The Journal of Symbolic Logic
Volume 82, Number 3, September 2017

THE DIOPHANTINE PROBLEM FOR ADDITION AND DIVISIBILITY OVER SUBRINGS OF THE RATIONALS

LEONIDAS CERDA-ROMERO AND CARLOS MARTINEZ-RANERO

Abstract. It is shown that the positive existential theory of the structure $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$, where S is a nonempty finite set of prime numbers, is undecidable. This result should be put in contrast with the fact that the positive existential theory of $(\mathbb{Z}; =, 0, 1, +, |)$ is decidable.

§1. Introduction. Hilbert's Tenth Problem (referred to as "H10" in the sequel) asks for the following: Given a polynomial equation (in several variables) and with coefficients in $\mathbb{Z}$, find a process according to which it can be determined in a finite number of steps whether the equation is solvable in $\mathbb{Z}$. Nowadays, one would ask whether the positive existential theory of the structure $(\mathbb{Z}; =, 0, 1, +, \cdot)$ is or not decidable. Building on works by M. Davis, H. Putnam and J. Robinson, Y. Matiyasevich gave in 1970 a negative answer to H10 (see [2]). Using J. Robinson's work [12] and Matiyasevich's result for H10 over $\mathbb{Z}$, one can show that, if S is a finite set of primes, then the Hilbert's Tenth problem over $\mathbb{Z}[S^{-1}]$ has a negative answer (see [13, p. 240] or [11, p. 982]). It is not known whether the analogue of H10 for the field $\mathbb{Q}$ of rational numbers is decidable or not.

In the late seventies, L. Lipshitz [5], and in parallel A. P. Bel'tyukov [1], showed that the positive existential theory of the structure $(\mathbb{Z}; =, 0, 1, +, |)$ is decidable (where $a \mid b$ is interpreted as "a divides b"). Namely, there is an algorithm for deciding whether or not an arbitrary sentence of the form

$$\exists x_1 \cdots \exists x_n \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) \mid g_i(x_1, \ldots, x_n),$$

where the f_i and g_i are linear polynomials with integer coefficients, is true over $\mathbb{Z}$. Note that the full theory is undecidable, essentially by techniques due to J. Robinson [12].

On the other hand, it is well known that the positive existential theory of the structure $(\mathbb{Q}; 0, 1, +, |)$ is decidable. It is worth mentioning that the structure $(\mathbb{Q}; 0, 1, +, |)$ is bi-interpretable with the structure $(\mathbb{Q}; 0, 1, +, \neq)$ (see [7, Theorem 3.1.9]). In view of the results above, the following question arises naturally.

Received March 7, 2016.
2010 *Mathematics Subject Classification.* 11U05.
Key words and phrases. positive-existential definability, S-integers, small rings.

0022-4812/17/8203-0017
DOI:10.1017/jsl.2016.64

QUESTION 1.1. *For which subrings $A \subseteq \mathbb{Q}$ is the positive existential theory of the structure $(A; =, 0, 1, +, |)$ decidable*?

It is well-known that the subrings of $\mathbb{Q}$ are of the form $\mathbb{Z}[S^{-1}]$, where S is a set of prime numbers. Let S denote a set of prime numbers and let $\mathcal{Z}$ denote the structure $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$. Note that analogues of Lipshitz's result on addition and divisibility have been obtained for several rings of functions (for example for polynomial rings over a decidable field—see [9], and for some richer structures—see [14]), so one may ask the analogue of Question 1.1 for all those rings.

Our main result is the following:

THEOREM 1.2. *If S is a nonempty finite set of prime numbers, then multiplication is positive existentially definable in $\mathcal{Z}$. In particular, the positive existential theory of the structure $\mathcal{Z}$ is undecidable.*

At first sight, it is slightly surprising that inverting a single prime makes a difference about the decidability of the structure. Nevertheless, inverting just one prime makes the group of units infinite. Moreover, our result can be contrasted with the following result of J. Denef (see [3]) where he shows that the positive existential theory of the structure $(\mathbb{Z}; 0, 1, +, |_p)$ is undecidable, where the symbol "$|_p$" has the following meaning for a fixed integer $p > 1$:

$$x \mid_p y \text{ if and only if there exist } z, i \in \mathbb{Z} \text{ such that } y = xzp^i.$$

Observe that the predicate $|_p$ is, in disguise, the divisibility in $\mathbb{Z}[\frac{1}{p}]$ restricted to $\mathbb{Z}$.

The main difficulties in adapting the arguments of J. Denef to our case come from the fact that our structure is not discrete. Nevertheless, we follow the classical strategy which consists of gradually defining the multiplication: first we square units, then we multiply a unit by an arbitrary element of the ring, and finally we define the squaring function. Multiplication is definable from the squaring function thanks to the identity $(x + y)^2 = x^2 + 2xy + y^2$.

We finish the introduction with a few questions that naturally arise from Theorem 1.2.

B. Poonen showed [11] that there exist sets S of primes of natural density 1 such that $\mathbb{Z}$ has a diophantine model in $\mathbb{Z}[S^{-1}]$ over the language of rings. This leads to the following question.

QUESTION 1.3. *Is there a set S consisting of infinitely many primes such that multiplication is positive existentially definable in the structure $\mathcal{Z}$*?

In [4], L. Lipshitz shows that if $\mathcal{O}$ is the ring of integers of a number field K, then multiplication can be recovered in a positive existential way from addition and divisibility if and only if K is not an imaginary quadratic extension of $\mathbb{Q}$. So more generally, we may ask:

QUESTION 1.4. *For which rings of algebraic S-integers is multiplication positive existentially definable from addition and divisibility*?

§2. Undecidability of the structure $\mathcal{Z}$. We recall that $\mathcal{Z}$ is by definition the structure $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$. In this section we prove Theorem 1.2 following the strategy described above. Before proceeding any further we need to introduce some notation.

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

Let $S = \{p_1, \ldots, p_M\}$ be a finite (nonempty) set of prime numbers. Consider the first order language with equality $\mathcal{L} = \{0, 1, +, |\}$, where the symbols 0, 1, + and | are interpreted as usual.

NOTATION 2.1. (1) $\mathfrak{as}(x, y)$ *stands for the formula* $x|y \wedge y|x$ (*namely, x and y are associate*).

(2) $x \pm y \mid w \pm z$ *stands for*

$$x + y \mid w + z \wedge x - y \mid w - z.$$

(3) *If* $\gamma = (\gamma_1, \ldots, \gamma_M)$ *is a vector of natural numbers, then* p^γ *will denote the product*

$$\prod_{i=1}^{M} p_i^{\gamma_i}.$$

(4) *We may write* $v \equiv w \pmod{l}$ *instead of* $l \mid v - w$ *in some formulas.*

DEFINITION 2.2. Let $\operatorname{ord}_p x$ be the p-adic order of $x \in \mathbb{Q}$. We define a norm function $N : \mathbb{Z}[S^{-1}] \longrightarrow \mathbb{Z}$ by

$$x \longmapsto x \prod p_i^{-\operatorname{ord}_{p_i} x}$$

if $x \neq 0$, and $N(0) = 0$.

We observe that the function N satisfies the following conditions:

- $N(xy) = N(x)N(y)$.
- $N(x) = 0$ if only if $x = 0$.
- $x \mid y$ if only if $N(x) \mid_{\mathbb{Z}} N(y)$, where $|_{\mathbb{Z}}$ means "divisibility in $\mathbb{Z}$", namely, there exists $k \in \mathbb{Z}$ such that $N(y) = kN(x)$.
- The norm of a unit is ± 1.

From now on, whenever it is clear from the context, we use the "|" symbol to indicate divisibility both in $\mathbb{Z}[S^{-1}]$ and in $\mathbb{Z}$.

We first show that the relation "different from 0" is positive existentially definable in $\mathcal{Z}$. In order to do this we need the following result of F. Pappalardi (see Theorem 3.1 [8]): Let $p_1, \ldots, p_M$ be as above. For all the primes q different from any of $p_1, \ldots, p_M$, we consider the quotient map $\pi : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} = \mathbb{F}_q$, since all the $p_i's$ map into units (by the universal property of localizations) the map π can be extended to a map $\overline{\pi} : \mathbb{Z}[S^{-1}] \to \mathbb{F}_q$. Let Γ denote the unit group of $\mathbb{Z}[S^{-1}]$ and let $\Gamma_q = \overline{\pi}(\Gamma)$, which can be interpreted as the reduction of Γ modulo q. We denote by $N_\Gamma(x)$ the number of primes $q \leq x$ such that q is not equal to any of the $p_1, \ldots, p_M$ and $\mathbb{F}_q^\times = \Gamma_q$.

THEOREM 2.3 (Pappalardi). *There exist constants* c_Γ *and* δ_Γ, *depending only on* Γ, *such that*

$$N_\Gamma(x) \leq \delta_\Gamma \frac{x}{\log x} + c_\Gamma \frac{x}{(\log\log x)^M \log x}.$$

Moreover, $\delta_\Gamma < 1$ *and it is explicitly computed in* [8].

LEMMA 2.4. *There exists a prime* q *not in* S, *and an integer* $b \in \{1, \ldots, q-1\}$, *such that* $qx + b$ *is never a unit as* x *varies in* $\mathbb{Z}[S^{-1}]$.

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

PROOF. We recall that the Prime Number Theorem tells us that

$$\pi(x) \sim \frac{x}{\log x},$$

where π is the prime-counting function. From Theorem 2.3 and the Prime Number Theorem, we can find a prime number $q \notin S$ so that $\Gamma_q \neq \mathbb{F}_q^\times$ since

$$N_\Gamma(x) \leq \left(\delta_\Gamma + c_\Gamma \frac{1}{(\log\log x)^M}\right) \frac{x}{\log x} \qquad \text{and} \qquad \delta_\Gamma < 1.$$

Choose b to be the residue modulo q of an element of $\mathbb{F}_q^\times \setminus \Gamma_q$. It is straightforward to check that q and b are as required. ⊣

LEMMA 2.5. *The relation "$\neq$" is positive existentially definable in the structure $\mathcal{Z}$.*

PROOF. Let q and b be integers given by Lemma 2.4. The formula

$$\psi_{\neq}(y) : \exists A, B, x (y \mid A \wedge qx + b \mid B \wedge A + B = 1)$$

defines the relation "$y \neq 0$" in $\mathcal{Z}$.

First note that the formula $\psi_{\neq}(y)$ translates to "There exist $r, s, x \in \mathbb{Z}[S^{-1}]$ such that $ry + s(qx + b) = 1$" in $\mathcal{Z}$.

If $y = 0$, then the formula is false, since by Lemma 2.4, $qx + b$ is never a unit in $\mathbb{Z}[S^{-1}]$.

Assume $y \neq 0$. Since q and b are relatively prime, by Dirichlet's theorem, there exists x such that $qx + b$ is a prime number, and furthermore coprime with $N(y)$. By Bézout's identity, there are integers r' and s such that

$$r'N(y) + s(qx + b) = 1.$$

Since $y = N(y)u$, where u is a unit, we have

$$\frac{r'}{u} y + s(qx + b) = 1. \qquad \dashv$$

REMARK 2.6. Lemma 2.5 allows us to write in our formulas expressions of the form $x \neq y$.

LEMMA 2.7. *Let x, y, z, and t be arbitrary elements of $\mathbb{Z}[S^{-1}]$. If for all i such that $1 \leq i \leq M$, we have $\operatorname{ord}_{p_i} x \neq \operatorname{ord}_{p_i} y$, $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} t$ and, furthermore $\mathfrak{as}(x \pm y, z \pm t)$ holds in $\mathcal{Z}$, then either $xt = yz$ or $xz = yt$.*

PROOF. Let u_1 and u_2 be units such that

$$x + y = u_1(z + t) \quad \text{and} \quad x - y = u_2(z - t). \tag{1}$$

Observe that since $\operatorname{ord}_{p_i} x \neq \operatorname{ord}_{p_i} y$, we have

$$\operatorname{ord}_{p_i}(x + y) = \min\{\operatorname{ord}_{p_i} x, \operatorname{ord}_{p_i} y\} = \operatorname{ord}_{p_i}(x - y)$$

and since $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} t$, we have

$$\operatorname{ord}_{p_i}(z + t) = \min\{\operatorname{ord}_{p_i} z, \operatorname{ord}_{p_i} t\} = \operatorname{ord}_{p_i}(z - t)$$

for all $1 \leq i \leq M$. Thus, for each $1 \leq i \leq M$, we have

$$\begin{cases} \operatorname{ord}_{p_i} u_1 + \min\{\operatorname{ord}_{p_i} z, \operatorname{ord}_{p_i} t\} = \min\{\operatorname{ord}_{p_i} x, \operatorname{ord}_{p_i} y\} \\ \operatorname{ord}_{p_i} u_2 + \min\{\operatorname{ord}_{p_i} z, \operatorname{ord}_{p_i} t\} = \min\{\operatorname{ord}_{p_i} x, \operatorname{ord}_{p_i} y\} \end{cases}$$

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

so that $\operatorname{ord}_{p_i} u_1 = \operatorname{ord}_{p_i} u_2$ (note that the hypothesis of the Lemma implies that all the terms in these equalities are actual integers). This implies that either $u_1 = u_2$ or $u_1 = -u_2$. We proceed by cases.

If $u_1 = u_2$, then from Equation (1), we have $x + y = u_1 z + u_1 t$ and $x - y = u_1 z - u_1 t$. By adding and subtracting these equations, we obtain $x = u_1 z$ and $y = u_1 t$, hence $xt = yz$.

If $u_1 = -u_2$, then from Equation (1), we have $x + y = u_1 z + u_1 t$ and $x - y = -u_1 z + u_1 t$. By adding and subtracting these equations again, we obtain $x = u_1 t$ and $y = u_1 z$, hence $xz = yt$. ⊣

The next Lemma is a first step to define the squaring function among units of $\mathbb{Z}[S^{-1}]$.

LEMMA 2.8. *Let x, y be units in $\mathbb{Z}[S^{-1}]$ with $x \neq \pm 1$ and $y \neq 1$. If for all i such that $1 \leq i \leq M$, we have $\operatorname{ord}_{p_i} x \neq \operatorname{ord}_{p_i} y$, then $y = x^2$ if and only if $\mathfrak{as}(x \pm 1, y \pm x)$ holds in $\mathcal{Z}$.*

PROOF. If $y = x^2$ then trivially $\mathfrak{as}(x \pm 1, y \pm x)$ holds in $\mathcal{Z}$ (since x is a unit). Suppose that $\mathfrak{as}(x \pm 1, y \pm x)$ is true in $\mathbb{Z}[S^{-1}]$. By Lemma 2.7, either $y = x^2$ or $xy = x$. Since x is a unit and $y \neq 1$, we conclude that $y = x^2$. ⊣

PROPOSITION 2.9. *The set*

$$\mathrm{SQ_u} = \{(x, y) \colon x, y \text{ are units in } \mathbb{Z}[S^{-1}] \text{ and } y = x^2\}$$

is positive existentially definable in the structure $\mathcal{Z}$.

PROOF. Write $I = \{0, 1, 2, 3\}^M$. The formula

$$\mathrm{Sq_u}(x, y) \colon x \mid 1 \wedge y \mid 1 \wedge \bigwedge_{\gamma \in I} \mathfrak{as}(p^{\gamma} x \pm 1, p^{2\gamma} y \pm p^{\gamma} x),$$

where $\gamma = (\gamma_1, \ldots, \gamma_M)$, defines the set $\mathrm{SQ_u}$.

Assume that $\mathrm{Sq_u}(x, y)$ holds. In particular, the formula

$$\mathfrak{as}(p^{\gamma} x \pm 1, p^{2\gamma} y \pm p^{\gamma} x)$$

holds for γ being such that

$$\gamma_i \in \{0, 1, 2, 3\} \setminus \left\{ -\operatorname{ord}_{p_i} x, -\frac{1}{2} \operatorname{ord}_{p_i} y, \operatorname{ord}_{p_i} x - \operatorname{ord}_{p_i} y \right\}$$

for each i. We have

- $\operatorname{ord}_{p_i} p^{\gamma} x = \gamma_i + \operatorname{ord}_{p_i} x \neq 0$,
- $\operatorname{ord}_{p_i} p^{2\gamma} y = 2\gamma_i + \operatorname{ord}_{p_i} y \neq 0$ and
- $\operatorname{ord}_{p_i} p^{\gamma} x - \operatorname{ord}_{p_i} p^{2\gamma} y = \gamma_i + \operatorname{ord}_{p_i} x - 2\gamma_i - \operatorname{ord}_{p_i} y \neq 0$,

so that $p^{\gamma} x$ and $p^{2\gamma} y$ satisfy the hypothesis of Lemma 2.8. We conclude that $y = x^2$. ⊣

REMARK 2.10. Proposition 2.9 allows us to write in our formulas expressions of the form $x^2, x^4, \ldots$ whenever x is a unit.

The next Lemma is the first step to show that multiplication between units and arbitrary elements is definable. Write $v(x, y, z)$ for the formula

$$\mathfrak{as}(y \pm 1, z \pm x) \wedge \mathfrak{as}(y \pm x, z \pm x^2).$$

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

LEMMA 2.11. *Let x be a unit in $\mathbb{Z}[S^{-1}]$ with $x \neq \pm 1$. If for all i such that $1 \leq i \leq M$, we have $\operatorname{ord}_{p_i} y \neq 0$, $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} x$, $\operatorname{ord}_{p_i} y \neq \operatorname{ord}_{p_i} x$ and $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} x^2$, then $z = xy$ if and only if $\mathcal{Z}$ satisfies $v(x, y, z)$.*

PROOF. Assume that the formula $v(x, y, z)$ holds in $\mathcal{Z}$. By Lemma 2.7, since $\mathfrak{as}(y \pm 1, z \pm x)$ holds, we have that either $z = xy$ or $x = yz$. Again by Lemma 2.7, since $\mathfrak{as}(y \pm x, z \pm x^2)$ holds, we have that either $z = xy$ or $x^3 = yz$. So the only case in which we may have $z \neq xy$ is when $x = yz$ and $x^3 = yz$, which would imply that $x = \pm 1$. ⊣

PROPOSITION 2.12. *The set*

$$P = \{(x, y, z) : x \text{ is a unit and } z = xy\}$$

is positive existentially definable in the structure $\mathcal{Z}$.

PROOF. Write $I = \{0, 1, 2, 3\}^M$. The formula

$$\operatorname{Pro}(x, y, z) \colon x \mid 1 \wedge \bigwedge_{(\delta,\gamma)\in I\times I} v(p^{\gamma}x, p^{\delta}y, p^{\delta+\gamma}z)$$

defines the set P. Note that if $z = xy$, then $\operatorname{Pro}(x, y, x)$ is trivially satisfied for $(x, y, z) \in P$, since $p^{\gamma}x$ is a unit. We now prove the converse. We choose δ_i such that

$$\delta_i \in \{0, 1, 2, 3\} \setminus \{-\operatorname{ord}_{p_i} y, \operatorname{ord}_{p_i} x - \operatorname{ord}_{p_i} z\}.$$

Once δ_i has been chosen, we choose γ_i such that

$$\gamma_i \in \{0, 1, 2, 3\} \setminus \{-\operatorname{ord}_{p_i} x, \delta_i + \operatorname{ord}_{p_i} y - \operatorname{ord}_{p_i} x, \delta_i + \operatorname{ord}_{p_i} z - 2\operatorname{ord}_{p_i} x\}.$$

From $\gamma_i \neq -\operatorname{ord}_{p_i} x$ we have $p^{\gamma}x \neq \pm 1$. In addition for each i, we have

- $\operatorname{ord}_{p_i} p^{\delta}y = \delta_i + \operatorname{ord}_{p_i} y \neq 0$,
- $\operatorname{ord}_{p_i} p^{\delta+\gamma}z - \operatorname{ord}_{p_i} p^{\gamma}x = \delta_i + \operatorname{ord}_{p_i} z - \operatorname{ord}_{p_i} x \neq 0$,
- $\operatorname{ord}_{p_i} p^{\delta}y - \operatorname{ord}_{p_i} p^{\gamma}x = \delta_i + \operatorname{ord}_{p_i} y - \gamma_i - \operatorname{ord}_{p_i} x \neq 0$ and
- $\operatorname{ord}_{p_i} p^{\delta+\gamma}z - \operatorname{ord}_{p_i} p^{2\gamma}x^2 = \delta_i + \operatorname{ord}_{p_i} z - \gamma_i - 2\operatorname{ord}_{p_i} x \neq 0$,

so that $p^{\gamma}x$, $p^{\delta}y$ and $p^{\delta+\gamma}z$ satisfy the hypothesis of Lemma 2.11. Since we assumed that $\operatorname{Pro}(x, y, z)$ holds, in particular $v(p^{\gamma}x, p^{\delta}y, p^{\delta+\gamma}z)$ holds, so we can conclude that $z = xy$. ⊣

REMARK 2.13. Proposition 2.12 allows us to write in our formulas polynomial expressions with coefficients in $\mathbb{Z}$ whenever the variable is a unit. For example, we can write the term $a_0 + a_1x + a_2x^2 + a_3x^3$ as follows:

$$\operatorname{Pro}(x, x, y) \wedge \operatorname{Pro}(x, y, z) \wedge w = a_0 + a_1x + a_2y + a_3z,$$

In particular, we can write expressions of the form $(x + 1)^n$ and $(x + 1)^n$ whenever x is a unit.

LEMMA 2.14. *Given $x_1, \ldots, x_n \neq 0$ in $S^{-1}\mathbb{Z}$, there exists a unit $u \neq 1$ such that each x_i divides $u - 1$.*

PROOF. Choose any prime q in S and consider

$$u = q^{\operatorname{lcm}\{\varphi(|N(x_i)|)\colon i=1,\ldots,n\}},$$

where "lcm" stands for "least common multiple". Since $N(x_i)$ divides

$$q^{\varphi(|N(x_i)|)} - 1$$

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

in $\mathbb{Z}$ (by Euler's theorem—note that $N(x_i)$ is prime with q by definition of the norm), also it divides $u-1$, hence

$$x_i = N(x_i)\prod p_j^{\operatorname{ord}_{p_j} x_i}$$

divides $u-1$ in $\mathbb{Z}[S^{-1}]$. ⊣

The formulas in the next Lemma are inspired by the ones in Lemma 3 of [10]. The adjustment that is needed is due to the fact that we are dealing with a nondiscrete structure.

In the following formulas, we will write u instead of (u_1,u_2,u_3,u_4). Let $I := \{0,1\}^M$. The following formula we will allow define the quadratic function in the structure $\mathcal{Z}$.

$$\varphi(x,y)\colon \exists u\Big(\bigwedge_{i=1}^{4} u_i \mid 1 \wedge \bigwedge_{i=1}^{3} u_i \neq 1 \wedge \varphi_0(x,y,u)\Big),$$

where $\varphi_0(x,y,u)$ is the conjunction of the following formulas:

$$\varphi_1(x,u_1)\colon \bigwedge_{\delta\in I} p^\delta x \pm 1 \mid u_1 - 1,$$

$$\varphi_2(y,u_1)\colon \bigwedge_{\gamma\in I} p^\gamma y \pm 1 \mid u_1 - 1,$$

$$\varphi_3(u_1)\colon p_1 \dots p_M + 1 \mid u_1 - 1,$$

$$\varphi_4(u_1,u_2)\colon (u_1-1)^{8M} \mid u_2 - 1,$$

$$\varphi_5(u_2,u_3)\colon u_2 - 1 \mid u_3 - 1,$$

$$\varphi_6(x,u_2,u_3,u_4)\colon \frac{u_3-1}{u_2-1}u_4 \equiv x \pmod{u_2-1},$$

$$\varphi_7(y,u_2,u_3,u_4)\colon \left(\frac{u_3-1}{u_2-1}u_4\right)^2 \equiv y \pmod{u_2-1}.$$

Remark 2.15. It is worth mentioning that in the formulas φ_6 and φ_7 we are using (abusing of) the congruence notation in order to make the forthcoming arguments more transparent.

However, for sake of completness we spell out, in gory details, the formula φ_6. First note that $\frac{u_3-1}{u_2-1} = z$ is equivalent to

$$\exists z'(u_3 - 1 = z' - z \wedge \operatorname{Pro}(u_2,z,z')).$$

Hence, $\varphi_6(x,u_2,u_3,u_4)$ can be written as:

$$\exists z', z''(u_2 - 1 | z'' - x \wedge \operatorname{Pro}(u_4,z,z'') \wedge\ u_3 - 1 = z' - z \wedge \operatorname{Pro}(u_2,z,z')).$$

Lemma 2.16. *Let x and y in $\mathbb{Z}[S^{-1}]$. If $\varphi(x,y)$ holds in $\mathcal{Z}$, then $y = x^2$.*

Proof. Let $\delta,\gamma \in I$ be such that, for each $1 \leq j \leq M$, we have

$$\operatorname{ord}_{p_j} p^\delta x \neq 0 \quad \text{and} \quad \operatorname{ord}_{p_j} p^\gamma y \neq 0.$$

Write $a = N(x)$ and $b = N(y)$, and for each i, $\alpha_i = \operatorname{ord}_{p_i} x$ and $\beta_i = \operatorname{ord}_{p_i} y$, so that

$$x = a\prod p_i^{\alpha_i} \quad \text{and} \quad y = b\prod p_i^{\beta_i}.$$

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

Since $\varphi_1(x, u_1)$ holds, we have that $N(\prod p_i^{\delta_i} x \pm 1)$ divides $N(u_1 - 1)$, hence if $x \neq 0$, then each α_i is nonzero and

$$\begin{aligned} |N(u_1 - 1)| &\geq \left| N\left(1 \pm x \prod p_i^{\delta_i}\right)\right| \\ &= \left| N\left(1 \pm a \prod p_i^{\alpha_i + \delta_i}\right)\right| \\ &= \left| a \prod_{\alpha_i + \delta_i \geq 0} p_i^{\alpha_i + \delta_i} \pm \prod_{\alpha_i + \delta_i < 0} p_i^{-\alpha_i - \delta_i} \right|. \end{aligned}$$

Analogously, since $\varphi_2(y, u_1)$ holds, if $y \neq 0$, then each β_i is nonzero and we have

$$\left| b \prod_{\beta_i + \gamma_i \geq 0} p_i^{\beta_i + \gamma_i} \pm \prod_{\beta_i + \gamma_i < 0} p_i^{-\beta_i - \gamma_i} \right| \leq |N(u_1 - 1)|.$$

Therefore, for each i such that $1 \leq i \leq M$, we have

$$|N(u_1 - 1)| \geq \begin{cases} \max\{|a|, |b|, p_i^{|\alpha_i| + \delta_i}, p_i^{|\beta_i| + \gamma_i}\} & \text{if } x \neq 0 \text{ and } y \neq 0, \\ \max\{|b|, p^{|\beta_i| + \gamma_i}\} & \text{if } x = 0 \text{ and } y \neq 0, \\ \max\{|a|, p^{|\alpha_i| + \delta_i}\} & \text{if } x \neq 0 \text{ and } y = 0. \end{cases} \tag{2}$$

We prove that in all cases, we have

$$|N(y - x^2)| < |N(u_2 - 1)|. \tag{3}$$

Indeed, if x and y are nonzero, then we have

$$\begin{aligned} |N(y - x^2)| &= \left| N\left(b \prod p_i^{\beta_i} - a^2 \prod p_i^{2\alpha_i}\right)\right| \\ &= \left| N\left(b \prod p_i^{\beta_i - 2\alpha_i} - a^2\right)\right| \\ &= \left| N\left(b \prod_{\beta_i - 2\alpha_i \geq 0} p_i^{\beta_i - 2\alpha_i} - a^2 \prod_{\beta_i - 2\alpha_i < 0} p_i^{2\alpha_i - \beta_i}\right)\right| \\ &\leq \left| b \prod_{\beta_i - 2\alpha_i \geq 0} p_i^{\beta_i - 2\alpha_i} - a^2 \prod_{\beta_i - 2\alpha_i < 0} p_i^{2\alpha_i - \beta_i}\right| \\ &\leq 2a^2 |b| \prod_{i=1}^{M} p_i^{2|\alpha_i| + |\beta_i|} \\ &< |N(u_1 - 1)|^{8M} \\ &\leq |N(u_2 - 1)|, \end{aligned}$$

where the strict inequality is justified by Equation (2) and the fact that

$$|N(u_1 - 1)| \geq 3$$

(since $\varphi_3(u_1)$ holds), and the last inequality by the fact that $\varphi_4(u_1, u_2)$ holds. Similarly, if $x = 0$ and $y \neq 0$, we have

$$|N(y)| = |b| < |N(u_1 - 1)|^{8M} \leq |N(u_2 - 1)|,$$

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

and if $x \neq 0$ and $y = 0$, then

$$|N(x^2)| = a^2 < |N(u_1 - 1)|^{8M} \leq |N(u_2 - 1)|.$$

On the other hand, since $\varphi_6(x, u_2, u_3, u_4)$ and $\varphi_7(y, u_2, u_3, u_4)$ hold, $u_2 - 1$ divides $y - x^2$. Hence, if $y - x^2 \neq 0$, then

$$|N(y - x^2)| \geq |N(u_2 - 1)|,$$

which contradicts the strict inequality (3). ⊣

LEMMA 2.17. *The set*

$$SQ = \{(x, y) \colon x, y \text{ are in } \mathbb{Z}[S^{-1}] \text{ and } y = x^2\}$$

is positive existentially definable in the structure $\mathcal{Z}$.

PROOF. We claim that the formula

$$\mathrm{Sq}(x, y) \colon (x = 0 \wedge y = 0) \vee \bigvee_{\delta \in I} (x = \pm p^{-\delta} \wedge y = p^{-2\delta}) \vee \varphi(x, y),$$

defines the set SQ. Indeed, if the formula holds, then it is immediate from Lemma 2.16 that $y = x^2$.

Suppose that $(x, y) \in SQ$. If $x = 0$ or $x = \pm p^{-\delta}$ for some $\delta \in I$, then $Sq(x, y)$ is trivially satisfied. Hence we can suppose $x \neq 0$ and $x \neq \pm p^{-\delta}$ for every $\delta \in I$.

For each $\delta \in I$, since $x \neq \pm p^{-\delta}$, we have $p^{\delta} x \pm 1 \neq 0$. We prove that $p^{\delta} y \pm 1 \neq 0$ for every δ. If $p^{\delta} y = \pm 1$, then $p^{\delta} x^2 = \pm 1$, hence $\delta_i + 2 \operatorname{ord}_{p_i} x = 0$, so that δ_i is even, namely $\delta_i = 0$ (since $\delta_i \in \{0, 1\}$). So we have $x = \pm 1$, which contradicts our hypothesis on x.

From Lemma 2.14, there is a unit u_1 distinct from 1 such that the formulas $\varphi_1(x, u_1)$, $\varphi_2(y, u_1)$ and $\varphi_3(u_1)$ are satisfied. Because $u_1 - 1$ is not zero we deduce, from Lemma 2.14 again, that there is a unit u_2 different from 1 such that the formula $\varphi_4(u_1, u_2)$ is satisfied. If we put

$$u_3 = u_2^{|N(x)|},$$

then u_3 is different from 1 (recall that $x \neq 0$), so that the formula $\varphi_5(u_2, u_3)$ is also satisfied.

Since

$$\frac{u_3 - 1}{u_2 - 1} = u_2^{|N(x)|-1} + \cdots + 1$$

and the right-hand side of this equality has $|N(x)|$ summands, we deduce that

$$\frac{u_3 - 1}{u_2 - 1} \equiv |N(x)| \pmod{u_2 - 1}.$$

If we choose

$$u_4 = \frac{x}{N(x)},$$

then the formulas $\varphi_6(x, u_2, u_3, u_4)$ and $\varphi_7(y, u_2, u_3, u_4)$ are satisfied. Thus, the formula $\varphi(x, y)$ is satisfied. ⊣

https://doi.org/10.1017/jsl.2016.64 Published online by Cambridge University Press

§3. **Acknowledgments.** We would like to thank Xavier Vidaux for many fruitful hours of conversations and his help in preparing this manuscript. We also like to thank Hector Pasten for providing a proof of Lemma 2.4. This is part of the first author doctoral thesis at the Universidad de Concepcion (Chile). The first author was supported by SENESCYT Convocatoria Abierta 2011 and partially supported by the project Fondecyt 1130134 of X. Vidaux. The second author was partially supported by Proyecto FONDECYT Iniciación No. 11130490.

REFERENCES

[1] A. P. Bel'tyukov, *Decidability of the universal theory of natural numbers with addition and divisibility*. ***Journal of Soviet Mathematics***, vol. 14 (1980), no. 5, pp. 1436–1444.

[2] M. Davis, *Hilbert's tenth problem is unsolvable*. ***The American Mathematical Monthly***, vol. 80 (1973), no. 3, pp. 233–269.

[3] J. Denef, *The diophantine problem for polynomial rings of positive characteristic,* ***Logic Colloquium 78*** (M. Boffa, D. van Dalen, and K. McAloon, editors), Elsevier, North-Holland, 1979, pp. 131–154.

[4] L. Lipshitz, *Undecidable existential problem for addition and divisibility in algebraic number rings II*. ***Proceedings of the American Mathematical Society***, vol. 64 (1977), no. 1, pp. 122–128.

[5] ———, *The diophantine problem for addition and divisibility.* ***Transactions of the American Mathematical Society***, vol. 235 (1978), pp. 271–283.

[6] ———, *Undecidable existential problem for addition and divisibility in algebraic number rings.* ***Transactions of the American Mathematical Society***, vol. 241 (1978), pp. 121–128.

[7] D. Marker, ***Model Theory: An Introduction***. Graduate Text in Mathematics, vol. 127, 2002.

[8] F. Pappalardi, *On the r-rank Artin conjecture.* ***Mathematics of Computation***, vol. 66 (1997), no. 218, pp. 853–868.

[9] T. Pheidas, ***The diophantine problem for addition and divisibility in polynomial rings***, Thesis, Purdue University, Springer-Verlag, New York, 1985.

[10] ———, *Undecidability result for power series rings of positive characteristic. II.* ***Proceedings of the American Mathematical Society***, vol. 100 (1987), no. 3, pp. 526–530.

[11] B. Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$. ***Journal of the American Mathematical Society***, vol. 16 (2003), no. 4, pp. 981–990.

[12] J. Robinson, *Definability and decision problems in arithmetic,* this Journal, vol. 14 (1949), pp. 98–114.

[13] A. Shlapentokh, *Defining integers*. ***Bulletin of Symbolic Logic***, vol. 17 (2011), no. 2, pp. 230–251.

[14] A. Sirokofskich, *Decidability of sub-theories of polynomials over a finite field,* ***Mathematical Theory and Computational Practice***, Lecture Notes in Computer Science, vol. 5635, Springer, Berlin, 2009, pp. 437–446.

DEPARTAMENTO DE MATEMÁTICA
UNIVERSIDAD DE CONCEPCIÓN
CASILLA 160-C, CONCEPCIÓN
CHILE
E-mail: leonidascerda@udec.cl

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
RIOBAMBA, ECUADOR
E-mail: lcerda@espoch.edu.ec

DEPARTAMENTO DE MATEMÁTICA
UNIVERSIDAD DE CONCEPCIÓN
CASILLA 160-C, CONCEPCIÓN
CHILE
E-mail: cmartinezr@udec.cl