deal with arithmetic in quaternion algebras and uniformization of Shimura curves. Implemented in Maple for PC-DOS and Windows systems. 2000.

[f-10: Al 00] Alsina, M.: Dominios fundamentales modulares, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-9: Ar-Ba 00-2] Arenas, A.; Bayer, P.: Heegner points on modular curves, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-8: Ar-Ba 00-1] Arenas, A.; Bayer, P.: Complex multiplication points on modular curves, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-7: Ba-Tr 00-3] Bayer, P.; Travesa, A.: Órdenes matriciales generados por grupos de congruencia, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-6: Ba-Tr 00-2] Bayer, P.; Travesa, A.: Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-5: Ba-Tr 00-1] Bayer, P.; Travesa, A.: Inmersiones de órdenes cuadráticos en el orden generado por $\Gamma_0(N)$, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-4: Go 00] González, J.: On the division polynomials of elliptic curves, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-3: Go 00] González, J.: Sobre *Q*-curvas asociadas a puntos racionales de curvas cocientes de $X_0(N)$, to appear in *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales,* (2000).

[f-2: Gu 00] Guàrdia, J.: A fundamental domain for the Fermat curves and their quotients, to appear in *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales,* (2000).

[f-1: Re-Vi 00] Reverter, A.; Vila, N.: Polynomials of Galois representations attached to elliptic curves, to appear in *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales,* (2000).

[-14: Cr-Ha 00-2] Crespo, T.; Hajto, Z.: Primitive unimodular groups of degree 2 as differential Galois groups, to appear in *Journal of Algebra*.

[-13: Cr-Ha 00-1] Crespo, T.; Hajto, Z.: Finite linear groups as differential Galois groups, *Prepublicacions de la Universitat Autònoma de Barcelona* n. 11/1998. Submitted for publication.

[-12: Di-Vi 00] Dieulefait, L.; Vila, N.: Projective linear groups as Galois groups over $\mathbb{Q}$ via modular representations, to appear in *Journal of Symbolic Computation.*

[-11: Go-La 00] González, J.: Lario, J-C.: The Manin ideal for modular $\mathbb{Q}$-curves. Submitted for publication.

[-10: Re-Vi 00-2] Reverter, A.; Vila, N.: Galois representations attached to the product of two elliptic curves, to appear in *Rocky Mountain Journal of Mathematics.*

[-9: Re-Vi 00-1] Reverter, A.; Vila, N.: Images of mod *p* Galois representations associated to elliptic curves. Submitted for publication.

[-8: Ve 00] Vela, M.: Obstruction to the solvability and explicit resolution of Galois embedding problems with cyclic kernel by means of generalized Clifford algebras. Submitted for publication.

[-7: Cr 99] Crespo, T.: Extensions cycliques de degré 8, *Comptes Rendus de l'Académie de Sciences de Paris,* 329 (1999), p. 753-756.

[-6: Go 99] González, J.: Isogenies of polyquadratic $\mathbb{Q}$-curves to their Galois conjugates. Submitted for publication.

[-5: Gu 99-5] Guàrdia, J.: Analytic invariants in Arakelov theory for curves, *Comptes Rendus de l'Académie de Sciences de Paris,* 329 (1999), p. 41-46.

[-4: Gu 99-4] Guàrdia, J.: Arakelov invariants of curves with large automorphism group. Submitted for publication.

[-3: Gu 99-3] Guàrdia, J.: A family of arithmetic surfaces of genus 3. Submitted for publication.

[-2: Gu 99-2] Guàrdia, J.: Explicit Geometry on a Family of Curves of Genus 3. Submitted for publication.

[-1: Gu 99-1] Guàrdia, J.: Arakelov computations in genus 3. Submitted for publication.

17. References

[1: Ba-Ri 98] Bayer, P.; Rio, A.: Dyadic exercises for octahedral extensions, *Journal für die reine und angewandte Mathematik*, 517 (1999), p. 1-17.

[2: Br-La 98] Brunat, J. M.; Lario, J.-C.: Galois Graphs: Walks, Trees, and Automorphisms, 10 (1999), p. 135-148.

[3: CGLR 98] Cardona, G.; Gonzàlez, J.; Lario, J.-C; Rio, A.: On curves of genus 2 with jacobian variety of GL_2-type, *Manuscripta Mathematica,* 98 (1999), p. 37-54.

[4: Cr 98] Crespo, T.: Construction of $2^m S_n$-fields containing a C_{2m}-field, *Journal of Algebra,* 201 (1998), p. 233-242.

[5: Go 98-2] Gonzàlez, J.: On the *j*-invariants of quadratic $\mathbb{Q}$-curves. Submitted for publication. 1998.

[6: Go 98-1] Gonzàlez, J.: Fermat jacobians of prime degree over finite fields, *Canadian Mathematical Bulletin,* 42, n. 1 (1999), p. 78-86.

[7: Go-La 98] Gonzàlez, J.; Lario, J.-C.: Rational and elliptic parametrizations of $\mathbb{Q}$-curves, *Journal of Number Theory,* 72, n. 1 (1998), p. 13-31.

[8: Qu 98] Quer, J.: La classe de Brauer de l'algèbre d'endomorphismes d'une variété abélienne modulaire, *Comptes Rendus de l'Académie de Sciences de Paris,* 327, n. 3 (1998), p. 227-230.

[9: Ba-Go 97] Bayer, P.; Gonzàlez, J.: On the Hasse-Witt invariants of modular curves, *Experimental Mathematics*, 6, n. 1 (1997), p. 57-76. MR# 98h: 11074.

[10: Go 97] Gonzàlez, J.: Hasse-Witt matrices for the Fermat curves of prime degree, *Tohoku Mathematical Journal,* 49, n. 2 (1997), p. 149-163. MR# 98b: 11064.

[11: Bo-Xa 96] Bosch, S.; Xarles, X.: Component groups of Néron models via rigid uniformization, *Mathematische Annalen,* 306, n. 3 (1996), p. 459-486. MR#97f: 14022.

[12: La-Ri 96] Lario, J.-C.; Rio, A.: Elliptic modularity for octahedral Galois representations, *Mathematical Research Letters*, 3, n. 3 (1996), p. 329-342. MR# 97d: 11088.

[13: Ar 95] Arenas, A.: Genera and rational equivalence classes of integral quadratic forms, *Journal of Number Theory,* 51, n. 2 (1995), p. 210-218. MR# 96b: 11047.

[14: Cr 95-2] Crespo, T.: Galois realization of central extensions of the symmetric group with kernel a cyclic 2-group, *Acta Arithmetica,* 70 (1995), p. 183-192. M# 96d: 12004.

[15: Cr 95-1] Crespo, T.: C_4-extensions of S_n as Galois groups, *Mathematica Scandinavica,* 76 (1995), p. 214-220. MR# 96k: 12008.

[16: De-Na 95] Deninger, C.; Nart, E.: On Ext^2 of motives over arithmetic curves, *American Journal of Mathematics,* 117, n. 3 (1995), p. 601-625. MR# 96c: 14017.

[17: La-Ri 95] Lario, J.-C.; Rio, A.: An octahedral-elliptic type equality in $Br_2(k)$, *Comptes Rendus de l'Académie de*

Sciences de Paris, 321, n. 1 (1995), p. 39-44. MR# 96i: 11121.

[18: Qu 95] Quer, J.: Liftings of projective 2-dimensional Galois representations and embedding problems, *Journal of Algebra,* 171 (1995), p. 541-566. MR# 96b: 12009.

[19: Co 94-2] Comalada, S.: On the Weierstrass class of semistable elliptic curves over quadratic fields, *Bulletin of the London Mathematical Society,* 26, n. 2 (1994), p. 137-139. MR# 95b: 11056.

[20: Co 94-1] Comalada, S.: Twists and reduction of an elliptic curve, *Journal of Number Theory,* 49, n. 1 (1994), p. 45-62. MR# 95g: 11047.

[21: Cr 94] Crespo, T.: Central extensions of the alternating group as Galois groups, *Acta Arithmetica,* 66 (1994), p. 229-236. MR# 95f: 12008.

[22: Na 93] Nart, E.: Formal group laws for certain formal groups arising from modular curves, *Compositio Mathematica,* 85, n. 1 (1993), p. 109-119. MR3 93k: 11058.

[23: Xa 93] Xarles, X.: The scheme of connected components of the Néron model of an algebraic torus, *Journal für die reine und angewandte Mathematik,* 437 (1993), p. 167-179. MR# 94d: 14044.

[24: Ba-La 92] Bayer, P.; Lario, J.C.: On Galois representations defined by torsion points of modular elliptic curves, *Compositio Mathematica,* 84, n. 1 (1992), p. 71-84. MR# 93j: 11031.

[25: Co-Na 92] Comalada, S.; Nart, E.: Modular invariant and good reduction of elliptic curves, *Mathematische Annalen,* 293, n. 2 (1992), p. 331-342. MR# 93g: 11058.

[26: Cr 92] Crespo, T.: Extensions de A_n par C_4 comme groupe de Galois, *Comptes Rendus de l'Académie de Sciences de Paris,* 315 (1992), p. 625-628. MR# 93i: 12007.

[27: Mo-Na 92] Montes, J.; Nart, E.: On a theorem of Öre, *Journal of Algebra,* 146, n. 2 (1992), p. 318-334. MR# 93f: 11077.

[28: Ar 91-2] Arenas, A.: A note on representations of integers by some ternary quadratic forms, *Indian Journal of Mathematics,* 33, n. 3 (1991), p. 269-274. MR# 96a: 11034.

[29: Ar 91-1] Arenas, A.: Rational equivalence of primitive integral binary quadratic forms, *Proceedings of the Royal Society of Edinburg,* 118 (1991), p. 157-160. MR# 93d: 11041.

[30: Ba-Fr 91] Bayer, P.; Frey, G.: Galois representations of octahedral type and 2-coverings of elliptic curves, *Mathematische Zeitschrift,* 207, n. 3 (1991), p. 395-408. MR# 92d: 11058.

[31: Cr 91] Crespo, T.: Embedding Galois problems and reduced norms, *Proceedings of the American Mathematical Society,* 112 (1991), p. 637-639. MR# 91j: 11021.

[32: Go 91] Gonzàlez, J.: Equations of hyperelliptic modular curves, *Annales de l'Institut Fourier,* 41, n. 4 (1991), p. 779-795. MR# 93g: 11064.

[33: Llo-Na-Vi 91] Llorente, P.; Nart, E.; Vila, N.: Decomposition of primes in number fields defined by trinomials, *Séminaire de Théorie des Nombres de Bordeaux,* 3, n. 1 (1991), p. 27-41. MR# 92j: 11124.

[34: Na-Xa 91] Nart, E.; Xarles, X.: Additive Reduction of Algebraic Tori, *Archiv der Mathematik,* 57, n. 5 (1991), p. 460-466. MR# 92m: 14056.

[35: Co 90-2] Comalada, S.: Elliptic curves with trivial conductor over quadratic fields, *Pacific Journal of Mathematics,* 144, n. 2 (1990), p. 237-258. MR# 91e: 11058.

[36: Co 90-1] Comalada, S.: Courbes elliptiques à bonne réduction d'invariant *j* fixé, *Comptes Rendus de l'Académie de Sciences de Paris,* 311, n. 11 (1990), p. 667-670. MR# 91j: 11044.

[37: Cr 90-2] Crespo, T.: Explicit solutions to embedding problems associated to orthogonal Galois representations, *Journal für die reine und angewandte Mathematik,* 409, (1990), p. 180-189. MR# 91j: 11020.

[38: Cr 90-1] Crespo, T.: Explicit construction of $2S_n$ Galois extensions, *Journal of Algebra,* 129, (1990), p. 312-319. MR# 91d: 11135.

[39: De-Na 90] Deninger, C.; Nart, E.: Formal groups and *L*-series, *Commentarii Mathematici Helvetici,* 65, n. 2 (1990), p. 318-333. MR# 91i: 14036.

[40: Tr 90-2] Travesa, A.: Generating functions for the number of abelian extensions of a local field, *Proceedings of the American Mathematical Society,* 108, n. 2 (1990), p. 331-339. MR# 90m: 11187.

[41: Tr 90-1] Travesa, A.: Nombre d'extensions abéliennes sur $\mathbb{Q}$, *Séminaire de Théorie des Nombres de Bordeaux,* 2, n. 2 (1990), p. 413-423. MR# 92a: 11122.

[42: Vi 90] Vila, N.: Local Artin root numbers associated to some classical polynomials, *Journal of Algebra,* 131, n. 11 (1990), p. 678-687. MR# 91e: 11043.

[43: Ar 89] Arenas, A.: On some equivalences of positive definite binary quadratic forms, *Proceedings of the Royal Society of Edinburg,* 113 (1989), p. 211-213. MR# 91e: 11038.

[44: Ba-Na 89] Bayer, P.; Nart, E.: Zeta functions and equivalence of quadratic forms, *L'Enseignement Mathématique,* 35, n. 3-4 (1989), p. 263-287. MR# 91e: 11040.

[45: Cr 89-2] Crespo, T.: Embedding problems with ramification conditions, *Archiv der Mathematik,* 53 (1989), p. 270-276. MR# 90k: 11145.

[46: Cr 89-1] Crespo, T.: Explicit construction of $\tilde{A}_n$-type fields, *Journal of Algebra,* 127 (1989), p. 452-461. MR# 91a: 12006, and MR# 94c: 12005.

[47: Na 89] Nart, E.: The Bloch complex in codimension one and arithmetic duality, *Journal of Number Theory,* 32, n. 3 (1989), p. 321-331. MR# 90j: 11057.

[48: Tu-Vi 89] Turull, A.; Vila, N.: On rigid equations of alternating groups and their Hasse-Witt invariants, *Journal of Algebra,* 125, n. 2 (1989), p. 431-443. MR# 90m: 11172.

[49: Ar 88] Arenas, A.: An arithmetic problem on the sum of

three squares, *Acta Arithmetica,* 51 (1988), p. 131-140. MR# 90c: 11070.

[50: Di-Llo-Qu 88] Díaz y Díaz, F.; Llorente, P.; Quer, J.: Cubic fields, a congruential criterion for Scholz's theorem and new real quadratic fields with 3-rang equal 4, *Archiv der Mathematik,* 50, n. 4 (1988), p. 356-359. MR# 89d: 11097.

[51: Llo-Qu 88-2] Llorente, P.; Quer, J.: On Totally Real Cubic Fields with Discriminant $D < 10^7$, *Mathematics of Computation,* 50, n. 182 (1988), p. 581-594. MR# 89g: 11099.

[52: Llo-Qu 88-1] Llorente, P.; Quer, J.: On the 3-Sylow subgroup of the class group of quadratic fields, *Mathematics of Computation,* 50, n. 181 (1988), p. 321-333. MR# 89b: 11083.

[53: Vi 88] Vila, N.: On stem extensions of S_n as Galois group over number fields, *Journal of Algebra,* 116, n. 1 (1988), p. 251-260. MR# 89g: 11107.

[54: Ar 87-2] Arenas, A.: On the summation of the singular series, *Manuscripta Mathematica,* 57 (1987), p. 469-475. MR# 88f: 11100.

[55: Ar 87-1] Arenas, A.: On integral representations by quadratic forms, *Linear and Multilinear Algebra,* 22 (1987), p. 149-160. MR# 89g: 15032.

[56: Ar-Ba 87] Arenas, A.; Bayer, P.: Arithmetic behaviour of the sum of three squares, *Journal of Number Theory,* 27, n. 3 (1987), p. 273-284. MR# 89c: 11053.

[57: Co-Na 87] Comalada, S.; Nart, E.: Courbes elliptiques avec bonne réduction partout, *Comptes Rendus de l'Académie de Sciences de Paris,* 305, n. 6 (1987), p. 223-224. MR# 88h: 11038.

[58: Qu 87] Quer, J.: Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, *Comptes Rendus de l'Académie de Sciences de Paris,* 305, n. 6 (1987), p. 215-218. MR# 88j: 11074.

[59: Ba-Llo-Vi 86] Bayer, P.; Llorente, P.; Vila, N.: M_{12} comme groupe de Galois sur $\mathbb{Q}$, *Comptes Rendus de l'Académie des Sciences de Paris,* 303, n. 7 (1986), p. 277-280. MR# 87m: 11111.

[60: Na 85] Nart, E.: On the index of a number field, *Transactions of the American Mathematical Society,* 289 (1985), p. 171-183. MR# 86h: 11082.

[61: Vi 85-2] Vila, N.: Polynomials over $\mathbb{Q}$ solving an embedding problem, *Annales de l'Institut Fourier,* 131, (1985), p. 79-83. MR# 86h: 11100.

[62: Vi 85-1] Vila, N.: On central extensions of A_n as Galois group over $\mathbb{Q}$, *Archiv der Mathematik,* 44, n. 5 (1985), p. 424-437. MR# 87b: 11111.

[63: Llo-Na-Vi 84] Llorente, P.; Nart, E.; Vila, N.: Discriminants of number fields defined by trinomials, *Acta Arithmetica,* 43 (1984), p. 367-373. MR# 85m: 11070.

[64: Llo-Na 83] Llorente, P.; Nart, E.: Effective determination of the decomposition of the rational primes in a cubic field, *Proceedings of the American Mathematical Society,* 87 (1983), p. 579-583. MR# 84d: 12003.

[65: Na-Vi 83] Nart, E.; Vila, N.: Equations with absolute Galois group isomorphic to A_n, *Journal of Number Theory,* 16 (1983), p. 6-13. MR# 85b: 11081.

[66: Ba-Ne 81] Bayer, P.; Neukirch, J.: On Automorphic Forms and Hodge Theory, *Mathematische Annalen,* 257, n. 2 (1981), p. 137-155. MR# 83a: 10045.

[67: Ba 79] Bayer, P.: Values of the Iwasawa *L*-functions at the point $s = 1$, *Archiv der Mathematik,* 32, n. 1 (1979), p. 38-54. MR# 80h: 12016.

[68: Ba-Ne 78] Bayer, P.; Neukirch, J.: On values of zeta functions and *l*-adic Euler characteristics, *Inventiones mathematicae,* 50, n. 1 (1978), p. 35-64. MR# 80b: 12009.

Acknowledgements

Many other people have collaborated in the STNB activities along these years. We take this opportunity to thank them all. Special thanks are due to professors E. Linés and J. Neukirch (both deceased), and P. Llorente for their guidance to the founder members of the STNB.

About the authors

The Seminari de Teoria de Nombres (UB-UAB-UPC) is made up of scientific personnel from three universities: Universitat de Barcelona (UB), Universitat Autònoma de Barcelona (UAB), and Universitat Politècnica de Catalunya (UPC). The STNB began as a research group in 1986 and has organized activities every year since . At present, several graduate students are writing their Ph. D. theses supervised by doctors in the group.

The research activity of the group is focussed on algebraic number theory and arithmetic algebraic geometry. The involved techniques are quadratic forms, Galois theory, modular curves, elliptic curves, abelian varieties, curves over finite, local and global fields, automorphic forms and arithmetic varieties and schemes.

In 1995, the STNB organized in Barcelona the 19èmes Journées Arithmétiques, a forum for presentation and discussion of recent number-theoretical developments with a long tradition and recognized as the main international meeting devoted to number theory. Among the universities or research institutes where members of the STNB have been working during substantial periods of time are: Berkeley, Bombay, Bonn, Essen, Freiburg, Harvard, Kraków, La Habana, Luminy, Mar del Plata, McGill, Oberwolfach, Princeton, Regensburg, Santander, Tokyo-Chuo, and Tokyo-Waseda.