Arch. Math. 97 (2011), 141–149

0003-889X/11/020141-9
published online July 7, 2011
DOI 10.1007/s00013-011-0277-7

Archiv der Mathematik

Additional results to a theorem of Eisenträger and Everest

Stefan Perlega

Abstract. Revisiting a recent result of Eisenträger and Everest who proved that Hilbert's tenth problem is undecidable over certain subrings of $\mathbb{Q}$, two additional theorems are proved. The theorems show that we can specify certain conditions for the sets of primes which define these rings. Thus, the freedom we have when choosing these rings is further illustrated.

Mathematics Subject Classification (2010). 11G05, 11U05.

Keywords. Elliptic curve, Hilbert's tenth problem, Isogeny, S-integers, Undecidability.

1. Hilbert's tenth problem over subrings of $\mathbb{Q}$. Hilbert's tenth problem asks if there is an algorithm which decides whether a multivariable polynomial over a ring R has a root over R. The problem was initially stated for $R = \mathbb{Z}$ by Hilbert in 1900 and negatively resolved by Matijasevich in 1970 (thus, he proved that there is no such algorithm). We say that Hilbert's tenth problem is *undecidable* over $\mathbb{Z}$. Since then, Hilbert's tenth problem has been resolved over many different rings but still remains unresolved over others—most notably over $\mathbb{Q}$. In the last decade some progress has been made by finding large subrings of $\mathbb{Q}$ over which Hilbert's tenth problem is undecidable. All subrings of $\mathbb{Q}$ are of the form $\mathcal{O}_{\mathbb{Q},\mathcal{W}} := \{x \in \mathbb{Q} | \operatorname{ord}_p(x) \geq 0 \ \forall p \notin \mathcal{W}\}$ for a set of primes $\mathcal{W} \subseteq \mathcal{P}$ ($\mathcal{P}$ will denote the set of all prime numbers). The ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is called the ring of $\mathcal{W}$-integers. Of course, the size of these rings is directly related to the size of the set $\mathcal{W}$ for which we will use the following measure:

Definition 1.1. Let $\mathcal{W} \subseteq \mathcal{P}$ be any set of prime numbers. If the limit

$$\lim_{n\to\infty} \frac{|\{p \leq n | p \in \mathcal{W}\}|}{\pi(n)}$$

exists, its value is called the *natural density* of $\mathcal{W}$.

A ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is computable if and only if the set $\mathcal{W}$ is computable (see Proposition A.6.4 of [4] for a proof of this fact). Since Hilbert's tenth problem only makes sense over computable rings R, we are only interested in computable sets of primes $\mathcal{W}$.
The first result of this form was the following:

Theorem 1.2. (Poonen, 2003). *There is a computable set of prime numbers $\mathcal{W} \subseteq \mathcal{P}$ with natural density 1 such that Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.*

Poonen's theorem was first published in [3]. An extensive proof can also be found in chapter 12 of [4]. The result was recently refined in the following way:

Theorem 1.3. (Eisenträger, Everest, 2009). *There are two computable sets of prime numbers $\mathcal{T},\mathcal{U} \subseteq \mathcal{P}$ such that $\mathcal{T} \cap \mathcal{U} = \emptyset, \mathcal{T} \cup \mathcal{U} = \mathcal{P}$ and Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and over $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$.*

The theorem was published in [2]. It does not make any statement about the density of the sets $\mathcal{T}$ and $\mathcal{U}$. In fact, we can choose this density virtually freely, as the following theorem makes clear:

Theorem 1.4. *Let $\mathcal{W} \subseteq \mathcal{P}$ be any computable set of prime numbers with natural density $r \in [0,1]$. Then there is a computable set $\mathcal{T} \subseteq \mathcal{P}$ with natural density r and a computable set $\mathcal{U} \subseteq \mathcal{P}$ with natural density $1-r$ such that $\mathcal{T} \cap \mathcal{U} = \emptyset, \mathcal{T} \cup \mathcal{U} = \mathcal{P}$ and Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and over $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$.*

Remark 1.5 For a real number $r \in [0,1]$ there exists a computable set of prime numbers $\mathcal{W} \subseteq \mathcal{P}$ with natural density r if and only if there are computable sequences of integers $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}}$ such that a_n/b_n converges to r. This includes all rational numbers in the interval $[0,1]$ but also certain irrational numbers like $\sqrt{2}/2$ or $1/\pi$.

It is also not clear from Theorem 1.3 if we can choose the sets $\mathcal{T},\mathcal{U}$ freely to the point that we can always separate two distinct primes with $\mathcal{T}$ and $\mathcal{U}$. We will show that this is possible and prove the following theorem:

Theorem 1.6. *Let $P_1, P_2 \subseteq \mathcal{P}$ be two finite sets of prime numbers such that $P_1 \cap P_2 = \emptyset$. Then there is a computable set $\mathcal{T} \subseteq \mathcal{P}$ with $P_1 \subseteq \mathcal{T}$ and a computable set $\mathcal{U} \subseteq \mathcal{P}$ with $P_2 \subseteq \mathcal{U}$ such that $\mathcal{T} \cap \mathcal{U} = \emptyset, \mathcal{T} \cup \mathcal{U} = \mathcal{P}$ and Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and over $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$.*

Remark 1.7 It is conjectured in [4] that the *diophantine class* of a ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ does not change if a finite number of primes is added to or removed from $\mathcal{W}$. If this result would be proved, it would make Theorem 1.6 redundant since it would imply that Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ if and only if it is undecidable over $\mathcal{O}_{\mathbb{Q},(\mathcal{W}\cup P_1)\setminus P_2}$ where $P_1, P_2 \subseteq \mathcal{P}$ are finite sets.

2. Proofs of Theorem 1.4 and 1.6. The proof of the two theorems will be very similar to the proof of Theorem 1.2 and adopt several techniques of the proof of Theorem 1.3. Therefore, we will not prove most of the propositions in this

section but rather refer to the proofs in [2–4] and point out the differences. We will make use of elliptic curves with certain properties, the existence of which will be guaranteed by the following proposition:

Proposition 2.1. *There are two elliptic curves E, E' over $\mathbb{Q}$ and a $\mathbb{Q}$-isogeny $\phi : E' \to E$ of prime degree $q \in \mathcal{P}, q > 2$ with the following properties:*

(1) $E(\mathbb{Q}) =< P >\cong \mathbb{Z}$.
(2) *The generator P of $E(\mathbb{Q})$ has integer coordinates with respect to a chosen Weierstrass equation.*
(3) *There is a rational point $P' \in E'(\mathbb{Q})$ with $\phi(P') = P$.*
(4) $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ *as topological groups.*
(5) *E does not have complex multiplication.*

Proof. Let E be defined by the equation $y^2 = x^3 - 120x + 740$ and E' by $y^2 = x^3 - 10920x + 439220$. These curves have conductor 900 and appear as D1 and D2 in Cremona's tables in [1].
The group $E(\mathbb{Q})$ is generated by $P = (16, -54)$ and $E'(\mathbb{Q})$ is generated by $P' = (61, 9)$. It can be read off Cremona's tables that there is an isogeny over $\mathbb{Q}, \phi : E' \to E$ of degree 3 and that the properties (1) and (3) are fulfilled.
The discriminant of the given Weierstrass equation for E is $\Delta = -2^8 3^9 5^2$. By Corollary 2.3.1, Chapter V of [6] an elliptic curve defined over $\mathbb{R}$ which has a negative discriminant is isomorphic to $\mathbb{R}/\mathbb{Z}$ as a topological group.
Finally, the j-invariant of E is $j = 2^{13}3^{-3}5$. Suppose that E had complex multiplication. Then the j-invariant of E would have to be an integer by Theorem 6.1, Chapter II of [6] which leads to a contradiction. Therefore, all properties are fulfilled. □

For the rest of this article (except when explicitly stated otherwise) we will fix two elliptic curves E and E', a Weierstrass equation of E, a generator P of $E(\mathbb{Q})$ and an isogeny $\phi : E' \to E$ of degree $q > 2$ fulfilling the properties of Proposition 2.1. Let nP denote the n-th multiple of P and let $x(Q), y(Q)$ denote the x and y-coordinate of a rational non-zero point Q on E. We also fix two disjoint finite sets of prime numbers $P_1, P_2 \subseteq \mathcal{P}$.
$\mathcal{T}$ and $\mathcal{U}$ will be constructed from sets of the following form:

Definition 2.2. Let S_{bad} denote the set of bad-reduction-primes of E (S_{bad} is a finite set by Proposition 5.1, Chapter VII of [5]). Let $n \geq 1$. Then we define $D_n := \{p \in \mathcal{P} | \text{ord}_p(x(nP)) < 0\}$. Observe that this is the same set as $\{p \in \mathcal{P} | \text{ord}_p(y(nP)) < 0\}$ since there are integers A_n, B_n, C_n with $B_n > 0$ such that $A_n C_n$ and B_n are coprime and $nP = (A_n/B_n^2, C_n/B_n^3)$. Let $S_n := D_n \setminus (S_{\text{bad}} \cup P_1 \cup P_2)$. Notice that $D_1 = S_1 = \emptyset$ since P has integral coordinates.

The most important property of the sets D_n, S_n is the following:

Proposition 2.3. *Let $m, n \geq 1$. Then $D_m \cap D_n = D_{\gcd(m,n)}$.*

This proposition can be proved in the same way as Proposition 12.2.1 of [4] (which actually has the slightly weaker statement $S_m \cap S_n = S_{\gcd(m,n)}$ where $S_n = D_n \setminus S_{\text{bad}}$, but its proof can be generalized without any problems). In particular, we observe that the following statement is true:

Corollary 2.4. *Let $\ell, p \in \mathcal{P}, \ell \neq p$. Then $D_\ell \cap D_p = S_\ell \cap S_p = \emptyset$.*

Proof. This follows from Proposition 2.3 and the fact that $D_1 = \emptyset$. □

The following definition of the value a_ℓ is the first essential deviation from the proofs of Theorem 1.2 and 1.3 (where a_ℓ is defined as the smallest positive integer with $S_{\ell^{a_\ell}} \neq \emptyset$).

Definition 2.5. For $\ell \in \mathcal{P}$ we define $a_\ell \in \mathbb{N}$ as the smallest positive integer with the property that $|S_{\ell^{a_\ell}}| \geq 2$. Further, we define $\mathcal{L} := \{\ell \in \mathcal{P} | a_\ell > 1\}$.

Since our definition of a_ℓ deviates from the original, this is also true for $\mathcal{L}$. But the main property of $\mathcal{L}$, finiteness, is still fulfilled. To prove this fact and to show that a_ℓ is always well-defined, we will employ the following two propositions:

Proposition 2.6. (Siegel). *Let E be an arbitrary elliptic curve over $\mathbb{Q}$ in Weierstrass form and $\mathcal{S} \subseteq \mathcal{P}$ a finite set of prime numbers. Then the set*

$$\{Q \in E(\mathbb{Q}) | x(Q) \in \mathcal{O}_{\mathbb{Q},\mathcal{S}}\}$$

is finite.

This is proved in Corollary 3.2.1, Chapter IX in [5].

Proposition 2.7. (Eisenträger, Everest). *There is a $N \in \mathbb{N}$ such that $|S_n| \geq 2$ for all $n \geq N$ which are coprime to q.*

This is an immediate corollary of Proposition 2.3 in [2] which makes use of property (3) in our Proposition 2.1.

Proposition 2.8.

- *For every $\ell \in \mathcal{P}$ the value a_ℓ is well-defined.*
- *The set $\mathcal{L}$ is finite.*

Proof. Let $\ell \in \mathcal{P}$. We set $\tilde{P} := S_{\text{bad}} \cup P_1 \cup P_2$. This set is finite. It follows from Proposition 2.1 that there is a $n \in \mathbb{N}$ with $\ell^n P \notin E(\mathcal{O}_{\mathbb{Q},\tilde{P}})$. So let $p \notin \tilde{P}$ be a prime number dividing the denominator of $x(\ell^n P)$. It follows again from Proposition 2.1 that there is a $m \geq n$ with $\ell^m P \notin E(\mathcal{O}_{\mathbb{Q},\tilde{P}\cup\{p\}})$ and consequently $|S_{\ell^m}| \geq 2$.
Further, we know from Proposition 2.7 that there are only finitely many $\ell \in \mathcal{P}$ with $|S_\ell| < 2$. Therefore, we can conclude that $a_\ell = 1$ for all but finitely many $\ell \in \mathcal{P}$ and $\mathcal{L}$ is a finite set. □

Now that the well-definedness of a_ℓ is secured, we can define the following primes:

Definition 2.9. Let $\ell, p \in \mathcal{P}$. Then we define

- $p_\ell := \max S_{\ell^{a_\ell}}$,
- $p'_\ell := \max(S_{\ell^{a_\ell}} \setminus \{p_\ell\})$,
- $p_{\ell,p} := \max(S_{\ell p} \setminus (S_\ell \cup S_p))$

whenever these maxima exist. Observe that $p_\ell \neq p_p$ and $p'_\ell \neq p'_p$ for $\ell \neq p$ by Proposition 2.3.

The primes p_ℓ, p'_ℓ and $p_{\ell,p}$ also appear in the proofs of Theorem 1.2 and 1.3. They are used to 'witness' points outside of $E(\mathcal{O}_{\mathbb{Q},\mathcal{T}})$, respectively $E(\mathcal{O}_{\mathbb{Q},\mathcal{U}})$. Since our definition of a_ℓ deviates from the original definition, also our definitions of p_ℓ and p'_ℓ are a little different. Still, these primes will serve exactly the same purpose.

Proposition 2.10. *Let $\ell \in \mathcal{P}$. Then ℓ divides both $|E(\mathbb{F}_{p_\ell})|$ and $|E(\mathbb{F}_{p'_\ell})|$.*

Proof. Let $\pi_{p_\ell} : E(\mathbb{Q}) \to E(\mathbb{F}_{p_\ell})$ denote the reduction modulo p_ℓ. The curve $E(\mathbb{F}_{p_\ell})$ is non-singular since $p_\ell \notin S_{\text{bad}}$. Let $\tilde{\mathcal{O}}$ denote its neutral element. It is easy to see that $\pi_{p_\ell}(nP) = \tilde{\mathcal{O}}$ if and only if $p_\ell \in D_n$. Therefore, we have that $\pi_{p_\ell}(P) \neq \tilde{\mathcal{O}}$ and $\ell^{a_\ell}\pi_{p_\ell}(P) = \pi_{p_\ell}(\ell^{a_\ell}P) = \tilde{\mathcal{O}}$. But this implies that $E(\mathbb{F}_{p_\ell})$ has an element of order ℓ. Thus, ℓ divides $|E(\mathbb{F}_{p_\ell})|$. The same argument applies to $|E(\mathbb{F}_{p'_\ell})|$. □

Proposition 2.11. *Let $c > 0$. Then there is a $L \in \mathbb{N}$ such that $p_{\ell,p} > c$ for all $\ell, p \in \mathcal{P}$ with $\max\{\ell, p\} \geq L$.*

Proof. The well-definedness of $p_{\ell,p}$ for sufficiently large $\max\{\ell, p\}$ is proved in Proposition 12.2.2 of [4].
It can be proved with Proposition 2.3 that $p_{\ell,p} \neq p_{\ell',p'}$ if $(\ell, p) \neq (\ell', p')$. Thus, there are only finitely many pairs of primes (ℓ, p) such that $p_{\ell,p} \leq c$. This proves the remainder of the statement. □

To prove the density statement of Theorem 1.4, we need to introduce the value μ_ℓ and an essential result about it. Both have been borrowed in exactly the same form from the proof of Theorem 1.2.

Definition 2.12. Let $\ell \in \mathcal{P}$. Then we define

$$\mu_\ell := \sup_{n \geq 2} \frac{|\{p \in S_\ell | p \leq n\}|}{\pi(n)}.$$

Notice that, since the supremum in Definition 2.12 is attained for some $n \leq \max S_\ell$, the value μ_ℓ is computable for each ℓ.

Proposition 2.13. *Let $\varepsilon > 0$. Then the set $\{\ell \in \mathcal{P} | \mu_\ell > \varepsilon\}$ has natural density zero.*

This is Proposition 12.4.1 of [4].
The next result also appears in exactly the same form in the proofs of Theorem 1.2 and 1.3:

Proposition 2.14. *Let $I \subseteq \mathbb{R}$ be an interval with non-empty interior. Then the set $\{\ell \in \mathcal{P} | y(\ell P) \in I\}$ has positive natural density.*

This is Corollary 12.5.2 of [4]. It uses the fact that $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$.
The next proposition is the second essential deviation from previous proofs. It introduces two sets of primes $\mathcal{V}$ and $\mathcal{V}'$ with eight certain properties. The proof of Theorem 1.2 uses one set $\mathcal{V}$ with the properties (2)–(7) while the proof of Theorem 1.3 uses two sets $\mathcal{V}, \mathcal{V}'$ with the properties (1)–(3) and (7).

Proposition 2.15. *There are two sets of prime numbers* $\mathcal{V} = \{\ell_i | i \in \mathbb{Z}_{>0}\}$ *and* $\mathcal{V}' = \{\ell'_i | i \in \mathbb{Z}_{>0}\}$ *which are computable and satisfy the following conditions:*

(1) $\mathcal{V} \cap \mathcal{V}' = \emptyset$.
(2) $\ell_i, \ell'_i \notin \mathcal{L}\ \forall i \geq 1$.
(3) $\ell_{i+1} > \ell_i$ *and* $\ell'_{i+1} > \ell'_i\ \forall i \geq 1$.
(4) $\mu_{\ell_i} \leq 2^{-i}$ *and* $\mu_{\ell'_i} \leq 2^{-i}\ \forall i \geq 1$.
(5) $p_{\ell_i,\ell_j} > 2^i$ *and* $p_{\ell'_i,\ell'_j} > 2^i\ \forall i, j$ *with* $i \geq j \geq 1$.
(6) $p_{\ell_i,\ell} > 2^i$ *and* $p_{\ell'_i,\ell} > 2^i\ \forall i \geq 1\ \forall \ell \in \mathcal{L}$.
(7) $|y(\ell_i P) - i| \leq \frac{1}{10i}$ *and* $|y(\ell'_i P) - i| \leq \frac{1}{10i}\ \forall i \geq 1$.
(8) $D_{\ell_i} \cap P_2 = \emptyset$ *and* $D_{\ell'_i} \cap P_1 = \emptyset\ \forall i \geq 1$.

Proof. Suppose that we have already constructed $\ell_1, \ldots, \ell_{i-1}$ and $\ell'_1, \ldots, \ell'_{i-1}$. By Proposition 2.13 the natural density of the set of prime numbers ℓ which satisfy $\mu_\ell \leq 2^{-i}$ is 1. Also, by Proposition 2.14 the set of primes ℓ with $|y(\ell P) - i| \leq \frac{1}{10i}$ has positive natural density. Thus, the intersection of these two sets also has positive natural density. In particular, it is an infinite set. Obviously, $\ell \notin \mathcal{L}$ and $\ell > \max\{\ell_{i-1}, \ell'_{i-1}\}$ are fulfilled for all sufficiently large prime numbers ℓ. By Corollary 2.4 also $D_\ell \cap P_2 = \emptyset$ and $D_\ell \cap P_1 = \emptyset$ are fulfilled for sufficiently large ℓ. Finally, we know from Proposition 2.11 that there is a $L \in \mathbb{N}$ such that $p_{\ell,\ell}, p_{\ell,\ell_j}, p_{\ell,\ell'_j}, p_{\ell,\tilde{\ell}} > 2^i$ is true for all prime numbers $\ell \geq L$ and for all $j \in \{1, \ldots, i-1\}$ and $\tilde{\ell} \in \mathcal{L}$. Therefore, we know that there are two distinct prime numbers ℓ_i and ℓ'_i such that all these conditions are fulfilled.
Computability of $\mathcal{V}$ and $\mathcal{V}'$ follows from the fact that μ_ℓ, D_ℓ, p_ℓ and $p_{\ell,p}$ can be computed effectively from ℓ and p. □

The remaining definitions and results are all takeovers from the proofs of Theorem 1.2 and 1.3.

Definition 2.16.

- $T_1 := \bigcup_{i \geq 1} D_{\ell_i}$.
- $U_1 := \bigcup_{i \geq 1} D_{\ell'_i}$.
- $T_2 := \{p_\ell | \ell \in \mathcal{P} \setminus \mathcal{V}\} \cup \{p_{\ell_i,\ell_j} | i, j \geq 1\} \cup \{p_{\ell_i,\ell} | i \geq 1, \ell \in \mathcal{L}\}$.
- $U_2 := \{p'_\ell | \ell \in \mathcal{P} \setminus \mathcal{V}'\} \cup \{p_{\ell'_i,\ell'_j} | i, j \geq 1\} \cup \{p_{\ell'_i,\ell} | i \geq 1, \ell \in \mathcal{L}\}$.

It is now an easy observation that $T_1 \cap P_2 = U_1 \cap P_1 = T_2 \cap P_1 = U_2 \cap P_2 = \emptyset$.

Proposition 2.17. $T_1 \cap T_2 = U_1 \cap U_2 = T_1 \cap U_1 = T_2 \cap U_2 = \emptyset$.

Proof. This follows from Proposition 2.3, $\mathcal{V} \cap \mathcal{V}' = \emptyset$ and the fact that $p_\ell \neq p'_\ell$ for all ℓ. □

We will need the following two lemmas to verify that all these sets have natural density zero. For $n \in \mathbb{Z}_{>0}$ let $\omega(n)$ denote the number of distinct prime factors of n.

Lemma 2.18. (Poonen). *Let* $t \in \mathbb{Z}_{>0}$. *Then the natural density of the set* $\{p \in \mathcal{P} | \omega(|E(\mathbb{F}_p)|) < t\}$ *is zero.*

This is proved in Lemma 9.3 of [3] and makes use of the requirement that E does not have complex multiplication.

Lemma 2.19. *The natural density of the sets* $\{p_\ell | \ell \in \mathcal{P}\}$ *and* $\{p'_\ell | \ell \in \mathcal{P}\}$ *is zero.*

Proof. For every $t \in \mathbb{Z}_{>0}$ we have that

$$\{p_\ell | \ell \in \mathcal{P}\} \subseteq \{p \in \mathcal{P} | \omega(|E(\mathbb{F}_p)|) < t\} \cup \{p_\ell | \ell \in \mathcal{P}, \omega(|E(\mathbb{F}_{p_\ell})|) \geq t\}.$$

By Lemma 2.18 it suffices to show that the natural density of the sets $T^t := \{p_\ell | \ell \in \mathcal{P}, \omega(|E(\mathbb{F}_{p_\ell})|) \geq t\}$ tends to 0 as $t \to \infty$. For every $p_\ell \in T^t$ we have that $2^{t-1}\ell \leq |E(\mathbb{F}_{p_\ell})|$ since ℓ always divides $|E(\mathbb{F}_{p_\ell})|$ by Proposition 2.10. From a theorem of Hasse (Theorem 1.1, Chapter V of [5]) we can derive that $|E(\mathbb{F}_{p_\ell})| \leq p_\ell + 1 + 2\sqrt{p_\ell} \leq 4p_\ell$. Thus, we conclude that $\ell \leq 2^{3-t}p_\ell$. For every $p \in T^t$ there is a unique $\ell \in \mathcal{P}$ such that $p = p_\ell$ and so we have that

$$|\{p \in T^t | p \leq n\}| \leq \pi(2^{3-t}n) = (2^{3-t} + o(1))\pi(n)$$

as $n \to \infty$. Thus, the natural density of T^t is bound by 2^{3-t} which tends to 0 as $t \to \infty$. This proves our assertion for $\{p_\ell | \ell \in \mathcal{P}\}$.
The assertion for $\{p'_\ell | \ell \in \mathcal{P}\}$ can be proved in exactly the same way (remember that Proposition 2.10 also asserts that ℓ divides $|E(\mathbb{F}_{p'_\ell})|$). □

Proposition 2.20. *The sets* T_1, U_1, T_2 *and* U_2 *all have natural density zero.*

Proof. We have that $T_1 \subseteq \bigcup_{i \geq 1} D_{\ell_i} \cup S_{\text{bad}}$. The fact that the latter set has natural density zero is proved in Proposition 12.6.5 of [4] (it uses the property $\mu_{\ell_i} \leq 2^{-i}$). Therefore, the natural density of T_1 is also zero and it follows due to similar reasons that the natural density of U_1 is zero as well.
The proof for the natural density of T_2 is also contained in the proof of Proposition 12.6.5 of [4]. It makes use of the properties (6) and (7) in Proposition 2.15 and the fact that the natural density of the set $\{p_\ell | \ell \in \mathcal{P}\}$ is zero, which we have proved in Lemma 2.19. The statement can be proved for U_2 analogously. □

Proposition 2.21. *The sets* T_1, U_1, T_2 *and* U_2 *are all computable.*

Proof. This can be proved in the same fashion as Proposition 12.6.4 in [4]. □

To prove the undecidability of Hilbert's tenth problem over our rings, we will employ the concepts of *diophantine definitions* and *diophantine models* which are discussed extensively in [4].

Definition 2.22. Let R be a ring. A set $A \subseteq R^n$ is called diophantine over R if there is a polynomial $f \in R[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that

$$A = \{x \in R^n | \exists y \in R^m : f(x, y) = 0\}.$$

One way to prove that Hilbert's tenth problem is undecidable over a ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ would be to show that $\mathbb{Z}$ is a diophantine subset of $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$. We will use the following more general concept:

Definition 2.23. Let R be a ring and let $\tau : \mathbb{Z} \to R^n$ be an injective map with the property that the two sets

$$D_+ := \{(\tau(x), \tau(y), \tau(x+y)) | x, y \in \mathbb{Z}\} \subseteq R^{3n},$$
$$D_\times := \{(\tau(x), \tau(y), \tau(xy)) | x, y \in \mathbb{Z}\} \subseteq R^{3n}$$

are diophantine over R. Then we say that R has a diophantine model of $\mathbb{Z}$.

Proposition 2.24. *Let R be a computable ring which has a diophantine model of $\mathbb{Z}$. Then Hilbert's tenth problem is undecidable over R.*

This can be proved with Proposition 3.4.4 of [4].

Proposition 2.25. *Let $\mathcal{W} \subseteq \mathcal{P}$ be a set of prime numbers that satisfies either*

$$T_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus T_2 \text{ or } U_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus U_2.$$

Then $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ has a diophantine model of $\mathbb{Z}$.

Proof. Let $\mathcal{W}$ be a set of prime numbers which satisfies $T_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus T_2$. It can be proved in the same fashion as Proposition 12.6.6 of [4] that there is a finite set $A \subseteq \mathbb{Z}$ with

$$E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) = \{\pm \ell_i P | i \geq 1\} \cup \{nP | n \in A\}$$

(the proof uses the fact that $\mathcal{L}$ is a finite set). This implies that the set $\{y(\ell_i P) | i \geq 1\}$ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ (see Proposition 12.6.8 of [4] for the details). Now the map $\Phi : \mathbb{Z} \to \mathcal{O}_{\mathbb{Q},\mathcal{W}}$,

$$\Phi(i) := \begin{cases} y(\ell_i P) & i \geq 1 \\ y(-\ell_{-i} P) & i < 0 \\ 0 & i = 0 \end{cases}$$

defines a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ as it is described in section 12.7 of [4] (the proof makes use of the property (7) in Proposition 2.15).
Now let $\mathcal{W}'$ be a set of primes with $U_1 \subseteq \mathcal{W}' \subseteq \mathcal{P} \setminus U_2$. Then it can be proved in the same way that there is a finite set $B \subseteq \mathbb{Z}$ with

$$E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) = \{\pm \ell'_i P | i \geq 1\} \cup \{nP | n \in B\}$$

as well as that $\{y(l'_i P) | i \geq 1\}$ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}'}$ and that the map $\Phi' : \mathbb{Z} \to \mathcal{O}_{\mathbb{Q},\mathcal{W}'}$,

$$\Phi'(i) := \begin{cases} y(\ell'_i P) & i \geq 1 \\ y(-\ell'_{-i} P) & i < 0 \\ 0 & i = 0 \end{cases}$$

defines a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{W}'}$. □

Proof of Theorem 1.6. Define $\mathcal{T} := T_1 \cup U_2 \cup P_1$ and $\mathcal{U} := \mathcal{P} \setminus \mathcal{T}$. First we observe that $\mathcal{T}$ is computable by Proposition 2.21 and since P_1 is a finite set. Since $\mathcal{P}$ is computable, it follows that $\mathcal{U}$ is also computable. Consequently, $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$ are computable rings. The inclusion $P_1 \subseteq \mathcal{T}$ is obvious and since $P_1 \cap P_2 = T_1 \cap P_2 = U_2 \cap P_2 = \emptyset$, the inclusion $P_2 \subseteq \mathcal{U}$ is also fulfilled. But $T_1 \subseteq \mathcal{T} \subseteq \mathcal{P} \setminus T_2$ and $U_1 \subseteq \mathcal{U} \subseteq \mathcal{P} \setminus U_2$ are fulfilled as well by Proposition 2.17 and since $T_2 \cap P_1 = U_1 \cap P_1 = \emptyset$. Therefore, it follows with Proposition 2.25

and Proposition 2.24 that Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and over $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$. □

Proof of Theorem 1.4. Let $\mathcal{W} \subseteq \mathcal{P}$ be a computable set of prime numbers with natural density $r \in [0,1]$. Then we define $\mathcal{T} := (\mathcal{W} \cup T_1 \cup U_2) \setminus (T_2 \cup U_1)$ and $\mathcal{U} := \mathcal{P} \setminus \mathcal{T}$. Again, we observe that $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$ are computable rings. Now we have that

$$\frac{|\{p \leq n | p \in \mathcal{W}\}|}{\pi(n)} - \frac{|\{p \leq n | p \in T_2\}|}{\pi(n)} - \frac{|\{p \leq n | p \in U_1\}|}{\pi(n)} \leq \frac{|\{p \leq n | p \in \mathcal{T}\}|}{\pi(n)}$$
$$\leq \frac{|\{p \leq n | p \in \mathcal{W}\}|}{\pi(n)} + \frac{|\{p \leq n | p \in T_1\}|}{\pi(n)} + \frac{|\{p \leq n | p \in U_2\}|}{\pi(n)}$$

for all $n \in \mathbb{N}$. Since T_1, T_2, U_1 and U_2 have natural density zero by Proposition 2.20, we conclude that the natural density of $\mathcal{T}$ is r and the natural density of $\mathcal{U}$ is $1 - r$. By Proposition 2.17 we have that $T_1 \subseteq \mathcal{T} \subseteq \mathcal{P} \setminus T_2$ and $U_1 \subseteq \mathcal{U} \subseteq \mathcal{P} \setminus U_2$ are fulfilled. Once again, we conclude with Propositions 2.25 and 2.24 that Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{T}}$ and over $\mathcal{O}_{\mathbb{Q},\mathcal{U}}$. □

References

[1] J. E. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed., Cambridge University Press, Cambridge, 1997.

[2] K. Eisenträger and G. Everest, Descent on elliptic curves and Hilbert's tenth problem, Proc. Amer. Math. Soc. **137** (2009), 1951–1959.

[3] B. Poonen, Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$, J. Amer. Math. Soc. **16** (2003), 981–990.

[4] A. Shlapentokh, Hilbert's Tenth Problem, Cambridge University Press, Cambridge, 2007.

[5] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[6] J. H. Silverman, Advanced Topics in the arithmetic of elliptic curves, Springer-Verlag, New York, 1994.

Stefan Perlega
Lazarettgasse 41/14,
1090 Vienna,
Austria
e-mail: s.perlega@gmx.at

Received: 28 September 2010

Revised: 11 April 2011