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

by Gunther Cornelissen, Thanases Pheidas and Karim Zahidi

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.

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 arbitrary 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 if $K = \mathbb{Q}$ ($\mathbb{Q}$), and for several other such $K$ (such as imaginary quadratic number fields [5], totally real fields [7], abelian number fields [11]) by reduction to the case $K = \mathbb{Q}$. This reduction consists in finding a diophantine model (cf. [2]) for integer arithmetic over $\mathcal{O}_K$. The problem is open for general number fields (for a survey see [9] and [12]), but has been solved conditionally, e.g. by Poonen [10] (who shows that the set if rational integers is diophantine over $\mathcal{O}_K$ if there exists an elliptic curve over $\mathbb{Q}$ that has rank one over both $\mathbb{Q}$ and $K$). In this paper, we give a more general condition as follows:

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

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

1
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 $\tilde{a} \in \mathbb{Z}$ with $\tilde{a}$ dividing $a$ and $|N(a)| \leq |\tilde{a}|^\ell$.

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

(i) there exists an abelian variety $G$ over $\mathbb{Q}$ such that $\text{rk} G(\mathbb{Q}) = \text{rk} G(K) > 0$;

(ii) there exists a commutative (not necessarily complete) group variety $G$ over $\mathbb{Z}$ such that $G(\mathcal{O}_K)$ is finitely generated and such that $\text{rk} G(\mathbb{Q}) = \text{rk} G(K) > 0$.

From (i) 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 $\mathbb{Q}$ such that it’s Jacobian satisfies this condition.

As we will prove below, part (ii) of this proposition is satisfied for the relative norm one torus $G = \ker(N_{K/L})$ 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 the main theorem 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 [10], but we have avoided continuous reference both for reasons of completeness and because our results have been obtained independently.

### 1. 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 $N = N_{K/Q}$ be the norm from $K$ to $\mathbb{Q}$, and let $n = [K : \mathbb{Q}]$ denote the degree of $K$. Let $| \cdot |$ 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 $\tilde{S} \subseteq (\mathcal{O} \times (\mathcal{O} - \{0\}))^n$ given by

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

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 $K$. 

\[2\]
Recall that there is no unique factorisation in general number fields, but we can use the following valuation-theoretic remedy:

1.1 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 \( a = \text{wn}(x) \) is a weak numerator and \( b = \text{wd}(x) \) is a weak denominator for \( x \).

1.2 Lemma. (i) For any \( x \in K \) a weak numerator and a weak denominator exists and is unique up to units.

(ii) For any valuation, \( v(x) > 0 \iff v(\text{wn}(x)) > 0 \) [and then \( v(\text{wn}(x)) = hv(x) \)], and \( v(x) < 0 \iff v(\text{wd}(x)) > 0 \) [and then \( v(\text{wd}(x)) = -hv(x) \)].

(iii) For \( a \in \mathcal{O}, x \in K \), “\( a = \text{wn}(x) \)” and “\( a = \text{wd}(x) \)” are diophantine over \( \mathcal{O} \).

Proof. Since \( \mathcal{O} \) is a Dedekind ring, \((x)\) has a unique factorisation in fractional ideals
\[ (x) = p_1 \cdots p_r \cdot q_1^{-1} \cdots q_s^{-1}. \]
We let \( a \) be a generator for the principal ideal \((p_1 \cdots p_r)^h\) and \( b \) a generator for \((q_1 \cdots q_s)^h\); these are obviously weak numerator/denominator for \( x \).

Uniqueness, (ii) and (iii) are obvious. \( \square \)

1.3 Lemma. (Denef-Lipshitz [8])
(i) If \( u \in \mathbb{Z} - \{0\} \) and \( \xi \in \mathcal{O} \) satisfy the divisibility condition
\[ 2^{n!+1} \prod_{i=0}^{n!-1} (\xi + i)^{n!} | u \]
then for any embedding \( \sigma : K \hookrightarrow \mathbb{C} \)
\[ (*)_u \quad |\sigma(\xi)| \leq \frac{1}{2} \sqrt[n!]{|N(u)|}. \]

(ii) If \( \tilde{u} \in \mathbb{Z} - \{0\}, q \in \mathbb{Z} \) and \( \xi \in \mathcal{O} \) satisfy \( (*)_{\tilde{u}} \) for any embedding \( \sigma : K \hookrightarrow \mathbb{C} \) and \( \xi \equiv q \mod \tilde{u} \), then \( \xi \in \mathbb{Z} \).

Proof. Easy to extract from the proof of Lemma 1 in [8]. \( \square \)

2. Lemmas on elliptic curves

Let \( E \) denote an elliptic curve of rank one over \( K \), written in Weierstrass form as
\[ E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \]
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 \( nP = (x_n, y_n) \).

2.1 Lemma. For any integer \( r \) the set \( rE(K) \) is diophantine over \( K \) and, if \( r \) is divisible by \( T \), then \( rE(K) = \langle rP \rangle \cong \mathbb{Z}_r \).

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. □

2.2 Lemma. There exists an integer $r > 0$ such that for any non-zero integers $m, n \in \mathbb{Z}$, $m$ divides $n$ if and only if $\text{wd}(x_m)|\text{wd}(x_n)$.

Proof. We reduce the claim to a statement about valuations using lemma 2.2(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 $v(x_m) < 0$, then $v(x_{mt}) = v(x_m) - 2v(t) \leq v(x_m)$ (13 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 (13 VII.6.1), such $r_0$ exists and it actually suffices to take $r_0 = 4\prod v(\Delta_E)$, where $\Delta_E$ 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 $\mathbb{Z}$. Indeed, the hypothesis means $r_0mP = r_0nP = 0$ in $E_v$. Since there exist integers $a, b \in \mathbb{Z}$ 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 [11] 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 $v(x_m) < 0$ 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 $n$. □

2.3 Lemma. Any $\xi \in \Omega - \{0\}$ divides the weak denominator of some $x_n$.

Proof. Let $v$ be a valuation lying over the prime $p_v$ of $\mathbb{Z}$, and assume that $v(\xi) = e_v > 0$. Then the group of non-singular points on $E$ modulo $v$ is finite, hence there exists an $n_v$ such that $n_vP = 0$ in this group, i.e., $v(x_{n_v}) < 0$. By the formal group law formula, we see that $v(x_{p_v^{e_v}n_vx}) = v(x_{n_v}) - 2v(p_v)_{v} < -e_v$. Putting

$$n = r \cdot \prod_{v(\xi) > 0} n_v p_v^{e_v}$$

will then certainly suffice. □

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

$$\text{wd}(x_m)|\text{wn}\left(\frac{x_n y_m}{y_n x_m} - q\right).$$
Proof. The formal power series expansion for addition on $E$ around 0 (\cite{[13]}, IV.2.3) implies that $\frac{x_n}{y_n} = q^m \frac{x_m}{y_m} + O((\frac{x_m}{y_m})^2)$, from which the result follows.

3. 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 2 for this $E$ — in particular, choose a suitable $r$ such that lemma 2.2 applies; we also choose $\ell$ which comes with the definition of $A$. We claim that the following formulæ give a diophantine definition of $Z$ in $\mathcal{O}$:

$$\xi \in Z \iff \exists m, n \in rT\mathbb{Z}, \exists u \in A - \{0\} \left\{ \begin{array}{l}
(1) \ m|n \\
(2) \ 2^{n+1} \prod_{i=0}^{n-1} (\xi^{\ell n!} + i)^{n!}|u \\
(3) \ u|\text{wd}(x_m) \\
(4) \ \text{wd}(x_m)|\text{wn}(\frac{x_n y_m}{x_m y_n} - \xi)\end{array} \right\}$$

3.1 Any $\xi \in Z$ satisfies the relations. If $\xi \in Z$, then a $u$ satisfying (2) exists because $A$ is division-dense. By lemma 2.3 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 2.4.

3.2 A $\xi$ satisfying the relations is integral. Let $q \in \mathbb{Z}$ satisfy $n = qm$ (which exists by (1)). Then lemma 2.4 implies that

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

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

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

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

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

(*) $\xi \equiv q \mod \tilde{u}; \quad \tilde{u}, q \in \mathbb{Z}$.

Condition (2) implies that Lemma 1.3(i) can be applied with $\ell^{n!}$ in place of $\xi$, so for any complex embedding $\sigma$ of $K$ we find

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

Because of (*)& (***), we can apply Lemma 1.3(ii) to conclude $\xi \in Z$.

3.3 The relations (1)-(4) are diophantine over $\mathcal{O}$. By 1.2 and 2.1 for $a \in \mathcal{O}$, the relations $\exists n \in rT\mathbb{Z} : a = \text{wn}(x_n)$ and $\exists n \in rT\mathbb{Z}$:
Let $a = \text{wd}(x_n)$ be 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 2.2. Conditions (2)-(4) are obviously diophantine using [1.2].

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

4.1 Rank-preservation over $\mathbb{Q}$. We use [3] as a general reference on abelian varieties and formal groups. Suppose there exists an abelian variety $G$ of dimension $d$ over $\mathbb{Q}$ such that $\text{rk}_G(\mathbb{Q}) = \text{rk}_G(K) > 0$ (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 $T \cdot G \cong G(K)$ 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 $0 = (1 : 0 : \ldots : 0)$ of $G$ (i.e., $\mathcal{O}_{G,0} = \mathbb{Q}[[t_1, \ldots, t_d]]$), and define

$$A_G := \{\text{wd}\left(\prod_{i=2}^N t_i(P)\right) : P \in T[G(K) : G(\mathbb{Q})] \cdot G(K) \text{ and } t_1(P) = 1\}.$$ 

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

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

(b) The analogue of lemma 2.3 remains valid:

Claim. $A_G$ is divisibility-dense.

Proof. Since any $\xi \in \mathcal{O} \setminus \{0\}$ divides its norm, it suffice to prove that any integer $z \in \mathbb{Z} \setminus \{0\}$ divides an element of $A_G$. Given a minimal model $\mathcal{G}_p$ for $G$ over a $p$-adic field $\mathbb{Q}_p$, let $\mathcal{G}_{p,0}$ denote the group of points whose reduction is non-singular modulo $p$. Then $\mathcal{G}_{p,0}$ is a clopen subset of $\mathcal{G}_p$, so $\mathcal{G}_p/\mathcal{G}_{p,0}$ is finite (and non-trivial only for the finite set of primes for which $\mathcal{G}_p$ has bad reduction). Hence we can choose a finite $r$ so large that $rP_i$ is non-singular modulo all primes for all generators $P_i$ of $G(\mathbb{Q})$. Pick a prime $p|z$, then since the group of non-singular points on $G$ modulo $p$ is finite, there exists $n_p$ such that $n_p rP = 0$ in this group, i.e., $v_p(t_i(P)) > 0$ for all $i$. The formal group $\hat{G}_0$ of $G$ around $0$ (defined by the power series that give the addition in terms of $\{t_i\}$) is a formal torus in characteristic zero, and
hence admits for any \( N > 0 \) a formal logarithmic isomorphism to a power of the additive group

\[
\phi : \hat{G}_0(p^N \mathbb{Z}_p) \cong \hat{G}_d(p^N \mathbb{Z}_p)
\]

preserving valuations. Hence for any \( n \),

\[
v(t_i(nP)) = v(\phi(t_i(nP))) = v(n(\phi(t_i(P)))) = v(n) + v(\phi(t_i(P))
\]

and we can find \( n \) such that \( v(t_i(P)) \) becomes arbitrary large as in (2.3) \( \Box \)

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

Remarks. (i) From available computer algebra, the construction of elliptic curves which fit the above can be automated. One can compute ranks of elliptic curves over \( \mathbb{Q} \) quite fast using \texttt{mwrank} by J. Cremona [1], and over number fields using the \texttt{gp}-package of D. Simon [14]. One finds for example unconditionally that the curve \( y^2 = x^3 + 8 \) has rank one over \( \mathbb{Q} \) and this rank stays the same over \( \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[4]{2}) \), hence the diophantine problem for the integers in these number fields has a negative answer (note that their Galois closures are non-abelian).

(ii) We ask: given \( K \), can one construct in some clever way a curve \( C \) over \( \mathbb{Q} \) such that its Jacobian satisfies the above conditions?

4.2 Rank-preservation over \( \mathbb{Z} \). 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 \( \mathbb{Z} \) such that \( G(\mathbb{Q}) \) is finitely generated and such that \( \text{rk} G(\mathbb{Z}) = \text{rk} G(\mathbb{Q}) > 0 \). As an example of this, let \( L \) be another number field, linearly disjoint from \( K \). Let \( \langle a_i \rangle \) denote a \( \mathbb{Z} \)-basis for \( L/\mathbb{Q} \) (this is also a basis for \( \mathcal{O}_{KL} \) over \( \mathcal{O}_K \)). Let \( T_L \) denote the norm one torus \( N_L^\mathbb{Q}(\sum a_i x_i) = 1 \). Then \( T_L(\mathbb{Z}) \cong \mathcal{O}_L^\times \) and

\[
T_L(\mathcal{O}_K) = \ker(N_K^{KL} : \mathcal{O}_K^{\times} \to \mathcal{O}_{KL}^{\times}),
\]

hence (by surjectivity of the relative norm) \( \text{rk} T_L(\mathcal{O}_K) = \text{rk} \mathcal{O}_{KL}^{\times} - \text{rk} \mathcal{O}_K^{\times} \).

In particular, \( T_L(\mathcal{O}_K) = T_L(\mathbb{Z}) \) iff

\[
\text{rk} \mathcal{O}_{KL} + s_{KL} = \text{rk} \mathcal{O}_K + s_K + r_L + s_L - 1
\]

where \( r_M, s_M \) denote the number of real, respectively half the number of complex embeddings of a number field \( M \).

(a) If \( K \) is totally real of degree \( d \), \( r_{KL} = dr_L, s_{KL} = ds_L \), hence we want \( r_L + s_L = 1 \), which we can achieve by choosing \( L \) quadratic imaginary; but then \( T_L(\mathbb{Z}) \) is of rank zero.
(b) If $K$ is totally complex of degree $d$, $r_K = 0, s_K = \frac{d}{2}$. Also $KL$ is then totally complex, so $r_{KL} = 0, s_{KL} = \frac{d}{2}[L : Q]$, hence we want $\frac{d}{2}(L : Q) - 1 = r_L + s_L - 1$, but since the right hand side is less than or equal to $[L : Q] - 1$, we find $d \leq 2$. Hence this strategy only works for $K$ quadratic imaginary.

The conclusion is that this approach covers Denef’s result from [6], except that he can discard the first condition in our theorem (existence of elliptic curve of rank one) by using a torus instead.

**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?

**Acknowledgements.** 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).

**References**

[1] J. Cheon and 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 and 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.

[3] G. Cornell and J.H. Silverman, *Arithmetic geometry*, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. Springer-Verlag (1986).

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

[5] M. Davis, Y. Matijasevič and 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 over algebraic integer rings. II*. Trans. Amer. Math. Soc. 257 (1980), no. 1, 227–236.

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

[9] T. Pheidas and 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.
[10] 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.

[11] H.N. Shapiro and A. Shlapentokh, *Diophantine relationships between algebraic number fields*. Comm. Pure Appl. Math. **42** (1989), no. 8, 1113–1122.

[12] 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.

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

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

Mathematisch Instituut, Universiteit Utrecht, Postbus 80010, 3508 TA Utrecht, Nederland (gc)

Department of Mathematics, University of Crete, P.O. Box 1470, Herakleio, Crete, Greece (tp)

Equipe de Logique Mathématique, U.F.R. de Mathématiques (case 7012), Université Denis-Diderot Paris 7, 2 place Jussieu, 75251 Paris Cedex 05, France (kz)

Email:
cornelissen@math.uu.nl,
pheidas@math.uoc.gr,
zahidi@logique.jussieu.fr

---

1All correspondence should be sent to this author.