Undecidability and Definability Using the Coprime Relation

Carl Jacobsen

28th April 2026

Master's Thesis Mathematics

Advisor: Prof. Dr. Philipp Hieronymi

Second Advisor: Dr. Tingxiang Zou

Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Contents

0 Overview

This master's thesis focuses on definability in the natural numbers equipped with the coprime relation '$\perp$' and a suitable function $f\colon \mathbb{N} \to \mathbb{N}$. It contains two main theorems. The first shows that $\mathrm{Th}(\mathbb{N}; \perp, f)$ is undecidable and the second describes the definable sets in $\langle \mathbb{N}; \perp, f\rangle$. Each theorem is followed by multiple examples of such functions f.

0.1 Undecidability using the coprime relation

In 1931 Gödel published his incompleteness theorems [Gö31]. A consequence of the first incompleteness theorem is that there is no algorithm deciding which sentences are true in $\langle \mathbb{N}; =, \times, +\rangle$, i.e. $\mathrm{Th}(\mathbb{N}; =, \times, +)$ is undecidable. This was contrary to the results of Presburger [Pre29] and Skolem [Sko30], which show that $\mathrm{Th}(\mathbb{N}; =, +)$ and $\mathrm{Th}(\mathbb{N}; =, \times)$ are decidable.

Skolem's result implies the decidability of $\mathrm{Th}(\mathbb{N}; \perp)$. Does this change if we add a function to $\langle \mathbb{N}; \perp\rangle$? In Chapter 1 we use the undecidability of $\mathrm{Th}(\mathbb{N}; =, \times, +)$ to prove that $\mathrm{Th}(\mathbb{N}; \perp, f)$ is undecidable for certain functions $f\colon \mathbb{N} \to \mathbb{N}$. The starting point is the next theorem of Woods, who studied the successor function $\mathrm{S}(n) \coloneqq n + 1$.

Theorem 0.1. *[Woo81]* $\mathrm{Th}(\mathbb{N}; \perp, \mathrm{S})$ *is undecidable.*

Generalizing Woods' arguments leads to Theorem 1.2 and Corollary 1.6. Let $\mathscr{L}$ be a language containing '$\perp$'. Define Π to be the set of prime powers and $\mathrm{Supp'}(n) \coloneqq \{p \in \Pi \mid p \not\perp n\}$.

Theorem 1.2. *Let* $\mathscr{M}$ *be an* $\mathscr{L}$*-structure on* $\mathbb{N}$*. If there are subsets* $\Pi^* \subseteq \Pi$ *and* $R \subseteq \Pi^* \times \Pi$*, both definable in* $\mathscr{M}$*, such that*

(i) $\Pi^*/\sim$ *is infinite and* Π^**,* R *are both closed under* $\sim$[1]

(ii) for all $m, n \in \mathbb{N}$ *with* $\mathrm{Supp'}(m) \subseteq \mathrm{Supp'}(n) \subset \Pi^*$ *there is some* $r \in \Pi$ *such that*

$$\mathrm{Supp'}(m) = \bigl\{p \in \mathrm{Supp'}(n) \mid R(p, r)\bigr\},$$

then $\mathrm{Th}(\mathscr{M})$ *is undecidable.*

Informally the theorem states the following. If for any $m, n \in \mathbb{N}$ with $m \mid n$ we can encode the prime divisors of m as a subset of the prime divisors of n using a single prime r, then we get undecidability. A good choice of $\Pi^* \subseteq \Pi$ allows us to consider only prime divisors that are easier to encode.

[1] i.e. $\forall p, p', q, q' \in \Pi\colon p \sim p', q \sim q' \implies \bigl(p \in \Pi^* \Leftrightarrow p' \in \Pi^*\bigr) \wedge \bigl(R(p,q) \Leftrightarrow R(p', q')\bigr)$

But the set of primes P and the divisibility relation may not be definable in $\langle \mathbb{N}; \perp, f \rangle$. Therefore we work with prime powers and the relation Supp'$(m) \subseteq$ Supp'(n) instead.

Using this theorem we prove in Chapter 1.2 that the following structures have an undecidable theory.

- $\langle \mathbb{N}; \perp, n \mapsto |L(n)| \rangle$ for $L \in \mathbb{Z}[X]$ with at least two non-zero coefficients
- $\langle \mathbb{N}; \perp, n \mapsto \varphi(n) \rangle$ for φ the Euler phi function
- $\langle \mathbb{N}; \perp, n \mapsto 1 + \prod_{p \not| n,\, p \in \mathrm{P}} p \rangle$
- $\langle \mathbb{N}; \perp, n \mapsto \rho(n) \rangle$ for $\rho \colon \mathbb{N} \to \mathrm{P}$ injective
- $\langle \mathbb{N}; \perp, n \mapsto a^n - 1 \rangle$ for $a > 1$
- $\langle \mathbb{N}; \perp, n \mapsto \lfloor \frac{an}{b} \rfloor \rangle$ for $a, b \in \mathbb{N}$ with $a \perp b, b \geq 2$

Previous results used '|' or '×' instead of '⊥' to prove undecidability of the theories of the following structures.

- $\langle \mathbb{N}; \,|\, , n \mapsto \rho(n) \rangle$ for $\rho \colon \mathbb{N} \to \mathrm{P}$ injective [CMR96]
- $\langle \mathbb{N}; =, \times, n \mapsto L_{a,b}(n) \rangle$ for $a, b \in \mathbb{N}_{>0}$ and $L_{a,b}(n) = an + b$ [Kor01]

0.2 Definability in the coprime setting

Julia Robinson proved in [Rob49] that $\langle \mathbb{N}; |, \mathrm{S} \rangle$ and $\langle \mathbb{N}; =, \times, + \rangle$ are interdefinable, where '|' is the divisibility relation and 'S' is the successor function. She wondered whether the result could be improved by replacing '|' with '⊥'. Woods showed that the question from Robinson is equivalent to a number-theoretic problem. Define $m \sim n$ if m and n have the same prime divisors.

Theorem 0.2. *[Woo81] The following claims are equivalent:*

(i) $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$ *and* $\langle \mathbb{N}; =, \times, + \rangle$ *are interdefinable*

(ii) there is some $k \in \mathbb{N}$ *such that for all* $m, n \in \mathbb{N}$ *we have*

$$\Big(\bigwedge_{i=0}^{k} \mathrm{S}^i(m) \sim \mathrm{S}^i(n) \Big) \implies m = n.$$

Claim (ii) is now called the *Erdős-Woods conjecture*. The conjecture, restricted to the set of prime powers Π, is a direct consequence of a result of Bang [Ban86]. Concretely we have for all $p, q \in \Pi$ that

$$\Big(\bigwedge_{i=0}^{2} \mathrm{S}^i(p) \sim \mathrm{S}^i(q) \Big) \implies p = q.$$

This was a key number-theoretic argument Richard used to obtain the following result.

Theorem 0.3. *[Ric85] Let $A \subseteq \mathbb{N}^N$ be definable in $\langle \mathbb{N}; =, \times, + \rangle$. Then $A \cap \Pi^N$ is definable in $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$.*

This leads to two questions. Does progress on the *Erdős-Woods conjecture* yield new results on definability in $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$? Given a function $f \colon \mathbb{N} \to \mathbb{N}$, when can we replace the successor function S by f and get similar results? Both questions are answered by Theorem 2.2.

For the definitions of ω-arithmetic and ω-translation see Chapter 2.1. Let $\vec{m}, \vec{n} \in \mathbb{N}^N$ and define $\vec{m} \sim_k \vec{n} \ :\Leftrightarrow\ \bigwedge_{i=0}^{k} \bigwedge_{j=1}^{N} f^i(m_j) \sim f^i(n_j)$.

Theorem 2.2. *Let $f \colon \mathbb{N} \to \mathbb{N}$ be definable in $\langle \mathbb{N}; =, \times, + \rangle$. If $\langle \mathbb{N}; \perp, f \rangle$ has ω-arithmetic and ω-translation, then for any $A \subseteq \mathbb{N}^N$ the following are equivalent:*

(i) A is definable in $\langle \mathbb{N}; \perp, f \rangle$

(ii) A is definable in $\langle \mathbb{N}; =, \times, + \rangle$ and there is some $k \geq 0$ such that for all $\vec{m} \in A, \vec{n} \in \mathbb{N}^N$ we have $\vec{m} \sim_k \vec{n} \ \Rightarrow\ \vec{n} \in A$.

We show that $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$ has ω-arithmetic and ω-translation in Lemma 2.8. Let $\mathrm{Def}(\mathbb{N}; \perp, f)$ denote the set of definable relations in $\langle \mathbb{N}; \perp, f \rangle$, analogously for $\langle \mathbb{N}; =, \times, + \rangle$. The next result combines Theorem 0.2 and Theorem 0.3.

Corollary 2.4. *Let $f \colon \mathbb{N} \to \mathbb{N}$ be definable in $\langle \mathbb{N}; =, \times, + \rangle$ and let $A \subseteq \mathbb{N}$ be definable in $\langle \mathbb{N}; \perp, f \rangle$. If $\langle \mathbb{N}; \perp, f \rangle$ has ω-arithmetic, ω-translation and there is some $k \in \mathbb{N}$ such that for all $m, n \in A$ we have*

$$m \sim_k n \implies m = n,$$

then for all $B \subseteq A^N$ we have $B \in \mathrm{Def}(\mathbb{N}; \perp, f)$ iff $B \in \mathrm{Def}(\mathbb{N}; =, \times, +)$.

The question whether $A \subseteq \mathbb{N}^N$ is definable in $\langle \mathbb{N}; \perp, f \rangle$ splits by Theorem 2.2 into the following two questions.

(a) Is A definable in $\langle \mathbb{N}; =, \times, + \rangle$?

(b) When does $\vec{m} \in A$ and $\vec{m} \sim_k \vec{n}$ imply $\vec{n} \in A$?

To show (a) one can use that any computably enumerable set is definable in $\langle \mathbb{N}; =, \times, + \rangle$. A theorem of Matiyasevich [Mat72] shows that the computably enumerable sets are the existentially definable sets in $\langle \mathbb{N}; =, \times, + \rangle$.

Answering (b) is a number-theoretic problem. A proof of the *Erdős-Woods conjecture* would solve it for $f = \mathrm{S}$.

But we can answer question (b) for certain functions. For $A \subseteq \mathbb{N}^N$ define $\mathrm{Cl}_0(A) := \big\{\vec{n} \in \mathbb{N}^N \mid \exists \vec{m} \in A \colon \vec{m} \sim \vec{n}\big\}$. This gives the next results.

- $\mathrm{Def}(\mathbb{N}; \perp, \omega) = \mathrm{Cl}_0\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$ for $\omega(n) := \#\big(\mathrm{Supp'}(n)/\sim\big)$
- $\mathrm{Def}(\mathbb{N}; \perp, !) = \mathrm{Def}(\mathbb{N}; =, \times, +)$ for $n! := 1 \cdot 2 \ldots n$

It was previously shown that $\mathrm{Def}(\mathbb{N}; |, !) = \mathrm{Def}(\mathbb{N}; =, \times, +)$ [Kor01].

Let $<_\Pi$ be the order restricted to Π. Bès and Richard showed in [BR98] that Theorem 0.3 also holds for $\langle \mathbb{N}; \perp, <_\Pi \rangle$. Let P_a be the set of primes and a-th powers of primes. They also proved that $\mathrm{Th}(\mathbb{N}; \perp, <_{\mathrm{P}_2})$ is undecidable. We prove the following for $a \geq 3$.

$$\mathrm{Def}(\mathbb{N}; \perp, <_{\mathrm{P}_a}) \supset \big\{A \cap \mathrm{P}_a^N \mid A \in \mathrm{Def}(\mathbb{N}; =, \times, +),\ A \subseteq \mathbb{N}^N\big\}$$

A curious consequence of Theorem 2.2 addresses a question proposed by Richard. Let Sq be the set of squares. Does the following equality hold?

$$\mathrm{Def}(\mathbb{N}; \perp, \mathrm{S}, \mathrm{Sq}) = \mathrm{Def}(\mathbb{N}; =, \times, +)$$

This would imply that the *Erdős-Woods conjecture* is true iff there is some $k \geq 1$ such that for all $m, n \in \mathbb{N}$ we have $m \in \mathrm{Sq},\ m \sim_k n \ \Rightarrow\ n \in \mathrm{Sq}$.

Conventions

We work in first-order logic without a logical symbol for equality. This setting is restrictive enough to obtain the definability results in Chapter 2, yet complex enough to produce the undecidability results in Chapter 1.

We further fix the following conventions:

- $0 \in \mathbb{N}$
- $\mathscr{L}$ is a language containing '$\perp$'
- $m \perp n$ iff there is no prime dividing m and n
- definability is meant without parameters.

1 Undecidability

In this chapter we will prove undecidability of $\mathrm{Th}(\mathbb{N}; \perp, f)$ for certain functions $f\colon \mathbb{N} \to \mathbb{N}$.

1.1 First theorem

We first introduce the basic notation of this thesis.

Definition 1.1. Define

(i) $\Pi \coloneqq \big\{ p \in \mathbb{N} \mid p \not\perp p,\ \forall m, n\colon (p \not\perp m, p \not\perp n) \;\Rightarrow\; m \not\perp n \big\}$

(ii) $\mathrm{Supp'}(n) \coloneqq \{ p \in \Pi \mid p \not\perp n \}$

(iii) $m \sim n \;:\Leftrightarrow\; \mathrm{Supp'}(m) = \mathrm{Supp'}(n)$.

Note that the following relations are definable in $\langle \mathbb{N}; \perp \rangle$:

$$\Pi,\ \{(p,n) \in \Pi \times \mathbb{N} \mid p \in \mathrm{Supp'}(n)\},\ \{(m,n) \in \mathbb{N}^2 \mid m \sim n\}.$$

Theorem 1.2. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure on $\mathbb{N}$. If there are subsets $\Pi^* \subseteq \Pi$ and $R \subseteq \Pi^* \times \Pi$, both definable in $\mathcal{M}$, such that*

(i) $\Pi^*/\sim$ is infinite and Π^*, R are both closed under $\sim$[2]

(ii) for all $m, n \in \mathbb{N}$ with $\mathrm{Supp'}(m) \subseteq \mathrm{Supp'}(n) \subset \Pi^*$ there is some $r \in \Pi$ such that
$$\mathrm{Supp'}(m) = \big\{ p \in \mathrm{Supp'}(n) \mid R(p, r) \big\},$$

then $\mathrm{Th}(\mathcal{M})$ is undecidable.

Fix $\mathcal{M}$, Π^* and R as in Theorem 1.2. To prove the theorem it is enough to show that $\langle \mathbb{N}; =, \times, + \rangle$ has an interpretation in $\mathcal{M}$. For this define $\mathbb{N}^* \coloneqq \{ c \in \mathbb{N} \mid \mathrm{Supp'}(c) \subset \Pi^* \}$ and $\mathrm{Supp}(c) \coloneqq \mathrm{Supp'}(c)/\sim$. We will prove that

$$\omega\colon \mathbb{N}^* \to \mathbb{N},\ c \mapsto \#\,\mathrm{Supp}(c)$$

is an interpretation of $\langle \mathbb{N}; =, \times, + \rangle$ in $\mathcal{M}$. Since $\Pi^*/\sim$ is infinite, ω is surjective. We need to show that the following relations are definable in $\mathcal{M}$:

$$\begin{gathered}\big\{ (c,d) \in \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) = \omega(d) \big\} \\ \big\{ (c,d,e) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) + \omega(d) = \omega(e) \big\} \\ \big\{ (c,d,e) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) \times \omega(d) = \omega(e) \big\}.\end{gathered}$$

[2] i.e. $\forall p, p', q, q' \in \Pi\colon p \sim p', q \sim q' \implies \big(p \in \Pi^* \Leftrightarrow p' \in \Pi^*\big) \wedge \big(R(p,q) \Leftrightarrow R(p',q')\big)$

If the set of prime numbers is definable in $\mathscr{M}$, one could take $\operatorname{Supp}(c)$ to be the set of prime divisors of c and simplify the notation in this section. Although the primes are definable in $\langle \mathbb{N}; \perp, \mathrm{S}\rangle$ by Theorem 0.3, Richard's proof uses number-theoretic arguments that do not generalize. To avoid this definability issue, we use prime powers instead and work modulo $\sim$.

The next definition is used to formalize the fact that $\omega(c) = \omega(d)$ iff for some $\tilde{e} \in \mathbb{N}$ there are bijections $\operatorname{Supp}(c) \to \operatorname{Supp}(\tilde{e})$ and $\operatorname{Supp}(d) \to \operatorname{Supp}(\tilde{e})$.

Definition 1.3. Let $c, d \in \mathbb{N}$ and let $Q \subset \Pi \times \Pi$ be a relation definable in $\mathscr{M}$ and closed under $\sim$.

(i) Write $\exists ! [p] \in \operatorname{Supp}(c) \colon Q(p, q)$ for the $\mathscr{L}$-formula

$$\exists p \in \text{Supp'}(c) \forall p' \in \text{Supp'}(c) \colon p \sim p' \;\Leftrightarrow\; Q(p', q).$$

(ii) Say that Q defines the bijection

$$\operatorname{Supp}(c) \to \operatorname{Supp}(d),\ [p] \mapsto [q] \colon Q(p, q)$$

if the following $\mathscr{L}$-formulas hold:

$$\begin{aligned} &\forall p \in \text{Supp'}(c) \exists ! [q] \in \operatorname{Supp}(d) \colon Q(p, q) \\ &\forall q \in \text{Supp'}(d) \exists ! [p] \in \operatorname{Supp}(c) \colon Q(p, q). \end{aligned}$$

Lemma 1.4. *The following relation is definable in $\mathscr{M}$:*

$$\big\{ (c, d) \in \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) = \omega(d) \big\}.$$

Proof. It is enough to prove that for $c, d \in \mathbb{N}^*$ we have $\omega(c) = \omega(d)$ iff $\Big($ there exist $\tilde{c}, \tilde{d}, e \in \mathbb{N}^*$ such that

$$\begin{aligned} \text{Supp'}(e) &= \text{Supp'}(c) \cap \text{Supp'}(d) \\ \text{Supp'}(c) &= \text{Supp'}(\tilde{c}) \dot{\cup} \text{Supp'}(e) \\ \text{Supp'}(d) &= \text{Supp'}(\tilde{d}) \dot{\cup} \text{Supp'}(e) \end{aligned}$$

and there exists $\tilde{e} \in \mathbb{N}$ such that R defines the two bijections

$$\begin{aligned} &\operatorname{Supp}(\tilde{c}) \to \operatorname{Supp}(\tilde{e}),\ [p] \mapsto [r] \colon R(p, r) \\ &\operatorname{Supp}(\tilde{d}) \to \operatorname{Supp}(\tilde{e}),\ [q] \mapsto [r] \colon R(q, r) \Big). \end{aligned}$$

"$\Leftarrow$" Clear. "$\Rightarrow$" Take $\tilde{c}, \tilde{d}, e \in \mathbb{N}^*$ such that $c \sim \tilde{c}e$, $d \sim \tilde{d}e$ and $\tilde{c} \perp \tilde{d}$. Write $\operatorname{Supp}(\tilde{c}) = \{[p_1], \dots [p_N]\}$ and $\operatorname{Supp}(\tilde{d}) = \{[q_1], \dots [q_N]\}$. Then apply (ii) of Theorem 1.2 with $m = p_i q_i$ and $n = \tilde{c}\tilde{d}$ to find some $r_i \in \Pi$ with

$$\text{Supp'}(p_i q_i) = \big\{ s \in \text{Supp'}(\tilde{c}\tilde{d}) \mid R(s, r_i) \big\}.$$

Lastly take $\tilde{e} = \prod_{i=1}^{N} r_i$. Then R defines the bijection $\text{Supp}(\tilde{c}) \to \text{Supp}(\tilde{e})$, $[p] \mapsto [r] \colon R(p,r)$, since for all $[p_i] \in \text{Supp}(\tilde{c}), [r_j] \in \text{Supp}(\tilde{e})$ we have $R(p_i, r_j) \Leftrightarrow p_i \in \text{Supp'}(p_j q_j) \Leftrightarrow i = j$. Similarly for $\text{Supp}(\tilde{d}) \to \text{Supp}(\tilde{e})$, $[q] \mapsto [r] \colon R(q,r)$. $\square$

To finish the proof of Theorem 1.2 it remains to prove the next lemma. In (ii) we formalize the fact that $\omega(c) \times \omega(d) = \omega(e)$ iff for some $\tilde{e} \in \mathbb{N}$ there are bijections $\text{Supp}(c) \times \text{Supp}(d) \to \text{Supp}(\tilde{e})$ and $\text{Supp}(e) \to \text{Supp}(\tilde{e})$.

Lemma 1.5. *The following two relations are definable in $\mathcal{M}$:*

(i) $\{(c,d,e) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) + \omega(d) = \omega(e)\}$

(ii) $\{(c,d,e) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) \times \omega(d) = \omega(e)\}$.

Proof. Note that the relation $\{(c,d) \in \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) = \omega(d)\}$ is definable in $\mathcal{M}$ by Lemma 1.4.

"(i)" Use that for $c, d, e \in \mathbb{N}^*$ we have $\omega(c) + \omega(d) = \omega(e)$ iff there exist $\tilde{c}, \tilde{d} \in \mathbb{N}^*$ such that

$$\omega(c) = \omega(\tilde{c}),\ \omega(d) = \omega(\tilde{d}),\ \tilde{c} \perp \tilde{d},\ \text{Supp'}(\tilde{c}) \cup \text{Supp'}(\tilde{d}) = \text{Supp'}(e).$$

"(ii)" We need to extend Definition 1.3 to products. Let $Q \subset \Pi \times \Pi \times \Pi$ be a relation definable in $\mathcal{M}$, closed under $\sim$. Say that Q defines the bijection

$$\text{Supp}(c) \times \text{Supp}(d) \to \text{Supp}(e),\ ([p],[q]) \mapsto [r] \colon Q(p,q,r)$$

if the following $\mathcal{L}$-formulas hold:

$$\forall p \in \text{Supp'}(c) \forall q \in \text{Supp'}(d) \exists! [r] \in \text{Supp}(e) \colon Q(p,q,r)$$
$$\forall r \in \text{Supp'}(e) \exists! [q] \in \text{Supp}(d) \exists! [p] \in \text{Supp}(c) \colon Q(p,q,r).$$

It is enough to show that for $c, d, e \in \mathbb{N}^*$ we have $\omega(c) \times \omega(d) = \omega(e)$ iff there exists $\tilde{c}, \tilde{d} \in \mathbb{N}^*, \tilde{e} \in \mathbb{N}$ such that the following three $\mathcal{L}$-formulas hold

- $\omega(c) = \omega(\tilde{c}),\ \omega(d) = \omega(\tilde{d}),\ e \perp \tilde{c},\ \tilde{c} \perp \tilde{d},\ \tilde{d} \perp e$
- the relation R defines the bijection

$$\text{Supp}(e) \to \text{Supp}(\tilde{e}),\ [s] \mapsto [r] \colon R(s,r)$$

- the relation $Q = \{(p,q,r) \in \Pi^3 \mid R(p,r) \wedge R(q,r)\}$ defines the bijection

$$\text{Supp}(\tilde{c}) \times \text{Supp}(\tilde{d}) \to \text{Supp}(\tilde{e}),\ ([p],[q]) \mapsto [r] \colon Q(p,q,r).$$

"$\Leftarrow$" Clear. "$\Rightarrow$" Since $\Pi^*/\sim$ is infinite, we can take $\tilde{c}, \tilde{d} \in \mathbb{N}^*$ such that the first $\mathscr{L}$-formula holds. Write $\mathrm{Supp}(\tilde{c}) = \{[p_1], \dots [p_N]\}$, $\mathrm{Supp}(\tilde{d}) = \{[q_1], \dots [q_M]\}$ and $\mathrm{Supp}(e) = \{[s_{1,1}], \dots [s_{N,M}]\}$. Apply (ii) of Theorem 1.2 with $m = p_i q_j s_{i,j}$ and $n = \tilde{c}\tilde{d}e$ to find some $r_{i,j} \in \Pi$ with

$$\mathrm{Supp'}(p_i q_j s_{i,j}) = \big\{t \in \mathrm{Supp'}(\tilde{c}\tilde{d}e) \mid R(t, r_{i,j})\big\}.$$

Lastly take $\tilde{e} = \prod_{1\le i\le N, 1\le j\le M} r_{i,j}$. Then Q defines the bijection, since for all $[p_i] \in \mathrm{Supp}(\tilde{c}), [q_j] \in \mathrm{Supp}(\tilde{d}), [r_{i',j'}] \in \mathrm{Supp}(\tilde{e})$ we have $Q(p_i, q_j, r_{i',j'}) \Leftrightarrow p_i, q_j \in \mathrm{Supp'}(p_{i'} q_{j'} s_{i',j'}) \Leftrightarrow i = i', j = j'$. Similarly for R. $\square$

This finishes the proof of the theorem. In the proof we used (ii) only for $m \in \mathbb{N}$ with $\omega(m) \in \{2, 3\}$. So we can replace it by:

(ii') for all $m, n \in \mathbb{N}$ with $\mathrm{Supp'}(m) \subseteq \mathrm{Supp'}(n) \subset \Pi^*$ and $\omega(m) = 3$ there is some $r \in \Pi$ such that

$$\mathrm{Supp'}(m) = \big\{p \in \mathrm{Supp'}(n) \mid R(p, r)\big\}.$$

The following two consequences reduce (ii) of Theorem 1.2 to modular arithmetic. For most applications we use the next corollary with $M = 1$.

Corollary 1.6. *Let $f\colon \mathbb{N} \to \mathbb{N}$ be a function. If there is some $\Pi^* \subseteq \Pi$ definable in $\langle \mathbb{N}; \perp, f\rangle$ and some $M \in \mathbb{N}$ with $\mathrm{Supp'}(M) \subseteq \Pi \setminus \Pi^*$ such that*

(i) $\Pi^*/\sim$ is infinite and Π^* is closed under $\sim$[3]

(ii) for every prime $p \in \Pi^*$ there is an $n_p \in \mathbb{N}$ with $n_p \perp p$ and $n_p \equiv 1 \mod M$, such that for all primes r we have

$$\begin{aligned} r \equiv 1 \mod Mp &\implies \forall r' \sim r\colon f(r') \not\equiv 0 \mod p \\ r \equiv n_p \mod Mp &\implies f(r) \equiv 0 \mod p, \end{aligned}$$

then $\mathrm{Th}(\mathbb{N}; \perp, f)$ is undecidable.

Remark 1.7. *Corollary 1.6 remains true if we replace (ii) by*

(ii') for every prime $p \in \Pi^*$ there is an $n_p \in \mathbb{N}$ with $n_p \perp p$ and $n_p \equiv 1 \mod M$, such that for all primes r we have

$$\begin{aligned} r \equiv 1 \mod Mp &\implies \forall r' \sim r\colon f(r') \equiv 0 \mod p \\ r \equiv n_p \mod Mp &\implies f(r) \not\equiv 0 \mod p. \end{aligned}$$

[3] i.e. $\forall p, p' \in \Pi\colon p \sim p' \implies (p \in \Pi^* \Leftrightarrow p' \in \Pi^*)$

Proof. We apply Theorem 1.2. Define for $p, r \in \Pi$ the relation

$$R(p,r) \;:\Longleftrightarrow\; \forall r' \sim r\colon f(r') \perp p.$$

Consider $m, n \in \mathbb{N}$ with Supp'$(m) \subseteq$ Supp'$(n) \subset \Pi^*$. For each prime divisor p of n with $p \perp m$ take some $n_p \in \mathbb{N}$ such that for primes r we have

$$r \equiv n_p \mod Mp \implies f(r) \equiv 0 \mod p.$$

Then use the Chinese remainder theorem and Dirichlet's theorem to find a prime r such that for every prime divisor p of n we have

$$r \equiv \begin{cases} 1 \mod Mp \text{ if } p \not\perp m \\ n_p \mod Mp \text{ if } p \perp m. \end{cases}$$

This finishes the proof, since

$$\text{Supp'}(m) = \big\{p \in \text{Supp'}(n) \mid \forall r' \sim r\colon f(r') \perp p\big\}.$$

□

1.2 Applications

We will show that $\mathrm{Th}(\mathbb{N}; \perp, f)$ is undecidable for certain functions $f\colon \mathbb{N} \to \mathbb{N}$.

Note that the constants '1' and '0' are definable in $\langle \mathbb{N}; \perp\rangle$. For any $n \in \mathbb{N}$ we have $n = 1 \Leftrightarrow \forall m\colon m \perp n$ and $n = 0 \Leftrightarrow \forall m\colon m \neq 1 \Rightarrow m \not\perp n$.

Polynomials are easy to work with in modular arithmetic. The main difficulty in applying Corollary 1.6 and Remark 1.7 is to prove that $\Pi^*/\sim$ is infinite. For this we use Schur's Theorem [GB71]: for any non-constant polynomial $L_0 \in \mathbb{Z}[X]$ there are infinitely many primes p such that for some $n \geq 0$ we have $p \mid L_0(n),\; L_0(n) \neq 0$.

Proposition 1.8. *Let $L \in \mathbb{Z}[X]$ be a polynomial with at least two non-zero coefficients. Then $\mathrm{Th}(\mathbb{N}; \perp, n \mapsto |L(n)|)$ is undecidable.*

Proof. We have two cases. First consider L with $L(1) \neq 0$. To apply Corollary 1.6 take $M = 1$ and

$$\Pi^* = \big\{p \in \Pi \mid p \perp |L(1)|,\; \exists n\colon n \perp p \not\perp |L(n)|\big\}.$$

For $L(X) = \sum_{i=0}^{N} a_i X^i$ define $i_0 := \min\{i \in \mathbb{N} \mid a_i \neq 0\}$ and $L_0(n) := \frac{L(n)}{n^{i_0}}$. The following set contains infinitely many primes by Schur's Theorem

$$\begin{aligned} &\big\{p \in \Pi \mid \exists n\colon n \perp p \not\perp |L(n)|\big\} \\ =&\big\{p \in \Pi \mid \exists n\colon n \perp p \not\perp L_0(n)\big\} \\ \supseteq&\big\{p \in \Pi \mid \exists n\colon p \not\perp L_0(n) \neq 0\big\} \setminus \text{Supp'}(a_{i_0}). \end{aligned}$$

So $\Pi^*/\sim$ is infinite. Next, for each prime $p \in \Pi^*$ take some $n_p \in \mathbb{N}$ with $n_p \perp p \not\perp L(n_p)$. Then for all $r \in \Pi$ we have

$$\begin{aligned} r \equiv 1 \mod p &\implies L(r) \equiv L(1) \not\equiv 0 \mod p \\ r \equiv n_p \mod p &\implies L(r) \equiv L(n_p) \equiv 0 \mod p. \end{aligned}$$

Next consider L with $L(1) = 0$. To apply Remark 1.7 take $M = 1$ and $\Pi^* = \{p \in \Pi \mid \exists n \colon n \perp p \perp |L(n)|\}$. It is clear that $\Pi^*/\sim$ is infinite. For each prime $p \in \Pi^*$ take some $n_p \in \mathbb{N}$ with $n_p \perp p \perp L(n_p)$. Then for all $r \in \Pi$ we have

$$\begin{aligned} r \equiv 1 \mod p &\implies L(r) \equiv L(1) \equiv 0 \mod p \\ r \equiv n_p \mod p &\implies L(r) \equiv L(n_p) \not\equiv 0 \mod p. \end{aligned}$$

□

Proposition 1.9. *Let* $H(n) := 1 + \prod_{p \not| n,\, p \in \mathrm{P}} p$ *and* $H(0) := 0$. *Then* $\mathrm{Th}(\mathbb{N}; \perp, H)$ *is undecidable.*

Proof. To apply Corollary 1.6 take $M = 1$ and $\Pi^* = \{p \in \Pi \mid p \perp H(1)\}$. For each prime $p \in \Pi^*$ take $n_p = p - 1$. Then for any prime r we have

$$\begin{aligned} r \equiv 1 \mod p &\implies \forall r' \sim r \colon H(r') \equiv 2 \not\equiv 0 \mod p \\ r \equiv -1 \mod p &\implies H(r) \equiv 0 \mod p. \end{aligned}$$

□

To work with the Euler phi function in modular arithmetic, we will use that for a prime p and $n \geq 1$ we have $\varphi(p^n) = (p-1)p^{n-1}$. Further note $n = 2 \Leftrightarrow \varphi(n) = 1 \wedge n \neq 1$.

Proposition 1.10. *Let* $\varphi \colon \mathbb{N} \to \mathbb{N}$ *be the Euler phi function and* $\varphi(0) := 0$. *Then* $\mathrm{Th}(\mathbb{N}; \perp, \varphi)$ *is undecidable.*

Proof. To apply Remark 1.7 take $M = 1$ and $\Pi^* = \{p \in \Pi \mid p \perp 2\}$. For each prime $p \in \Pi^*$ take $n_p = p - 1$. Then for any prime r we have

$$\begin{aligned} r \equiv 1 \mod p &\implies \forall r' \sim r \colon \varphi(r') \equiv (r-1)\frac{r'}{r} \equiv 0 \mod p \\ r \equiv -1 \mod p &\implies \varphi(r) \equiv -2 \not\equiv 0 \mod p. \end{aligned}$$

□

The function $\rho \colon \mathbb{N} \to \mathrm{P}$ directly encodes every number into a prime.

Proposition 1.11. *Let $\rho\colon \mathbb{N} \to \mathrm{P}$ be injective, where P is the set of primes. Then $\mathrm{Th}(\mathbb{N}; \perp, \rho)$ is undecidable.*

Proof. To apply Theorem 1.2 take $\Pi^* = \Pi$ and

$$R(p, r) \;:\Longleftrightarrow\; \exists m\colon p \not\perp m,\; r \not\perp \rho(m).$$

Then for all $m \in \mathbb{N}_{>0}$ we have $\mathrm{Supp'}(m) = \big\{p \in \Pi \mid R(p, \rho(m))\big\}$. □

In Chapter 3 we provide evidence for the claim that the next structure is interdefinable with $\langle \mathbb{N}; =, \times, + \rangle$.

Proposition 1.12. *Let $a \in \mathbb{N}_{>1}$. Then $\mathrm{Th}(\mathbb{N}; \perp, n \mapsto a^n - 1)$ is undecidable.*

Proof. For $r \in \Pi$ with $r \perp a$ define $\mathrm{ord}_r(a)$ to be the smallest $n \geq 1$ such that $r \mid a^n - 1$. Then for any $n \geq 1$ we have $r \mid a^n - 1$ implies $\mathrm{ord}_r(a) \mid n$. A consequence of Bang's result [Ban86][4] is that for all $n > 1$ there is a prime r such that $\mathrm{ord}_r(a) = n^2$.

To apply Theorem 1.2 take $\Pi^* = \Pi$ and define $R(p, r)$ to be true iff there exists $m' \in \mathbb{N}$ such that

$$\big(p \not\perp m',\; r \not\perp a^{m'} - 1\big) \wedge \big(\forall n'\colon r \not\perp a^{n'} - 1 \;\Rightarrow\; \mathrm{Supp'}(m') \subseteq \mathrm{Supp'}(n')\big).$$

Let $m, n > 1$ with $\mathrm{Supp'}(m) \subseteq \mathrm{Supp'}(n)$. Take a prime r such that $\mathrm{ord}_r(a) = m^2$. We need to show that $\mathrm{Supp'}(m) = \{p \in \mathrm{Supp'}(n) \mid R(p, r)\}$.

"$\subseteq$" For $p \in \mathrm{Supp'}(m)$ take $m' = m^2$. Consider $n' \in \mathbb{N}$ with $r \not\perp a^{n'} - 1$. Then $r \mid a^{n'} - 1$ and $\mathrm{ord}_r(a) \mid n'$.

"$\supseteq$" Let $p \in \mathrm{Supp'}(n)$ with $R(p, r)$ and let m' be given by $R(p, r)$. Then $r \mid a^{m'} - 1$ gives $\mathrm{ord}_r(a) \mid m'$ and $r \not\perp a^{(m^2)} - 1$ gives $\mathrm{Supp'}(m') \subseteq \mathrm{Supp'}(m)$. Hence $m' \sim m$ and $p \not\perp m$. □

1.3 Floor function

Let $a \geq 1$, $b \geq 2$ and $G(n) \coloneqq \lfloor \frac{an}{b} \rfloor$ where $\lfloor \cdot \rfloor$ denotes the floor function. We will show that $\mathrm{Th}(\mathbb{N}; \perp, G)$ is undecidable. The first step is to prove that $\{n \in \mathbb{N} \mid n \sim b\}$ and $\{n \in \mathbb{N} \mid n \sim ab\}$ are definable in $\langle \mathbb{N}; \perp, G \rangle$. This is done in the next three lemmas. If one is satisfied with the undecidability of $\mathrm{Th}(\mathbb{N}; \perp, G, b)$, then these may be skipped.

[4] Also stated as Theorem 52 in [Bès02].

Lemma 1.13. *Let $a, b \geq 2$ with $a \perp b$. Then there is some $k \geq 1$, dependent on a and b, such that for all $n \in \mathbb{N}$ we have $n = b^{k+1}$ iff*

$$\omega(n) = \omega(b),\ \omega(G^{k+1}(n)) = \omega(a),\ n \perp G^{k+1}(n),\ \bigwedge_{i=1}^{k} G^i(n) \sim nG^{k+1}(n).$$

Proof. "⇒" Clear, since $G(b^{k+1}) = ab^k$. "⇐" Let $\psi_k(n)$ denote the conjunction $\omega(n) = \omega(b)$, $\omega(G^{k+1}(n)) = \omega(a)$, $n \perp G^{k+1}(n)$, $\bigwedge_{i=1}^{k} G^i(n) \sim nG^{k+1}(n)$. For $i, n \in \mathbb{N}$ define

$$u_i(n) \coloneqq aG^i(n) - bG^{i+1}(n)$$

such that $G^{i+1}(n) = \frac{aG^i(n) - u_i(n)}{b}$ and $u_i(n) \in [0, b)$.

First note that for any $k \geq 1, n \in \mathbb{N}$ with $\psi_k(n)$ we have

$$G^l(n) \neq G^{l+1}(n)$$

for all $0 \leq l \leq k$. Assume not. Then $G^l(n) = G^{k+1}(n)$ and $G^{k+1}(n) \sim nG^{k+1}(n)$, which would contradict $1 \neq n \perp G^{k+1}(n)$.

Claim: There is some $k \geq 1$ such that for all $n \in \mathbb{N}$ we have $\psi_k(n)$ implies $u_i(n) = 0$ for all $0 \leq i \leq k$.

If the claim is true for some k, consider $n \in \mathbb{N}$ with $\psi_k(n)$. Then $aG^i(n) = bG^{i+1}(n)$ for all $0 \leq i \leq k$. This gives $b \mid n$, $b \sim n$, $a \mid G^{k+1}(n)$, $a \sim G^{k+1}(n)$ and $b^{k+1} \mid n$. Therefore $G^{k+1}(n) = \frac{a^{k+1}n}{b^{k+1}} \sim a$, which implies $n = b^{k+1}$. This proves the lemma.

Assume the claim is false. Then at least one of two cases occurs.

Case 1: There are infinitely many $k \geq 1$ such that for some $n \in \mathbb{N}$ we have $\psi_k(n)$ and $0 < u_i(n)$ for all $0 \leq i \leq k$.

We find a sequence $k \mapsto n_k$ such that $\psi_k(n_k)$ holds and $0 < u_i(n_k)$ for all $0 \leq i \leq k$. Consider $i, k \in \mathbb{N}$ with $0 \leq i \leq \omega(a) + \omega(b) \leq \frac{k}{2}$. Then $\omega(G^{\lfloor \frac{k}{2} \rfloor + i}(n_k)) = \omega(a) + \omega(b)$. Using the monotonicity of $G\colon \mathbb{N} \to \mathbb{N}$ and $G^{l+1}(n_k) \neq G^l(n_k)$ for $0 \leq l \leq k$ gives

$$G^{\lfloor \frac{k}{2} \rfloor + i}(n_k) \xrightarrow[k \to \infty]{} \infty.$$

Since $\omega\big(G^{\lfloor \frac{k}{2} \rfloor + i}(n_k)\big) = \omega(a) + \omega(b)$ we find a sequence $k \mapsto q_{i,k} \in \Pi$ with $q_{i,k} \mid G^{\lfloor \frac{k}{2} \rfloor + i}(n_k)$ and $q_{i,k} \xrightarrow[k \to \infty]{} \infty$. Using $G^{\lfloor \frac{k}{2} \rfloor + i}(n_k) \sim G^{\lfloor \frac{k}{2} \rfloor}(n_k)$ we can find for each k some $i, j \in \mathbb{N}, 0 \leq i < j \leq \omega(a) + \omega(b)$ such that $q_{i,k} \sim q_{j,k}$.

For such i,j we have

$$\begin{aligned}
u_{\lfloor \frac{k}{2}\rfloor+i}(n_k) &= aG^{\lfloor \frac{k}{2}\rfloor+i}(n_k) - bG^{\lfloor \frac{k}{2}\rfloor+i+1}(n_k)\\
&= aG^{\lfloor \frac{k}{2}\rfloor+i}(n_k) - \frac{b^2}{a}G^{\lfloor \frac{k}{2}\rfloor+i+2}(n_k) - \frac{b}{a}u_{\lfloor \frac{k}{2}\rfloor+i+1}(n_k)\\
&= aG^{\lfloor \frac{k}{2}\rfloor+i}(n_k) - \frac{b^{j-i}}{a^{j-i-1}}G^{\lfloor \frac{k}{2}\rfloor+j}(n_k) + O_{b,\omega(ab)}(1)\\
&\geq \frac{1}{a^{j-i-1}}\gcd\bigl(G^{\lfloor \frac{k}{2}\rfloor+i}(n_k), G^{\lfloor \frac{k}{2}\rfloor+j}(n_k)\bigr) + O_{b,\omega(ab)}(1) \xrightarrow[k\to\infty]{} \infty.
\end{aligned}$$

This contradicts $0 \leq u_{\lfloor \frac{k}{2}\rfloor+i}(n_k) < b$.

Case 2: There are infinitely many $k \geq 1$ such that there are $i,j,n \in \mathbb{N}$, $0 \leq i,j \leq k$ with $\psi_k(n)$ and $u_i(n) = 0 < u_j(n)$.

Fix such i,j,n,k. Then $b \mid G^i(n)$ and $a \mid G^{i+1}(n)$. Since $G^l(n) \sim nG^{k+1}(n)$ for all $1 \leq l \leq k$ we get $\operatorname{Supp}(ab) \subseteq \operatorname{Supp}(G^l(n))$. By assumption $\omega(G^l(n)) = \omega(a)+\omega(b)$. Therefore $ab \sim G^l(n) \sim nG^{k+1}(n)$. The key point is that $aG^j(n)$ is an element of

$$S \coloneqq \bigl\{v \in \mathbb{N} \mid \exists w,u \in \mathbb{N}_{>0}\colon u < b,\ v-w = u,\ \operatorname{Supp}(vw) \subseteq \operatorname{Supp}(a\cdot b!)\bigr\},$$

which we claim is finite.

To prove that S is finite we use Theorem 1.1 of [BS96]. It implies that if H is a finitely generated subgroup of $\mathbb{C}^*$, then the equation

$$x - y = 1$$

has only finitely many solutions in H. So take

$$H \coloneqq \bigl\{r \in \mathbb{Q} \mid \exists v,u \in \mathbb{N}_{>0}\colon r = \frac{v}{u},\ \operatorname{Supp}(vu) \subseteq \operatorname{Supp}(a\cdot b!)\bigr\}$$

which is finitely generated by the prime divisors of $a \cdot b!$.

Consider $a > b$. Again by monotonicity of G and $G^{l+1}(n) \neq G^l(n)$ we have $G^l(n) \geq \frac{k}{2}$ for all $k \geq l \geq \frac{k}{2}$. We can assume k is large enough such that $\frac{k}{2} > \max(S)$. Further we can assume j is chosen such that for all $j < l \leq k\colon u_l(n) = 0$. This gives $b^{k-j} \mid G^{j+1}(n)$. Now

- if $j \geq \frac{k}{2}$ then $G^j(n) \geq \frac{k}{2} > \max(S) \geq aG^j(n)$
- if $j < \frac{k}{2}$ then $b^{k-j} \leq G^{j+1}(n) \leq \frac{a}{b}G^j(n) \leq \max(S) < \frac{k}{2} < b^{\frac{k}{2}}$

both cases yield a contradiction.

Consider $1 < a < b$. Similarly as above, we have $G^l(n) \geq \frac{k}{2}$ for all $l \leq \frac{k}{2}$. We can assume k is large enough such that $\frac{k}{2} > \max(S)$. Further we can assume j is chosen such that $u_l(n) = 0$ for all $0 \leq l < j$. This gives $a^j \mid G^j(n)$. Now

- if $j \le \frac{k}{2}$ then $G^j(n) \ge \frac{k}{2} > \max(S) \ge aG^j(n)$
- if $j > \frac{k}{2}$ then $a^j \le G^j(n) \le \max(S) < \frac{k}{2} < a^{\frac{k}{2}}$

both cases yield a contradiction. $\square$

The previous lemma can fail when $a = 1$. For example consider $b = 12$ and $n = 18 \cdot 12^k$ for $k \ge 1$. We still have the following lemma.

Lemma 1.14. *Let $b \ge 2$. Then there is some $k \ge 1$, dependent on b, such that for all $m \in \mathbb{N}$ we have $m \sim b$ iff there is some $n \sim m$ such that*

$$\omega(n) = \omega(b),\ G^{k+1}(n) = 1,\ \bigwedge_{i=1}^{k} G^i(n) \sim n.$$

Proof. The only part of the proof of Lemma 1.13 that fails when $a = 1$ is the inequality $\frac{k}{2} < a^{\frac{k}{2}}$. So we can take $k \ge 1$ large enough such that Case 1 cannot occur. This means that for all $n \in \mathbb{N}$ with $\omega(n) = \omega(b)$, $G^{k+1}(n) = 1$ and $\bigwedge_{i=1}^{k} G^i(n) \sim n$ we find some $0 \le j \le k$ with $u_j(n) = 0$.

Then $b \mid G^j(n)$ and $b \sim G^j(n) \sim n$. $\square$

We summarize the last two lemmas in the next one.

Lemma 1.15. *Let $a \ge 1, b \ge 2$ with $a \perp b$. Then the relations $\{n \in \mathbb{N} \mid n \sim b\}$ and $\{n \in \mathbb{N} \mid n \sim ab\}$ are definable in $\langle \mathbb{N}; \perp, n \mapsto \lfloor \frac{an}{b} \rfloor \rangle$.*

Proof. Consider $a > 1$. By Lemma 1.13 there is some $k \ge 1$ such that for all $n \in \mathbb{N}$ we have $n = b^{k+1}$ iff

$$\omega(n) = \omega(b),\ \omega(G^{k+1}(n)) = \omega(a),\ n \perp G^{k+1}(n),\ \bigwedge_{i=1}^{k} G^i(n) \sim nG^{k+1}(n).$$

To formulate the above as an $(\perp, G)$-formula, we use $\omega(n) = \omega(b)$ iff

$$\exists p_1, \dots p_{\omega(b)} \in \Pi\colon\ \text{Supp'}(n) = \bigcup_{i=1}^{\omega(b)} \text{Supp'}(p_i),\ \bigwedge_{1 \le i < j \le \omega(b)} p_i \perp p_j.$$

Similarly for $\omega(G^{k+1}(n)) = \omega(a)$. Further note $G^i(n) \sim nG^{k+1}(n) \Leftrightarrow \text{Supp'}(G^i(n)) = \text{Supp'}(n) \cup \text{Supp'}(G^{k+1}(n))$. Then conclude with $n \sim ab \Leftrightarrow n \sim G(b^{k+1})$ and $n \sim b \Leftrightarrow n \sim b^{k+1}$.

The case $a = 1$ is done similarly. $\square$

To apply Corollary 1.6 and Remark 1.7 we use that G induces the map $\mathbb{Z}/bp\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $[n] \mapsto [G(n)]$ to get the next proposition.

Proposition 1.16. *Let* $a \geq 1, b \geq 2$ *with* $a \perp b$. *Then* $\mathrm{Th}(\mathbb{N}; \perp, n \mapsto \lfloor \frac{an}{b} \rfloor)$ *is undecidable.*

Proof. Consider $a > b$. To apply Corollary 1.6 take $M = b$ and

$$\Pi^* = \big\{p \in \Pi \mid p \perp ab,\ p \perp \lfloor \frac{a}{b} \rfloor,\ \forall q \sim p\colon q > b\big\}.$$

We need to show that Π^* is definable in $\langle \mathbb{N}; \perp, G\rangle$. This follows from $G(1) = \lfloor \frac{a}{b} \rfloor$, Lemma 1.15 and the claim that for every prime $p \perp b$ we have

$$p < b \iff \exists n\colon n \perp b,\ p \not\perp G(np).$$

"$\Leftarrow$" Since $p \mid G(np)$, we have $p \mid npa - bG(np)$ and $0 < npa - bG(np) < b$.
"$\Rightarrow$" Take any $n \geq 1$ with $n \equiv a^{-1} \mod b$. Then $npa - p \equiv 0 \mod b$. So using $p < b$ gives $G(np) = \frac{npa-p}{b} \not\perp p$.

Let $p \in \Pi^*$ be prime and $0 < \tilde{a} < b$ such that $a \equiv \tilde{a} \mod b$. Since $p > b$ we get $p \perp \tilde{a}$. Take n_p such that $n_p \equiv a^{-1}\tilde{a} \mod bp$. Then $n_p \equiv 1 \mod b$ and for all $r \in \Pi$ we have

$$\begin{aligned} r \equiv 1 \mod bp &\implies \lfloor \frac{ar}{b} \rfloor \equiv \lfloor \frac{a}{b} \rfloor \not\equiv 0 \mod p \\ r \equiv n_p \mod bp &\implies \lfloor \frac{ar}{b} \rfloor \equiv \lfloor \frac{an_p}{b} \rfloor \equiv \lfloor \frac{\tilde{a}}{b} \rfloor \equiv 0 \mod p. \end{aligned}$$

Consider $a < b$. To apply Remark 1.7 take $M = b$ and $\Pi^* = \{p \in \Pi \mid p \perp ab,\ \forall q \sim p\colon G(q) \notin \{0,1\}\}$. Lemma 1.15 implies that Π^* is definable. Let $p \in \Pi^*$ be prime, then $p > 2$. Take n_p such that $n_p \equiv 1 \mod b$ and $n_p \equiv 2 \mod p$. Then $an_p \equiv a \mod b$, so $\lfloor \frac{an_p}{b} \rfloor = \frac{an_p - a}{b}$ and for all $r \in \Pi$ we have

$$\begin{aligned} r \equiv 1 \mod bp &\implies \lfloor \frac{ar}{b} \rfloor \equiv \lfloor \frac{a}{b} \rfloor \equiv 0 \mod p \\ r \equiv n_p \mod bp &\implies \lfloor \frac{ar}{b} \rfloor \equiv \lfloor \frac{an_p}{b} \rfloor \equiv \frac{an_p - a}{b} \not\equiv 0 \mod p. \end{aligned}$$

□

2 Definability

In this chapter we will focus on the definable subsets of $\langle \mathbb{N}; \perp, f\rangle$ for certain functions $f\colon \mathbb{N} \to \mathbb{N}$.

2.1 Second theorem

The proof of Theorem 1.2 implies that all structures in Chapter 1.2 have

$$\omega\colon \mathbb{N}^* \to \mathbb{N},\ c \mapsto \#\,\mathrm{Supp}(c)$$

as an interpretation of $\langle \mathbb{N}; =, \times, +\rangle$. The idea of Theorem 2.2 is to translate definable sets in $\langle \mathbb{N}; =, \times, +\rangle$ via ω to definable sets in $\langle \mathbb{N}; \perp, f\rangle$. For this theorem we take $\mathbb{N}^* = \mathbb{N}_{>0}$.

Definition 2.1. Let $\mathscr{M}$ be a $\mathscr{L}$-structure on $\mathbb{N}$.

(i) $\mathscr{M}$ has ω-arithmetic if the map $\omega\colon \mathbb{N}_{>0} \to \mathbb{N}$ is an interpretation of $\langle \mathbb{N}; =, \times, +\rangle$ in $\mathscr{M}$.

(ii) $\mathscr{M}$ has ω-translation if the relation $\big\{(c,p) \in \mathbb{N}_{>0} \times \Pi \mid \omega(c) \sim p\big\}$ is definable in $\mathscr{M}$.

Let $\mathrm{Def}(\mathscr{M})$ denote the set of definable relations in $\mathscr{M}$. If $\omega^{-1}(\times) \in \mathrm{Def}(\mathscr{M})$ then $\omega^{-1}(=) \in \mathrm{Def}(\mathscr{M})$ via $\omega(c) = \omega(d) \Leftrightarrow \exists p \in \Pi\colon \omega(c) \times \omega(p) = \omega(d)$. We have by the proof of Lemma 1.5(i) also $\omega^{-1}(+) \in \mathrm{Def}(\mathscr{M})$. Therefore the following are equivalent:

- $\mathscr{M}$ has ω-arithmetic
- for all $A \in \mathrm{Def}(\mathbb{N}; =, \times, +)$ we have $\omega^{-1}(A) \in \mathrm{Def}(\mathscr{M})$
- $\omega^{-1}(\times) = \big\{(c,d,e) \in (\mathbb{N}_{>0})^3 \mid \omega(c) \times \omega(d) = \omega(e)\big\} \in \mathrm{Def}(\mathscr{M})$.

The translation via ω needs to allow for some error described by the following notation. For $\vec{m}, \vec{n} \in \mathbb{N}^N$ define $\vec{m} \sim_k \vec{n} \;:\Leftrightarrow\; \vec{m} \sim_{f,k} \vec{n} \;:\Leftrightarrow\; \bigwedge_{i=0}^{k} \bigwedge_{j=1}^{N} f^i(m_j) \sim f^i(n_j)$ and for $A \subseteq \mathbb{N}^N$ define $\mathrm{Cl}_k(A) := \mathrm{Cl}_{f,k}(A) := \big\{\vec{n} \in \mathbb{N}^N \mid \exists \vec{m} \in A\colon \vec{m} \sim_k \vec{n}\big\}$. We now state the theorem.

Theorem 2.2. *Let $f\colon \mathbb{N} \to \mathbb{N}$ be definable in $\langle \mathbb{N}; =, \times, +\rangle$. If $\langle \mathbb{N}; \perp, f\rangle$ has ω-arithmetic and ω-translation, then*

$$\mathrm{Def}(\mathbb{N}; \perp, f) = \bigcup_{k=0}^{\infty} \mathrm{Cl}_k\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big).$$

Note that Cl_0 is independent of f. The next examples motivate some definitions from Chapter 1.1 as analogues of basic concepts in number theory.

- $\mathrm{Cl}_0(=) = \sim$
- $\mathrm{Cl}_0(\mathrm{P}) = \Pi$
- $\mathrm{Cl}_0(<) = \mathbb{N} \times \mathbb{N}_{>1} \cup \{(0,1)\}$
- $\mathrm{Cl}_0\big(\{p \in \mathrm{P} \mid p \not\perp n\}\big) = \mathrm{Supp'}(n)$
- $\mathrm{Cl}_0(\,|\,) = \big\{(m,n) \in \mathbb{N}^2 \mid \mathrm{Supp'}(m) \subseteq \mathrm{Supp'}(n)\big\}$

Further a relation $R \subseteq \mathbb{N}^N$ is closed under $\sim$ iff $\mathrm{Cl}_0(R) = R$.

We show Theorem 2.2 by proving the following stronger proposition. This allows us to study definability within $\langle \mathbb{N}; \perp, <_A \rangle$ in Chapter 2.4.

Proposition 2.3. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure with ω-arithmetic and ω-translation. If $f\colon \mathbb{N} \to \mathbb{N}$ is definable both in $\langle \mathbb{N}; =, \times, + \rangle$ and $\mathcal{M}$, then*

$$\mathrm{Def}(\mathbb{N}; \perp, f) \subseteq \bigcup_{k=0}^{\infty} \mathrm{Cl}_k\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big) \subseteq \mathrm{Def}(\mathcal{M}).$$

Proof. Let $A \subseteq \mathbb{N}^N$ be definable in $\langle \mathbb{N}; \perp, f \rangle$ by the $(\perp, f)$-formula ψ. Then $A \in \mathrm{Def}(\mathbb{N}; =, \times, +)$, as f is definable in $\langle \mathbb{N}; =, \times, + \rangle$. Let k_ψ be maximal such that f^{k_ψ} appears in ψ. A simple induction on formulas shows that for all $\vec{m}, \vec{n} \in \mathbb{N}^N$ with $\vec{m} \sim_{k_\psi} \vec{n}$ we have

$$\langle \mathbb{N}; \perp, f \rangle \models \psi(\vec{m}) \iff \langle \mathbb{N}; \perp, f \rangle \models \psi(\vec{n}).$$

Hence $A = \mathrm{Cl}_{k_\psi}(A) \in \mathrm{Cl}_{k_\psi}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$.

For $c, d \in \mathbb{N}_{>0}$ define $c \approx d :\Leftrightarrow \omega(c) = \omega(d)$ and $c \sim_{\omega,k} d :\Leftrightarrow \omega(c) \sim_k \omega(d)$. Consider the following commutative diagram.

$$\begin{tikzcd}
{[c]_\approx} \arrow[rrr, mapsto] \arrow[dddd] & & & {[c]_{\sim_{\omega,k}}} \arrow[dddd] \\
& \mathbb{N}_{>0}/\approx \arrow[r, "\iota_{\omega,k}"] \arrow[dd, "\omega_\approx"'] & \mathbb{N}_{>0}/\sim_{\omega,k} \arrow[dd, "\omega_k"] & \\
& & & \\
& \mathbb{N} \arrow[r, "\iota_k"'] & \mathbb{N}/\sim_k & \\
\omega(c) \arrow[rrr, mapsto] & & & {[\omega(c)]_{\sim_k}}
\end{tikzcd}$$

Note that $\omega_\approx$ and ω_k are bijective.

Let $A \in \mathrm{Cl}_k\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$. Then $A = \mathrm{Cl}_k(A)$ and $A = \iota_k^{-1}\big(\iota_k(A)\big)$. Since $f\colon \mathbb{N} \to \mathbb{N}$ is definable in $\langle \mathbb{N}; =, \times, + \rangle$ we have that $A \in \mathrm{Def}(\mathbb{N}; =, \times, +)$.

Using ω-arithmetic we find some $C \in \mathrm{Def}(\mathcal{M})$ such that $\omega^{-1}(A) = C$. Therefore $\omega_{\approx}^{-1}(A) = \{[\vec{c}]_{\approx} \mid \vec{c} \in C\}$ and

$$\begin{aligned} A &= \iota_k^{-1}\big(\omega_k \circ \omega_k^{-1} \circ \iota_k(A)\big) = \iota_k^{-1}\big(\omega_k \circ \iota_{\omega,k} \circ \omega_{\approx}^{-1}(A)\big) \\ &= \big\{\vec{n} \in \mathbb{N}^N \mid \exists \vec{c} \in C \colon \iota_k(\vec{n}) = \omega_k \circ \iota_{\omega,k}([\vec{c}]_{\approx})\big\}. \end{aligned}$$

To show that A is definable in $\mathcal{M}$ we need to show that the maps ι_k, ω_k and $\iota_{\omega,k}$ are definable. To make this precise we introduce the following notation.

Let $\sim_P$ and $\sim_Q$ be two equivalence relations on $\mathbb{N}$ and $F \colon \mathbb{N}/\sim_P \to \mathbb{N}/\sim_Q$ be a map. Say an $\mathcal{L}$-formula $\psi(x, y)$ defines F if for all $m, n \in \mathbb{N}$ we have $F([m]_P) = [n]_Q \Leftrightarrow \psi(m, n)$.

To see that ι_k is definable, view $\mathbb{N}$ as $\mathbb{N}/=$ and use $\iota_k([m]_=) = [n]_{\sim_k} \Leftrightarrow m \sim_k n$. Next, using that f is definable in $\langle \mathbb{N}; =, \times, + \rangle$ and ω-arithmetic we see that $\big\{(c, d) \in \mathbb{N}^2_{>0} \mid \omega(c) \sim_k \omega(d)\big\}$ is definable in $\mathcal{M}$. This implies that $\iota_{\omega,k}$ is definable via $\iota_{\omega,k}([c]_{\approx}) = [d]_{\sim_{\omega,k}} \Leftrightarrow \omega(c) \sim_k \omega(d)$.

For the last map note that $\big\{(c, d) \in \mathbb{N}^2_{>0} \mid \omega(d) \perp f^i(\omega(c))\big\}$ is definable in $\mathcal{M}$. Further for $c \geq 1, n \geq 0$ we have $f^i(n) \sim f^i(\omega(c))$ iff

$$\forall p \in \Pi, d \in \mathbb{N}_{>0} \colon \omega(d) \sim p \;\Rightarrow\; \big(p \perp f^i(n) \;\Leftrightarrow\; \omega(d) \perp f^i(\omega(c))\big).$$

So using ω-translation we get that ω_k is definable via $\omega_k([c]_{\sim_{\omega,k}}) = [n]_{\sim_k} \Leftrightarrow \bigwedge_{i=0}^k f^i(n) \sim f^i(\omega(c))$. $\square$

Lemma 2.8 implies that $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$ has ω-arithmetic and ω-translation. We get the following extension of Theorem 0.3. Taking $A = \mathbb{N}$ yields a generalization of Theorem 0.2.

Corollary 2.4. *Let $f \colon \mathbb{N} \to \mathbb{N}$ be definable in $\langle \mathbb{N}; =, \times, + \rangle$ and let $A \subseteq \mathbb{N}$ be definable in $\langle \mathbb{N}; \perp, f \rangle$. If $\langle \mathbb{N}; \perp, f \rangle$ has ω-arithmetic, ω-translation and there is some $k \in \mathbb{N}$ such that for all $m, n \in A$ we have*

$$m \sim_k n \implies m = n,$$

then for all $B \subseteq A^N$ we have $B \in \mathrm{Def}(\mathbb{N}; \perp, f)$ iff $B \in \mathrm{Def}(\mathbb{N}; =, \times, +)$.

Proof. "$\Rightarrow$" Clear. "$\Leftarrow$" We need both inclusions of Theorem 2.2. Let $k' \in \mathbb{N}$ be such that $A \in \mathrm{Cl}_{k'}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$. Using $\mathrm{Cl}_{k'} \circ \mathrm{Cl}_{k'} = \mathrm{Cl}_{k'}$ gives $\mathrm{Cl}_{k'}(A) = A$. For $B \subseteq A^N$ with $B \in \mathrm{Def}(\mathbb{N}; =, \times, +)$ consider $\vec{m} \in B$ and $n \in \mathbb{N}$. If $m_i \sim_{\max\{k',k\}} n$ then $m_i \in A$ and $m_i = n$. Conclude with $B = \mathrm{Cl}_{\max\{k',k\}}(B) \in \mathrm{Cl}_{\max\{k',k\}}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$. $\square$

2.2 Showing ω-arithmetic and ω-translation

The next lemma shows that most structures in Chapter 1.2 have ω-arithmetic. For $\Pi^* \subseteq \Pi$ recall the notation $\mathbb{N}^* = \{c \in \mathbb{N} \mid \text{Supp'}(c) \subset \Pi^*\}$.

Lemma 2.5. *Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $\Pi^* \subseteq \Pi$ definable in $\mathcal{M}$. If*

(i) $(\Pi \setminus \Pi^*)/\sim$ *is finite*

(ii) $\{(c, d, e) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \mid \omega(c) \times \omega(d) = \omega(e)\}$ *is definable in $\mathcal{M}$,*

then $\mathcal{M}$ has ω-arithmetic.

Proof. Note that for each $i \geq 0$ the relation $\{c \in \mathbb{N}_{>0} \mid \omega(c) = i\}$ is definable in $\langle \mathbb{N}; \perp \rangle$. Let $N := \#(\Pi \setminus \Pi^*)/\sim$. For $c \in \mathbb{N}_{>0}, d \in \mathbb{N}^*$ we have $\omega(c) = \omega(d)$ iff there exists $c_1 \in \mathbb{N}_{>0}$ and $c_2, d_1, d_2 \in \mathbb{N}^*$ such that

- $d_1 \perp d_2,\ \text{Supp'}(c_1) \subseteq \Pi \setminus \Pi^*$
- $\text{Supp'}(c) = \text{Supp'}(c_1) \cup \text{Supp'}(c_2)$
- $\text{Supp'}(d) = \text{Supp'}(d_1) \cup \text{Supp'}(d_2)$
- $\omega(c_2) = \omega(d_2),\ \bigvee_{i=0}^{N} \omega(c_1) = i = \omega(d_1)$.

The right side of the equivalence can be expressed by an $\mathcal{L}$-formula. So $\omega^{-1}(\times)$ is definable in $\mathcal{M}$ via $\omega(c) \times \omega(d) = \omega(e)$ iff $\exists \tilde{c}, \tilde{d}, \tilde{e} \in \mathbb{N}^*$:

$$\omega(c) = \omega(\tilde{c}),\ \omega(d) = \omega(\tilde{d}),\ \omega(e) = \omega(\tilde{e}),\ \omega(\tilde{c}) \times \omega(\tilde{d}) = \omega(\tilde{e}).$$

□

All applications in Chapter 1.2 implicitly used Lemma 1.5. Therefore if $(\Pi \setminus \Pi^*)/\sim$ is finite we can apply the last lemma. This is clear for all structures studied except in Proposition 1.8. There it may fail for non-linear polynomials.[5] In the linear case $L(n) = a_1 n + a_0$, a simple calculation shows $\Pi^* = \{p \in \Pi \mid p \perp L(1) \gcd(a_1, a_0)\}$. We obtain the next remark.

Remark 2.6. *The following structures have ω-arithmetic.*

- $\langle \mathbb{N}; \perp, n \mapsto |a_1 n + a_0| \rangle$ *for* $a_1, a_0 \in \mathbb{Z} \setminus \{0\}$
- $\langle \mathbb{N}; \perp, n \mapsto \varphi(n) \rangle$ *for φ the Euler phi function*
- $\langle \mathbb{N}; \perp, n \mapsto 1 + \prod_{p \not\perp n,\, p \in \mathrm{P}} p \rangle$
- $\langle \mathbb{N}; \perp, n \mapsto \rho(n) \rangle$ *for* $\rho\colon \mathbb{N} \to \mathrm{P}$ *injective*

[5] If $L(n) = n^2 + 1$ and $\Pi^* = \{p \in \Pi \mid p \perp 2,\ \exists n\colon n \perp p \not\perp L(n)\}$, then for a prime $p > 2$ we have $p \notin \Pi^*$ iff $\nexists n \in \mathbb{N}\colon n^2 \equiv -1 \mod p$ iff $p \equiv 3 \mod 4$. So $(\Pi \setminus \Pi^*)/\sim$ is infinite.

- $\langle \mathbb{N}; \perp, n \mapsto a^n - 1 \rangle$ *for* $a > 1$
- $\langle \mathbb{N}; \perp, n \mapsto \lfloor \frac{an}{b} \rfloor \rangle$ *for* $a, b \in \mathbb{N}$ *with* $a \perp b, b \geq 2$

This thesis does not provide a general theorem for ω-translation. We still have the next two lemmas.

Lemma 2.7. *Let* $f \colon \mathbb{N} \to \mathbb{N}$ *be definable in* $\langle \mathbb{N}; =, \times, + \rangle$. *If* $\langle \mathbb{N}; \perp, f \rangle$ *has* ω*-arithmetic and there is some* $k \geq 0$ *such that for all* $p, q \in \Pi$ *we have*

$$\bigwedge_{i=0}^{k} \omega\big(f^i(p)\big) = \omega\big(f^i(q)\big) \implies p \sim q,$$

then $\langle \mathbb{N}; \perp, f \rangle$ *has* ω*-translation.*

Proof. Note for $i \geq 0$ that $\omega \circ f^i \colon \mathbb{N} \to \mathbb{N}$ is definable in $\langle \mathbb{N}; =, \times, + \rangle$. Using ω-arithmetic we get that $\big\{(c, d) \in \mathbb{N}_{>0}^2 \mid \omega\big(f^i(\omega(c))\big) = \omega(d)\big\}$ is definable in $\langle \mathbb{N}; \perp, f \rangle$. Conclude that $\langle \mathbb{N}; \perp, f \rangle$ has ω-translation via

$$\omega(c) \sim p \iff \exists d_0 \ldots d_k \colon \bigwedge_{i=0}^{k} \omega\big(f^i(\omega(c))\big) = \omega(d_i), d_i \sim f^i(p).$$

□

We can apply Theorem 0.3 to get ω-translation for the successor function.

Lemma 2.8. $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$ *has* ω*-arithmetic and* ω*-translation.*

Proof. By Remark 2.6 we have that $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$ has ω-arithmetic. By Theorem 0.3 we know that the set of primes P and the relation $\{(p, q) \in \Pi^2 \mid p < q\}$ are definable in $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$.

We use that two primes are the same iff the number of smaller primes is the same. Conclude that $\langle \mathbb{N}; \perp, \mathrm{S} \rangle$ has ω-translation via $\omega(c) \sim p$ iff there exist $p', c', d, d' \in \mathbb{N}_{>0}$ such that

- $p' \sim p,\ p' \in \mathrm{P},\ \omega(c') \sim \omega(c),\ \omega(c') \in \mathrm{P}$
- $\forall q \colon q \in \mathrm{P} \ \Rightarrow\ (q \not\perp d \ \Leftrightarrow\ q < p')$
- $\forall e \colon \omega(e) \in \mathrm{P} \ \Rightarrow\ \big(\omega(e) \not\perp \omega(d') \ \Leftrightarrow\ \omega(e) < \omega(c')\big)$
- $\omega(d) = \omega\big(\omega(d')\big)$.

□

We have the following counterexample.

Lemma 2.9. *There is an injective* $\rho\colon \mathbb{N} \to \mathrm{P}$ *such that* $\langle \mathbb{N}; \perp, \rho\rangle$ *does not have* ω*-translation.*

Proof. Let ρ be the following sequence of primes: $\rho(0) = 5$, $\rho(1) = 7$, $\rho(2) = 3$, $\rho(3) = 2$ and $\rho(n)$ is the n-th prime for $n \geq 4$. Note that $\langle \mathbb{N}; \perp, \rho\rangle$ has ω-arithmetic by Remark 2.6.

Assume that $\langle \mathbb{N}; \perp, \rho\rangle$ has ω-translation. Since $m \sim_{\rho,1} n \;\Rightarrow\; m = n$ we can apply Corollary 2.4 to get

$$\mathrm{Def}(\mathbb{N}; \perp, \rho) = \mathrm{Def}(\mathbb{N}; =, \times, +).$$

But Proposition 5 in [CMR96] shows that $\mathrm{Def}(\mathbb{N}; \times, \rho) \neq \mathrm{Def}(\mathbb{N}; =, \times, +)$.

□

2.3 Applications

We will apply Theorem 2.2 to two functions $f\colon \mathbb{N} \to \mathbb{N}$ where we can answer the question (b): when does $\vec{m} \in A$ and $\vec{m} \sim_{f,k} \vec{n}$ imply $\vec{n} \in A$?

Proposition 2.10. *Let* $\omega(n) = \#\,\mathrm{Supp}(n)$ *with* $\omega(0) := 0$*. Then*

(i) $\mathrm{Def}(\mathbb{N}; \perp, \omega) = \mathrm{Cl}_0\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$

(ii) $\mathrm{Def}(\mathbb{N}; =, \perp, \omega) = \mathrm{Def}(\mathbb{N}; =, \times, +)$.

This proposition implies $\mathrm{Def}(\mathbb{N}; \perp, \omega) \subseteq \mathrm{Def}(\mathbb{N}; \perp, \mathrm{S})$. Contrary to this, Woods proved in [Woo81] that $\mathrm{Def}(\mathbb{N}; =, \perp, \mathrm{S}) = \mathrm{Def}(\mathbb{N}; =, \times, +)$ is equivalent to the *Erdős-Woods conjecture*. A similar unintuitive consequence is presented at the end of Chapter 2.4.

To prove the proposition we need one more result of Woods [Woo81]:

$$\mathrm{Def}(\mathbb{N}; =, \perp, +) = \mathrm{Def}(\mathbb{N}; =, \times, +).$$

Proof. "(i)" We use Theorem 2.2. It is clear that $\langle \mathbb{N}; \perp, \omega\rangle$ has ω-translation. For ω-arithmetic we use Woods' result. So, if the following three relations are definable in $\langle \mathbb{N}; \perp, \omega\rangle$

- $\big\{(c, d) \in \mathbb{N}^2 \mid \omega(c) = \omega(d)\big\}$
- $\big\{(c, d) \in \mathbb{N}^2 \mid \omega(c) \perp \omega(d)\big\}$
- $\big\{(c, d, e) \in \mathbb{N}^3 \mid \omega(c) + \omega(d) = \omega(e)\big\}$,

then we can define $\{(c,d,e) \in \mathbb{N}^3 \mid \omega(c) \times \omega(d) = \omega(e)\}$ and get ω-arithmetic.

First note that $\{(l,m,n) \in \mathbb{N}^3 \mid l \sim mn\}$ is definable in $\langle \mathbb{N}; \perp \rangle$ and $m \sim n \Rightarrow \omega(m) = \omega(n)$. So the first relation is definable if we prove that

$$\omega(c) = \omega(d) \iff \forall k \perp cd\colon \omega(ck) \sim \omega(dk).$$

"$\Rightarrow$" Clear. "$\Leftarrow$" Assume $\omega(c) < \omega(d)$. Take a prime p and some $k \in \mathbb{N}, k \perp d$ such that $\omega(dk) = \omega(d) + \omega(k) = p$. Then this contradicts $\omega(ck) < \omega(dk) = p \sim \omega(ck)$.

The second relation is clear. For the last one use $\omega(c) + \omega(d) = \omega(e)$ iff

$$\exists \tilde{c}, \tilde{d}\colon \tilde{c} \perp \tilde{d},\ \omega(\tilde{c}) = \omega(c),\ \omega(\tilde{d}) = \omega(d),\ \omega(\tilde{c}\tilde{d}) = \omega(e).$$

"(ii)" The inclusion "$\subseteq$" is clear. "$\supseteq$" Note that addition is definable via $n + m = k$ iff $\exists c, d, e\colon c \perp d,\ \omega(cd) = \omega(e),\ \omega(c) = n,\ \omega(d) = m,\ \omega(e) = k$. We conclude with Woods' results. $\square$

Proposition 2.11. *Let* $n! \coloneqq \prod_{i=1}^{n} i$ *with* $0! \coloneqq 1$. *Then*

$$\mathrm{Def}(\mathbb{N}; \perp, !) = \mathrm{Def}(\mathbb{N}; =, \times, +).$$

Proof. Note that $\mathrm{Supp'}(n!) = \bigcup_{i=1}^{n} \mathrm{Supp'}(i)$. Write $n!!$ for $(n!)!$ and let $m, n \in \mathbb{N}_{>0}$. We show that the order is definable in $\langle \mathbb{N}; \perp, ! \rangle$ via $m < n \Leftrightarrow \mathrm{Supp'}(m!!) \subset \mathrm{Supp'}(n!!)$.

"$\Leftarrow$" Clear. "$\Rightarrow$" Follows from Bertrand's Postulate, which implies that for all $m \in \mathbb{N}_{>1}$ there is a prime p such that $m! < p \leq 2m! \leq (m+1)! \leq n!$.

So the successor function is definable in $\langle \mathbb{N}; \perp, ! \rangle$. Remark 2.6 implies that $\langle \mathbb{N}; \perp, ! \rangle$ has ω-arithmetic. Since $m = n \Leftrightarrow \omega(m!!) = \omega(n!!)$ we can apply Lemma 2.7 and conclude with Corollary 2.4. $\square$

2.4 Restricted order

For $A \subseteq \mathbb{N}$ let $<_A$ be the order restricted to A. Bès and Richard proved in [BR98] that Theorem 0.3 also holds for $\langle \mathbb{N}; \perp, <_{\Pi} \rangle$. Let $\mathrm{P}_a \coloneqq \mathrm{P} \cup \{p^a \mid p \in \mathrm{P}\}$. They also proved that $\mathrm{Th}(\mathbb{N}; \perp, <_{\mathrm{P}_2})$ is undecidable. We extend these results to the following proposition.

Proposition 2.12. *Let* $a \geq 3$. *Then*

$$\mathrm{Def}(\mathbb{N}; \perp, <_{\mathrm{P}_a}) \supseteq \{A \cap \mathrm{P}_a^N \mid A \in \mathrm{Def}(\mathbb{N}; =, \times, +),\ A \subseteq \mathbb{N}^N\}.$$

Bertrand's Postulate implies that for any $p \in \mathrm{P}$ and $n \in \mathbb{N}_{>0}$ there is a prime between p^n and p^{n+1}. So it is enough to prove the following stronger proposition.

Proposition 2.13. *Let $A \subseteq \mathbb{N}$ be definable in $\langle \mathbb{N}; =, \times, + \rangle$ and $\mathrm{P}_a \subseteq A$ for some $a \geq 3$. If for all $m, n \in A$ with $m < n$ and $m \sim n$ there is a prime between m and n, then*

$$\mathrm{Def}(\mathbb{N}; \perp, <_A) \supseteq \big\{ B \cap A^N \mid B \in \mathrm{Def}(\mathbb{N}; =, \times, +),\ B \subseteq \mathbb{N}^N \big\}.$$

The Dressler conjecture states that for all $m, n \in \mathbb{N}$ with $m < n$ and $m \sim n$ there is a prime between m and n. See [CD99] for evidence of this conjecture.

Let $\pi\colon \mathbb{N} \to \mathbb{N}$ be the prime-counting function. The following result, due to Ingham [Ing37], is key. For $a \geq 3$ there is some $k \geq 1$[6] such that for all $n \geq k$ we have

$$\pi\big((n+1)^a\big) - \pi(n^a) \geq 1.$$

The above statement with $a = 2$ and $k = 1$ is the Legendre conjecture.

We split the proof into several lemmas. The first few show that $\langle \mathbb{N}; \perp, <_A \rangle$ has ω-arithmetic. They adapt the proof for undecidability of $\mathrm{Th}(\mathbb{N}; \perp, <_{\mathrm{P}_2})$ from [BR98].

Lemma 2.14. *The following are definable in $\langle \mathbb{N}; \perp, <_A \rangle$:*

- A *via* $m \in A \ \Leftrightarrow\ \exists n\colon m <_A n$
- $\leq_A$ *via* $p \leq_A q \ \Leftrightarrow\ (p, q \in A,\ q \not<_A p)$
- P *via* $p \in \mathrm{P} \ \Leftrightarrow\ (p \in \Pi,\ \forall q \sim p\colon q \not<_A p)$
- $\mathrm{S}_{\mathrm{P}}\colon A \to \mathrm{P},\ n \mapsto \min\big(\mathrm{P} \cap (n, \infty)\big)$ *via* $p = \mathrm{S}_{\mathrm{P}}(n) \ \Leftrightarrow\ (n \in A,\ p \in \mathrm{P},\ n <_A p,\ \nexists r \in \mathrm{P}\colon n <_A r <_A p)$.

As P is definable in $\langle \mathbb{N}; \perp, <_A \rangle$, we take $\mathrm{Supp}(c) \coloneqq \{p \in \mathrm{P} \mid p \not\perp c\}$. We want to show that the following functions are definable:

- $\mathrm{pow_a}\colon\ \mathrm{P} \to \mathrm{P}_a,\ p \mapsto p^a$
- $\iota \coloneqq \mathrm{S}_{\mathrm{P}} \circ \mathrm{pow_a}\colon\ \mathrm{P} \to \mathrm{P}.$

This follows if P_a is definable. To prove this we introduce for each $1 \leq i \leq a$ the partial function $\text{w-pow}_i\colon \mathbb{N} \to A$ given by the graph

$$\Big\{(p, q) \in \mathrm{P} \times A \mid \exists! r_1 \ldots r_i \in A\colon p = r_1,\ \bigwedge_{j=1}^{i-1} r_j < r_{j+1}, r_j \sim r_{j+1},\ r_i = q\Big\}.$$

[6]For $a = 3$ Dudek proved $k \leq \exp \circ \exp(33.217)$ [Dud16].

Lemma 2.15. $\mathrm{P}_a \setminus \mathrm{P}$ *is definable in* $\langle \mathbb{N}; \perp, <_A \rangle$.

Proof. Let $p_0 = \min \mathrm{P} \cap (2^{a-1}, \infty)$. Then consider $c_2, \ldots c_a, c \in \mathbb{N}$ with $\bigwedge_{i \neq j} c_i \perp c_j$, $\bigcup_{i=2}^{a} \mathrm{Supp}(c_i) = \mathrm{Supp}(c)$, $\forall p \in \mathrm{P}\colon p_0 \leq p \leq \max \mathrm{Supp}(c) \Rightarrow p \in \mathrm{Supp}(c)$ and $\min \mathrm{Supp}(c) = p_0$.

Then the following two points are equivalent:

- $\bigwedge_i \mathrm{Supp}(c_i) = \big\{ p \in \mathrm{P} \mid \text{w-pow}_i(p) = p^a,\ p_0 \leq p \leq \max \mathrm{Supp}(c) \big\}$
- $\bigwedge_{i,j} \forall p \in \mathrm{Supp}(c_i) \setminus \{\max \mathrm{Supp}(c)\}, \mathrm{S_P}(p) \in \mathrm{Supp}(c_j) \ \Rightarrow$

$$\text{w-pow}_{j-1}(\mathrm{S_P}(p)) < \text{w-pow}_i(p) < \text{w-pow}_j(\mathrm{S_P}(p)).$$

This follows by an induction on $\omega(c)$, using that by Bertrand's Postulate we have for $p \geq 2^{a-1}$ that

$$\mathrm{S_P}(p)^{a-1} < p^a < \mathrm{S_P}(p)^a.$$

Each element of A is definable as a constant in $\langle \mathbb{N}; \perp, <_A \rangle$ since for $m \in A$ and $N \coloneqq \#\big(A \cap [0, m)\big)$ we have

$$\{m\} = \Big\{ n \in A \mid \exists! l_1 \ldots l_N \in A\colon \bigwedge_{i=1}^{N-1} l_i <_A l_{i+1},\ l_N <_A n \Big\}.$$

This implies that the finite set $(\mathrm{P}_a \setminus \mathrm{P}) \cap (1, p_0^a)$ is definable in $\langle \mathbb{N}; \perp, <_A \rangle$.

So for $p \in \mathrm{P}, p \geq p_0, p' \in A$ we define $p' = p^a$ via $\exists c_2 \ldots c_a, c \in \mathbb{N}$:

- $\forall q \in \mathrm{P}\colon p_0 \leq q \leq \max \mathrm{Supp}(c) \Rightarrow q \in \mathrm{Supp}(c)$
- $\bigwedge_{i \neq j} c_i \perp c_j$, $\bigcup_{i=2}^{a} \mathrm{Supp}(c_i) = \mathrm{Supp}(c)$, $\min \mathrm{Supp}(c) = p_0$
- $\bigwedge_{i,j} \forall q \in \mathrm{Supp}(c_i) \setminus \{\max \mathrm{Supp}(c)\}\colon\ \mathrm{S_P}(q) \in \mathrm{Supp}(c_j) \ \Rightarrow$

$$\text{w-pow}_{j-1}(\mathrm{S_P}(q)) < \text{w-pow}_i(q) < \text{w-pow}_j(\mathrm{S_P}(q))$$

- $\bigvee_i p \in \mathrm{Supp}(c_i),\ p' = \text{w-pow}_i(p)$

$\square$

To show that $\omega^{-1}(=)$ is definable, we use the fact that for primes $p_1, \ldots p_N$ and $q_1, \ldots q_M$ we have $p_1 < q_1 < p_2 \cdots < q_M \Rightarrow N = M$. This fact is applied using the next lemma to encode any prime by an arbitrarily larger prime.

Since $\mathrm{S_P^k}(2) > k$ we can avoid possible exceptions in Ingham's result by taking $\mathrm{S_P^k}$ of each prime p.

Lemma 2.16. *For $p \in \mathrm{P}$ define $T_p \coloneqq \{\iota^i \circ \mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(p) \mid i \in \mathbb{N}\}$. Then*

(i) $T_p \cap T_q = \emptyset$ *for* $p \neq q \in \mathrm{P}$

(ii) $T_p = \Big\{q \in \mathrm{P} \mid \exists c \in \mathbb{N} \colon q \in \mathrm{Supp}(c),\ \mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(p) \in \mathrm{Supp}(c),\ \forall r \in \mathrm{Supp}(c) \setminus \{\max \mathrm{Supp}(c)\} \colon \iota(r) \in \mathrm{Supp}(c)\Big\}$.

The second point implies that the relation $\{(p,q) \in \mathrm{P} \times \mathrm{P} \mid q \in T_p\}$ is definable in $\langle \mathbb{N}; \perp, <_A \rangle$.

Proof. "(i)" Assume there are $i < j$ with $\iota^i \circ \mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(p) = \iota^j \circ \mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(q)$. As ι restricted to $\mathrm{P} \cap (k, \infty)$ is injective we get for $q' = \iota^{j-i-1} \circ \mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(q)$ and $p' = \mathrm{S}_\mathrm{P}^k(p)$ that

$$\mathrm{S}_\mathrm{P}^2 \circ \mathrm{pow_a}(p') = \mathrm{S_P} \circ \mathrm{pow_a}(q').$$

Therefore $\pi(q'^a) - \pi(p'^a) = 1$ and $q' > p' + 1 > p' > k$, which contradicts Ingham's result.

"(ii)" This is clear as $c \sim \prod_{i=0}^{\omega(c)-1} \iota^i \circ \mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(p)$ iff

- $\mathrm{S_P} \circ \iota \circ \mathrm{S}_\mathrm{P}^k(p) \in \mathrm{Supp}(c)$
- $\forall r \in \mathrm{Supp}(c) \setminus \{\max \mathrm{Supp}(c)\} \colon \iota(r) \in \mathrm{Supp}(c)$.

□

We summarize the previous work in the next lemma.

Lemma 2.17. $\omega^{-1}(=)$ *is definable in* $\langle \mathbb{N}; \perp, <_A \rangle$.

Proof. For this we use $\omega(c) = \omega(d) \iff \exists e \colon e \perp c,\ e \perp d,\ \omega(c) = \omega(e) = \omega(d)$ and prove for $c \perp d$ that $\omega(c) = \omega(d)$ iff there exists $e \in \mathbb{N}$ such that

- $\forall p \in \mathrm{Supp}(c) \cup \mathrm{Supp}(d) \exists! r \in \mathrm{Supp}(e) \colon r \in T_p$
- $\forall r \in \mathrm{Supp}(e) \exists! p \in \mathrm{Supp}(c) \cup \mathrm{Supp}(d) \colon r \in T_p$
- $\min\big(\mathrm{Supp}(e)\big) \in \mathrm{Supp}(c)$
- $\forall r \in \mathrm{Supp}(e) \setminus \big\{\max \mathrm{Supp}(e)\big\} \colon$

$$r \in \bigcup_{p \in \mathrm{Supp}(c)} T_p \iff \min\big(\mathrm{Supp}(e) \cap (r, \infty)\big) \in \bigcup_{q \in \mathrm{Supp}(d)} T_q.$$

"$\Rightarrow$" Write $\mathrm{Supp}(c) = \{p_1 \dots p_N\}$ and $\mathrm{Supp}(d) = \{q_1 \dots q_N\}$. Then take $r_1 = \min(T_{p_1})$, $r_{2i} = \min\big(T_{q_i} \cap (r_{2i-1}, \infty)\big)$ and $r_{2i+1} = \min\big(T_{p_{i+1}} \cap (r_{2i}, \infty)\big)$ for $i \geq 1$. Conclude with $e = \prod_{i=1}^{2N} r_i$.

"$\Leftarrow$" The first two points imply that we have the bijection

$$\chi\colon\ \mathrm{Supp}(c) \cup \mathrm{Supp}(d) \to \mathrm{Supp}(e),\ p \mapsto r \colon r \in T_p.$$

Thus $\omega(c) + \omega(d) = \omega(e)$. Write $\mathrm{Supp}(e) = \{r_1, \dots r_N\}$ with $r_i < r_{i+1}$. The last two points imply that $\chi^{-1}(r_i) \in \mathrm{Supp}(c)$ iff i is odd and that N is even. Therefore $\omega(c) = N/2 = \omega(d)$. □

The proof of Lemma 1.5(i) implies that $\omega^{-1}(+)$ is definable in $\langle \mathbb{N}; \perp, <_A \rangle$. We combine this with the prime-counting function to prove the next lemma.

Lemma 2.18. *$\langle \mathbb{N}; \perp, <_A \rangle$ has ω-arithmetic and ω-translation.*

Proof. The relation $\big\{(c, p) \in \mathbb{N} \times \mathrm{P} \mid \omega(c) = \pi(p)\big\}$ is definable in $\langle \mathbb{N}; \perp, <_A \rangle$ via $\omega(c) = \pi(p)$ iff $\exists d \colon \big(\omega(c) = \omega(d),\ \forall q \in \mathrm{P} \colon q \leq p \ \Leftrightarrow\ q \in \mathrm{Supp}(d)\big)$.

Define $\omega^{-1}(\times)$ via $\omega(c) \times \omega(d) = \omega(e)$ iff there exists some $\tilde{d} \in \mathbb{N}$ such that $\omega(\tilde{d}) = \omega(d)$ and there are $p, q \in \mathrm{Supp}(\tilde{d})$ with $\omega(c) = \pi(p)$, $\omega(e) = \pi(q)$,

$$\forall r \in \mathrm{Supp}(\tilde{d}) \setminus \{q\} \colon \pi\big(\min \mathrm{Supp}(\tilde{d}) \cap (r, \infty)\big) = \pi(r) + \omega(c).$$

This gives ω-arithmetic.

This implies that the relation $\big\{(c, d) \in \mathbb{N}^2_{>0} \mid \pi(\omega(c)) = \omega(d)\big\}$ is definable in $\langle \mathbb{N}; \perp, <_A \rangle$. Define ω-translation via $\omega(c) = p$ iff

$$\omega(c) \in \mathrm{P},\ \exists d \in \mathbb{N}_{>0} \colon \omega(d) = \pi(p),\ \pi(\omega(c)) = \omega(d).$$

□

To conclude the proof of Proposition 2.13 we apply Proposition 2.3 with the function

$$\epsilon \colon \mathbb{N} \to \mathbb{N},\ n \mapsto \begin{cases} \mathrm{S}_{\mathrm{P}}(n) & \text{if } n \in A \\ 1 & \text{else.} \end{cases}$$

Lemma 2.19. *We have*

(i) $\mathrm{Cl}_{\epsilon,1}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big) \supseteq \big\{B \cap A^N \mid B \in \mathrm{Def}(\mathbb{N}; =, \times, +),\ B \subseteq \mathbb{N}^N\big\}$

(ii) $\mathrm{Def}(\mathbb{N}; \perp, <_A) = \mathrm{Cl}_{\epsilon,1}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$.

Proof. "(i)" The assumption on A implies that for all $m, n \in A$ with $m \sim n$ and $\mathrm{S_P}(m) \sim \mathrm{S_P}(n)$ we have $m = n$. Note that for $m \in A, n \in \mathbb{N} \setminus A$ we have $\epsilon(m) \not\sim 1 = \epsilon(n)$. Therefore $m \sim_{\epsilon,1} n$ iff $(m = n \in A) \vee (m, n \notin A,\ m \sim n)$. So for $B \in \mathrm{Def}(\mathbb{N}; =, \times, +)$ we have

$$\mathrm{Cl}_{\epsilon,1}(B) = \Big\{c \in \mathrm{Cl}_0(B) \mid \exists b \in B\colon \bigwedge_{i=1}^{N} \begin{cases} b_i \in A \ \Rightarrow \ b_i = c_i \\ b_i \notin A \ \Rightarrow \ c_i \notin A \end{cases} \Big\}.$$

Conclude with $B \cap A^N \in \mathrm{Def}(\mathbb{N}; =, \times, +)$.

"(ii)" We have by Proposition 2.3 that

$$\mathrm{Cl}_{\epsilon,1}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big) \subseteq \mathrm{Def}(\mathbb{N}; \perp, <_A).$$

Further (i) implies that $\{\perp, <_A\} \subset \mathrm{Cl}_{\epsilon,1}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$. So for the other inclusion note that $\mathrm{Cl}_{\epsilon,1}\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big)$ is closed under unions, complements and projections. $\square$

The proof of Lemma 2.19 describes all definable sets in $\langle \mathbb{N}; \perp, <_A \rangle$. It allows us to prove that equality is not definable in $\langle \mathbb{N}; \perp, <_{\mathrm{P}_a} \rangle$ or $\langle \mathbb{N}; \perp, <_{\Pi} \rangle$.

We end this chapter with an unintuitive consequence, only possible in first-order logic without a logical symbol for equality. Theorem 2.20 in [BR98] gives that addition is not definable in $\langle \mathbb{N}; =, \perp, <_{\mathrm{P}_3} \rangle$. With the last lemma and Proposition 2.10 we get the following proper inclusions:

$$\mathrm{Def}(\mathbb{N}; \perp, \omega) \subset \mathrm{Def}(\mathbb{N}; \perp, <_{\mathrm{P}_3}) \subset \mathrm{Def}(\mathbb{N}; =, \perp, <_{\mathrm{P}_3}) \subset \mathrm{Def}(\mathbb{N}; =, \perp, \omega).$$

This is possible as the graph of ω is not definable in $\langle \mathbb{N}; \perp, \omega \rangle$.

3 Open Problems

This chapter presents some remaining questions motivated by Theorem 2.2.

The theorem describes the definable sets in $\langle \mathbb{N}; \perp, f\rangle$ for any $f\colon \mathbb{N} \to \mathbb{N}$ such that $\langle \mathbb{N}; \perp, f\rangle$ has ω-arithmetic and ω-translation. We have seen in Remark 2.6 that most structures in Chapter 1.2 have ω-arithmetic. But there was one exception. The next problem would resolve it.

Problem. *Let $L \in \mathbb{Z}[X]$ be a non-linear polynomial with at least two non-zero coefficients. Does $\langle \mathbb{N}; \perp, n \mapsto |L(n)|\rangle$ have ω-arithmetic?*

Then the following problem would allow us to apply Theorem 2.2.

Problem. *Do the following structures have ω-translation?*

- $\langle \mathbb{N}; \perp, n \mapsto |L(n)|\rangle$ *for $L \in \mathbb{Z}[X]$ with at least two non-zero coefficients*
- $\langle \mathbb{N}; \perp, n \mapsto \varphi(n)\rangle$ *for φ the Euler phi function*
- $\langle \mathbb{N}; \perp, n \mapsto 1 + \prod_{p \not| n,\, p\in \mathrm{P}} p\rangle$
- $\langle \mathbb{N}; \perp, n \mapsto a^n - 1\rangle$ *for $a > 1$*
- $\langle \mathbb{N}; \perp, n \mapsto \lfloor \frac{an}{b} \rfloor\rangle$ *for $a, b \in \mathbb{N}$ with $a \perp b, b \geq 2$*

Some plausible number-theoretic claims would imply that $\langle \mathbb{N}; \perp, F_a\rangle$ has ω-translation. For example the following two:

- $\forall p \in \Pi \exists k \geq 0 \forall q \in \Pi\colon \Big(\bigwedge_{i=0}^{k} \omega(F_a^i(p)) = \omega(F_a^i(q))\Big) \;\Rightarrow\; p = q$
- $\forall p \in \Pi \exists k \geq 0 \forall q \in \Pi\colon \Big(\bigwedge_{i=0}^{k} \omega(F_a(p^i)) = \omega(F_a(q^i))\Big) \;\Rightarrow\; p = q.$

The next step in studying the definable subsets of $\langle \mathbb{N}; \perp, f\rangle$ would be to understand the question (b): when does $\vec{m} \in A$ and $\vec{m} \sim_{f,k} \vec{n}$ imply $\vec{n} \in A$?

We solve this for the following two functions.

Proposition 3.1. *Let $H(n) = 1 + \prod_{p \not| n,\, p\in \mathrm{P}} p$ and $F_a(n) = a^n - 1$ for $a > 1$.*

(i) Assume that $\langle \mathbb{N}; \perp, H\rangle$ has ω-translation. Then

$$\mathrm{Def}(\mathbb{N}; \perp, H) = \mathrm{Cl}_0\big(\mathrm{Def}(\mathbb{N}; =, \times, +)\big).$$

(ii) Assume that $\langle \mathbb{N}; \perp, F_a\rangle$ has ω-translation. Then

$$\mathrm{Def}(\mathbb{N}; \perp, F_a) = \mathrm{Def}(\mathbb{N}; =, \times, +).$$

Proof. Note that $\langle \mathbb{N}; \perp, F_a \rangle$ and $\langle \mathbb{N}; \perp, H \rangle$ have ω-arithmetic by Remark 2.6.

"(i)" We apply Theorem 2.2. Further note that $\mathrm{Cl}_{H,k} = \mathrm{Cl}_0$ for all $k \in \mathbb{N}$, since $m \sim n \Rightarrow H(m) = H(n)$.

"(ii)" Corollary 1.7 of [Ric85] states that for all $m, n \in \mathbb{N}$ we have

$$F_a(m) \sim F_a(n) \iff m = n \vee \big(a + 1 \sim 2,\ \{m, n\} = \{1, 2\}\big).$$

Now $m \sim_{F_a,1} n \Leftrightarrow m = n$ and we conclude by Corollary 2.4 with $A = \mathbb{N}$.

□

This leaves the following problem.

Problem. *Can we solve question (b) for any of the following functions?*

- $n \mapsto |L(n)|$ *for* $L \in \mathbb{Z}[X]$ *with at least two non-zero coefficients*
- φ*, the Euler phi function*
- $n \mapsto \lfloor \frac{an}{b} \rfloor$ *for* $a, b \in \mathbb{N}$ *with* $a \perp b, b \geq 2$

We have a partial answer to (b) for the Euler phi function. Let $p \in \Pi$ and $k, n \in \mathbb{N}$. Then $p \sim_{\varphi,k} n \Leftrightarrow p = n \vee (p \sim n,\ \exists q \in \mathrm{P}\colon q^{k+1} \mid p, q^{k+1} \mid n)$.

The last problem would weaken the prime powers assumption on A in Proposition 2.12.

Problem. *Let* $A \subseteq \mathbb{N}$ *be definable in* $\langle \mathbb{N}; =, \times, + \rangle$ *such that* $\mathrm{P} \subset A$ *and for each* $p \in \mathrm{P}$ *there exists* $q \in A$ *with* $p^2 < q \sim p$*. If for all* $m, n \in A$ *with* $m < n$ *and* $m \sim n$ *there is a prime between* m *and* n*, does this imply*

$$\mathrm{Def}(\mathbb{N}; \perp, <_A) \supseteq \big\{B \cap A^N \mid B \in \mathrm{Def}(\mathbb{N}; =, \times, +),\ B \subseteq \mathbb{N}^N\big\}?$$

References

[Ban86] AS Bang. Taltheoretiske undersøgelser. *Tidsskrift for mathematik*, 4:70–80, 1886.

[Bès02] Alexis Bès. A survey of arithmetical definability. *A tribute to Maurice Boffa*, pages 1–54, 2002.

[BR98] Alexis Bès and Denis Richard. Undecidable extensions of skolem arithmetic. *The Journal of Symbolic Logic*, 63(2):379–401, 1998.

[BS96] F. Beukers and H.P. Schlickewei. The equation x+y=1 in finitely generated groups. *Acta Arithmetica*, 78, 01 1996.

[CD99] Todd Cochrane and Robert E. Dressler. Gaps between integers with the same prime factors. *Mathematics of Computation*, 68(225):395–401, 1999.

[CMR96] Patrick Cegielski, Yuri Matiyasevich, and Denis Richard. Definability and decidability issues in extensions of the integers with the divisibility predicate. *The Journal of Symbolic Logic*, 61(2):515–540, 1996.

[Dud16] Adrian W Dudek. An explicit result for primes between cubes. *Functiones et Approximatio Commentarii Mathematici*, 55(2):177–197, 2016.

[GB71] Irving Gerst and John Brillhart. On the prime divisors of polynomials. *The American Mathematical Monthly*, 78(3):250–266, 1971.

[Gö31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[Ing37] Albert Edward Ingham. On the difference between consecutive primes. *Quarterly Journal of Mathematics*, 1:255–266, 1937.

[Kor01] Ivan Korec. A list of arithmetical structures complete with respect to the first-order definability. *Theoretical Computer Science*, 257(1):115–151, 2001. Weak Arithmetics.

[Mat72] Yu V Matiyasevich. Diophantine sets. *Russian Mathematical Surveys*, 27(5):124, oct 1972.

[Pre29] Mojzesz Presburger. Uber die vollstandigkeit eines gewissen systems der arithmetik ganser zahlen. In *Comptes-Rendus du ler Congress des Mathematiciens des Pays Slavs, 1929*, 1929.

[Ric85] Denis Richard. All arithmetical sets of powers of primes are first-order definable in terms of the successor function and the coprimeness predicate. *Discrete Mathematics*, 53:221–247, 1985.

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14(2):98–114, 1949.

[Sko30] Thoralf Skolem. Über einige satzfunktionen in der arithmetik. *Skrifter utgitt av Det Norske Videnskaps-Akademi i Oslo, I. Matematisk-naturvidenskapelig klasse*, pages 1–28, 1930.

[Woo81] Alan Woods. Some problems in logic and number theory and their connections. *Ph. D. Thesis, Univ. of Manchester*, 1981.