Journal de Théorie des Nombres de Bordeaux **17** (2005), 727–735

Division-ample sets and the Diophantine problem for rings of integers

par Gunther CORNELISSEN, Thanases PHEIDAS et Karim ZAHIDI

Résumé. Nous demontrons que le dixième problème de Hilbert pour un anneau d'entiers dans un corps de nombres K admet une réponse négative si K satisfait à deux conditions arithmétiques (existence d'un ensemble dit *division-ample* et d'une courbe elliptique de rang un sur K). Nous lions les ensembles division-ample à l'arithmétique des variétés abéliennes.

Abstract. We prove that Hilbert's Tenth Problem for a ring of integers in a number field K has a negative answer if K satisfies two arithmetical conditions (existence of a so-called *division-ample* set of integers and of an elliptic curve of rank one over K). We relate division-ample sets to arithmetic of abelian varieties.

1. Introduction

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. *Hilbert's Tenth Problem* or *the diophantine problem* for $\mathcal{O}_K$ is the following: is there an algorithm (on a Turing machine) that decides whether an arbitary diophantine equation with coefficients in $\mathcal{O}_K$ has a solution in $\mathcal{O}_K$.

The answer to this problem is known to be negative for $K = \mathbf{Q}$ ([5]) and for the following fields K by reduction to the field $K = \mathbf{Q}$: K of complex degree ≤ 2 over a totally real field (Denef and Lipshitz [6], [7], [8]), K with exactly one pair of complex embeddings (Pheidas [9] and Shlapentokh [14]) and subfields of all those (including cyclotomic fields, and hence all abelian number fields; Shapiro and Shlapentokh [12]). This reduction consists in finding a *diophantine model* (cf. [3]) for integer arithmetic over $\mathcal{O}_K$. The problem is open for general number fields (for a survey see [10] and [13]), but has been solved conditionally, e.g. by Poonen [11] (who shows that the set of rational integers is diophantine over $\mathcal{O}_K$ if there exists an elliptic

Manuscrit reçu le 8 janvier 2004.

The authors thank Jan Van Geel for very useful help and encouragement. The third author was supported by a Marie-Curie Individual Fellowship (HPMF-CT-2001-01384).

curve over $\mathbf{Q}$ that has rank one over both $\mathbf{Q}$ and K). In this paper, we give a more general condition as follows:

Theorem 1.1. *The diophantine problem for the ring of integers $\mathcal{O}_K$ of a number field K has a negative answer if the following exist:*

(1) *an elliptic curve defined over K of rank one over K;*
(2) *a* division-ample *set $A \subseteq \mathcal{O}_K$.*

Definition. A set $A \subseteq \mathcal{O}_K$ is called *division-ample* if the following three conditions are satisfied:

- (diophantineness) A is a diophantine subset of $\mathcal{O}_K$;
- (divisibility-density) Any $x \in \mathcal{O}_K$ divides an element of A;
- (norm-boundedness) There exists an integer $\ell > 0$, such that for any $a \in A$, there is an integer $\tilde{a} \in \mathbf{Z}$ with $\tilde{a}$ dividing a and $|N(a)| \leq |\tilde{a}|^{\ell}$.

Proposition 1.1. *A division ample set exists if either*

(1) *there exists an abelian variety G over $\mathbf{Q}$ such that*

$$\operatorname{rk} G(\mathbf{Q}) = \operatorname{rk} G(K) > 0; \quad or$$

(2) *there exists a commutative (not necessarily complete) group variety G over $\mathbf{Z}$ such that $G(\mathcal{O}_K)$ is finitely generated and such that* $\operatorname{rk} G(\mathbf{Z}) = \operatorname{rk} G(\mathcal{O}_K) > 0$.

From (1) in this proposition, it follows that our theorem includes that of Poonen, but it isolates the notion of "division-ampleness" and shows it can be satisfied in a broader context. It would for example be interesting to construct, for a given number field K, a curve over $\mathbf{Q}$ such that its Jacobian satisfies this condition.

As we will prove below, part (2) of this proposition is satisfied for the relative norm one torus $G = \ker(N_K^{KL})$ for a number field L linearly disjoint from K, if K is quadratic imaginary (choosing L totally real).

It would be interesting to know other division-ample sets, in particular, such that are not subsets of the integers.

The proof of theorem 1.1 will use divisibility on elliptic curves and a Lemma from algebraic number theory of Denef and Lipshitz. Some of our arguments are similar to ones in [11], but we have avoided continuous reference both for reasons of completeness and because our results have been obtained independently.

2. Lemmas on number fields

In this Section we collect a few facts about general number fields which will play a rôle in subsequent proofs. Fix K to be a number field, let $\mathcal{O} = \mathcal{O}_K$ be its ring of integers, and let h denote the class number of $\mathcal{O}$.

Let $N = N_{\mathbf{Q}}^{K}$ be the norm from K to $\mathbf{Q}$, and let $n = [K : \mathbf{Q}]$ denote the degree of K. Let $|$ denote "divides" in $\mathcal{O}$.

First of all, we will say a subset $S \subseteq K^n$ is "diophantine over $\mathcal{O}$" if its set of representatives $\widetilde{S} \subseteq (\mathcal{O} \times (\mathcal{O} - \{0\}))^n$ given by

$$\widetilde{S} := \{(a_i, b_i)_{i=1}^n \in (\mathcal{O} \times (\mathcal{O} - \{0\}))^n \mid (a_i/b_i)_{i=1}^n \in S\}$$

is diophantine over $\mathcal{O}$. Recall that "$x \neq 0$" is diophantine over $\mathcal{O}$ ([8] Prop. 1(b)), hence S is diophantine over $\mathcal{O}$ if and only if it is diophantine over K.

Recall that there is no unique factorisation in general number fields, but we can use the following valuation-theoretic remedy:

Definition. Let $x \in K$. If $x^h = \frac{a}{b}$ for $a, b \in \mathcal{O}$ with $(a, b) = 1$ (the ideal generated by a and b), we say that $a = \mathrm{wn}(x)$ is *a weak numerator* and $b = \mathrm{wd}(x)$ is *a weak denominator* for x.

Lemma 2.1. (1) *For any $x \in K$ a weak numerator and a weak denominator exists and is unique up to units.*

(2) *for any valuation v,*

- $v(x) > 0 \iff v(\mathrm{wn}(x)) > 0$, *and then* $v(\mathrm{wn}(x)) = hv(x)$;
- $v(x) < 0 \iff v(\mathrm{wd}(x)) > 0$, *and then* $v(\mathrm{wd}(x)) = -hv(x)$.

(3) *For $a \in \mathcal{O}, x \in K$, "$a = \mathrm{wn}(x)$" and "$a = \mathrm{wd}(x)$" are diophantine over $\mathcal{O}$.*

Proof. Since $\mathcal{O}$ is a Dedekind ring, (x) has a unique factorisation in fractional ideals

$$(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1}.$$

We let a be a generator for the principal ideal $(\mathfrak{p}_1 \cdots \mathfrak{p}_r)^h$ and b a generator for $(\mathfrak{q}_1 \cdots \mathfrak{q}_s)^h$; these are obviously a weak numerator/denominator for x. Uniqueness, (2) and (3) are obvious. □

Lemma 2.2 (Denef-Lipshitz [8]). (1) *If $u \in \mathbf{Z} - \{0\}$ and $\xi \in \mathcal{O}$ satisfy the divisibility condition*

$$2^{n!+1} \prod_{i=0}^{n!-1} (\xi + i)^{n!} \mid u$$

then for any embedding $\sigma : K \hookrightarrow \mathbf{C}$

$$(*)_u \qquad |\sigma(\xi)| \leq \frac{1}{2} \sqrt[n!]{|N(u)|}.$$

(2) *If $\widetilde{u} \in \mathbf{Z} - \{0\}, q \in \mathbf{Z}$ and $\xi \in \mathcal{O}$ satisfy $(*)_{\widetilde{u}}$ for any embedding $\sigma : K \hookrightarrow \mathbf{C}$ and $\xi \equiv q \bmod \widetilde{u}$, then $\xi \in \mathbf{Z}$.*

Proof. Easy to extract from the proof of Lemma 1 in [8]. □

3. Lemmas on elliptic curves

Let E denote an elliptic curve of rank one over K, written in Weierstrass form as

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

let T be the order of the torsion group of $E(K)$, and let P be a generator for the free part of $E(K)$. Define $x_n, y_n \in K$ by $nP = (x_n, y_n)$.

Lemma 3.1. *For any integer r the set $rE(K)$ is diophantine over K and, if r is divisible by T, then $rE(K) = \langle rP \rangle \cong (\mathbf{Z}, +)$.*

Proof. A point $(x, y) \in K \times K$ belongs to $rE(K) - \{0\}$ if and only if $\exists \ (x_0, y_0) \in E(K) \ : \ (x, y) = r(x_0, y_0)$. As the addition formulæ on E are algebraic with coefficients from K, this is a diophantine relation. The last statement is obvious. □

Lemma 3.2 ([2] for $K = \mathbf{Q}$, [11]). *There exists an integer $r > 0$ such that for any non-zero integers $m, n \in \mathbf{Z}$,*

$$m|n \iff \mathrm{wd}(x_{rm})| \, \mathrm{wd}(x_{rn}).$$

Proof. We reduce the claim to a statement about valuations using Lemma 2.1(ii). The theory of the formal group associated to E implies that if $n = mt$ and v is a finite valuation of K such that $v(x_{rm}) < 0$, then $v(x_{rmt}) \leq v(x_{rm}) - 2v(t) \leq v(x_{rm})$ ([15] VII.2.2).

For the converse, we start by choosing r_0 in such a way that r_0P is non-singular modulo all valuations v on K. By the theorem of Kodaira-Néron ([15], VII.6.1), such r_0 exists and it actually suffices to take $r_0 = 4\prod_v v(\Delta_E)$, where Δ_E is the minimal discriminant of E, and the product runs over all finite valuations on K for which $v(\Delta_E) \neq 0$. Note that then, $v(x_{r_0n}) < 0 \iff r_0nP = 0$ in the group E_v of non-singular points of E modulo v.

We claim that for an arbitrary finite valuation v on K, if $v(x_{r_0n}) < 0$ and $v(x_{r_0m}) < 0$, then $v(x_{(r_0m, r_0n)}) < 0$, where $(\cdot, \cdot)$ denotes the gcd in $\mathbf{Z}$. Indeed, the hypothesis means $r_0mP = r_0nP = 0$ in E_v. Since there exist integers $a, b \in \mathbf{Z}$ with $(r_0m, r_0n) = ar_0m + br_0n$, we find $(r_0m, r_0n)P = 0$ in E_v, and hence the claim.

The main theorem of [1] states that for any sufficiently large $M (\geq M_0)$, there exists a finite valuation v such that $v(x_M) < 0$ but $v(x_i) \geq 0$ for all $i < M$. We choose $r = r_0M_0$. Pick such a valuation v for $M = rm$. The hypothesis implies that $v(x_{rn}) < 0$ and hence $v(x_{r(m,n)}) < 0$. But $r(m, n) \leq rm$ and $v(x_i) \geq 0$ for any $i < rm$. Hence $r(m, n) = rm$ so m divides n. □

Lemma 3.3. *Any $\xi \in \mathcal{O} - \{0\}$ divides the weak denominator of some x_n.*

Proof. The set $E(\mathcal{O}/\xi)$ is finite but contains $\{nP \bmod \xi\}_{n\in\mathbf{Z}}$. Hence there are $a \neq b \in \mathbf{Z}$ with $aP = bP \bmod \xi$, so $NP = 0 \bmod \xi$ for $N = a - b \neq 0$. Therefore, ξ divides $\mathrm{wd}(x_N)$. □

Lemma 3.4. *Let m, n, q be integers with $n = mq$. Then*

$$\mathrm{wd}(x_m) | \mathrm{wn}(\frac{x_n y_m}{y_n x_m} - q).$$

Proof. The formal power series expansion for addition on E around 0 ([15], IV.2.3) implies that $\frac{x_n}{y_n} = q\frac{x_m}{y_m} + O((\frac{x_m}{y_m})^2)$, whence the result. □

4. Proof of the main theorem

Let $\xi \in \mathcal{O}$. Given an elliptic curve E of rank one over K as in the main theorem, we use the notation from Section 3 for this E — in particular, choose a suitable r such that Lemma 3.2 applies; we also choose ℓ which comes with the definition of A. We claim that the following formulæ give a diophantine definition of $\mathbf{Z}$ in $\mathcal{O}$:

$$\xi \in \mathbf{Z} \iff \exists\, m, n \in rT\mathbf{Z},\ \exists\, u \in A - \{0\} \begin{cases} (1) & m|n \\ (2) & 2^{n!+1} \prod_{i=0}^{n!-1} (\xi^{\ell n!} + i)^{n!} | u \\ (3) & u^h | \mathrm{wd}(x_m) \\ (4) & \mathrm{wd}(x_m) | \mathrm{wn}(\frac{x_n y_m}{x_m y_n} - \xi) \end{cases}$$

4.1. Any $\xi \in \mathbf{Z}$ satisfies the relations. If $\xi \in \mathbf{Z}$, then a u satisfying (2) exists because A is division-dense. By Lemma 3.3, there exists an m satisfying (3) for this u. Define $n = m\xi$ for this m. Then (1) is automatic and (4) is the contents of Lemma 3.4.

4.2. A ξ satisfying the relations is rational. Let $q \in \mathbf{Z}$ satisfy $n = qm$ (which exists by (1)). Then Lemma 3.4 implies that

$$\mathrm{wd}(x_m) | \mathrm{wn}(\frac{x_n y_m}{x_m y_n} - q),$$

which can be combined with (4) using the non-archimedean triangle inequality to give

$$\mathrm{wd}(x_m) | \mathrm{wn}(\xi - q) = (\xi - q)^h.$$

By (3), then also $u | \xi - q$.

By norm-boundedness of A we can find $\widetilde{u} \in \mathbf{Z}$ such that $\widetilde{u} | u$ and $|N(u)| \leq \widetilde{u}^\ell$. We still have

$$(*)\quad \xi \equiv q \bmod \widetilde{u};\quad \widetilde{u}, q \in \mathbf{Z}.$$

Condition (2) implies that Lemma 2.2(1) can be applied with $\xi^{\ell n!}$ in place of ξ, so for any complex embedding σ of K we find

$$(**) \quad |\sigma(\xi)| \leq \frac{1}{2}|N(u)|^{\frac{1}{\ell n!}} \leq \frac{1}{2}N(\widetilde{u})^{\frac{1}{n!}}.$$

Because of $(*)$ and $(**)$, we can apply Lemma 2.2(2) to conclude $\xi \in \mathbf{Z}$.

4.3. The relations (1)-(4) are diophantine over $\mathscr{O}$. By 2.1 and 3.1, for $a \in \mathscr{O}$, the relations $\exists n \in rT\mathbf{Z} : a = \mathrm{wn}(x_n)$ and $\exists n \in rT\mathbf{Z} : a = \mathrm{wd}(x_n)$ are diophantine. By the diophantineness of A, the membership $u \in A$ is diophantine, and $u \neq 0$ is diophantine ([8], Prop. 1(b)). Condition (1) is diophantine because of Lemma 3.2. Conditions (2)-(4) are obviously diophantine using 2.1. □

5. Proof of the proposition and discussion of division-ample sets

5.1. Rank-preservation over Q. Suppose there exists an abelian variety G of dimension d over $\mathbf{Q}$ such that $\mathrm{rk}\, G(\mathbf{Q}) = \mathrm{rk}\, G(K) > 0$ (note that $G(K)$ is finitely generated by the Mordell-Weil theorem). Let T denote the (finite) order of the torsion of $G(K)$ and consider the free group $TG(K) \cong \mathbf{Z}^r$. The assumption implies that $G(\mathbf{Q})$ is of finite index $[G(K) : G(\mathbf{Q})]$ in $G(K)$. The choice of an ample line bundle on G gives rise to a projective embedding of G in some projective space with coordinates $\langle x_i \rangle_{i=1}^N$, where G is cut out by finitely many polynomial equations and the addition on G is algebraic in those coordinates. Suppose $\{t_i\}$ are algebraic function of the coordinates, and local uniformizers at the unit $\mathbf{0} = (1 : 0 : \cdots : 0)$ of G (i.e., $\hat{\mathscr{O}}_{G,\mathbf{0}} = \mathbf{Q}[[t_1, \ldots, t_d]]$). Define

$$A_G := \{\mathrm{wd}(t_2(P)) \ : \ P \in T[G(K) : G(\mathbf{Q})] \cdot G(K) \text{ and } t_1(P) = 1\}.$$

We claim that A_G is division-ample. Indeed, the three conditions are satisfied:

(a) A_G is obviously diophantine over $\mathscr{O}$ (the diophantine definition comes from the chosen embedding of G).

(b) The analogue of Lemma 3.3 remains valid, so A_G is divisibility-dense. Indeed, it suffices to prove that a given non-zero integer ξ divides $t_2(NP)$ for some N (where $t_1(NP) = 1$). Since $G(\mathbf{Z}/\xi)$ is finite, there is a non-zero N for wich $NP = \mathbf{0} \bmod \xi$, and then $t_2(NP) = 0 \bmod \xi$.

(c) Since by assumption, all elements of A_G are in $\mathbf{Z}$, we can set $\widetilde{a} = a$, $\ell = n$ for any $a \in A_G$ to get the required norm-boundedness.

Remark. From available computer algebra, the construction of elliptic curves which fit the above can be automated. One can compute ranks of elliptic curves over $\mathbf{Q}$ quite fast using `mwrank` by J. Cremona [4], and over number fields using the gp-package of D. Simon [16]. Michael Stoll has written a MAGMA-package that computes the rank of Jacobians of genus two curves over $\mathbf{Q}$ ([17]). Unfortunately, the current state of affairs in computational arithmetical geometry doesn't include an algorithm for the rank of abelian varieties of dimension ≥ 2 over arbitrary number fields (although the necessary descent theory exists). We will therefore restrict to examples involving elliptic curves.

Example. In the style of Poonen's result, the elliptic curve $y^2 = x^3 + 8x$ has rank one over $\mathbf{Q}$ and over $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(\sqrt[4]{2})$. However, this curve acquires rank two over $\mathbf{Q}(\sqrt[5]{2})$.

The curve $y^2 = x^3 + 14x$ has rank two over $\mathbf{Q}$ and over $\mathbf{Q}(\sqrt[5]{2})$, and the curve $y^2 = x^3 + \sqrt[5]{2}x^2 + 8x$ has rank one over $\mathbf{Q}(\sqrt[5]{2})$.

We conclude that the diophantine theory of the ring of integers of $\mathbf{Q}(\sqrt[n]{2})$ is undecidable for $n \leq 5$ ($n \leq 3$ also covered by known results).

Remark. We ask: given K, can one construct in some clever way a curve C over $\mathbf{Q}$ such that its Jacobian satisfies the above conditions?

5.2. Rank-preservation over Z. A similar construction (of which we leave out the details) can be performed if there exists a commutative (not necessarily complete) group variety G over $\mathbf{Z}$ such that $G(\mathcal{O})$ is finitely generated and such that $\operatorname{rk} G(\mathbf{Z}) = \operatorname{rk} G(\mathcal{O}) > 0$. We will work out an easy example. Maybe a variation of this example can help one eliminate the second condition in the main theorem.

Example. Let L be another number field, linearly disjoint from K. Let $\langle a_i \rangle$ denote a $\mathbf{Z}$-basis for $L/\mathbf{Q}$ (this is also a basis for $\mathcal{O}_{KL}$ over $\mathcal{O}_K$). Let T_L denote the norm one torus $N^L_{\mathbf{Q}}(\sum a_i x_i) = 1$. Then $T_L(\mathbf{Z}) \cong \mathcal{O}_L^*$ and

$$T_L(\mathcal{O}_K) = \ker(N^{KL}_K : \mathcal{O}_{KL}^* \to \mathcal{O}_K^*),$$

hence (by surjectivity of the relative norm) $\operatorname{rk} T_L(\mathcal{O}_K) = \operatorname{rk} \mathcal{O}_{KL}^* - \operatorname{rk} \mathcal{O}_K^*$. In particular, $T_L(\mathcal{O}_K) = T_L(\mathbf{Z})$ iff

$$r_{KL} + s_{KL} = r_K + s_K + r_L + s_L - 1$$

where r_M, s_M denote the number of real, respectively half the number of complex embeddings of a number field M. If L and K are linearly disjoint, $r_{KL} = r_K r_L$, and the condition simplifies to

$$(r_K + s_K - 1)(r_L - 1) + (r_K + 2s_K - 1)s_L = 0.$$

The only non-trivial solution is $r_K = 0, s_K = 1$ (i.e., K complex quadratic) choosing $r_L > 1, s_L = 0$.

Remark. In all these examples, division-ample sets are actually subsets of the integers. Can one find a division-ample set which does not consists of just ordinary integers?

Remark (December 2005). Mazur and Rubin have shown that there exist infinitely many number fields over which the rank of every elliptic curve *defined over* $\mathbf{Q}$ is even, assuming the Parity Conjecture. More specifically, they show that if $E/\mathbf{Q}$ is an elliptic curve and $K/\mathbf{Q}$ a Galois extension such that $\mathrm{Gal}(K/\mathbf{Q})$ has a non-cyclic 2-Sylow and such that the discriminant of E is coprime to that of K, then the root number of E/K is $+1$ (compare: Rubin, talk at AIM-workshop (2005); Rubin and Mazur in: Kazuya Kato's Birthday volume of Doc. Math. (2003), pp. 585–607).

On the other hand, Poonen and Shlapentokh have remarked that the argument in [11] continues to hold under the weaker assumption that there exists an elliptic curve over $\mathbf{Q}$ retaining its positive rank over the number field K (not necessarily of rank one), see: Poonen, talk at AIM-workshop (2005); Shlapentokh, Elliptic Curves Retaining Their Rank in Finite Extensions and Hilbert's Tenth Problem, preprint (2004).

References

[1] J. CHEON. S. HAHN, *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve.* Acta Arith. **88** (1999), no. 3, 219–222.

[2] G. CORNELISSEN, *Rational diophatine models of integer divisibility*, unpublished manuscript (May, 2000).

[3] G. CORNELISSEN. K. ZAHIDI, *Topology of Diophantine sets: remarks on Mazur's conjectures.* Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 253–260, Contemp. Math. **270**, Amer. Math. Soc., Providence, RI, 2000.

[4] J. CREMONA, `mwrank`, www.maths.nott.ac.uk/personal/jec/, 1995-2001.

[5] M. DAVIS, Y. MATIJASEVIČ. J. ROBINSON, *Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution.* Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. **XXVIII**, Northern Illinois Univ., De Kalb, Ill., 1974), pp. 323–378.

[6] J. DENEF, *Hilbert's tenth problem for quadratic rings.* Proc. Amer. Math. Soc. **48** (1975), 214–220.

[7] J. DENEF, *Diophantine sets of algebraic integers, II.* Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236.

[8] J. DENEF, L. LIPSHITZ, *Diophantine sets over some rings of algebraic integers.* J. London Math. Soc. (2) **18** (1978), no. 3, 385–391.

[9] T. PHEIDAS, *Hilbert's tenth problem for a class of rings of algebraic integers.* Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620.

[10] T. PHEIDAS. K. ZAHIDI, *Undecidability of existential theories of rings and fields: a survey,* in: "Hilbert's tenth problem: relations with arithmetic and algebraic geometry" (Ghent, 1999). Contemp. Math. **270**, Amer. Math. Soc. (2000), 49–105.

[11] B. POONEN, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers.* Algorithmic Number Theory (eds. C. Fieker, D. Kohel), 5th International Symp. ANTS-V, Sydney, Australia, July 2002, Proceedings, Lecture Notes in Computer Science **2369**, Springer-Verlag, Berlin, 2002, pp. 33-42.

[12] H. SHAPIRO, A. SHLAPENTOKH, *Diophantine relations between algebraic number fields.* Comm. Pure Appl. Math. **XLII** (1989), 1113-1122.

[13] A. SHLAPENTOKH, *Hilbert's tenth problem over number fields, a survey,* in: "Hilbert's tenth problem: relations with arithmetic and algebraic geometry" (Ghent, 1999). Contemp. Math. **270**, Amer. Math. Soc. (2000), 107–137.

[14] A. SHLAPENTOKH, *Extensions of Hilbert's tenth problem to some algebraic number fields.* Comm. Pure Appl. Math. **XLII** (1989), 939–962.

[15] J.H. SILVERMAN, *The arithmetic of elliptic curves.* Graduate Texts in Math. **106**, Springer-Verlag, New York, 1986.

[16] D. SIMON, *Computing the rank of elliptic curves over number fields.* LMS J. Comput. Math. **5** (2002), 7–17.

[17] M. STOLL, *Hyperelliptic curves* MAGMA*-package*, `www.math.iu-bremen.de/stoll/magma/`.

Gunther CORNELISSEN
Mathematisch Instituut
Universiteit Utrecht
Postbus 80010
3508 TA Utrecht, Nederland
E-mail : `cornelissen@math.uu.nl`

Thanases PHEIDAS
Department of Mathematics
University of Crete
P.O. Box 1470
Herakleio, Crete, Greece
E-mail : `pheidas@math.uoc.gr`

Karim ZAHIDI
Equipe de Logique Mathématique
U.F.R. de Mathématiques (case 7012)
Université Denis-Diderot Paris 7
2 place Jussieu
75251 Paris Cedex 05, France
Adresse actuelle:
Departement Wiskunde, Statistiek & Actuariaat
Universiteit Amtwerpen
Prinsstraat 13
2000 Antwerpen, België
E-mail : `zahidi@logique.jussieu.fr`