Vernieuwingsimpuls / Innovational Research
Grant application form (detailed proposal) 2004 VICI scheme

Registration form (basic details)

1a. Details of applicant

Name, title(s): Bas Edixhoven, Prof. dr.
Male/female: male
Address for correspondence: Mathematisch Instituut, Postbus 9512, 2300 RA Leiden, The Netherlands
Telephone: +31-71-527-7136
Fax: +31-71-527-7101
E-mail: edix@math.leidenuniv.nl
Website: `http://www.math.leidenuniv.nl/~edix/`
Preference for English correspondence: no
Doctorate (date): June 5, 1989.
Use of extension clause: no

1b. Title of research proposal

Arithmetic geometry, motives: computational aspects.

1c. Summary of research proposal (max. 300 words, plus max. 5 keywords)

The research focuses on the problem of efficiently counting the solutions of systems of polynomial equations over finite fields. An important example is the following. For a prime number p and integers a and b one asks for the number of pairs of integers (x, y) with $0 \leq x < p$ and $0 \leq y < p$ such that p divides $-y^2+x^3+ax+b$. In 1984, Schoof published an algorithm for computing these numbers using about $(\log p)^9$ bit operations. This algorithm has become the basis for elliptic curve cryptography, one of today's most promising cryptosystems, with practical applications in e-commerce, smart-cards, and wherever cryptography is used.

For general systems, counting the solutions is intractable: there is no polynomial time algorithm, i.e., one that uses only a number of bit operations that is at most a fixed power of the length of the input. However, if the number of variables and the degrees of the equations are fixed, polynomial time algorithms might exist.

The goal of this proposal is to find such algorithms, making use of the most advanced techniques in arithmetic geometry that are currently available. Apart from its applications to cryptography, this proposal will help make these techniques, which have a reputation of being extremely abstract and complex, available computationally.

The main tool for counting solutions is cohomology. Schoof uses first degree étale cohomology. The goal of this proposal is to open hitherto inaccessible higher étale cohomology for computation. In December 2000, Edixhoven proposed a novel strategy for the case of motives associated to modular forms. If successful, an important by-product will be a polynomial algorithm for computing étale cohomology with its Galois action. This pioneering strategy, using Arakelov theory to estimate the required precision of the numerical computations, links arithmetic geometry to numerical analysis, computer algebra and number theory.

Keywords: finite fields, motives, higher étale cohomology, computational aspects, Arakelov geometry.

1d. NWO Council area: EW ("Exacte wetenschappen").

1e. Host institution: University of Leiden.

Research proposal

2. Description of the proposed research (max. 8000 words on max. 16 pages (exclusive 2e and 2f); a description of subprojects (for additional postdocs and PhD students) is required)

2.a. Research topic

The research will take place in the sub-field arithmetic algebraic geometry of mathematics. Its most innovative part concerns the complexity of the problem of counting the solutions of certain systems of polynomial equations over finite fields.

The simplest finite fields are the prime fields $\mathbb{F}_p$, with p a prime number; they are obtained by performing the usual operations (addition, subtraction, multiplication and division) on integers, modulo p. For example, the field $\mathbb{F}_2$ consists of the elements 0 and 1, and has the property $1 + 1 = 0$ (familiar from logic). The number of elements of an arbitrary finite field is a power of a prime number, i.e., of the form p^n. For every integer q of this form there exists an essentially unique finite field of that size, with "essentially" meaning that two finite fields of the same size are isomorphic. We will denote such a field by $\mathbb{F}_q$.

A system of polynomial equations over a finite field $\mathbb{F}_q$ looks as follows:

$$\begin{aligned} f_1(x_1, x_2, \ldots, x_n) &= 0 \\ f_2(x_1, x_2, \ldots, x_n) &= 0 \\ &\vdots \\ f_r(x_1, x_2, \ldots, x_n) &= 0. \end{aligned}$$

The x_i are the variables, and each f_j is a polynomial in the x_i, with coefficients in $\mathbb{F}_q$, i.e., a finite sum of terms of the form $ax_1^{d_1} \cdots x_n^{d_n}$ with a in $\mathbb{F}_q$ and the d_i integers greater than or equal to zero. The set of solutions in $\mathbb{F}_q$ of this system of equations is the set of $n$tuples $(a_1, \ldots, a_n)$, with the a_i in $\mathbb{F}_q$, such that $f_j(a_1, \ldots, a_n) = 0$ for all j.

The problem that one wants to solve is that of determining, in a *reasonable* amount of time (or, equivalently, of bit operations), the *number* of solutions (and not the solutions themselves) for certain systems of polynomial equations over finite fields. More precisely, one would like to have an algorithm giving the number of solutions in time at most some fixed power of the length of the input (i.e., a polynomial time algorithm).

For the class of all systems, even the problem of deciding whether or not a solution exists is known to be unfeasible: in terms of complexity theory this problem is called NP-complete. To see this, one notes that for $q = 2$ the problem becomes that of deciding whether or not a Boolean expression in the variables $x_1, \ldots, x_n$ can be satisfied, a problem known under the name SAT, and known to be NP-complete (Cook's theorem, see [17]). As a consequence, one really expects that no polynomial

time algorithm exists for the class of all systems. On the other hand, there are important sub-classes where polynomial time algorithms do exist.

In the classes to be considered in this proposal, one fixes the number of variables, and possibly the degrees of the equations, but *not* the size q of the finite field. The problem is then to find algorithms giving the number of solutions in time polynomial in the logarithm of q and in the degrees of the equations.

Around 1984, Schoof found a polynomial time algorithm for the case of one equation of degree three in two variables x and y:

$$y^2 = x^3 + ax + b,$$

the case of elliptic curves (see [21]). More precisely, his algorithm uses about $(\log q)^9$ bit operations. After some substantial improvements by Atkin and Elkies (see [6]) that reduced the number of bit operations to about $(\log q)^4$ when q is a prime number, Schoof's algorithm has become the basis of elliptic curve cryptography, one of today's most promising cryptographic systems, with practical applications in e-commerce, smart-cards and wherever cryptography is used. For finite fields $\mathbb{F}_q$ with $q = p^n$ and p small the same reduction of the number of bit operations was achieved by Couveignes (see [2]).

Recently, progress has been made by Satoh [19], Kedlaya [11], Wan and Lauder [14, 15, 12], Fouquet, Gaudry, Gürel and Harley [9, 10], and Denef and Vercauteren [5] in the case where one fixes the characteristic p of the finite field $\mathbb{F}_q$ (the prime number p of which q is a power). Let us write $q = p^m$. Using a so-called p-adic method (more on this will be said later) Satoh obtained an algorithm for counting points on elliptic curves over $\mathbb{F}_q$ in about m^3 bit operations, hence improving on the work of Schoof, Atkin and Elkies. By a more abstract cohomological approach, Kedlaya succeeded in treating the case of hyper-elliptic curves for p different from 2:

$$y^2 = f(x),$$

where f has arbitrary degree, in time $m^3 \deg(f)^4$. Fouquet, Gaudry, Gürel, Harley, Denef and Vercauteren have generalized Kedlaya's approach to more general types of curves:

$$y^d = f(x), \quad y^p - y = f(x), \quad \text{etc.},$$

with similar running times. Wan and Lauder, approaching the problem from the point of view of p-adic exponential sums and Dwork's trace formula, have given a polynomial time algorithm for the class of all systems of polynomial equations in a fixed number of variables. For certain types of curves they have optimized their arguments, and have obtained algorithms with a running time similar to those obtained by the authors above.

Summarizing this recent progress, one can say that, at least from a theoretical point of view, the problem of counting the solutions of systems of polynomial equations over finite fields of a fixed characteristic p and in a fixed number of variables has been solved. However, if p is not bounded, then almost nothing is known about the existence of polynomial algorithms. The p-adic methods lead to algorithms of which the running time grows at least linearly in p, hence exponentially in $\log p$, even for elliptic curves. Schoof's original approach has been applied to curves and abelian varieties by Pila (see [18]), giving a polynomial time algorithm when the dimension of the abelian variety, or the genus of the curve, is fixed. As Pila makes use of explicit systems of equations for abelian varieties, his algorithm behaves extremely badly as a function of the dimension of the abelian variety, and hence, in the case of curves, as a function of the genus of the curve.

This is an appropriate point to state one of the main objectives of this research proposal:

> one main objective is to find polynomial time algorithms for counting the number of solutions of systems of polynomial equations over finite fields, where the number of variables is fixed.

The innovative element of this objective is that there is no restriction on the characteristic of the finite field. The methods that we will use for achieving this objective lead to some other important applications that will be stated below, when we explain our approach.

The proposed research is important for cryptography, because of its relation to Schoof's algorithm. If some day elliptic curve cryptography is broken, or admits a sub-exponential attack, our research might provide a solution. More generally speaking, making the cohomological machinery that we will discuss below available algorithmically is a fundamental and important problem. This project will help researchers from other areas of mathematics and other sciences apply the powerful but abstract results from algebraic geometry. Moreover, it will provide many occasions for mutually fruitful collaborations with other mathematicians in the Netherlands (algebraic geometers, the number theory group in Leiden, EIDMA, ...).

2.b. Approach

It seems impossible to avoid a higher level of technicality in this section. In order to give the less initiated reader at least some idea of the originality and innovative elements of the methods that we want to use, we start by giving a short description.

The usual tool for counting solutions efficiently is cohomology: the number of solutions is the number of fixed points of the so-called Frobenius morphism, and is equal to the alternating sum of the traces of the Frobenius morphism on the cohomology groups. Schoof uses étale cohomology of degree one with coefficients modulo small prime numbers l, in the form of points of order l on elliptic curves. For small p, the p-adic methods alluded to above use p-adic cohomologies, which are closely related to de Rham cohomology. These p-adic cohomologies are computationally tractable, but lead to polynomial time algorithms only for finite fields of small characteristic. At present, there are no good algorithms for computing higher degree étale cohomology with Frobenius action, and to find such is an important problem in algorithmic number theory. The proposed research aims to provide such algorithms, which is a second main objective of this proposal:

> a second main objective is to find a polynomial algorithm for computing higher degree étale cohomology with Frobenius action.

We stress that the aim is to compute not only the dimensions of cohomology spaces, but also the Frobenius action on them, which means computation of (realizations of) motives.

A natural starting point is then to study the simplest kinds of motives for which there are no polynomial algorithms (yet): rank two motives over the rational numbers, of (pure) weight at least two (elliptic curves correspond to weight one). Conjecturally (Langlands's program) such motives correspond to modular forms. In December 2000, Edixhoven gave a talk at the MSRI in Berkeley where he sketched a novel strategy for treating this case. (For notes and a streaming video of this lecture, please visit the section "quelques exposés" on Edixhoven's personal web page.) This strategy also leads to a third main objective of this proposal:

> a third main objective is the computation of the mod l Galois representations associated to modular forms, in time polynomial in l.

For example, this would show that Ramanujan's τ-function can be evaluated at p in time polynomial in $\log p$. The strategy consists in a reduction to torsion points on Jacobian varieties (of dimension

quadratic in l) and a careful distinction between symbolic and numeric parts of the computation. The method can already be used experimentally, but one still needs a bound on the precision required in the numerical part. The results that are needed to provide such a bound have an analog in the function field case, where the classical Grothendieck-Riemann-Roch formula provides a proof. We expect that the analogous formula in Arakelov theory can be applied successfully, but much work needs to be done. This test case, already important in itself, should give the right ideas for more general cases. The generalization to higher étale cohomology groups of small dimension should not be too hard. On the other hand, treating curves of arbitrary genus still requires new ideas, because the dimension of the relevant cohomology group is not bounded.

Let us now give more details on the methods to be used, at a level intended for experts in arithmetic algebraic geometry. For simplicity, we will just discuss the case of the motive corresponding to the modular form Δ. We recall that Δ is the function on the complex upper half plane $\mathbb{H}$ given by the formula:

$$\Delta = \sum_{n\geq 1} \tau(n) q^n = q \prod_{n\geq 1} (1-q^n)^{24},$$

where q is the function sending z to $\exp(2\pi i z)$. This function Δ is such that $\Delta(dq/q)^{\otimes 6}$ is invariant for the usual action by $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by fractional linear transformations. In other words, Δ is a cusp form of weight 12 and level 1. As the space of such forms is one-dimensional, Δ is an eigenform for the Hecke operators T_n, meaning that the L-function of Δ has the following Euler product expansion:

$$L_\tau(s) = \sum_{n\geq 1} \tau(n) n^{-s} = \prod_p (1 - \tau(p)p^{-s} + p^{11}p^{-2s})^{-1},$$

where p ranges over all prime numbers and where the real part of s is at least $13/2$. By a theorem of Deligne (see [3 and 20]), L_τ is the L-function of a pure motive M_Δ of weight 11 and rank 2 over $\mathbb{Q}$ with good reduction at all primes. More precisely, M_Δ is a piece of the dual of the cohomology of degree 11 of the 10-fold product E^{10} of the universal elliptic curve $f\colon E \to Y$ over the moduli space Y of elliptic curves, and $\Delta\,(dq/q)dz_1 \cdots dz_{10}$ generates half of the de Rham realization of M_Δ. It follows that for each prime number l, there exists a two-dimensional $\mathbb{F}_l$-vector space V_l with continuous action by the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, unramified at all primes $p \neq l$, such that the trace of Frobenius at p is the image of $\tau(p)$ in $\mathbb{F}_l$. In fact, V_l is just the dual of the mod l étale realization of M_Δ.

Following Schoof, the idea is now to compute $\tau(p)$ mod l for sufficiently many small primes l, such that the product P of those l is at least $4p^{11/2}$. Then one knows $\tau(p)$ because one knows it modulo P and one knows that $|\tau(p)| \leq 2p^{11/2}$ (Ramanujan's inequality, proved by Deligne [4]). Analytic number theory implies that one only needs to take prime numbers l of size at most about $6\log p$. Hence the problem of computing $\tau(p)$ in time polynomial in $\log p$ is reduced to computing V_l with its Galois action, either of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ or of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, in time polynomial in l.

Now the dual $V_l^\vee$ of V_l is a subspace of the degree 11 étale cohomology of the 11-dimensional variety E^{10} over $\overline{\mathbb{Q}}$. Elements of such cohomology groups, constructed via injective resolutions, do not have any direct interpretation suitable for computation. Fortunately, via the morphism $E^{10} \to Y$, $V_l^\vee$ also occurs in $\mathrm{H}^1(Y_{\overline{\mathbb{Q}}}, \mathcal{F}_l)$, with $\mathcal{F}_l = \mathrm{Sym}^{10}\,\mathrm{R}^1 f_* \mathbb{F}_l$. Hence, at the price of replacing the constant coefficients $\mathbb{F}_l$ on E^{10} by the non-constant sheaf $\mathcal{F}_l$ on the curve Y, one has reduced the problem to a first degree étale cohomology group on a curve. The elements of $\mathrm{H}^1(Y_{\overline{\mathbb{Q}}}, \mathcal{F}_l)$ are the isomorphism classes of $\mathcal{F}_l$-torsors on $Y_{\overline{\mathbb{Q}}}$. One can show that such objects admit a suitable explicit representation and can be used for computations, *once one has solved the equations for finding them.* But, as we do not know how to find these torsors in polynomial time, a second reduction is needed.

By definition, the sheaf $\mathrm{R}^1 f_* \mathbb{F}_l$ becomes an extension of $\mathbb{F}_l$ by $\mu_l^\vee$ over the cover $Y_1(l) \to Y$ of degree $l^2 - 1$. This explains that V_l is a subspace of $J_1(l)(\overline{\mathbb{Q}})[l]$, where $J_1(l)$ is the Jacobian variety of the compactification $X_1(l)$ of $Y_1(l)$. This subspace is the intersection of the kernels of the endomorphisms $T_q - \tau(q)$ for q prime, $q \leq l^2/24$. Hence at the cost of replacing Y by $X_1(l)$, we have replaced the non-constant sheaf $\mathcal{F}_l$ by $\mathbb{F}_l$. The price we pay is that $X_1(l)$ has genus about $l^2/24$, hence the computations concerning the l-torsion of $J_1(l)$ will have to be done in polynomial time in the genus of $X_1(l)$. This seems impossible to do, if one approaches this problem algebraically.

Couveignes has suggested to use numerical analysis and algebraic number theory, via the following strategy. The $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on V_l defines a finite Galois extension $\mathbb{Q} \to K_l$, with group the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}(V_l)$. All we need to do is to find the minimal polynomial f_α over $\mathbb{Q}$ of some generator α of K_l of reasonable height, since then we find the Frobenius element at p by factoring f_α over $\mathbb{F}_p$. To achieve that, it is enough to have a sufficiently good approximation α' (in the complex numbers, say) of α, with respect to the height of the algebraic number α (there are good algorithms to compute f_α from α', see [1, §2.7.2]). For example, to know a rational number a/b with a and b integers of absolute value at most some number M, it is enough to know it up to an error of at most $1/2M^2$. It is important to understand that only α' needs to be known explicitly, together with a bound on the height of α.

In order to make Couveignes's strategy work, we have to explain how we want to choose α such that its height is small enough, and how to approximate it. First we choose a non-zero element x of V_l, viewing V_l as the subspace of $\mathrm{H}_1(X_1(l)(\mathbb{C}), \mathbb{F}_l)$ cut out by the Hecke operators $T_q - \tau(q)$ with q prime, $q \leq l^2/24$; this is computable in time polynomial in l with say modular symbols algorithms. Then we note that it suffices to produce a suitable generator α in the field of definition $\mathbb{Q}(x)$ of x, when viewing x as an element of $J_1(l)(\overline{\mathbb{Q}})[l]$, since K_l is the Galois closure of $\mathbb{Q}(x)$. The idea is now to view x as the class of some divisor on $X_1(l)_{\overline{\mathbb{Q}}}$ with the same field of definition as x, and to take for α the evaluation of some function on $X_1(l)_{\mathbb{Q}}$ on that divisor. More precisely, one proceeds as follows. We let g denote the genus and P_0 a rational cusp of $X_1(l)$. Then we have diagram:

$$X_1(l)(\mathbb{C})^g \longrightarrow\!\!\!\!\!\!\rightarrow J_1(l)(\mathbb{C}) = \mathbb{C}^g/\Lambda$$

$$(Q_1, \ldots, Q_g) \longmapsto [Q_1 + \cdots + Q_g - gP_0] = \sum_{i=1}^{g} \int_{P_0}^{Q_i} (\omega_1, \ldots, \omega_g),$$

where the $(\omega_1, \ldots, \omega_g)$ is a $\mathbb{Z}$-basis of $\mathrm{H}^0(X_1(l)_{\mathbb{Z}}, \Omega)$, and where Λ is the period lattice of this basis, i.e., the image of $\mathrm{H}_1(X_1(l)(\mathbb{C}), \mathbb{Z})$ under integration of the ω_i. Here one chooses the ω_i such that Λ has a $\mathbb{Z}$-basis of reasonably small elements. Now x is an element of $l^{-1}\Lambda/\Lambda \subset \mathbb{C}^g/\Lambda$, and we want to choose $(Q_1, \ldots, Q_g)$ such that its image in $\mathbb{C}^g/\Lambda$ is x. Let $\mathcal{L}$ denote the line bundle on $X_1(l)_{\mathbb{C}}$ corresponding to x. Then $\mathcal{L}(gP_0)$ is a line bundle of degree g, hence it almost certainly has the property that $\mathrm{H}^0(X_1(l)_{\mathbb{C}}, \mathcal{L}(gP_0))$ is of dimension one. (The line bundles of degree g that do not have this property form a subset of complex codimension one.) We assume for the moment that $\mathrm{H}^0(X_1(l)_{\mathbb{C}}, \mathcal{L}(gP_0))$ is one-dimensional. Then, up to permutation, there is a unique g-tuple $(Q_1, \ldots, Q_g)$ mapping to x, and we put $\alpha := j(Q_1) + \cdots + j(Q_g)$, where j is the standard j-function on $X_1(l)_{\mathbb{Q}}$. Then α is in $\mathbb{Q}(x)$, and almost certainly a generator. The height of the divisor $Q_1 + \cdots + Q_g$ cannot be too large because it is equivalent to the point x, whose height is zero because it is a torsion point. Consequently, the height of α cannot be large. To approximate α, one can numerically lift the straight line from 0 to x in a fundamental domain in $\mathbb{C}^g$ to a path in $X_1(l)(\mathbb{C})^g$ starting at $(P_0, \ldots, P_0)$. As the map from $X_1(l)(\mathbb{C})^g$

to $J_1(l)(\mathbb{C})$ is étale outside a subset of real codimension at least two, it is almost certainly étale over that straight line, which means that the lifting problem can be solved by say Newton's method.

This method for producing and approximating α is not completely satisfactory because of the "almost certainly" that occurs three times. Also, in the numerical part, the straight line in question should in fact not get too close to the ramification locus. For this reason, we propose to "randomize" the method as follows. We choose at random $P_1, \ldots, P_g$ in $X_1(l)(K)$, corresponding to elliptic curves lying in one isogeny class, with complex multiplications, for example by $\mathbb{Q}(i)$. Then K is a solvable Galois extension of $\mathbb{Q}$. If one chooses the P_i reasonably, the degree of K and the logarithm of discriminant of K are polynomial in l. We put $D := P_1 + \cdots + P_g$, which is a divisor on $X_1(l)_K$. Now we may assume that $\mathrm{H}^0(X_1(l)_{\mathbb{C}}, \mathcal{L}(D))$ is one-dimensional. Hence there is a unique effective divisor D' of degree g on $X_1(l)_{K(x)}$ such that $\mathcal{L} \cong \mathcal{O}_{X_1(l)_{\mathbb{C}}}(D' - D)$. Then we put $\alpha := j(Q_1) + \cdots + j(Q_g)$, where $D' = Q_1 + \cdots + Q_g$. In order to approximate $(Q_1, \ldots, Q_g)$ one has to lift the translation by $[P_1 + \cdots + P_g - gP_0]$ of the straight line from 0 to x. The sub-extension $\mathbb{Q}(x)$ of $K(x)$ can be determined effectively by Galois theory: the Galois group of K_l over $\mathbb{Q}$ contains $\mathrm{SL}_2(\mathbb{F}_l)$, whereas $\mathbb{Q} \to K$ is solvable. The remaining problem is to bound the height of the divisor D'. As $[D' - D] = x$, one expects that the height of D' is at most about the height of D plus that of x. The height of D is under control, because we choose the P_i ourselves, and the height of x is small because x is torsion. Arakelov theory will be used to make these height arguments rigorous.

The problem of bounding the height of D' in terms of that of D also exists in the function field case. We will now show how the Grothendieck-Riemann-Roch formula solves the problem in that case. Let S be a non-singular irreducible projective curve over an algebraically closed field k, and let $\pi\colon X \to S$ be a proper smooth family of curves, with a section P. Let η be the generic point of S, let $\mathcal{L}_\eta$ be a torsion line bundle on X_η, and D a horizontal divisor of degree g (g is the genus of X_η) such that $\mathrm{H}^0(X_\eta, \mathcal{L}_\eta(D_\eta))$ is one-dimensional. Then there exists a unique effective horizontal divisor D' of degree g such that $\mathcal{L}_\eta$ is isomorphic to $\mathcal{O}_{X_\eta}(D' - D)$. We let $\mathcal{L}$ be the unique extension of $\mathcal{L}_\eta$ over X such that $P^*(\mathcal{L}) \cong \mathcal{O}_S$. Then $\mathcal{L}$ is torsion in $\mathrm{Pic}(X)$, and:

$$\mathcal{L} \cong \mathcal{O}_X(D' - D - \pi^* E)$$

for some divisor E on S (E is unique up to rational equivalence). It follows that D' is numerically equivalent to $D + \pi^* E$, which means that for every divisor F on X one has the equality of intersection numbers $\langle D', F\rangle = \langle D, F\rangle + \langle \pi^* E, F\rangle$. In this geometric case, heights are intersection numbers. Let $\mathcal{M}$ be an ample line bundle on X. Then the height of a divisor F with respect to $\mathcal{M}$ is the intersection number $\langle F, \mathcal{M}\rangle$. We have:

$$\langle D', \mathcal{M}\rangle = \langle D, \mathcal{M}\rangle + \langle \pi^* E, \mathcal{M}\rangle = \langle D, \mathcal{M}\rangle + \deg(E)\deg(\mathcal{M}),$$

where $\deg(\mathcal{M})$ is the degree of $\mathcal{M}$ on the fibers of π. So we must bound $\deg(E)$ from above. Now $\pi_*\mathcal{L}(D)$ is an invertible $\mathcal{O}_S$-module. Let s be a non-zero rational section of $\pi_*\mathcal{L}(D)$, then we can take $E = -\operatorname{div}(s)$, and view s as a global section of $\mathcal{L}(D + \pi^* E)$, with divisor D'. We have $\deg(E) = -\deg(\pi_*\mathcal{L}(D))$. The Grothendieck-Riemann-Roch theorem for π says:

$$\deg(\pi_*\mathcal{L}(D)) - \dim_k(\mathrm{R}^1 f_*\mathcal{L}(D)) = \frac{1}{2}\langle D, D - \Omega^1_{X/S}\rangle + \frac{1}{12}\langle \Omega^1_{X/S}, \Omega^1_{X/S}\rangle.$$

If D is a sum of sections $P_1 + \cdots + P_g$, we find:

$$\deg(E) = -\dim_k(\mathrm{R}^1 f_*\mathcal{L}(D)) - \frac{1}{2}\sum_{i \neq j}\langle P_i, P_j\rangle - \frac{1}{12}\langle \Omega^1_{X/S}, \Omega^1_{X/S}\rangle + \sum_i \langle P_i, \Omega^1_{X/S}\rangle.$$

The first three terms of the right hand side of the last identity are less than or equal to zero. The last term is the sum of the heights of the P_i, with respect to $\Omega^1_{X/S}$, hence is not too large.

This computation in the function field case is a strong indication that the arithmetic Riemann-Roch theorem from Arakelov theory (see [7, 8, 23,and 22]) can be successfully applied to bound the height of D' in the number field case. We expect that the number of digits needed in the numerical part of the computation of f_α is polynomial in l.

2.c. Innovation

We mention some innovative aspects of our approach.

1. Point counting without restriction on the characteristic p of the finite field.
2. Explicit computation of mod l Galois representations associated to modular forms of higher weight. This should be seen as a first step beyond class field theory into making the Langlands correspondence available computationally. This also applies to the function field case.
3. Computing higher degree étale cohomology with its Galois action.
4. The use of numerical analysis together with computer algebra in the context of jacobian varieties of curves of high genus.
5. The application of Arakelov theory in this context.

2.d. Plan of work

2.d.1. Developments since 2002

Up to this point, this proposal is the same as the one that was submitted, without success, alas, in 2002. Before giving the plan of work let us give an account of the developments since 2002, at a level intended for experts in arithmetic algebraic geometry.

In the p-adic methods, the most important progress is Lauder's use of differential equations for families of varieties, via the Gauss-Manin connection (see [13]). Also, Satoh's method for elliptic curves over $\mathbb{F}_q$ with $q = p^m$ has been improved to a running time m^2 instead of m^3. For hyperelliptic curves of small genus and $p = 2$, the same running time m^2 has been achieved by "arithmetic geometric mean" methods by Mestre, Lercier and Lubicz (see [16]). Carls's thesis (Groningen and Leiden) extends this last method to higher dimension, and arbitrary p. Gerkmann's thesis (Essen) extends Kedlaya's method to more general varieties. These results concerning the p-adic methods have no consequences, good or bad, for this research proposal.

In 2003 and 2004, Edixhoven and some collaborators worked out part of the plan of work of the 2002 version of this proposal. First of all, Edixhoven extended the height estimate from the case above, for curves with everywhere good reduction in the function field case, to curves with everywhere stable reduction over function fields. He did some successful computer calculations for elliptic curves, that showed how formal integration of power series can be used efficiently for the numerical part. He showed that in our case we can approximate all Galois conjugates of the algebraic number α above. This means that lattice reduction (LLL algorithm) is no longer required to pass from approximations to exact knowledge. Edixhoven found, by reducing the geometry of $X_1(l)$modulo l, a divisor D (supported in the cusps) that satisfies the essential condition that the space of global sections of $\mathcal{L}(D)$ is one-dimensional. Hence the randomization of D proposed above is no longer necessary in this

case. Edixhoven showed, by considering the term $\mathrm{R}^1 f_* \mathcal{L}(D)$, that the numerical work can be done r-adically for a suitable small prime number r. In this way, the complexity of the approximation method is significantly easier to analyze.

Edixhoven and Robin de Jong (a PhD student of van der Geer in Amsterdam) succeeded in applying the arithmetic Faltings Riemann Roch theorem and the arithmetic Noether formula to get an upper bound for $\langle D' - D, P \rangle + \log \# \mathrm{R}^1 f_* \mathcal{L}(D)$ which they can show to be polynomial in l. The Green's functions that arise here are controlled by very recent work of Merkl, and, independently, Jorgensen and Kramer. This control also allows us to pass from bounds on intersection numbers on $X_1(l)$ to bounds for the height of the minimum polynomial of α. Couveignes is making a serious study of the complexity of the numerical analysis part. Together, Couveignes, Edixhoven, and de Jong found a construction of a suitable function f on $X_1(l)$ such that $\alpha := f(Q_1) + \cdots + f(Q_g)$ is a generator of $\mathbb{Q}(x)$. As a consequence, all the occurrences of the term "almost certainly" in the preceding parts of this proposal can be replaced by certainties.

2.d.2. Mod l Galois representations associated to modular forms

This part of the project is now in a state where Edixhoven, de Jong, and Couveignes are working out the details, and writing them up. This will still take some time, but there is no doubt that a joint article on this part can be finished in 2005. That article will clearly prove that the mod l Galois representations associated to the modular form Δ can be computed in time polynomial in l. The article will be written in such a way that the subsequent generalization to arbitrary modular forms only requires some technicalities that do not arise for Δ (for example, if the level N of the form is not square free, the semistable models of the $X_1(Nl)$ are not explicitly known). This generalization will be the subject of a second article. Robin de Jong will start as Postdoc 1 (see the budget below) in Leiden in January 2005.

Johan Bosman started as a PhD student in June 2004. He will explicitly compute the Galois representations associated to Δ for as many primes l as possible. From that he will be able to compute $\tau(p)$ for primes p that are much larger than currently possible. His computations should also give an idea of the real precision needed for the numerical work, which we expect to be much smaller than the theoretical upper bound that Edixhoven and de Jong will prove. From January 2005 on, Bosman will be PhD 1 in the budget below.

Once the existence of a polynomial time algorithm is established, it becomes important to study the running time l^m in more detail, and try to get the exponent m to be as small as possible. This involves, among others, a more detailed study of the Arakelov invariants of modular curves, and possibly also some variations on the approach. This will be a task for PhD 2 and Postdoc 2. The details will depend on the candidates for these positions.

2.d.3. The function field case

A subproject that has not yet been mentioned is to apply the same approach to function fields, for example, in the case of Drinfeld modular curves. In that case, our methods give an algorithm to compute the two-dimensional representations modulo l of absolute Galois groups of function fields in one variable over finite fields. As one can use ordinary algebraic geometry instead of Arakelov geometry, this case is easier, and no problems are to be expected. As we now know that the numerical part can be done at a place of good reduction (as in the number field case), this part should not cause new problems.

PhD 3 will be assigned to this subproject.

2.d.4. More general motives, point counting

Once we know how to treat motives associated to modular forms, we will try to treat more general motives, and do point counting on varieties corresponding to the motives that we can treat. For example, a long term project will be to try to deal with curves of arbitrary genus, although truly new ideas will be required here. Another long term project is to try to use the motives that one can treat for applications to cryptology, just as elliptic curves, but here too, new ideas are required. Postdoc 3 will be selected for this subproject.

2.d.5. Popularizing mathematics

In addition to the description of the proposed research, we want to say a few words on education. We want to contribute to the existing initiatives (Pythagoras, Stichting Vierkant voor Wiskunde) for improving the public image of mathematics, and for providing interested students in high schools and elementary schools with interesting and challenging material. Since August 2003, Edixhoven is president of the board of Vierkant voor Wiskunde. The Summer camps organized by Vierkant attract roughly the same number of participants as the total number of first year mathematics students in all of the Netherlands, which shows how important these initiatives are. Edixhoven also helps with setting up a Dutch server for WIMS (WWW Interactive Multipurpose Server), a server for Interactive mathematics (and other things) on the Internet, see `http://wims.unice.fr/`.

2.d.6 Collaboration

Details on the research groups in mathematics of the host institution (Universiteit Leiden) can be found at the address: `http://www.math.leidenuniv.nl`. Of particular interest is the number theory group, in view of the use of algorithmic algebraic number theory and effective Galois theory in the project; it is for this research group (in addition to the geometry group) that the results of the project are the most interesting. We therefore expect a particularly fruitful collaboration between the future geometry group and the number theory group (the most important one in the Netherlands). The expertise of the differential equations and the numerical analysis groups can become important for the analytic part of Arakelov geometry and the numerical part of the project.

Nationally, we expect the following collaborations.

- van der Put and Top in Groningen, for the subproject concerning Drinfeld modular curves.
- Moonen and van der Geer in Amsterdam (Arakelov theory, Shimura varieties, algebraic geometry in general).
- EIDMA (cryptography, error correcting codes).

International collaborations.

- Couveignes (Toulouse), who is interested in the entire project, and has precise ideas about the numerical part.
- Stein (Harvard), for algorithmic questions on modular symbols.
- Moret-Bailly, Autissier (Rennes), Abbes and Ullmo (Paris), Zhang (New York), for Arakelov theory related to modular curves.
- Kedlaya (M.I.T.), Lauder (Oxford), Wan (Irvine), Berthelot and Le Stum (Rennes), to keep in touch with the developments of p-adic methods; in particular, Edixhoven is still a member of the Arithmetic Algebraic Geometry TMR Network, attached to Rennes.

2.e. Literature references

1. H. Cohen. *A course in computational algebraic number theory.* Graduate Texts in Mathematics 138, Springer-Verlag, 1993.

2. J.M. Couveignes. *Computing l-isogenies using the p-torsion.* Algorithmic number theory (Talence, 1996), 59–65, Lecture Notes in Comput. Sci., 1122, Springer, Berlin, 1996.

3. P. Deligne. *Formes modulaires et représentations l-adiques.* Séminaire Bourbaki exp. 355. Lecture Notes in Mathematics **179**, Springer, Heidelberg, 1969.

4. P. Deligne. *La conjecture de Weil, I.* Publ. Math. I.H.E.S. **43**, 1974, 273–307.

5. J. Denef and F. Vercauteren. *Computing zeta functions of hyper-elliptic curves over finite fields of characteristic 2.* Advances in cryptology—CRYPTO 2002, 369–384, Lecture Notes in Comput. Sci., 2442, Springer, Berlin, 2002.

6. N. Elkies. *Elliptic and modular curves over finite fields and related computational issues.* In "Computational perspectives in number theory: Proceedings of a conference in honour of A.O.L. Atkin", (D.A. Buell and J.T. Teitelbaum), American Mathematical Society International Press 7, 1988, 21–76.

7. G. Faltings. *Calculus on arithmetic surfaces.* Ann. of Math. (2) **119** (1984), no. 2, 387–424.

8. G. Faltings. *Lectures on the arithmetic Riemann-Roch theorem.* Notes taken by Shouwu Zhang. Annals of Mathematics Studies, 127. Princeton University Press, 1992.

9. M. Fouquet, P. Gaudry and R. Harley. *An extension of Satoh's algorithm and its implementation.* J. Ramanujan Math. Soc. **15** (2000), no. 4, 281–318.

10. P. Gaudry and N. Gürel. *An extension of Kedlaya's point-counting algorithm to super-elliptic curves.* In C. Boyd (ed.), Advances in Cryptology — ASIACRYPT 2001, Lecture Notes in Computer Science 1807, Springer-Verlag (2000), 19–34.

11. K. Kedlaya. *Counting points on hyper-elliptic curves using Monsky-Washnitzer cohomology.* J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338.

12. A.G.B. Lauder. *Computing zeta functions of Kummer curves via multiplicative characters.* Preprint, 2002,
Available at: `http://web.comlab.ox.ac.uk/oucl/work/alan.lauder`

13. A.G.B. Lauder. *Deformation theory and the computation of zeta functions.* Proceedings of the London Mathematical Society, Vol. 88 Part 3, (2004), 565-602

14. A.G.B. Lauder and D. Wan. *Counting points on varieties over finite fields of small characteristic.* Preprint, 2001,
Available at: `http://web.comlab.ox.ac.uk/oucl/work/alan.lauder`

15. A.G.B. Lauder and D. Wan. *Computing zeta functions of Artin-Schreier curves over finite fields.* To appear in LMS J. Comp. Math.,
Available at: `http://web.comlab.ox.ac.uk/oucl/work/alan.lauder`

16. R. Lercier and D. Lubicz. *A Quasi Quadatric Time Algorithm for Hyperelliptic Curve Point Counting.*
Available at: `www.math.u-bordeaux.fr/~lubicz/`

17. B.M. Moret. *The theory of computation.* Addison-Wesley, 1998.

18. J. Pila. *Frobenius maps of abelian varieties and finding roots of unity in finite fields.* Math. Comp. **55** (1990), no. 192, 745–763.

19. T. Satoh. *The canonical lift of an ordinary elliptic curve over a finite field and its point counting.* J. Ramanujan Math. Soc. **15** (2000), no. 4, 247–270.

20. A.J. Scholl. *Motives for modular forms.* Invent. math. **100** (1990), 419–430.

21. R.J. Schoof. *Elliptic curves over finite fields and the computation of square roots mod p.* Math. Comp. **44** (1985), no. 170, 483–494.

22. C. Soulé. *Lectures on Arakelov geometry.* With the collaboration of D. Abramovich, J.-F. Burnol and J. Kramer. Cambridge Studies in Advanced Mathematics, 33. Cambridge University Press, 1992.

23. L. Szpiro. *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell.* Astérisque No. 127 (1985), Société Mathématique de France, 1990.

24. S. Zhang. *Admissible pairing on a curve.* Invent. math. **112** (1993), no. 1, 171–193.

Cost estimates

3.a. Budget

	2005	2006	2007	2008	2009	total
Staff costs (in k€):						
Applicant (0.4fte)	52	53	55	57	59	276
Postdoc 1 (1.0 fte)	48	49				97
Postdoc 2 (1.0 fte)		48	49			97
Postdoc 3 (1.0 fte)			48	49		97
PhD 1 (1.0 fte)	35	38	40	42		155
PhD 2 (1.0 fte)	35	38	40	42		155
PhD 3 (1.0 fte)		35	38	40	42	155
programmer (0.2 fte)	6	6	6	6	6	30
Non-staff costs (in k€):						
Computers/software	20	5	5	4	4	38
Books/Journals	2	2	2	2	2	10
Foreign visitors	5	5	5	5	5	25
Organization int. workshops		20			20	40
Travel and subsistence	10	10	10	10	10	50
Popularizing mathematics	5	5	5	5	5	25
Total	218	314	303	262	153	1250

3.b. Have you requested any additional grants for this project either from NWO or from any other institution? No.

Curriculum vitae

4.a. Personal details
Title(s), initial(s), first name, surname: Prof. dr. , S.J., Bas, Edixhoven.
Male/female: male.
Date and place of birth: March 12, 1962, Leiden, The Netherlands.
Nationality: Dutch.
Native country parents: Netherlands.

4.b. Master's (Doctoraal)
University/College of Higher Education: University of Utrecht.
Date: August 1985.
Main subject: Mathematics.

4.c. Doctorate
University/College of Higher Education: University of Utrecht.
Date: June 5, 1989.
Supervisor (Promotor): Prof. dr. F. Oort.
Title of thesis: Stable models of modular curves and applications.

4.d. Work experience since graduating

1. Charles B. Morrey junior Assistant Professor at the university of California at Berkeley, from July 1989 until July 1991, full time, fixed term.

2. Constantijn en Christiaan Huygens fellow, employed by N.W.O., from July 1991 until October 1992, based at the university of Utrecht, full time, fixed term.

3. Professor at the university of Rennes 1, since October 1992 (promoted to "première classe" since September 1998), full time, tenured ("en détachement" since September 2002). Supervised four PhD. students: Jeroen van Beele (with Murre, PhD. Leiden, 1994), Pierre Parent (Rennes, 1999, now "maître de conférences" at the university of Bordeaux), Andreï Yafaev (Rennes, 2000, now lecturer at University College of London), Gabor Wiese (started in December 2001).

4. Professor at the university of Leiden, from September 1, 2002, full time, tenured. PhD. students: Gabor Wiese followed me to Leiden, Theo van den Bogaart started on September 1, 2002, Johan Bosman started on June 1, 2004. Assistants: Martin Lübke, "universitair docent". Postdoc: Robin de Jong will start on January 1, 2005.

4.e. Man-years of research (since doctorate) 14 years and 9 months.

4.f. Brief summary of research over last five years

Edixhoven works in arithmetic geometry. Algebraic geometers study geometric properties of solutions of systems of polynomial equations. Classically, the coefficients and solutions were complex numbers. Number theorists consider integer or rational coefficients and solutions. The goal of arithmetic geometry is to understand the relations between algebraic geometry and number theory.

Three important notions in arithmetic geometry are "algebraic variety" (abstraction of system of polynomial equations), "zeta function" and "cohomology". Zeta functions associated to algebraic varieties are generating functions defined using the numbers of solutions in finite fields. Cohomology associates vector spaces equipped with certain structures to algebraic varieties. One important aim of arithmetic geometry is to understand the relations between the values of zeta functions at integers and properties of the set of rational solutions. Cohomology plays an important role here. Cohomology also provides representations of Galois groups, which is essential for Langlands's program (relations between such representations and "automorphic" representations of matrix groups). The most striking results obtained in this field are the proof of Weil's conjectures (Dwork, Grothendieck, Deligne), Faltings's proof of Mordell's conjecture, Fontaine's theory (comparison between certain cohomologies), Wiles's proof of Fermat's Last Theorem, and Lafforgue's result on Langlands's conjectures.

Edixhoven's research fits well in this general picture. The main themes are: modular forms, modular curves and more general Shimura varieties, Galois representations, Néron models, elliptic curves, Schoof's algorithm.

Shimura varieties are algebraic varieties defined by matrix groups, hence directly related to Langlands's program. For example, the group of 2 by 2 matrices gives modular curves, modular forms, modular parameterizations (and hence arithmetic information) of elliptic curves (Wiles, Kolyvagin, Kato).

Number 11 of the list of publications is applied, in that article, to arithmetic of elliptic curves. Coleman, Kaskel and Ribet used article 15 in their study of "torsion packets". Darmon and Merel used article 16 for some variants of Fermat's Last Theorem. Article 44 gives strong results on a conjecture of Manin. Articles 22 and 24 are other examples of applications of the geometry of modular curves.

Article 13 solves a problem concerning certain Hecke algebras, using motives and Fontaine's theory. It eliminates an hypothesis often made in deformation theory of Galois representations, and shows that Ramanujan's inequality should be strict.

Articles 14, 18, 20 and 23 solve instances of the André–Oort conjecture on "special points" on Shimura varieties. Article 20 fills a gap in Wolfart's work on algebraicity of values of hypergeometric functions at algebraic numbers. Article 23 is applied by Cornut in his proof of a conjecture by Mazur on the arithmetic of elliptic curves.

Finally, the article 45 and many of the lectures from 80 on are concerned with computational aspects of modular forms, and form the start of the proposed research project.

4.g. International activities

Participant of the Research Training Network "Arithmetic Algebraic Geometry" of the European Community, under the programs "Improving Human Potential and the Socio-Economic Knowledge Base" and "Training and Mobility of Researchers (and of one of its predecessors: "p-adic methods in Algebraic Geometry").

Participant of the Erasmus Mundus Master program ALgebra, Geometry And Number Theory by the universities of Bordeaux, Leiden and Padova, see

www.math.u-bordeaux1.fr/ALGANT/.

See the list of publications for invited lectures at international conferences, and for joint publications.

Recent invitations.

1. Research Center "Centre de Recerca Matematica Institut d'Estudis Catalans" in Barcelona, August 1996.
2. University of Georgia at Athens, one week in February 1997, for a series of four lectures.
3. Miller visiting professor, University of California at Berkeley, March, April and May 1997.
4. Tata institute for fundamental research, Bombay. Three weeks in February 1998.
5. Mathematical Sciences Institute, Madras, one week in February 1998.
6. M.I.T., Boston, one week in January 2000.
7. University of Utrecht, one month: June 20000.
8. Oberwolfach, "Arithmetic Geometry", one week, August 2000.
9. MSRI, Berkeley, one week in December 2000.
10. Research Center "Centre de Recerca Matematica Institut d'Estudis Catalans" in Barcelona, two weeks in July 2001, for teaching a course at a Summer School.
11. Lorentz Instituut, University of Leiden, one week in September 2001, and one week in December 2001.
12. McGill University, Montreal, invited lecturer for the CNTA/ACTN meeting, May 2002.
13. Oberwolfach, "Arithmetic and Differential Galois groups", one week, July 2002.
14. Invited lecturer at the Lenstra Treurfeest, Berkeley, March 2003.
15. American Institute of Mathematics Research Conference Center, Palo Alto, workshop "Future Directions in Algorithmic Number Theory", March 2003.
16. Luminy, conference on p-adic and mod p representations of p-adic groups and Iwasawa theory, one week, June 2003.
17. Rennes, conference "Semaine cohomologique de Rennes", June 2003.
18. Oberwolfach, workshop "Explicit methods in number theory", one week, July 2003.
19. Banff, conference "Current trends in arithmetic geometry and number theory", Banff International Research Center, August 2003.
20. Luminy, conference "Groupes de Galois arithmétiques et différentiels", one week, March 2004.
21. Miniworkshop "Calcul de représentations Galoisiennes associées à une forme modulaire" held in Rennes, one week in May 2004, with Jean-Marc Couveignes and Robin de Jong.

22. Conference “Shimura varieties, lattices and symmetric spaces”, Graduate School Zürich Berlin, Ascona, May 2004.

23. University of Essen, Conference on the occasion of Frey’s 60th birthday, June 2004.

24. Oberwolfach, workshop “Arithmetic Algebraic Geometry”, one week, August 2004.

4.h. Other academic activities

Participation in the organization of conferences, etc.

1. Algebraic geometry seminar of the university of Rennes (one session per week), April 1993 until July 1999.

2. Conference on the work of Wiles and Taylor, Lunteren, March 1995.

3. Seminar at the Institut Henri Poincaré on the work of Wiles and Taylor.

4. Conference in the honour of F. Oort’s 60th birthday, Utrecht, June 1995.

5. Special session on modular forms, during the Conference of the Mathematical Societies of the Netherlands, Belgium, Luxemburg and the U.S.A., Antwerp, May 1996.

6. Summer School on elliptic curves, August 11–29, 1997, ICTP, Trieste, Italy.

7. Instructional conference “Formes modulaires et représentations galoisiennes : une introduction”, Luminy, November 3–7, 1997.

8. Conference and workshop “Arithmetic Geometry”, Utrecht, June 2000.

9. Cryptography seminar of the university of Rennes and the CELAR (Centre Electronique de l’Armement), since December 2001.

10. Geometry seminar at the university of Leiden, since October 2002.

11. EIDMA-Stieltjes Graduate course “Mathematics of cryptology”, Lorentz Center, Leiden, one week, September 2003.

12. Workshop “Mathematics of cryptology”, Lorentz Center in Leiden, one week, September/October 2003.

13. Workshop “On the conjecture of André and Oort: Special points in Shimura varieties”, Lorentz Center in Leiden, one week, December 2003.

14. Workshop “Algebraic Cycles and Motives”, together with Jan Nagel (Lille) and Chris Peters (Grenoble), Lorentz Center in Leiden, one week, August/September 2004.

Membership of editorial boards.

1. Compositio Mathematica (editor since 2000, (co)managing editor since 2003).

2. Journal de Théorie des Nombres de Bordeaux (1998–2004).

3. Expositiones Mathematicae (since 2003).

4. Journal of Number Theory (since 2004).

Membership of committees.

1. Wetenschapscommissie Stieltjes Instituut.

2. Program board mathematics for the Lorentz center.

3. Commission de spécialistes (hiring committee of the department of mathematics) of the Université de Toulouse 2.

4. Committee for the evaluation of the "Laboratoire d'Analyse, Géométrie et Applications", université Paris 13, April 2003.

5. Beoordelingscommissie wiskunde, Open competitie N.W.O., vanaf 2003.

6. Lid van het C.J. Kokfonds.

Administrative responsibilities.

1. Co-director (together with X.P. Wang of Nantes) of the "Ecole Doctorale Mathématiques de l'Ouest" (graduate affairs of the universities of Angers, Brest, Nantes and Rennes), 1996–2000.

2. Member of the "commission des thèses" of the "Réseau Doctoral Ouest Mathématiques" (a committee that proposes referees for PhD. theses). Until September 2002.

3. Director of the DEA (Diplôme d'Etudes Approfondies) "Mathématiques fondamentales et applications", 2000-2001.

4. President of the library committee of the departments of mathematics and computer science in Leiden.

5. President of the "Opleidings Commissie Wiskunde" at Leiden university, since 2004.

Collaboration with industry.

1. Organization of a small research project ("stage de DEA", 5 months) on geometric error correcting codes, done at Canon Recherche France (Rennes).

2. Organization of a long term research project on geometric error correcting codes at Canon Recherche France (Rennes).

3. In the process of establishing a contract with the French Ministry of Defense (CELAR, Rennes).

Re-edition of mathematical texts.

1. Edixhoven has launched a project to have the volumes of Grothendieck's "Séminaire de Géométrie Algébrique" typeset in TeX, by volunteers. (For details, see personal home page.)

Public relations for and popularization of mathematics.

1. President of the board of "Stichting Vierkant voor Wiskunde", since August 2003.
2. Coordination of the mathematical part at Leiden of the "nationale wetenschapsdag", annually, since October 2003.

4.i. Scholarships and prizes (last five years)

1. Prime d'encadrement doctoral et de recherche, from October 1994 until September 2002, about 4.5k€ extra salary, annually.
2. Junior Member of the Institut Universitaire de France, from July 1995 until July 2000, about 15k€ for research, annually, plus a reduction of 2/3 of the teaching load.
3. Correspondent of the Dutch Academy of Sciences, from April 2001 until September 2002 (ended automatically after return to the Netherlands), no money involved.

List of publications

Many of the following items can be found on the author's personal web page.

5. Publications

International (refereed) journals

1. *Minimal resolution and stable reduction of $X_0(N)$.* Annales de l'Institut Fourier, Grenoble, **40**, 1, 31–67 (1990).
2. *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein".* Courbes modulaires et courbes de Shimura, Astérisque 196–197, 59–70 (1991).
3. *Elliptic curves over the rationals with bad reduction at only one prime.* Co-auteurs: A. de Groot and J. Top. Mathematics of Computation **54**, 413–419 (1990).
4. *On the Manin constants of modular elliptic curves.* Arithmetic Algebraic Geometry, Progress in Mathematics 89 (G. van der Geer, F. Oort, J. Steenbrink editors), 25–39, Birkhäuser (1990).
5. *Néron models and tame ramification.* Compositio Mathematica **81**, 291–306 (1992).

S 6. *The weight in Serre's conjectures on modular forms.* Inventiones Mathematicae **109**, 563–594 (1992).

7. *Arithmetic part of Faltings's proof.* This is Chapter XI of the book "Diophantine approximation and abelian varieties", Lecture Notes in Mathematics 1566 (Edixhoven and Evertse, eds.), Springer-Verlag (1993).

8. *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur).* Séminaire Bourbaki, exposé 782 (1994). Astérisque 227, 209–227 (1995).

9. *On the prime-to-p part of the groups of connected components of Néron models.* Compositio Mathematica 97, 29–49 (1995).

10. *The p-part of the group of components.* With Q. Liu and D. Lorenzini. Journal of Algebraic Geometry, Volume 5, Number 4, October 1996, 801–813.

S 11. *Specialization of Heegner divisors on jacobians of Shimura curves.* Appendix to the article "A rigid analytic Gross-Zagier formula and arithmetic applications" by M. Bertolini and H. Darmon. Annals of Mathematics 146, 138–147 (1997).

12. *Serre's conjecture.* In : Modular Forms and Fermat's Last Theorem (Gary Cornell, Joseph Silverman and Glenn Stevens, editors). Springer-Verlag, 1997, 209–242.

13. *On the semi-simplicity of the U_p operator on modular forms.* With R.F. Coleman. Mathematische Annalen 310, 119–127, (1998).

14. *Special points on the product of two modular curves.* Compositio Mathematica 114, 315–328 (1998).

S 15. *On Néron models, divisors, and modular curves.* Journal of the Ramanujan Mathematical Society 13, 157–194 (1998).

16. *Sur un résultat d'Imin Chen.* With Bart de Smit. Mathematical Research Letters, Volume 7, Number 2–3, 147–154 (2000).

17. *Pull-back components of the space of holomorphic foliations on* **CP***(N), N at least 3.* With D. Cerveau et A. Lins Neto. Journal of Algebraic Geometry 10 (2001), no. 4, 695–711.

18. *On the André-Oort conjecture for Hilbert modular surfaces.* In "Moduli of abelian varieties", Progress in Mathematics 195 (2001), 133–155, Birkhäuser.

19. *Rational elliptic curves are modular (after Breuil, Conrad, Diamond and Taylor).* Séminaire Bourbaki, 52ème année, 1999–2000, exposé 871. Astérisque 276, 161–188 (2002).

20. *Subvarieties of Shimura varieties.* With A. Yafaev. Annals of Mathematics, Volume 157, No. 2, March 2003, 621–645.

21. *Hasse invariant and group cohomology.* With C. Khare. Documenta Mathematica 8 (2003), 43–50.

22. *The Néron model of $J_1(p)$ has connected fibers.* With B. Conrad and W. Stein. Documenta Mathematica 8 (2003), 331–408.

23. *Special points on products of modular curves.* Accepted for publication in Duke Mathematical Journal. [arXiv:math.NT/0302138]

24. *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one,* with appendices by Jean-François Mestre and Gabor Wiese. Accepted for publication in the Journal de Mathématiques de Jussieu. [arXiv:math.NT/0312019]

National (refereed) journals

25. *Le rôle de la conjecture de Serre dans la démonstration du théorème de Fermat.* Gazette des Mathématiciens, October 1995, 25–41.

Books, or contributions to books

The contributions mentioned here are also mentioned above, under "international refereed journals" because their contents have been refereed, and are of international character.
Most of the editorial work on the second item (LNM 1566) was done by Edixhoven.

26. *On the Manin constants of modular elliptic curves.* Arithmetic Algebraic Geometry, Progress in Mathematics 89 (G. van der Geer, F. Oort, J. Steenbrink editors), 25–39, Birkhäuser (1990).

27. *Diophantine approximation and abelian varieties*, Lecture Notes in Mathematics 1566 (Edixhoven and Evertse, eds.), Springer-Verlag (1993, 2nd printing 1997).

28. *Serre's conjecture.* In : Modular Forms and Fermat's Last Theorem (Gary Cornell, Joseph Silverman and Glenn Stevens, editors). Springer-Verlag, 1997, 209–242.

29. *On the André-Oort conjecture for Hilbert modular surfaces.* Moduli of abelian varieties, Progress in Mathematics 195 (2001), 133–155, Birkhäuser.

Other

Items 31–42 are available from the author's personal home page.

30. *The Polyakov measure and the modular height function.* Proceedings of the Arbeitstagung "Arithmetische Algebraische Geometrie 1987", Wuppertal (org.: G. Faltings and G. Wüstholz).

31. *Stable models of modular curves and applications.* Thesis, university of Utrecht, June 1989.

32. *Relations entre développements en série de Fourier d'une nouvelle forme.* Proceedings of the conference "Arithmétique et surfaces algébriques", Caen, June 11-12, 1993.

33. *Algèbre avancée.* Syllabus for a third year course in Rennes (in french).

34. *Théorie algébrique des nombres.* Syllabus for a fourth year course in Rennes (in french).

35. *Groupes et algèbres de Lie.* Syllabus for a DEA course (5th year) in Rennes (in english).

36. *Variétés abéliennes.* Syllabus for a DEA course (5th year) in Rennes (in english).

37. *Géométrie variable.* Syllabus for a DEA course (5th year) in Rennes (in english).

38. *Variétés jacobiennes.* Syllabus for a DEA course (5th year) in Rennes (in english).

39. *The modular curves $X_0(N)$.* Syllabus for a Summer Course in Trieste, August 1997.

40. *Meetkunde/Geometry.* Syllabus for a 3rd/4th year course in Leiden, Fall 2002.

S 41. *Point counting after Kedlaya.* Syllabus for the EIDMA-Stieltjes Graduate course "Mathematics of Cryptology", at the Lorentz Center in Leiden, September 2003.

42. *Van piramides tot modulaire krommen.* Inaugural lecture, Leiden, January 2004, printed version, 20 pages. Also: Nieuw Archief voor Wiskunde, June 2004, 98–105.

43. *De Rham cohomology.* Syllabus, 25 pages, for a 3rd year geometry course in Leiden, Spring 2004.

44. *Modular parametrizations at primes of bad reduction.* Article in preparation.

S 45. *Computation of mod l Galois representations associated to modular forms.* Together with J-M. Couveignes and R. de Jong. Article in preparation.

Selection of invited lectures (for a complete list, see the author's personal web page).

46. *The Polyakov measure and the modular height function.* Arithmetische Algebraische Geometrie, Wuppertal, June 1987.

47. *Hecke action on component groups of Néron models of jacobians of modular curves.* Abelian varieties, number theory and physics, Schloss Ringberg, July 1988.

48. *The graph method for $X_0(p^2)$.* Algorithmes en théorie des nombres, Luminy, September 1988.

49. *On the Manin constants of strong Weil curves.* Compactification of the moduli space of abelian varieties, Oberwolfach, May 1989.

50. *Néron models of abelian varieties and tame ramification.* Queens University (Canada), January 1990.

51. *On the weight of the modular form in Serre's conjectures.* Meeting of the Am. Math. Soc., 863, San Fransisco, January 1991.

52. *Sur la mauvaise réduction des paramétrisations modulaires des courbes elliptiques sur* $\mathbf{Q}$. Séminaire d'Arithmétique et Géométrie Algebrique, Orsay (France), January 1992.

53. *Points rationnels de torsion de courbes elliptiques sur des corps de nombres (d'après Kamienny et Mazur).* Séminaire Bourbaki, Paris, March 1994.

54. *Fermat's Last Theorem.* Closing lecture at the annual conference of the Dutch mathematical society. Leiden, April 1994.

55. *The prime-to-p part of the groups of connected components of Néron models.* Journées p-adiques, Strasbourg, November 1994.

56. *Les groupes de composantes connexes des modèles de Néron.* Séminaire d'arithmétique et de géométrie algébrique d'Orsay, January 1995.

57. *On the Galois representations associated to modular forms. Lowering the level.* Two lectures at the conference on the results of Wiles, Lunteren (Netherlands), March 1995.

58. *Ajustement du niveau et du poids. La propriété de Gorenstein pour les algèbres de Hecke.* Two lectures at the "Séminaire sur les travaux de Wiles", I.H.P., Paris, April 1995.

59. *Introduction to the arithmetic theory of modular forms.* Series of three lectures during an "instructional conference" at Trento, June 1995.

60. *Lissité, semi-stabilité et altérations, d'après de Jong.* Journée IUF à l'IHES, October 1995.

61. *Groups of connected components of Néron models.* Number theory seminars of Cambridge and of Oxford, October/November 1995.

62. *Simplicity of Frobenius eigenvalues in Galois representations associated to modular forms.* Conference at the 50th anniversary of the SMC, Amsterdam, February 1996.

63. *Oort's conjecture for pairs of elliptic curves.* Arithmetic Geometry conference, Berlin, March 21–26, 1996.

64. *Two results on modular curves.* Conference on p-adic methods in algebraic geometry, Platja d'Aro (Spain), September 23–27, 1997.

65. *Points spéciaux sur le produit de deux courbes modulaires.* Séminaire de géométrie algébrique et arithmétique, Orsay, October 22, 1997.

66. *On the Manin constants of modular parametrizations of elliptic curves.* Series of four lectures at Athens (Georgia, U.S.A.), February 25-28, 1997.

67. *On the semi-simplicity of the U_p-operator on modular forms.* Number theory seminar, Berkeley, April 2, 1997.

68. *Polynomial relations between j-invariants of elliptic curves.* Mathematics colloquium, Berkeley, May 1, 1997.

69. *On Néron models, divisors, and modular curves.* Institut Henri Poincaré, June 23, 1997.

70. *The modular curves $X_0(N)$.* Minicourse of 7 hours at the "Summer School on elliptic curves", August 11–29, 1997, ICTP, Trieste.

71. *Polynomial relations between j-invariants of elliptic curves.* Mathematics colloquium, Tata Institute, Bombay, February 19, 1998.

72. *On the semi-simplicity of the U_p-operator on modular forms.* Mathematics colloquium, Mathematical Sciences Institute of Madras, February 27, 1998.

73. *On the André-Oort conjecture.* Journées Arithmétiques, Rome, July 12–17, 1999.

74. *Sur la conjecture d'André-Oort.* Séminaire automorphe, January 2000, Paris.

75. *Sur la modularité des courbes elliptiques rationnelles.* Séminaire Bourbaki, March 2000, Paris.

76. *Hecke modules, and suitable deformation problems.* Arithmetic Geometry, June 2000, Utrecht.

77. *On the André-Oort conjecture.* Workshop Arithmetic Geometry, Oberwolfach, July 31, 2000.

78. *Subvarieties of Shimura varieties.* AMS meeting New York, November 2000.

79. *Sous-variétés de variétés de Shimura.* Séminaire d'arithmétique et de géométrie algébrique d'Orsay, November 2000.

S 80. *On the computation of coefficients of modular forms.* Workshop Computational Arithmetic Geometry, MSRI, Berkeley, December 2000.

81. *Modular forms, Galois representations and local Langlands.* Course of 15 hours at the "Centre de Recerca Matemàtica", Barcelona, July 2001.

S 82. *On computing coefficients of modular forms.* Conference "L-functions from algebraic geometry", Lorentz Center, Leiden, September 2001.

83. *Computing spaces of modular forms mod 2 of weight one.* Miniworkshop on Algebraic Varieties, Rome, January 18–19, 2002.

84. Plenary Lecture at the Seventh Canadian Number Theory Association meeting to take place on May 19-25, 2002 in Montreal, Quebec (Canada).

85. *Modular parametrisations 1*, *Modular parametrisations 2*, *Non-triviality of Heegner points 1: André–Oort conjecture*, *Non-triviality of Heegner points 2.* Ecole d'été de l'Institut de Mathématiques de Jussieu (Paris), *la conjecture de Birch et Swinnerton-Dyer*, four one hour lectures, July 2002.

S 86. *Computing etale cohomology with Galois action.* Arithmetic and Differential Galois groups, Oberwolfach, July 2002.

87. *Galois action and complex multiplication.* Workshop "Explicit algebraic number theory", held at the Lorentz center, University of Leiden, September 2002.

88. *Formes modulaires modulo p de poids un et symboles modulaires.* Algebraic geometry seminar, Rennes, October 2002.

S 89. *Counting solutions of systems of equations over finite fields.* Colloquium, Groningen, October 2002.

90. *Formes modulaires modulo p de poids un et symboles modulaires.* Seminar, Université de Paris 7, November 2002.

S 91. *Equations for covers of $\mathbf{P}^1$.* Intercity Number Theory seminar, Nijmegen, November 2002.

92. *On rational points on modular curves, after Pierre Parent.* Cohomology of Moduli Spaces, Amsterdam, December 2002.

S 93. *Counting solutions of systems of equations over finite fields.* Colloquium, Amsterdam, January 2003.

S 94. *Counting solutions of systems of equations over finite fields.* Colloquium, Leiden, January 2003

S 95. *Counting solutions of systems of equations over finite fields.* This weeks discoveries colloquium, Leiden, February 2003.

96. *On special $n$tuples of elliptic curves.* Berkeley, Lenstra Treurfeest, invited speaker, March 2003.

S 97. *About point counting over arbitrary finite fields.* Palo Alto, Workshop on Future directions in algorithmic number theory, invited lecturer, March 2003.

S 98. *On the computation of the field of definition of torsion points on jacobians.* Intercity Seminarium Getaltheorie, April 2003.

99. *A propos des sous-variétés spéciales des variétés de Shimura; la conjecture d'André-Oort.* Semaine cohomologique de Rennes, June 2003.

S 100. *Computing fields of definition of torsion points.* Workshop "Explicit methods in number theory", Oberwolfach, July 2003.

S 101. *Point counting on hyperelliptic curves.* Three one hour lectures, EIDMA-Stieltjes Graduate Course, Lorentz Center, Leiden, September 2003.

S 102. *A possible generalisation of Schoof's algorithm.* Workshop "Mathematics of Cryptology", Leiden, September/October 2003.

S 103. *Sur le calcul du corps de définition d'un point de torsion d'une jacobienne d'une courbe de genre quelconque.* Séminaire de Théorie des Nombres de Montpellier, October 2003.

104. *A simple introduction to special points in Shimura varieties.* Colloquium, Utrecht, December 2003.

105. *Galois action on special points.* Intercity Seminar Number Theory, Utrecht, December 2003.

106. *Galois Orbits, Hecke Correspondences, Intersections.* Workshop "Special points in Shimura Varieties", Lorentz Center, Leiden, December 2003.

107. *Van piramides tot modulaire krommen.* Inaugural lecture, Leiden, January 2004.

S 108. *Sur le calcul du corps de définition d'un point de torsion d'une jacobienne d'une courbe de genre quelconque.* Séminaire de cryptographie, Rennes, January 2004.

109. *Stacks: geometry.* Intercity Seminar Geometry, Leiden, February 2004.

110. *Mijn favoriete rekenmachine is gratis.* Nationale Wiskunde Dagen, Noordwijkerhout, February 2004.

111. *Stacks: sheaves and cohomology.* Intercity Seminar Geometry, Utrecht, February 2004.

112. *The André-Oort conjecture.* Conference on Shimura varieties, lattices and symmetric spaces, organised by the ETH Zürich and the Humboldt University of Berlin. Monte Verità, Ascona, May 2004.

S 113. *On certain l-torsion points of $J_1(l)$.* At the conference "From Arithmetic to Cryptology", Essen, July 2004.

S 114. *Computation of mod l Galois representations associated to modular forms.* Workshop Arithmetic Algebraic Geometry (organisers Faltings, Harder, Katz), Oberwolfach, August 2004.

Signature

I hereby declare that I have completed this form truthfully:
Name: Bas Edixhoven
Place: Leiden
Date: August 20, 2004.