PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 6, June 2009, Pages 1951–1959
S 0002-9939(08)09740-2
Article electronically published on December 18, 2008

DESCENT ON ELLIPTIC CURVES AND HILBERT'S TENTH PROBLEM

KIRSTEN EISENTRÄGER AND GRAHAM EVEREST

(Communicated by Ken Ono)

Abstract. Descent via an isogeny on an elliptic curve is used to construct two subrings of the field of rational numbers, which are complementary in a strong sense, and for which Hilbert's Tenth Problem is undecidable. This method further develops that of Poonen, who used elliptic divisibility sequences to obtain undecidability results for some large subrings of the rational numbers.

1. Hilbert's tenth problem

In 1970, Matijasevič [10], building upon earlier work of Davis, Putnam and Robinson [5], resolved negatively Hilbert's Tenth Problem for the ring $\mathbb{Z}$ of rational integers. This means there is no general algorithm which will decide if a polynomial equation, in several variables, with integer coefficients has an integral solution. Equivalently, one says that Hilbert's Tenth Problem is *undecidable* for the integers. See [14, Chapter 1] for a full overview and background reading. The same problem, except now over the rational field $\mathbb{Q}$, has not been resolved. In other words, it is not known if there is an algorithm which will decide if a polynomial equation with integer coefficients (or rational coefficients, it doesn't matter) has a rational solution.

Recently, Poonen [11] took a giant leap in this direction by proving the same negative result for some large subrings of $\mathbb{Q}$. To make this precise, given a prime p of $\mathbb{Z}$, let $|.|_p$ denote the usual p-adic absolute value. Let S denote a set of rational primes. Write

$$\mathbb{Z}_S = \mathbb{Z}[1/S] = \{x \in \mathbb{Q} : |x|_p \leq 1 \text{ for all } p \notin S\},$$

for the ring of S-integers of $\mathbb{Q}$.

Theorem 1.1 (Poonen [11])**.** *There are recursive sets S of primes having density* 1 *with the property that Hilbert's Tenth Problem for $\mathbb{Z}_S$ is undecidable.*

Received by the editors October 9, 2007, and, in revised form, August 28, 2008.
2000 *Mathematics Subject Classification.* Primary 11G05, 11U05.
Key words and phrases. Elliptic curve, elliptic divisibility sequence, Hilbert's Tenth Problem, isogeny, primitive divisor, S-integers, undecidability.
The authors thank the ICMS in Edinburgh for the workshop on Number Theory and Computability in 2007 funded by EPSRC and the LMS.
The first author was partially supported by NSF grant DMS-0801123 and a grant from the John Templeton Foundation.

Given the importance of Theorem 1.1, it is surely worth investigating more closely the subrings $\mathbb{Z}_S$ of $\mathbb{Q}$ to which it applies. Besides the intrinsic interest, the hope remains that a solution for the rational field might be accessed through the rings $\mathbb{Z}_S$. The aim of this paper is to extend Poonen's method in a non-trivial fashion, by using descent on elliptic curves. As motivation, note that although the rings $\mathbb{Z}_S$ in Theorem 1.1 are formed by inverting sets of primes with density 1, the sets of primes are necessarily co-infinite. It is not even clear from [11] whether a finite collection of such rings will generate $\mathbb{Q}$. In this paper we provide examples where two rings suffice, and which are complementary in a strong sense. Write $\mathbb{P}$ for the set of all prime numbers.

Definition 1.2. Two subsets of $\mathbb{P}$ are said to be *complementary* if their union is $\mathbb{P}$. They are said to be *exactly complementary* if, in addition, they have empty intersection. A subset of $\mathbb{Z}$ is said to be *recursive* if there is an algorithm to decide if any given integer lies in that subset.

Theorem 1.3. *There are exactly complementary recursive sets $S, T \subset \mathbb{P}$ such that Hilbert's Tenth Problem is undecidable for both rings $\mathbb{Z}_S$ and $\mathbb{Z}_T$.*

Given sets S and T as in Theorem 1.3, any element $q \in \mathbb{Q}^*$ can be written

$$q = st \text{ with } s \in \mathbb{Z}_S^*, t \in \mathbb{Z}_T^*, \tag{1}$$

in a way that is unique up to sign. Equation (1) is a kind of *diophantine definition* (see [14, Chapter 1]) of the product group

$$\mathbb{Z}_S^* \times \mathbb{Z}_T^*$$

over the group $\mathbb{Q}^*$. Hitherto, the concept of diophantine definition has been studied only for rings and it is not known whether the property in (1) will permit some kind of 'lifting' of undecidability to the rational field.

Theorem 1.1 was proved by constructing a *diophantine model* of the positive integers in the ring $\mathbb{Z}_S$ using integer sequences (*elliptic divisibility sequences*) constructed from elliptic curves. Consult [11] and [14, Chapter 12] for the background and full details of the definitions.

Definition 1.4. We say a set $A \subseteq \mathbb{Z}_S$ is *diophantine* over $\mathbb{Z}_S$ to mean that A is a projection of the set of solutions of a diophantine equation over $\mathbb{Z}_S$. In other words, there exists $f \in \mathbb{Z}_S[y, x_1, \ldots, x_n]$ such that

$$a \in A \iff \exists \underline{t} \in \mathbb{Z}_S^n \text{ with } f(a, t_1, \ldots, t_n) = 0.$$

A *diophantine model* of $\mathbb{N}$ over $\mathbb{Z}_S$ is a bijection $\mathbb{N} \longleftrightarrow A$, where A is diophantine over $\mathbb{Z}_S$ with the additional property that the graphs of $+$ and $\times$ correspond to diophantine subsets of A^3.

As in [11, 14] the undecidability of $\mathbb{Z}$ is essentially equivalent to that of $\mathbb{N}$, together with $+$ and $\times$. Technically it is easier to model this latter set. Definition 1.4 is important because it allows undecidability results to be lifted from the positive integers to the set A. Exactly the same issue arises in this paper. On this point the arguments are identical.

1.1. **Background results.** Definition 1.4 brings to the fore the role played by diophantine equations. What follows is a brief overview of earlier results, which shows how advances have been made by changing the underlying equation. In [9], Kim and Roush resolved Hilbert's Tenth Problem negatively for rings $\mathbb{Z}_S$ when S consists of a single prime. The underlying equation involved a quadratic form, much in the spirit of earlier work by Julia Robinson. A negative answer to Hilbert's Tenth Problem for rings $\mathbb{Z}_S$, when S is finite, follows by using the concept of *diophantine class* as in [14, Chapter 4]. Shlapentokh [13] resolved Hilbert's Tenth Problem for some large subrings of number fields, where the underlying diophantine equation arose from a homogeneous polynomial known as a *norm form*. Poonen's Theorem [11], Theorem 1.1, is important because, for the first time, it resolved Hilbert's Tenth Problem for certain rings $\mathbb{Z}_S$ when S is infinite. His underlying equation was an elliptic curve and the definition of diophantine model was satisfied by using an elliptic divisibility sequence. Theorem 1.1 has been generalized to subrings of number fields in [12]. In another interesting direction, Cornelissen and Zahidi [3] also used an elliptic divisibility sequence to obtain decidability results.

2. Elliptic curves

Let E denote an elliptic curve,

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

where $a_1, \ldots, a_6$ denote integers. Consult [2, 15] for the basic properties of elliptic curves. Suppose $Q \in E(\mathbb{Q})$ denotes a non-torsion rational point. The shape of the defining equation (2) forces the denominator of the x-coordinate of a rational point to be a square, and that of the y-coordinate to be a cube. For $1 \leq n \in \mathbb{N}$, write nQ for the n-th multiple of Q according to the usual addition law on E. Then

$$nQ = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3}\right), \tag{3}$$

with A_n, B_n, and C_n denoting integers which satisfy $B_n > 0$ and $\gcd(B_n, A_nC_n) = 1$. The sequence $B = (B_n)$ is known as an *elliptic divisibility sequence*. An important property of B (the 'divisibility' part of its name) is the following:

$$n|m \text{ in } \mathbb{N} \text{ implies } B_n|B_m \text{ in } \mathbb{N}. \tag{4}$$

Definition 2.1. Let $B = (B_n)$ denote a sequence with integer terms. We say an integer $d > 1$ is a *primitive divisor* of the term $B_n \neq 0$ if

(a) $d \mid B_n$ and
(b) $\gcd(d, B_m) = 1$ for all non-zero terms B_m with $0 < m < n$.

In 1988, Silverman [16] proved an analogue of Bang's theorem [1] that the terms of elliptic divisibility sequences have primitive divisors for all sufficiently large indices.

Remark 2.2. If l denotes any prime divisor of d as in Definition 2.1, then it is referred to as a *primitive prime divisor* of B_n. Provided l is a prime of non-singular (hereafter *good*) reduction for E, an important group-theoretic interpretation of the situation is that n is the order of the point $Q \bmod l$ on the reduced curve. It follows that

$$B_m \equiv 0 \bmod l \text{ if and only if } n|m. \tag{5}$$

2.1. **Two primitive divisors.** Silverman's Theorem ensures that for all sufficiently large n, every term B_n has a primitive divisor. More can be said when descent via an isogeny is possible.

Proposition 2.3. *Suppose $Q \in E(\mathbb{Q})$ is a non-torsion point which generates an elliptic divisibility sequence $B = (B_n)$. Let $\sigma : E' \to E$ denote an isogeny of prime degree q and assume $Q = \sigma(Q')$ for some rational point $Q' \in E'(\mathbb{Q})$. Then all terms B_n, with n sufficiently large and coprime to q, have at least*[1] *two distinct primitive prime divisors.*

The techniques needed for the proof of Proposition 2.3 draw upon those used in [6], [7] and [8]. Write $\sigma^* : E \to E'$ for the dual isogeny, also of prime degree q. The compositions $\sigma\sigma^*$ and $\sigma^*\sigma$ are the maps $[q]$ (times q) on E and E' respectively. Given $\sigma : E' \to E$ and $Q = \sigma(Q')$, write $b = (b_n)$ for the elliptic divisibility sequence corresponding to Q'.

Definition 2.4. Given any elliptic divisibility sequence $B = (B_n)$, write B_n^* for the *primitive part* of B_n. This is the maximal divisor of B_n that is coprime to all the terms B_m with $0 < m < n$.

Lemma 2.5. *There are positive constants h and h' with $h = qh'$ such that for large n:*

- $\log B_n \sim hn^2$,
- $\log b_n \sim h'n^2$,
- $\log B_n^* \geq .547hn^2$.

Proof of Lemma 2.5. The first two formulae represent a strong form of Siegel's Theorem [15, Chapter IX]. See also [7] for a direct proof using elliptic transcendence theory. For the third formula, use [8, Lemma 3.3]. From this follows a lower bound of the form

$$\log B_n^* \geq \log B_n - \sum_{p|n} \log\left(p^2 B_{\frac{n}{p}}\right).$$

Now apply the first formula together with the upper bound

$$\sum_p \frac{1}{p^2} < .453.$$

The constants $h = \hat{h}(Q)$ and $h' = \hat{h}(Q')$ represent the canonical height of Q and Q' on their respective curves. The relation $h = qh'$ is a property of the canonical height under isogeny. □

Proof of Proposition 2.3. Let p denote any prime of non-singular reduction for E (or E'; the two curves share the same set of good reduction primes). By applying an isomorphism to E' if necessary, Velu's formulae [17] imply

$$\operatorname{ord}_p(b_n) \leq \operatorname{ord}_p(B_n) \leq \operatorname{ord}_p(b_{qn}) \text{ for all } n \geq 0. \tag{6}$$

For all sufficiently large n, the term b_n has a primitive prime divisor l_n. Assume that n is large enough to guarantee that l_n is a prime of good reduction. Then l_n is a divisor of B_n by (6). If $\gcd(q, n) = 1$, we claim that l_n is actually a primitive

[1] 'At least' means no fewer than.

prime divisor of B_n. If not, then $l_n|B_m$, for some $0 < m < n$, chosen minimally. In group-theoretic terms (see Remark 2.2), this means

$$mQ \equiv nQ' \equiv O \bmod l_n$$

on the corresponding reduced curves. Now (5) implies the following divisibility relations:

$$m|n \text{ and } n|qm.$$

Since q is prime, these force $n = qm$, contradicting the assumption that $\gcd(q, n) = 1$.

The proof is now completed using the data about growth rates of the various sequences in Lemma 2.5. Note [6, 7] that the contribution to B_n from primes of singular (hereafter *bad*) reduction is negligible. In particular, it follows that B_n^* grows asymptotically faster than its divisor b_n^*. It remains to show that for all large enough n, B_n^* has a prime divisor which is coprime to b_n^*. This forces B_n^* to have at least two distinct prime divisors, which is the desired conclusion. To prove this last claim use the following property of elliptic divisibility sequences from the p-adic theory of elliptic curves. The property can be sourced in [15, Chapter IV] and is stated in [8, Lemma 3.1]. It says that provided $l_n > 2$ and $l_n|b_n$,

$$\operatorname{ord}_{l_n}(b_{qn}) = \operatorname{ord}_{l_n}(b_n) + \operatorname{ord}_{l_n}(q). \tag{7}$$

If $l_n| \gcd(B_n^*, B_n^*/b_n^*)$, then (6) implies that

$$\operatorname{ord}_{l_n}(b_{qn}) > \operatorname{ord}_{l_n}(b_n).$$

Now (7) shows that the only way this can happen is if $l_n|q$. We may assume n is large enough to avoid this possibility. □

3. Proof of Theorem 1.3

Proof of Theorem 1.3. Assume E is an elliptic curve and there is an isogeny $\sigma : E' \to E$ of prime degree q such that:

- $E(\mathbb{Q}) = \langle Q \rangle \simeq \mathbb{Z}$,
- $E(\mathbb{R})$ has only one real-connected component,
- Q is the image of a $\mathbb{Q}$-rational point under σ,
- $B_q > 1$.

Example 3.1. $y^2 = x^3 - 4$, $Q = [2, 2]$. This curve has conductor 432, which appears as $b1$ in Cremona's tables [4]. There is a 3-isogeny[2] from the curve (called $b2$) $y^2 = x^3 + 108$ which maps $[6, 18]$ to Q. The properties claimed are easily checked.

By Proposition 2.3, for all sufficiently large primes l, B_l has at least two distinct primitive prime divisors. (Any prime divisor of a term B_l, with l a prime, is necessarily a primitive prime divisor, using (5): the essential contribution of Proposition 2.3 is that it guarantees at least two distinct prime divisors.) Also, by Proposition 2.3, each term $B_{ll'}$, where l, l' are distinct primes, has at least two distinct primitive prime divisors, except possibly for a finite number of pairs (l, l'), provided the primes l and l' are distinct from q.

[2] An example meeting the needs of the proof will necessarily have degree greater than 2. This is because a curve with a 2-isogeny will have a rational 2-torsion point.

Definition 3.2. For every prime l, let $a_l \geq 1$ denote the smallest integer such that $B_{l^{a_l}} > 1$. Let L denote the set of primes l such that $a_l > 1$. Then L is finite by Siegel's Theorem. In Example 3.1, $2 \in L$ because $B_2 = 1$. Also, [15, Proposition 2.5], the set of everywhere good reduction points forms a subgroup of $E(\mathbb{Q})$. It follows that for each bad reduction prime p, this subgroup contains the kernel of reduction mod p. Thus $b_p > 1$ exists such that $p|B_n$ if and only if $b_p|n$. Write b for the computable number consisting of the largest of the b_p.

Exactly as in [11], use Vinogradov's Theorem [18, Chapter XI] on the additive circle

$$E(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z} \simeq [0, 1).$$

This theorem guarantees that the multiples lQ, with l prime, are dense in the real curve $E(\mathbb{R})$. With b as in Definition 3.2, choose a set U of primes inductively as follows: given $l_1, \ldots, l_{i-1}$ choose l_i to be the smallest prime outside $L \cup \{q\}$ with $l_i > l_j > b$ for all $j < i$ and

$$|y_i - i| < 1/10i, \text{ where } l_i Q = (x_i, y_i). \tag{8}$$

3.1. **Definition of S.** For all sufficiently large n define p_n to be the largest primitive prime divisor of B_n, which is also a good reduction prime: this exists by [16]. Let the set S_1 consist of the prime divisors of all the terms $B_{l_i}, i \in \mathbb{N}$. The elements of S_1 are all good reduction primes because $l_i > b$ for all $i \in \mathbb{N}$. Now define the set S_2 by

$$S_2 = \{p_l : l \text{ prime} \neq l_i \forall i\} \cup \{p_{l_i l_j} : 1 \leq j \leq i\} \cup \{p_{l l_i} : l \in L, i \in \mathbb{N}\}. \tag{9}$$

Clearly $S_1 \cap S_2 = \emptyset$. Let S denote any set containing S_1 but disjoint from S_2. The primes in S_2 act as witnesses to elements being outside of $E(\mathbb{Z}_S)$. In other words, as in [11, 14],

$$\bigcup_i \{\pm l_i Q\} = E(\mathbb{Z}_S), \tag{10}$$

with at most finitely many exceptions. For convenience, a proof of (10) is now indicated. Clearly all $\pm l_i Q \in E(\mathbb{Z}_S)$ because the primes dividing terms B_{l_i} lie in $S_1 \subseteq S$. On the other hand, for all large enough n,

$$\begin{aligned} n \neq \pm l_i \text{ some } i \quad &\Longrightarrow \quad l|n \text{ for some } l \neq l_i \text{ or } l_i l_j | n \text{ or } l l_i | n, l \in L \\ &\Longrightarrow \quad \exists p | B_n \text{ with } p = p_l \text{ or } p = p_{l_i l_j} \text{ or } p = p_{l l_i}, l \in L \\ &\Longrightarrow \quad \exists p | B_n \text{ with } p \in S_2 \subseteq S' \\ &\Longrightarrow \quad nQ \notin E(\mathbb{Z}_S). \end{aligned}$$

Write A for the set $A = \{y_i : l_i Q = (x_i, y_i)\}$. The bijection required by Definition 1.4 is $i \leftrightarrow y_i$. Plainly A is diophantine over $\mathbb{Z}_S$, using the underlying diophantine equation of the elliptic curve.

Lemma 3.3. *The graphs of $+$ and $\times$ correspond to diophantine subsets of A^3.*

Lemma 3.3 is proved in [11, Section 10]. For example, it follows from (8) that $m + n - q$ differs from $y_m + y_n - y_q$ by at most $3/10$. Therefore adding on $\mathbb{N}$ corresponds to adding on A, then rounding to the nearest element. In other words, $m + n = q$ corresponds to a diophantine predicate on A. Multiplication is similar because it can be obtained by squaring and adding. It follows *mutatis mutandis* that $\mathbb{N}$ has a diophantine model in $\mathbb{Z}_S$ and therefore Hilbert's Tenth Problem is undecidable in $\mathbb{Z}_S$.

3.2. **Definition of T.** Define p'_n, for all sufficiently large n with $q \nmid n$, to be the second largest good reduction primitive prime divisor of B_n. This exists by Proposition 2.3. Now define $T_1 = S_1$ and

$$T_2 = \{p'_l : l_i \neq l \text{ prime}\} \cup \{p'_{l_i l_j} : 1 \leq j \leq i\} \cup \{p'_{ll_i} : l \in L, i \in \mathbb{N}\}. \tag{11}$$

The hypothesis that $B_q > 1$ implies $q \notin L$. This is used to guarantee that p'_{ll_i} exists for all large i. Let T denote any set containing T_1 but disjoint from T_2. In exactly the same way as before,

$$\bigcup_i \{\pm l_i Q\} = E(\mathbb{Z}_T),$$

with at most finitely many exceptions. Again $\mathbb{N}$ has a diophantine model in $\mathbb{Z}_T$ and therefore Hilbert's Tenth Problem is undecidable in $\mathbb{Z}_T$. Note that $S_2 \cap T_2 = \emptyset$, so choose

$$S = \mathbb{P} - S_2 \text{ and } T = \mathbb{P} - T_2.$$

This results in $S \cup T = \mathbb{P}$. Subsequently, it will be argued that the sets $S_i, T_i, i = 1, 2$ are recursive. It follows that both S and T can be chosen to be recursive. This completes the proof that complementary sets can be found. This argument will now be refined.

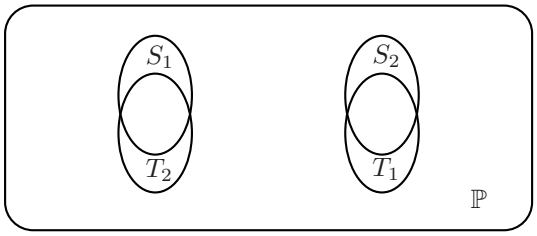
3.3. **Exactly complementary sets.** To show that S and T may be chosen in an exactly complementary fashion, choose the sets S_1 and S_2 exactly as before. Now choose a set U' of primes inductively as follows: given $l'_1, \ldots, l'_{i-1}$ choose l'_i to be the smallest prime outside $U \cup L \cup \{q\}$ with $l'_i > l'_j > b$ for all $j < i$ and

$$|y'_i - i| < 1/10i, \text{ where } l'_i Q = (x'_i, y'_i). \tag{12}$$

The set U' exists by Vinogradov's Theorem again. Define the set T_1 to consist of all prime divisors of the terms $B_{l'_i}, i \in \mathbb{N}$. The set T_1 contains only good reduction primes, also $T_1 \cap S_1 = \emptyset$ and $T_1 \cap S_2 \neq \emptyset$. Now choose T_2 as follows:

$$T_2 = \{p'_l : l'_i \neq l \text{ prime}\} \cup \{p_{l'_i l'_j} : 1 \leq j \leq i\} \cup \{p_{ll'_i} : l \in L, i \in \mathbb{N}\}. \tag{13}$$

Then T_2 is disjoint from $T_1 \cup S_2$, but it has non-empty intersection with S_1. Now let S denote any recursive set containing $S_1 \cup T_2$ but disjoint from $S_2 \cup T_1$, for example, $S = S_1 \cup T_2$. Then S will contain S_1 and be disjoint from S_2. Let T be the complement of S. The set T will necessarily contain $S_2 \cup T_1$ and be disjoint from $S_1 \cup T_2$. It follows that T will contain T_1 and be disjoint from T_2. A Venn diagram helps to explain the relationship between these sets.



The undecidability results follow exactly as before, and this completes the proof of Theorem 1.3.

3.4. **Recursive sets.** The sets of primes S_1, S_2, T_1, T_2 contain only good reduction primes. The sets U and U' are recursive because the members form a strictly increasing sequence, the terms of which can be computed in order. In what follows, let $p > 0$ denote a prime of good reduction, and let n_p denote the order of Q mod p. Now $p|B_{l_i}$ for some i if and only if $n_p \in U$, which can be checked because U is recursive. It follows that S_1 is recursive. To see if S_2 is recursive, first show how to check if $p = p_l$ for some $l \notin U$. Factorizing $E_p = |E(\mathbb{F}_p)|$, one can decide if there is a prime factor $l|E_p$ such that $l \notin U$ because U is recursive, then check if $p = p_l$. To see if $p = p_{l_i l_j}$ for some $1 \leq j \leq i$, factorize n_p to see if it is the product of two elements $l_i, l_j \in U$ and $p = p_{l_i l_j}$. The latter condition can be checked by factorizing earlier terms: in fact, only B_{l_i} and B_{l_j} need to be checked. Checking to see if $p = p_{ll_i}$ for some $l \in L$ is similar. The set L is recursive because membership can be determined as follows: $l \in L$ if and only if $B_l = 1$. This completes the proof that S_2 is recursive. The proofs for T_1 and T_2 are almost identical, except that one checks for the second largest prime factor. □

References

[1] A. S. Bang, *Taltheoretiske Undersølgelser*, Tidskrift f. Math. **5** (1886), 70–80 and 130–137.

[2] J. W. S. Cassels, *Lectures on Elliptic Curves,* London Math. Soc. Student Texts **24**, Cambridge Univ. Press, 1991. MR1144763 (92k:11058)

[3] G. Cornelissen and K. Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, Journal für die Reine und Angewandte Mathematik **613** (2007), 1–33. MR2377127

[4] J. E. Cremona *Elliptic Curve Data*, updated 14-1-02, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`

[5] M. Davis, H. Putnam and J. Robinson, *The decision problem for exponential diophantine equations,* Annals of Math. (2) **74** (1961), 425–436. MR0133227 (24:A3061)

[6] G. Everest, V. Miller and N. Stephens, *Primes generated by elliptic curves,* Proc. Amer. Math. Soc. **132** (2004), 955–963. MR2045409 (2005a:11076)

[7] G. Everest and H. King, *Prime powers in elliptic divisibility sequences,* Math. Comp. **74** (2005), 2061–2071. MR2164113 (2006d:11057)

[8] G. Everest, G. Mclaren, and T. Ward, *Primitive divisors of elliptic divisibility sequences*, Journal of Number Theory **118**, no. 1 (2006), 71–89. MR2220263 (2007a:11074)

[9] K. H. Kim and F. W. Roush, *An approach to rational Diophantine undecidability,* Proceedings of the Asian Mathematical Conference, Hong Kong, 1990, World Sci. Publishing, 1992, 242–248. MR1168248

[10] Y. Matijasevič, *The Diophantineness of enumerable sets,* Dokl. Akad. Nauk. SSSR **191** (1970), 279–282. MR0258744 (41:3390)

[11] B. Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$*,* J. Amer. Math. Soc. **16**, no. 4 (2003), 981–990. MR1992832 (2004f:11145)

[12] B. Poonen and A. Shlapentokh, *Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models for large subrings of number fields,* Journal für die Reine und Angewandte Mathematik **588** (2005), 27–47. MR2196727 (2006m:11178)

[13] A. Shlapentokh, *A ring version of Mazur's conjecture on topology of rational points*, Int. Math. Res. Notices **7** (2003), 411–423. MR1939572 (2004j:11147)

[14] A. Shlapentokh, *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*, Cambridge University Press, Cambridge, 2007. MR2297245

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[16] J. H. Silverman, *Wieferich's criterion and the abc-conjecture,* J. Number Theory **30**, no. 2, (1988), 226–237. MR961918 (89m:11027)

[17] J. Velu, *Isogénies entre courbes elliptiques*. C. R. Acad. Sci. Paris **273** (1971), 238–241. MR0294345 (45:3414)
[18] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Interscience Publishers, London and New York, 1954. MR0062183 (15:941b)

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802
E-mail address: eisentra@math.psu.edu

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom
E-mail address: g.everest@uea.ac.uk