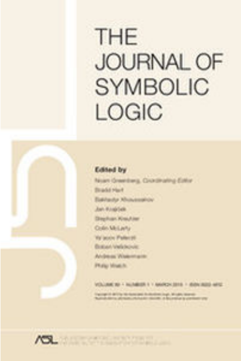

The laws of integer divisibility, and solution sets of linear divisibility conditions

L. van den Dries and A. J. Wilkie

The Journal of Symbolic Logic / Volume 68 / Issue 02 / June 2003, pp 503 - 526
DOI: 10.2178/jsl/1052669061, Published online: 12 March 2014

Link to this article: http://journals.cambridge.org/abstract_S0022481200008756

How to cite this article:
L. van den Dries and A. J. Wilkie (2003). The laws of integer divisibility, and solution sets of linear divisibility conditions . The Journal of Symbolic Logic, 68, pp 503-526 doi:10.2178/jsl/1052669061

Request Permissions : Click here

The Journal of Symbolic Logic
Volume 68, Number 2, June 2003

THE LAWS OF INTEGER DIVISIBILITY, AND SOLUTION SETS OF LINEAR DIVISIBILITY CONDITIONS

L. VAN DEN DRIES AND A. J. WILKIE

Abstract. We prove linear and polynomial growth properties of sets and functions that are existentially definable in the ordered group of integers with divisibility. We determine the laws of addition with order and divisibility.

§1. Introduction. For integers a, b we write $a \mid b$ to indicate that a divides b, that is, $ax = b$ for some integer x. Bel'tyukov [1] and Lipshitz [4] found an algorithm to decide whether any given *existential* sentence about the structure $(\boldsymbol{Z}, 0, 1, +, -, <, \mid)$ is true in that structure. Here we study properties of the subsets of $\boldsymbol{Z}^n$ that are existentially definable in this structure, and also find a simple axiomatization for the universal sentences true in the structure. These two items are closely related in our model-theoretic approach. Roughly speaking, in §3 we give a list of axioms that are obviously satisfied by the substructures of elementary extensions of the above standard model. Conversely, every model of these axioms can be embedded into an elementary extension of the above standard model, as we show in §8. It follows that we have the correct axioms. The nature of the embedding procedure leads to interesting properties of existentially definable sets, which we call "subdivisibility sets" below.

A *basic divisibility set in* $\boldsymbol{Z}^m$ is a finite intersection of sets of the form

$$\{x \in \boldsymbol{Z}^m : \lambda(x) \mid \mu(x)\} \quad \text{and} \quad \{x \in \boldsymbol{Z}^m : \lambda(x) \geq 0\},$$

where the polynomials $\lambda, \mu \in \boldsymbol{Z}[X]$ are of degree at most 1 in $X = (X_1, \dots, X_m)$. The basic divisibility sets in $\boldsymbol{Z}^m$ generate a boolean algebra of subsets of $\boldsymbol{Z}^m$, and a *divisibility set in* $\boldsymbol{Z}^m$ is by definition a set in this boolean algebra. We also consider projections of these sets: a *subdivisibility set in* $\boldsymbol{Z}^m$ is by definition the image of a finite union of basic divisibility sets in $\boldsymbol{Z}^{m+n}$ (for some n) under the projection map

$$(x_1, \dots, x_{m+n}) \mapsto (x_1, \dots, x_m) : \boldsymbol{Z}^{m+n} \to \boldsymbol{Z}^m.$$

With x, y, z ranging over $\boldsymbol{Z}$ we have the equivalence

$$x \nmid y \iff \exists z (x \mid y + z \text{ and } 0 < z < |x|) \text{ or } (x = 0 \text{ and } |y| > 0).$$

It follows that the complement in $\boldsymbol{Z}^m$ of each basic divisibility set in $\boldsymbol{Z}^m$ is a subdivisibility set. Hence each divisibility set in $\boldsymbol{Z}^m$ is a subdivisibility set. Thus the divisibility sets in $\boldsymbol{Z}^m$ are exactly the subsets of $\boldsymbol{Z}^m$ that are *quantifier-free definable*

Received February 4, 2002; revised October 21, 2002.

in $(\boldsymbol{Z}, 0, 1, +, -, <, |)$, and the subdivisibility sets in $\boldsymbol{Z}^m$ are exactly the subsets of $\boldsymbol{Z}^m$ that are *existentially definable* in $(\boldsymbol{Z}, 0, 1, +, -, <, |)$.

EXAMPLES. Subsets of $\boldsymbol{Z}^m$ definable in $(\boldsymbol{Z}, 0, 1, +, -, <)$ are divisibility sets in $\boldsymbol{Z}^m$ (Presburger). The set $E := \{x \in \boldsymbol{N} : x \neq 2^n \text{ for all } n \in \boldsymbol{N}\}$ of non-powers of 2 is a subdivisibility set in $\boldsymbol{Z}$:

$$x \in E \iff x \geq 0 \text{ and } \exists y (y > 0, 2y + 1 \mid x).$$

Define $\gcd : \boldsymbol{Z}^2 \to \boldsymbol{Z}$ by $\gcd(a, b) =$ the unique $c \in \boldsymbol{N}$ such that $a\boldsymbol{Z} + b\boldsymbol{Z} = c\boldsymbol{Z}$. The graph of gcd is a subdivisibility set in $\boldsymbol{Z}^3$, as noted in [5]:

$$\gcd(x, y) = z \iff z \geq 0, z \mid x, z \mid y \text{ and } \exists u, v (z = u + v, x \mid u \text{ and } y \mid v).$$

If S is a divisibility set in $\boldsymbol{Z}^m$ and $f : S \to \boldsymbol{Z}^n$ is a map whose graph is a subdivisibility set in $\boldsymbol{Z}^{m+n}$, then the complement of this graph is also a subdivisibility set in $\boldsymbol{Z}^{m+n}$. The set $\{(x, x^2) : x \in \boldsymbol{Z}\}$ (graph of the squaring function) is not a subdivisibility set in $\boldsymbol{Z}^2$, but its complement is; see [5].

By [1] and [4], each subdivisibility set is recursive. In [5] the algorithm of [4] is made into a decision procedure of class NP; hence each subdivisibility set is in the class NP. Also, [5] has an example of an NP-complete subdivisibility set in $\boldsymbol{Z}^3$. Here we focus on other structural properties of these sets, such as the following.

PROPOSITION 1.1. *Let $E \subseteq \boldsymbol{N}$ be an infinite subdivisibility set. Then E contains an infinite arithmetic progression $a + \boldsymbol{N}b$ $(a, b \in \boldsymbol{N}, b > 0)$.*

For sets A, B, E with $E \subseteq A \times B$ and $a \in A$, we put $E(a) := \{b \in B : (a, b) \in E\}$.

THEOREM 1.2. *Let $E \subseteq \boldsymbol{N}^2$ be a subdivisibility set. Then either there is an $a \in \boldsymbol{N}$ such that $E(a)$ is infinite, or there are positive real constants c and d such that for all $(x, y) \in E$ we have $y < cx + d$.*

COROLLARY 1.3. *Let $S \subseteq \boldsymbol{Z}^n$ and let $f : S \to \boldsymbol{Z}$ be a function whose graph is a subdivisibility set in $\boldsymbol{Z}^{n+1}$. Then f has the following properties*:

(1) *there is a constant $c > 0$ such that $|f(x)| \leq c|x|$ for all non-zero $x \in S$, where $|x| = |x_1| + \cdots + |x_n|$ for $x \in \boldsymbol{Z}^n$;*

(2) *either there is $a \in \boldsymbol{Z}$ such that $f^{-1}(a)$ is infinite, or there is a constant $c > 0$ such that for all $x \in S$, if $f(x) \neq 0$, then $|f(x)| \geq c|x|$.*

PROOF. For (1) we put $E := \{(|x|, |f(x)|) \in \boldsymbol{N}^2 : x \in S\}$. Then clearly $E(a)$ is finite for each $a \in \boldsymbol{N}$. Hence Theorem 1.2 gives the desired result. For (2) we apply the theorem to $E := \{(|f(x)|, |x|) \in \boldsymbol{N}^2 : x \in S\}$. ⊣

We also obtain decidability results, and uniform versions of the above:

PROPOSITION 1.4. *There is an algorithm that takes as inputs existential formulas $\phi(y_1, \ldots, y_n)$ in the language $\{0, 1, +, -, <, |\}$, and decides for any such formula whether it defines a finite subset of $\boldsymbol{Z}^n$. If S is a subdivisibility set in $\boldsymbol{Z}^{m+n}$, then the set $\{a \in \boldsymbol{Z}^m : S(a)$ is infinite$\}$ is a subdivisibility set in $\boldsymbol{Z}^m$.*

In §5 we prove our main technical proposition 5.2. Then we derive easily the above properties of subdivisibility sets in §6. The next result is proved in §7.

THEOREM 1.5. *Let $E \subseteq \boldsymbol{N}^2$ be a subdivisibility set. Then there are positive real constants C, K such that for all $x > 0$ in $\boldsymbol{N}$, if $E(x) \neq \emptyset$, then $y < Cx^K$ for some $y \in E(x)$.*

EXAMPLE. Let $E := \{(x, y) \in \boldsymbol{N}^2 : x + i \mid y \text{ for } i = 1, \dots, k \text{ and } y > 0\}$, where k is any positive integer. Then the conclusion of the theorem holds with $K = k$ (and a suitable C), but not for any $K < k$.

COROLLARY 1.6. *Let $S \subseteq \boldsymbol{N}^n$ and $f : S \to \boldsymbol{N}$ an unboundedfunction whose graph is a subdivisibility set in $\boldsymbol{Z}^{n+1}$. Then there is a real constant $c > 0$ such that for infinitely many $x \in S$ we have $f(x) > |x|^c$.*

PROOF. Let $E := \{(f(x), |x|) : x \in S\}$. By Theorem 1.5 there is $K > 0$ such that for infinitely many $x \in S$ we have $|x| < f(x)^K$. Then the desired result holds for $c = 1/K$. ⊣

The following problems seem to be still open. Can we replace $f(x) > |x|^c$ by $f(x) > c|x|$ in Corollary 1.6? Is the set $\{x \in \boldsymbol{N} : x \neq n^2 \text{ for all } n\}$ of non-squares a subdivisibility set in $\boldsymbol{Z}$?

Much of the above was done in 1980, motivated by trying to find a simple set of axioms—the laws of integer divisibility—for the universal theory of the structure $(\boldsymbol{Z}, 0, 1, +, -, <, |)$. We achieved this for the expansion of this structure by the p-adic divisibility relations (see §8). One byproduct at that time was Proposition 1.1, subsequently improved by Lipshitz [5]. The present paper is a belated account of our work in 1980, but we include results that we didn't know then, such as Proposition 1.4 and Theorem 1.5. Our interest in these matters was rekindled by "Problem 1" of Moschovakis [7]. Originally Corollary 1.6 was going to be used in a partial solution of this problem. After our work on the present paper was finished the first author found a more elementary and complete solution of "Problem 1" in the main case of interest. This will be presented elsewhere.

§2. Conventions.

Throughout m and n range over $\boldsymbol{N} = \{0, 1, 2, \dots, \}$. By "prime number" we mean (as usual) an integer > 1 that is not a product of two smaller positive integers. For any ordered abelian group $(A, <)$, and elements $a, b \in A$ we define:

$$a \ll b \iff |a| < n|b| \text{ for all } n > 0.$$

Instead of $a \ll b$ we also write $b \gg a$.

Beginning with §4 we often deal with a finitely generated ordered abelian group $(A, <)$ with least positive element 1. In that situation $A_0 \subset A_1 \subset \cdots \subset A_n$ will denote the strictly increasing sequence of subgroups of A that are convex with respect to the given ordering $<$ on A, so $A_0 = \{0\}$, $A_1 = \boldsymbol{Z}.1, \dots, A_n = A$. In addition, we put $r(i) := \operatorname{rk}(A_i)$, and we choose positive elements $e_1, \dots, e_N \in A$, with $N = r(n)$, such that $e_1, \dots, e_{r(i)}$ is a basis of the free abelian group A_i for $i = 1, \dots, n$. In particular, $e_1 = 1$.

Given an elementary extension ${}^*\boldsymbol{Z}$ of the ring of integers $\boldsymbol{Z}$, we put

$${}^*\boldsymbol{N} := \{x \in {}^*\boldsymbol{Z} : x \geq 0\},$$

and more generally, for each set $S \subseteq \boldsymbol{Z}^n$ definable in the ring $\boldsymbol{Z}$, say by the formula $\phi(y_1, \dots, y_n)$ in the language of rings, we let ${}^*S$ be the subset of ${}^*\boldsymbol{Z}^n$ that is defined in the ring ${}^*\boldsymbol{Z}$ by $\phi(y_1, \dots, y_n)$.

The fraction field of an integral domain R is denoted by $\operatorname{Frac}(R)$.

§3. The laws of integer divisibility. In this section we introduce *groups with $\boldsymbol{Z}$-like divisibilities*. In §8 these algebraic objects will turn out to be exactly the models of the "laws of integer divisibility". Groups with $\boldsymbol{Z}$-like divisibilities carry information about the global behaviour of divisibility sets in a coordinate-free way. This will be useful to us.

Let A be an (additively written) abelian group.

A *divisibility* on A is a binary relation div on A such that for all $a, b, c \in A$

(1_{div}) $0 \operatorname{div} a \Longrightarrow a = 0$;
(2_{div}) $a \operatorname{div} -a$;
(3_{div}) $(a \operatorname{div} b \text{ and } b \operatorname{div} c) \Longrightarrow a \operatorname{div} c$;
(4_{div}) $(a \operatorname{div} b \text{ and } a \operatorname{div} c) \Longrightarrow a \operatorname{div} b + c$;
(5_{div}) $(na \operatorname{div} nb \Longleftrightarrow a \operatorname{div} b)$, for each $n > 0$.

Let div be a divisibility on A. One easily derives (in this order) that div is reflexive, that for each $a \in A$ the set

$$a \operatorname{div} A := \{b \in A : a \operatorname{div} b\}$$

is a subgroup of A, and that A is torsion-free. The binary relation $\sim$ on A defined by

$$a \sim b \Longleftrightarrow (a \operatorname{div} b \text{ and } b \operatorname{div} a)$$

is an equivalence relation, and the quotient set $A/\sim$ is (partially) ordered by setting $a^{\sim} \leq b^{\sim}$ iff $a \operatorname{div} b$.

For $a, b \in A$ we say that *a weakly divides b* (notation: $a\,{}^w\!\operatorname{div} b$) if $a \operatorname{div} nb$ for some $n > 0$. Note that then ${}^w\!\operatorname{div}$ is again a divisibility on A.

Let p be a prime number. The divisibility div is said to be *p-adic* if for all $a, b \in A$ we have:

(1_p) not $(pa \operatorname{div} a)$;
(2_p) $b \operatorname{div} pa \Longrightarrow (b \operatorname{div} a \text{ or } pa \operatorname{div} b)$;
(3_p) $a \operatorname{div} b \Longrightarrow pa \operatorname{div} ia + b$ for some $i \in \{0, \dots, p-1\}$;
(4_p) $a \operatorname{div} b$ or $b \operatorname{div} a$ (so $A/\sim$ is totally ordered).

Let p be a prime number. The usual p-adic valuation $v_p : \boldsymbol{Q} \to \boldsymbol{Z} \cup \{\infty\}$ on $\boldsymbol{Q}$ induces the divisibility $|_p$ on $\boldsymbol{Z}$ by setting, for $a, b \in \boldsymbol{Z}$:

$$a \mid_p b \Longleftrightarrow v_p(a) \leq v_p(b).$$

The divisibility $|_p$ is p-adic in the sense above, and $|_p$ as well as its complement are existentially definable in $(\boldsymbol{Z}, |)$, where $\boldsymbol{Z}$ is considered as additive group: with a, b, x ranging over $\boldsymbol{Z}$ we have

$$a \mid_p b \Longleftrightarrow \exists x (a \mid x \text{ and } b \mid x \text{ and } pb \nmid x)$$
$$a \nmid_p b \Longleftrightarrow pb \mid_p a.$$

Hence the subdivisibility sets in $\boldsymbol{Z}^m$ coincide with the subsets of $\boldsymbol{Z}^m$ that are existentially definable in the structure $\boldsymbol{Z}_{\text{div}} := (\boldsymbol{Z}, 1, <, |, |_2, |_3, |_5, \dots)$, where $\boldsymbol{Z}$ is viewed as additive group. It turns out to be convenient to consider the expansion $\boldsymbol{Z}_{\text{div}}$ of $(\boldsymbol{Z}, 1, <, |)$ as the basic model-theoretic object of study rather than $(\boldsymbol{Z}, 1, <, |)$ itself.

Note that the divisibility $|$ on $\boldsymbol{Z}$ is the intersection of the divisibilities $|_p$ as p ranges over all prime numbers.

In the definition below p ranges over the prime numbers.

A *group with $\boldsymbol{Z}$-like divisibilities* is a structure

$$(A, 1, <, \operatorname{div}, (\operatorname{div}_p))$$

where $(\operatorname{div}_p) = (\operatorname{div}_2, \operatorname{div}_3, \operatorname{div}_5, \dots)$, such that for all $a, b \in A$:

(Div1) $(A, <)$ is an ordered abelian group with smallest positive element 1;
(Div2) div is a divisibility on A, and $1 \operatorname{div} a$;
(Div3) $(0 < a, 0 < b, \text{ and } a \operatorname{div} b) \Longrightarrow a \leq b$;
(Div4) div_p is a p-adic divisibility on A, for each p;
(Div5) $a \operatorname{div} b \Longrightarrow a \operatorname{div}_p b$, for each p;
(Div6) $(a \operatorname{div} b \text{ and } pa \operatorname{div}_p b) \Longrightarrow pa \operatorname{div} b$, for each p.

Note that (Div3) expresses a compatibility between $<$ and div, and that (Div5) and (Div6) express compatibilities between div and div_p.

Let $\mathscr{A} = (A, 1, <, \operatorname{div}, (\operatorname{div}_p))$ be a group with $\boldsymbol{Z}$-like divisibilities. It follows from (Div3) that if $0 < a \in A$, then the subgroup $a \operatorname{div} A$ of A has smallest positive element a. Hence, if $a, b \in A$ have the same archimedean class (that is, $|a| \leq n|b|$ and $|b| \leq n|a|$ for some $n > 0$), then

$$a \operatorname{div} b \Longleftrightarrow ka = b \text{ for some } k \in \boldsymbol{Z}.$$

Note that any substructure of $\mathscr{A}$ is also a group with $\boldsymbol{Z}$-like divisibilities. Any subgroup B of A that contains 1 gives rise to a substructure $\mathscr{B} = (B, \dots)$ by restricting $<$, div and each div_p to B.

Given any prime number p we equip the $\boldsymbol{Q}$-linear space $A \otimes \boldsymbol{Q}$ with the valuation w_p defined up to equivalence by the requirement that

$$w_p(x) \leq w_p(y) \Longleftrightarrow x \operatorname{div}_p y$$

for $x, y \in A \subseteq A \otimes \boldsymbol{Q}$, where each $x \in A$ is identified with $x \otimes 1 \in A \otimes \boldsymbol{Q}$. For use in §4 we note that then $(A \otimes \boldsymbol{Q}, w_p, 1)$ is a correct $(\boldsymbol{Q}, v_p)$-linear space in the sense of [2], so its elementary theory is fully understood.

The ordered additive group of integers $(\boldsymbol{Z}, <)$ has a unique expansion to a group with $\boldsymbol{Z}$-like divisibilities, namely $\boldsymbol{Z}_{\text{div}} := (\boldsymbol{Z}, 1, <, |, (|_p))$. Note that $\boldsymbol{Z}_{\text{div}}$ has a unique embedding $k \mapsto k.1$ into any group $\mathscr{A}$ with $\boldsymbol{Z}$-like divisibilities; we shall identify $\boldsymbol{Z}_{\text{div}}$ via this embedding with a substructure of $\mathscr{A}$, so that $\boldsymbol{Z}_{\text{div}} \subseteq \mathscr{A}$, in particular, $k = k.1 \in A$ for $k \in \boldsymbol{Z}$. We can now state one of our main results, to be proved in §8.

THEOREM 3.1. *Each group with $\boldsymbol{Z}$-like divisibilities can be embedded into some elementary extension of $\boldsymbol{Z}_{\text{div}}$.*

The following lemma will be used in §8.

LEMMA 3.2. *Let $\mathscr{A}$ be a group with $\boldsymbol{Z}$-like divisibilities, and $n > 0$. Then the additive map $k \mapsto k + (n \operatorname{div} A) : \boldsymbol{Z} \to A/n \operatorname{div} A$ is surjective with kernel $n\boldsymbol{Z}$, and thus induces a group isomorphism $\boldsymbol{Z}/n\boldsymbol{Z} \cong A/n \operatorname{div} A$.*

PROOF. It is clear that the kernel is $n\boldsymbol{Z}$. For surjectivity, let $p(1), \dots, p(s)$ be the distinct prime factors of n, and write $n = p(1)^{e(1)} \cdots p(s)^{e(s)}$. Let $b \in A$. For $i = 1, \dots, s$ we apply axiom (3) for $p(i)$-adic divisibilities $e(i)$-times in succession, starting with the fact that $1 \operatorname{div}_{p(i)} b$, to produce $r(i) \in \{0, \dots, p(i)^{e(i)} - 1\}$ such that $p(i)^{e(i)} \operatorname{div}_{p(i)} r(i) + b$. The Chinese Remainder Theorem then gives an integer r such that $r \equiv r(i) \mod p(i)^{e(i)}$ for $i = 1, \dots, s$. Hence $p(i)^{e(i)} \operatorname{div}_{p(i)} r + b$ for

$i = 1, \dots, s$. It then follows by repeated application of the axioms (Div6) that $n \operatorname{div} r + b$. This proves surjectivity. ⊣

§4. **Bounded induction domains.** For some results on subdivisibility sets it suffices to embed groups with $\boldsymbol{Z}$-like divisibilities into elementary extensions of the ring of integers. But for more subtle results we need to embed them into models of a theory weaker than full arithmetic, namely *bounded induction*. This theory can only define functions of polynomial growth (Parikh), and this fact is important in the proof of Theorem 1.5. In this section we develop elementary number theory in models of bounded induction as needed in proving our embedding results.

An *ordered domain* is a (commutative) integral domain with a total ordering $<$ on its underlying set that is compatible with the ring operations:

$$0 < 1, \quad a < b \Longrightarrow a + c < b + c, \quad (a < b \text{ and } c > 0) \Longrightarrow ac < bc,$$

for all a, b, c in the ring. A *bounded induction domain* is an ordered domain $(R, 0, 1, +, -, \cdot, <)$ (written as R below) whose ordered semiring $R^{\geq 0}$ of nonnegative elements satisfies the induction scheme $I\Delta_0$ for bounded formulas; see [8]. (The induction axioms of $I\Delta_0$ mention the successor function, which on $R^{\geq 0}$ is given by $x' = x + 1$.)

In the rest of this section we fix a bounded induction domain R, and we let a, b, c, d (sometimes with subscripts) range over R. We identify $\boldsymbol{Z}$ with an ordered subring of R via its unique embedding into R. For proofs of some of the facts mentioned below we refer the reader to [8].

Divisibility. The binary relation $|$ on R is defined by

$$a \mid b \Longleftrightarrow ax = b \text{ for some } x \in R.$$

Instead of writing $a \mid b$ we also say "a divides b", or "a is a divisor of b", or "b is a multiple of a". Note that $|$ is a divisibility on the additive group of R. We also define: $a \equiv b \mod c \Longleftrightarrow c \mid a - b$. A *congruence class modulo c* is a coset $a + Rc$.

For any a, b there is a unique $c \geq 0$ such that $aR + bR = cR$; this c is called the *greatest common divisor of a and b*, and denoted by $\gcd(a, b)$. If $a, b > 0$, then $ab/\gcd(a, b)$ is the least positive common multiple of a and b, and is denoted by $\operatorname{lcm}(a, b)$. We say that $c_1, \dots, c_n$ are *coprime* if $\gcd(c_i, c_j) = 1$ for $1 \leq i < j \leq n$. Given coprime $c_1, \dots, c_n$, and given any $b_1, \dots, b_n$, there is a such that $a \equiv b_i \mod c_i$ for $i = 1, \dots, n$, and then, for $c = c_1 \cdots c_n$:

$$\{x \in R : x \equiv b_i \mod c_i \text{ for } i = 1, \dots, n\} = a + cR \quad \text{(Chinese remainder theorem).}$$

Given $c_1, c_2 > 0$, the set $S := \{x \in R : x \equiv b_i \mod c_i \text{ for } i = 1, 2\}$ is nonempty iff $b_1 \equiv b_2 \mod \gcd(c_1, c_2)$; if this last condition is satisfied, then S is a congruence class modulo $\operatorname{lcm}(c_1, c_2)$.

A *prime* (in R) is by definition an element $p > 0$ in R that generates a prime ideal (p) of R. Equivalently, it is an element $p > 1$ that has no positive divisors except 1 and itself. The primes that lie in the subring $\boldsymbol{Z}$ of R are exactly the prime numbers. (N.B.: throughout "prime number" refers only to primes in $\boldsymbol{Z}$.) Given a prime p the local ring $R_{(p)} := \{\frac{a}{b} : p \nmid b\}$ is a valuation ring of $\operatorname{Frac}(R)$, with corresponding valuation v_p on $\operatorname{Frac}(R)$. For a prime p we define the divisibility $|_p$ on the additive group of R by $a \mid_p b \iff v_p(a) \leq v_p(b)$. A routine verification left to the reader yields the following.

LEMMA 4.1. *$R_{\text{div}} := (R, 1, <, \mid, \mid_2, \dots)$ is a group with $\boldsymbol{Z}$-like divisibilities.*

LEMMA 4.2. *Let $\mathscr{A} = (A, 1, <, \text{div}, \text{div}_2, \dots)$ be a finitely generated group with $\boldsymbol{Z}$-like divisibilities, and let p be a prime number. Suppose R is $\aleph_1$-saturated. Then*

(1) *(A, div_p) can be embedded into $(R, \mid_p)$;*

(2) *suppose $\mathscr{B}$ is a convex substructure of $\mathscr{A}$, and $\phi : \mathscr{B} \to R_{div}$ is an embedding; then there is an embedding $\psi : (A, \text{div}_p) \to (R, \mid_p)$ such that $\psi(x) = \phi(x)$ for all $x \in B$.*

PROOF. It is easy to check that $(A \otimes \boldsymbol{Q}, w_p, 1)$ is a correct $(\boldsymbol{Q}, v_p)$-linear space as defined in [2, pages 24–27]. Similarly, $(\text{Frac}(R), v_p, 1)$ is an $\aleph_1$-saturated correct $(\boldsymbol{Q}, v_p)$-linear space. Then by [2, Theorem 3] there exists an embedding

$$\xi : (A \otimes \boldsymbol{Q}, w_p, 1) \to (\text{Frac}(R), v_p, 1)$$

of $(\boldsymbol{Q}, v_p)$-linear spaces. Since $w_p(1) \leq w_p(x)$ for all $x \in A$ we have $0 = v_p(1) \leq v_p(\xi x)$ for all $x \in A$, that is, $\xi A \subseteq R_{(p)}$. Let $e_1, \dots, e_N$ be a basis of the free abelian group A. By saturation we can take $f_1, \dots, f_N \in R$ such that $v_p(f_i - \xi e_i) > v_p(\xi x)$ for all non-zero $x \in A$ and $i = 1, \dots, N$. Then the homomorphism $\psi : A \to R$ of additive groups determined by $\psi(e_i) = f_i$ for $i = 1, \dots, N$, has the property that $v_p(\xi x) = v_p(\psi x)$ for all $x \in A$. Thus ψ embeds (A, div_p) into $(R, \mid_p)$.

The proof of part (2) is a slight elaboration of that of part (1): First use [2, Theorem 3] to obtain an embedding $\xi : (A \otimes \boldsymbol{Q}, w_p, 1) \to (\text{Frac}(R), v_p, 1)$ of $(\boldsymbol{Q}, v_p)$-linear spaces such that $\xi(x) = \phi(x)$ for all $x \in B$. Take the basis $e_1, \dots, e_N$ of A in such a way that $e_1, \dots, e_M$ is a basis of B for some $M \leq N$. (This is possible by the convexity assumption.) Next we take $f_1, \dots, f_N$ as in the proof of (1) such that in addition $f_1 = \phi e_1, \dots, f_M = \phi e_M$. Then the map ψ obtained as in the proof of (1) has the desired property. ⊣

Throughout the rest of this section p will range over primes of R.

Factorization into prime powers.

LEMMA 4.3. *Each $a > 1$ has a prime divisor. For $x \in$ Frac(R) and $a, b \in R$ we have*

$$x \in R \iff v_p(x) \geq 0 \textit{ for all } p,$$
$$a \mid b \iff v_p(a) \leq v_p(b) \textit{ for all } p.$$

PROOF. For the first assertion, see [8, Th. 1.10]. For the second assertion, write $x = b/a$ with a, b coprime. The third assertion follows from the second one. ⊣

See [8, page 11] for the construction of a Δ_0-formula $\theta(x, y, z)$ that defines in the semiring $R^{\geq 0}$ a ternary relation to be thought of as "$x^y = z$". Indeed, this ternary relation is the graph of a partial function; if $a, b, c \geq 0$ and $R^{\geq 0} \models \theta(a, b, c)$, we shall write a^b for the element c. If a^b is defined (this includes the requirements $a, b \geq 0$), then so is $a_1^{b_1}$ for $0 \leq a_1 \leq a$ and $0 \leq b_1 \leq b$. If a^{b_1} and a^{b_2} are defined, so is $a^{b_1+b_2}$, and $a^{b_1+b_2} = a^{b_1}a^{b_2}$. If $a \geq 0$ then a^0 and a^1 are defined, with $a^0 = 1$ and $a^1 = a$. Thus for $b = n$ and $a \geq 0$ the "power" a^b is always defined, and equals the product of n factors a.

Put $L_p := \{y \in R^{\geq 0} : p^y \text{ is defined}\}$, an additively closed initial segment of $R^{\geq 0}$. One can extract the following from [8, pages 9–10].

LEMMA 4.4. *$\{p^y : y \in L_p\} = \{a > 0 :$ there is no prime $q \neq p$ such that $q \mid a\}$. For each $a > 0$ there is a largest $e \in L_p$ such that $p^e \mid a$ and $p^{e+1} \nmid a$.*

Let $\mathrm{Log}_p := L_p \cup -L_p$, a convex subgroup of the ordered additive group R, and put $p^{-y} := 1/p^y \in \mathrm{Frac}(R)$ for $y \in L_p$. Then $\{p^y : y \in \mathrm{Log}_p\}$ is a multiplicative subgroup of $\mathrm{Frac}(R)$, which is mapped isomorphically by v_p onto the value group of v_p. Thus we may identify this value group as an ordered group with the ordered subgroup Log_p of R; with this identification we have $v_p(p^y) = y$ for $y \in \mathrm{Log}_p$. If we need to indicate the dependence on R we shall write $\mathrm{Log}_p(R)$ instead of Log_p.

LEMMA 4.5. *If $b > 0$, then the set $\mathcal{P} := \{p : v_p(b) > 0\}$ and the function $p \mapsto v_p(b) : \mathcal{P} \to R^{\geq 0}$ are Δ_0-definable. Conversely, let $\mathcal{P}$ be a Δ_0-definable set of primes and $e : \mathcal{P} \to R^{\geq 0}$ a Δ_0-definable function. Then the following are equivalent*

(1) *there exists $b > 0$ such that $v_p(b) = e(p)$ for all $p \in \mathcal{P}$, and $v_p(b) = 0$ for all $p \notin \mathcal{P}$;*
(2) *there exists $a > 0$ such that $e(p) \leq v_p(a)$ for each $p \in \mathcal{P}$.*

PROOF. The first assertion follows from [8]. For the second part, it is clear that (1) implies (2). That (2) implies (1) follows by induction on a. ⊣

Given a Δ_0-definable set $\mathcal{P}$ of primes and a Δ_0-definable function $e : \mathcal{P} \to R^{\geq 0}$ such that condition (2) in the lemma is satisfied, there is a unique $b > 0$ with the property described in (1) (by Lemma 4.3); this b is denoted by $\prod_{p \in \mathcal{P}} p^{e(p)}$. (This notation will be used in §5.)

Counting. In this subsection we let v (sometimes with subscripts) range over nonnegative elements of R. We put $[v] := \{i \in R : 1 \leq i \leq v\}$. A *bounded arithmetic progression* (or b.a.p.) is a set of the form $a + [v]d = \{a + id : i \in [v]\}$ with $d > 0$; more precisely, we call such a set $a + [v]d$ a *b.a.p. with difference d*; note that then $d \mid y - x$ for all $x, y \in a + [v]d$. If S is a b.a.p. with more than one element, then there are unique a, d, v such that $d > 0$ and $S = a + [v]d$, and there are $x, y \in S$ with $d = x - y$. For any b.a.p. $S = a + [v]d$ $(d > 0)$ we put $|S| := v$, and we note that for finite S this is the number of elements of S. The intersection of two b.a.p.'s $a_1 + [v_1]d_1$ and $a_2 + [v_2]d_2$ $(d_1, d_2 > 0)$ is a b.a.p. with difference $\mathrm{lcm}(d_1, d_2)$.

We are going to apply to this situation a general fact [3] about finitely additive measures. Let Ω be a set and A an (additively written) abelian group. If $\mathcal{C}$ is a collection of subsets of Ω such that $\mathcal{C}$ contains the empty set, and contains with any two sets also their union and their intersection, then a function $\mu : \mathcal{C} \to A$ is said to be *additive* if $\mu(\emptyset) = 0$ and $\mu(S_1 \cup S_2) = \mu(S_1) + \mu(S_2) - \mu(S_1 \cap S_2)$ for all $S_1, S_2 \in \mathcal{C}$.

PROPOSITION 4.6. *Suppose $\mu : \mathcal{G} \to A$ is a function defined on a collection $\mathcal{G}$ of subsets of Ω that contains the empty set, and contains with any two sets their intersection. Suppose that $\mu(\emptyset) = 0$ and for all $S, S_1, \ldots, S_n \in \mathcal{G}$ with $n \geq 2$ and*

$S = S_1 \cup \cdots \cup S_n$ we have

$$\mu(S) = \sum_i \mu(S_i) - \sum_{i<j} \mu(S_i \cap S_j) + \sum_{i<j<k} \mu(S_i \cap S_j \cap S_k) - \cdots .$$

Then μ can be extended as follows.

(1) *Let $\mathscr{C}$ be the collection of all finite unions of sets in $\mathscr{S}$, so $\mathscr{C}$ contains with any two sets also their intersection. Then μ extends uniquely to an additive function $\mathscr{C} \to A$.*

(2) *Let $\mathscr{C}'$ be the collection of finite unions of sets $U \setminus V$ where $U, V \in \mathscr{C}$. Then $\mathscr{C}'$ contains with any two sets X, Y also $X \cup Y$, $X \cap Y$, and $X \setminus Y$, and μ extends uniquely to an additive function $\mathscr{C}' \to A$.*

A proof can be obtained from arguments in [3].

Lemma 4.7. *Let $\mathscr{C}$ be the collection of all finite unions of b.a.p.'s. Then the map $S \mapsto |S|$ (for b.a.p.'s S) has a unique additive extension $U \mapsto |U| : \mathscr{C} \to R$.*

Proof. Suppose $S, S_1, \dots, S_n$ are b.a.p.'s and $S = S_1 \cup \cdots \cup S_n$, $n \geq 2$. By the proposition above it suffices to show that then

$$|S| = \sum_i |S_i| - \sum_{i<j} |S_i \cap S_j| + \sum_{i<j<k} |S_i \cap S_j \cap S_k| - \cdots .$$

We may of course assume that S has more than one element, and then the difference d of S divides the difference of any S_i with more than one element. So we may write $S = a + [v]d$ and $S_i = a_i + [v_i]d_i$ with $d_i > 0$ and $d \mid d_i$, for $i = 1, \dots, n$. By a translation we can assume $a = 0$, and then a division by d reduces us to the case that $d = 1$, so $S = [v]$. For this case, and for fixed $n \geq 2$ we prove the displayed inclusion-exclusion identity above by an easy induction on v. This induction is allowed since the claim to be proved amounts to saying that the ordered semiring $R^{\geq 0}$ satisfies a sentence $\forall v \phi(v)$, where $\phi(v)$ is a Δ_0-formula. We leave the details to the reader. ⊣

Let $\mathscr{C}$ continue to denote the collection of all finite unions of b.a.p.'s, and let $\mathscr{C}'$ be the collection of finite unions of sets $U \setminus V$ where $U, V \in \mathscr{C}$. Then by part (2) of Proposition 4.6 the additive function $U \mapsto |U| : \mathscr{C} \to R$ extends uniquely to an additive function $X \mapsto |X| : \mathscr{C}' \to R$. We can think of $|X|$ as *the number of elements of X*; indeed, if X is finite, it *is* the number of elements of X. If $X, X_1, \dots, X_n \in \mathscr{C}'$ and $X_1, \dots, X_n \subseteq X$, then

$$|X \setminus (X_1 \cup \cdots \cup X_n)| = |X| - \sum_i |X_i| + \sum_{i<j} |X_i \cap X_j| - \sum_{i<j<k} |X_i \cap X_j \cap X_k| + \cdots .$$

This inclusion-exclusion result is used to prove the next lemma, which in turn is needed to obtain our main technical result, in §5.

Lemma 4.8. *Let $\varepsilon \in \boldsymbol{Q}$, $0 < \varepsilon < 1$, and let m, J be positive integers. Then there is $c = c(\varepsilon, m, J) \in \boldsymbol{N}$ such that for each $\alpha \in \mathrm{Frac}(R)$ with $\alpha > c$ the following holds: for any finite set P of primes with $\prod_{p \in P} p < \alpha^m$, and any map assigning to each $p \in P$ a finite sequence $\lambda_{p,1}, \dots, \lambda_{p,j(p)}$ of elements of R, with $0 \leq j(p) \leq J$ and $j(p) < p$, there exists $z \in R$ that satisfies the following inequalities and incongruences:*

$$\alpha < z < \alpha + \varepsilon\alpha, \qquad z \not\equiv \lambda_{p,j} \mod p, \quad (p \in P, \quad j = 1, \dots, j(p)).$$

PROOF. Let $0 < \alpha \in \mathrm{Frac}(R)$, let P be a finite set of primes with $\prod := \prod_{p \in P} p < \alpha^m$, and let for each $p \in P$ elements $\lambda_{p,1}, \dots, \lambda_{p,j(p)} \in R$ be given, with $0 \leq j(p) \leq J$, $j(p) < p$. We have to show that if α is larger than some natural number depending only on (ε, m, J), then there is a $z \in R$ satisfying the inequalities and incongruences of the lemma. We may assume that $\lambda_{p,1}, \dots, \lambda_{p,j(p)}$ are distinct, for each $p \in P$. Let Z be the set of all $z \in R$ that satisfy the inequalities and incongruences of the lemma. We shall use the inclusion-exclusion principle above to show that Z is nonempty (for large enough α). For each positive $d \mid \prod$, let $Z(d)$ be the set of all $z \in R$ such that $\alpha < z < \alpha + \varepsilon\alpha$ and such that for each prime divisor p of d there is $j \in \{1, \dots, j(p)\}$ with $z \equiv \lambda_{p,j} \mod p$. So $Z(1) = \{z \in R : \alpha < z < \alpha + \varepsilon\alpha\}$ is a b.a.p. with difference 1, and $Z(p) \in \mathscr{C}$ for each $p \in P$, hence $Z = Z(1) \setminus \bigcup_{p \in P} Z(p) \in \mathscr{C}'$. Moreover,

$$Z(p_1 \cdots p_k) = Z(p_1) \cap \cdots \cap Z(p_k) \in \mathscr{C}, \quad (p_1, \dots, p_k \text{ distinct elements of } P).$$

Let μ be the number of primes in P. Then

$$|Z| = |Z(1)| - \sum_{p \in P} |Z(p)| + \cdots + (-1)^k \sum |Z(d)| + \cdots + (-1)^\mu |Z(\textstyle\prod)|,$$

where the sum in $(-1)^k \sum |Z(d)|$ is over all positive $d \mid \prod$ with exactly k prime factors. Consider such a divisor $d = p_1 \cdots p_k$. Then $Z(d)$ is the union of $\prod_{i=1}^k j(p_i)$ disjoint b.a.p.'s, each of the form $Z_\lambda = \{z \in (\alpha, \alpha + \varepsilon\alpha) : z \equiv \lambda \mod d\}$ with $\lambda \in R$. Note that $\frac{\varepsilon\alpha}{d} - 1 \leq |Z_\lambda| \leq \frac{\varepsilon\alpha}{d} + 1$. So $|Z(d)|$ differs from $\frac{\varepsilon\alpha}{d} \prod_{i=1}^k j(p_i) = \varepsilon\alpha \prod_{i=1}^k \frac{j(p_i)}{p_i}$ by at most $\prod_{i=1}^k j(p_i) \leq J^k \leq J^\mu$. Hence by the inclusion-exclusion identity above $|Z|$ differs from

$$\varepsilon\alpha(1 - \sum_{p \in P} \frac{j(p)}{p} + \cdots + (-1)^k \sum \frac{j(p_1) \cdots j(p_k)}{p_1 \cdots p_k} + \cdots) = \varepsilon\alpha \prod_{p \in P} (1 - \frac{j(p)}{p})$$

by at most $2^\mu \cdot J^\mu = (2J)^\mu$.

A lower bound for $\prod_{p \in P}(1 - \frac{j(p)}{p})$ in terms of J and μ is obtained as follows. Put $c(J) := \prod_{p \leq J} p$, a positive integer. Then

$$\begin{aligned} \prod_{p \in P} (1 - \frac{j(p)}{p}) &\geq \frac{1}{c(J)} \prod_{p \in P, p > J} (1 - \frac{j(p)}{p}) \geq \frac{1}{c(J)} \prod_{r=1}^{\mu} \frac{r}{J + r} \\ &\geq \frac{1}{c(J)} \frac{1}{J^\mu} (\frac{1}{2} \cdot \frac{2}{3} \cdots \frac{\mu}{\mu + 1}) = \frac{1}{c(J) J^\mu (\mu + 1)}, \end{aligned}$$

so $|Z| \geq \frac{\varepsilon\alpha}{c(J)J^\mu(\mu+1)} - (2J)^\mu$. Hence Z will be nonempty if $\frac{\varepsilon\alpha}{c(J)J^\mu(\mu+1)} > (2J)^\mu$, and this will be the case if $\alpha > (2J^2)^\mu(\mu + 1)c(J)\varepsilon^{-1}$. For $\mu = 0$ this last inequality is equivalent to $\alpha > c(J)\varepsilon^{-1}$. Suppose $\mu > 0$. Then we use $2^\mu \geq \mu + 1$, $c(J)^\mu \geq c(J)$ and $\varepsilon^{-\mu} \geq \varepsilon^{-1}$ to obtain that Z is nonempty if $\alpha > \left(4J^2 c(J)\varepsilon^{-1}\right)^\mu$, that is, $\alpha^m > N^\mu$ where $N := N(\varepsilon, m, J) := \left(4J^2 c(J)\varepsilon^{-1}\right)^m$. We have $\mu! \leq P < \alpha^m$, so $\alpha^m > N^\mu$ certainly holds if $\mu! \geq N^\mu$, which holds if $\mu \geq 3N$ (because $n! > (n/e)^n$ for all $n > 0$). If $\mu < 3N$, then $\alpha^m > N^\mu$ if $\alpha^m > N^{3N}$, that is, if $\alpha > N^{3N/m}$. Thus the lemma holds for any integer $c \geq N^{3N/m}$. ⊣

We thank Doug Hoover who gave this proof in 1980 on our request (for $R = \boldsymbol{Z}$).

§5. Mapping a group with $\boldsymbol{Z}$-like divisibilities into a bounded induction domain. Throughout this section we fix the following data:

(i) a finitely generated group with $\boldsymbol{Z}$-like divisibilities $\mathscr{A} = (A, 1, <, \mathrm{div}, (\mathrm{div}_p))$;
(ii) an $\aleph_1$-saturated bounded induction domain R;
(iii) for each prime number p an embedding $\phi_p : (A, \mathrm{div}_p) \to (R, |_p)$ of groups with divisibility.

Recall that $A_0 \subset A_1 \subset \cdots \subset A_n$ denotes the strictly increasing sequence of subgroups of A that are convex with respect to the given ordering $<$ on A, with A_i of rank $r(i)$. We also fix positive elements $e_1, \ldots, e_N$ of the free abelian group A, with $N = r(n)$, such that $e_1, \ldots, e_{r(i)}$ is a basis of the free abelian group A_i for $i = 1, \ldots, n$. In particular, $e_1 = 1$. We put $e := (e_1, \ldots, e_N)$, and for each $f = (f_1, \ldots, f_N) \in R^N$ we let $\phi_f : A \to R$ be the group morphism determined by $\phi_f e_i = f_i$ for $i = 1, \ldots, N$. *Throughout the rest of this section p ranges over the primes of R.*

LEMMA 5.1. *There exist $F \in R^{>0}$ and $f = (f_1, \ldots, f_N) \in R^N$ such that*

(1) *ϕ_f embeds (A, div_p) into $(R, |_p)$ for each prime number p;*
(2) *$p \mid F$ for each prime number p;*
(3) *for each $p \mid F$ and non-zero $a \in A$ we have $v_p(\phi_f a) < v_p(F)$;*
(4) *for each $p \mid F$ and all $a, b \in A$: $a \,\mathrm{div}\, b \Longrightarrow v_p(\phi_f a) \leq v_p(\phi_f b)$.*

PROOF. By saturation there is positive $F \in R$ such that for each prime number p we have $v_p(\phi_p a) < v_p(F)$ for all non-zero $a \in A$. By the Chinese Remainder Theorem and saturation there are $f_1, \ldots, f_N \in R$ such that

$$v_p(f_i - \phi_p e_i) \geq v_p(F) \quad \text{for } i = 1, \ldots, N \text{ and all prime numbers } p.$$

Take such $f_1, \ldots, f_N$, and put $f = (f_1, \ldots, f_N)$.

Let p be a prime number. Then $v_p(\phi_f a - \phi_p a) \geq v_p(F)$ for $a \in A$, hence $v_p(\phi_f a) = v_p(\phi_p a) < v_p(F)$ for non-zero $a \in A$. It follows that the map ϕ_f is an embedding (of groups with divisibility) from (A, div_p) into $(R, |_p)$.

By saturation there exists a positive infinite $K \in R$ such that for all $p \mid F$ with $p < K$ and all non-zero $a \in A$ we have $v_p(\phi_f a) < v_p(F)$, and for all $a, b \in A$ we have

$$a \,\mathrm{div}\, b \Longrightarrow v_p(\phi_f a) \leq v_p(\phi_f b).$$

Thus replacing F by a suitable divisor we may assume that properties (2), (3) and (4) of the lemma hold. ⊣

In the rest of the section we also fix $f = (f_1, \ldots, f_N)$ and F with the properties in this lemma.

Suppose we perturb $f_1, \ldots, f_N$ to $g_1, \ldots, g_N \in R$ with $g_i \equiv f_i \mod F$ for $i = 1, \ldots, N$. Then with $g := (g_1, \ldots, g_n)$, the group homomorphism $\phi_g : A \to R$ satisfies $v_p(\phi_g a) = v_p(\phi_f a)$ for all non-zero $a \in A$ and each $p \mid F$. Hence for each $p \mid F$ we have

(i) $v_p(\phi_g a) < v_p(F)$ for all non-zero $a \in A$, and
(ii) $a \,\mathrm{div}\, b \Longrightarrow v_p(\phi_g a) \leq v_p(\phi_g b)$ for all $a, b \in A$.

The maps $A \to R$ that we are going to construct will be such perturbations ϕ_g of our given map ϕ_f.

Let $1 \leq L \leq N$ and $B = \boldsymbol{Z}e_1 \oplus \cdots \oplus \boldsymbol{Z}e_L$. A *full subset of* B is by definition a finite set $U \subseteq B$ such that, whenever $k_1e_i + a_1 \in U$ and $k_2e_i + a_2 \in U$ where $k_1, k_2 \in \boldsymbol{Z}$, $1 \leq i \leq L$, and $a_1, a_2 \in \boldsymbol{Z}e_1 \oplus \cdots \oplus \boldsymbol{Z}e_{i-1}$, then $k_1a_2 - k_2a_1 \in U$. Clearly, each finite subset of B can be augmented to a full subset of B, and if U is a full subset of A, then $U \cap B$ is a full subset of B.

Let U be a full subset of B. A U*-map* is by definition a map $\phi : B \to R$ such that

(1_U) ϕ is an embedding of ordered groups $(B, <) \to (R, <)$ with $\phi(1) = 1$;

(2_U) $\phi e_i \equiv f_i \mod F$ for $i = 1, \ldots, L$.

(3_U) whenever $a, b \in U$ and $a^w \operatorname{div} b$, then $\phi a^w | \phi b$;

(4_U) whenever $a, b \in U \setminus \{0\}$ and $p \nmid F$ with $p \mid \phi a$ and $p \mid \phi b$, then $v_p(\phi a) = v_p(\phi b)$ and there is $u \in U$ such that $u^w \operatorname{div} a$, $u^w \operatorname{div} b$, and $p \mid \phi u$.

Note that then ϕ is for each prime number p an embedding (of groups with divisibility) from $(B, \operatorname{div}_p)$ into $(R, |_p)$, and that for any $a, b \in U$ and m with $a \operatorname{div} mb$ we have $\phi a \mid m\phi b$. (This observation does not use clause (4_U).)

Keep in mind that, given B, the notion of "full subset" depends on our choice of basis e, and the notion of "U-map" depends on $(\mathscr{A}, R, e, f, F)$. We can now state a key technical result.

PROPOSITION 5.2. *Let* $n > 1$, *let* U *be a full subset of* A, *and put* $A' := A_{n-1}$, $U' := U \cap A'$, *so* U' *is a full subset of* A'. *Suppose* $\phi : A' \to R$ *is a* U'*-map. Let* $M := r(n-1)+1$. *Then there are* $Q, q \in R$ *with* $Q > 0$ *such that for each sufficiently large* $x \in R$ *with* $x \equiv q \mod Q$ *there is a* U*-map* $A \to R$ *that extends* ϕ *and sends* e_M *to* x.

PROOF. If $p \nmid F$ and there exists $a \in U' \setminus \{0\}$ with $p \mid \phi a$ we take such an a and put $v(p) := v_p(\phi a)$; in fact, $v(p)$ is independent of the choice of a by $(4_{U'})$.

We introduce two disjoint sets of primes:

$$\mathscr{P}_1 := \{p : p \nmid F, \text{ there are } a \in U' \setminus \{0\} \text{ and } b \in U \setminus A' \text{ with } p \mid \phi a \text{ and } a^w \operatorname{div} b\}$$

$$\mathscr{P}_2 := \{p : p \nmid F, p \notin \mathscr{P}_1, p \mid \phi a \text{ for some } a \in U' \setminus \{0\}\}.$$

Define $Q \in R^{>0}$ by

$$Q := F \cdot \prod_{p \in \mathscr{P}_1} p^{v(p)+1} \cdot \prod_{p \in \mathscr{P}_2} p.$$

In the rest of the proof x ranges over elements of R. Consider the following systems of congruences and incongruences on x:

(1) $x \equiv f_M \mod F$;

(2) $kx + \phi a \equiv 0 \mod p^{v(p)}, kx + \phi a \not\equiv 0 \mod p^{v(p)+1}$ where $p \in \mathscr{P}_1, k \in \boldsymbol{Z}$, $a \in A'$ are such that $k \neq 0, ke_M + a \in U$ and $p \mid \phi b$ for some $b \in U' \setminus \{0\}$ with $b^w \operatorname{div} ke_M + a$;

(3) $kx + \phi a \not\equiv 0 \mod p$, where $p \in \mathscr{P}_2, 0 \neq k \in \boldsymbol{Z}, a \in A', ke_M + a \in U$.

Using $(4_{U'})$ one finds that any two congruences in (2) above with the *same* prime $p \in \mathscr{P}_1$:

$$k_1x + \phi a_1 \equiv 0 \mod p^{v(p)}, \quad k_2x + \phi a_2 \equiv 0 \mod p^{v(p)}$$

have the same congruence class modulo $p^{v(p)}$ as solution set. (Here is why: for $i = 1, 2$ we have $k_ie_M + \phi a_i \in U$, and there is $b_i \in U' \setminus \{0\}$ with $b_i{}^w \operatorname{div} k_ie_M + a_i$. By $(4_{U'})$ there is $u \in U' \setminus \{0\}$ with $u^w \operatorname{div} b_1$, $u^w \operatorname{div} b_2$, and $p \mid \phi u$, so $v(p) =$

$v_p(\phi b_1) = v_p(\phi b_2) = v_p(\phi u)$. So $u^w \operatorname{div} k_i e_M + a_i$ for $i = 1, 2$. It follows that $u^w \operatorname{div} k_2 a_1 - k_1 a_2 \in U'$, and thus $\phi u^{\,w} |\, k_2\phi a_1 - k_1 \phi a_2$, so $v_p(k_2\phi a_1 - k_1\phi a_2) \geq v(p)$. Hence, if $x_1, x_2 \in R$, $k_1 x_1 + \phi a_1 \equiv 0 \mod p^{v(p)}$, and $k_2 x_2 + \phi a_2 \equiv 0 \mod p^{v(p)}$, then $k_1 k_2 (x_1 - x_2) \equiv 0 \mod p^{v(p)}$, so $x_1 \equiv x_2 \mod p^{v(p)}$.)

Each incongruence modulo $p^{v(p)+1}$ in (2) eliminates only one congruence class modulo $p^{v(p)+1}$ from consideration. Thus by the Chinese Remainder Theorem and saturation there is $q \in R$ such that each $x \equiv q \mod Q$ satisfies all congruences and incongruences of (1), (2) and (3) above. We fix such a q, and show that the conclusion of the proposition holds with these values of Q and q. We distinguish two cases.

Case 1. $N = M$. Take $D \in R$ such that $D > \phi A'$. It is a tedious exercise to check that any $x > D$ with $x \equiv q \mod Q$ has the property that the unique group homomorphism $\phi_x : A \to R$ that extends ϕ and sends e_M to x is a U-map. To assist the reader in this verification we point out that ϕ_x trivially satisfies conditions (1_U) and (2_U). In checking (3_U), assume $a, b \in U \setminus \{0\}$ and $a^w \operatorname{div} b$; it follows that $|a| \leq m|b|$ for some $m > 0$, hence we cannot have $a \in U \setminus U'$ and $b \in U' \setminus \{0\}$; also, if $a, b \in U \setminus U'$, then a, b have the same archimedean class, hence $ka = lb$ for suitable non-zero $k, l \in \boldsymbol{Z}$, hence $\phi_x(a)^w | \phi_x(b)$; if $a, b \in U'$, then one uses that $\phi_x(a) = \phi(a)$ and $\phi_x(b) = \phi(b)$; in the remaining case that $a \in U'$ and $b \in U \setminus U'$ we take $m > 0$ such that $a \operatorname{div} mb$, and prove $\phi(a) \mid m\phi_x(b)$ by checking for $p \mid F$, $p \in \mathscr{P}_1$ and $p \in \mathscr{P}_2$ separately that $v_p(\phi(a)) \leq v_p(\phi_x(mb))$. For $p \mid F$ this inequality follows since ϕ_x satisfies (2_U). For $p \in \mathscr{P}_1 \cup \mathscr{P}_2$, use the side conditions in the systems (2) and (3) of congruences and incongruences satisfied by x. As to condition (4_U): Let $a, b \in U \setminus \{0\}$, and let $p \nmid F$ with $p \mid \phi_x a$ and $p \mid \phi_x b$. If $a \in U'$ and $b \in U \setminus U'$, then $p \in \mathscr{P}_1$, and one can continue from there. If $a, b \in U \setminus U'$, write $a = ke_M + c$ and $b = le_M + d$ with non-zero $k, l \in \boldsymbol{Z}$ and $c, d \in A'$. Then $p \notin \mathscr{P}_2$, $kd - lc \in U'$ and $p \mid \phi(kd - lc)$. If $kd \neq lc$, then $p \in \mathscr{P}_1$, and we have a reduction to a previous case. If $kd = lc$, then $kb = la$, hence $v_p(\phi_x a) = v_p(\phi_x b)$, and $u := a$ satisfies $u^w \operatorname{div} a$, $u^w \operatorname{div} b$ and $p \mid \phi_x u$.

Case 2. $N > M$. Let $B := \boldsymbol{Z}e_1 \oplus \cdots \oplus \boldsymbol{Z}e_{N-1}$ and $U_B := U \cap B$. We can assume inductively that we have a positive $D \in R$ such that for each $x > D$ with $x \equiv q \mod Q$ we can extend ϕ to a U_B-map $\phi_x : B \to R$ with $\phi_x(e_M) = x$. We may also assume that

$$D > \Big(F \cdot \prod_{p \in \mathscr{P}'} p^{v(p)+1}\Big)^2, \quad \mathscr{P}' := \{p : p \nmid F, p \mid \phi a \text{ for some } a \in U' \setminus \{0\}\}.$$

Claim. For each $x > D$ with $x \equiv q \mod Q$ the map ϕ_x can be extended to a U-map $A \to R$.

Towards establishing this claim we fix for the rest of the proof any $x > D$ with $x \equiv q \mod Q$. We introduce two disjoint sets of primes, where the first one does not depend on x, but the second one does:

$$\mathscr{P}'_1 := \{p : p \nmid F, \text{ there are } a \in U' \setminus \{0\} \text{ and } c \in U \setminus B \text{ with } p \mid \phi a \text{ and } a^w \operatorname{div} c\}$$

$$\mathscr{P}'_2 := \{p : p \nmid F, p \notin \mathscr{P}'_1, p \mid \phi_x b \text{ for some } b \in U_B \setminus \{0\}\}.$$

Let y range over R, and consider the following systems of congruences, incongruences, and inequalities on y:

(i) $y \equiv f_N \mod F$;

(ii) $ky + \phi_x b \equiv 0 \mod p^{v(p)}, ky + \phi_x b \not\equiv 0 \mod p^{v(p)+1}$ where $p \in \mathscr{P}_1', 0 \neq k \in \boldsymbol{Z}, b \in B$ are such that $ke_N + b \in U$ and $p \mid \phi a$ for some $a \in U' \setminus \{0\}$ with $a^w \operatorname{div} ke_N + b$;

(iii) $ky + \phi_x b \not\equiv 0 \mod p$, where $p \in \mathscr{P}_2', 0 \neq k \in \boldsymbol{Z}, b \in B, ke_N + b \in U$;

(iv) $m_1 x < m_2 y < m_3 x$, where $m_1, m_2, m_3 > 0$ and $m_1 e_M < m_2 e_N < m_3 e_M$.

We leave it as a tedious exercise to the reader to show that if y satisfies (i), (ii), (iii) and (iv), then the group homomorphism $A = B \oplus \boldsymbol{Z} e_N \to R$ that extends ϕ_x and sends e_N to y is a U-map. (The verifications are similar to those in *Case 1*.) So it is enough to show that (i), (ii), (iii) and (iv) have a common solution y. Put

$$G := F \cdot \prod_{p \in \mathscr{P}_1'} p^{v(p)+1}.$$

Note that $D > G^2$. Applying the Chinese Remainder Theorem as in *Case 1* we find that there is an $r \in R$ with $0 \leq r < G$ such that each $y \equiv r \mod G$ satisfies (i) and (ii). Let z range over R. It suffices to find z such that $y = Gz + r$ satisfies (iii) and (iv). With $y = Gz + r$ the system (iii) reduces to:

(iii)' $z \not\equiv \lambda_{p,j} \mod p$, where $p \in \mathscr{P}_2', j = 1, \dots, J$ with $J := |U \setminus B|$, and where $\lambda_{p,j} \in R$ for $p \in \mathscr{P}_2'$ and $j \in \{1, \dots, J\}$.

Next we turn to the countably many inequalities in (iv), the conjunction of any finite number of which is implied by a single inequality in (iv). A single such inequality for $y = Gz + r$ takes the form $m_1 x < m_2 Gz + m_2 r < m_3 x$ (where $m_1, m_2, m_3 > 0$ and $m_1 e_M < m_2 e_N < m_3 e_M$), which is equivalent to

$$\frac{m_1 x}{m_2 G} - \frac{r}{G} < z < \frac{m_3 x}{m_2 G} - \frac{r}{G} \quad (\text{in } \operatorname{Frac}(R)).$$

Put $\alpha := \frac{m_1 x}{m_2 G}$. Take $\varepsilon > 0$ in $\boldsymbol{Q}$ such that $\alpha + \varepsilon\alpha < \frac{m_3 x}{m_2 G} - \frac{r}{G}$ (any positive rational $< \frac{m_3}{m_1} - 1$ will do). By saturatedness it suffices to show that there exists z with $\alpha < z < \alpha + \varepsilon\alpha$ that satisfies any given finite number of incongruences in (iii)' above. Let $p_1, \dots, p_\mu$ be the primes that occur as moduli in a given finite number of such incongruences, $\mu \in \boldsymbol{N}$, and let $\prod := \prod_{i=1}^{\mu} p_i$. Note that there is $C \in \boldsymbol{N}$ such that $p_i \leq Cx$ for $i = 1, \dots, \mu$. On the other hand, $x > D > G^2$, so $\alpha^2 > \left(\frac{m_1}{m_2}\right)^2 x > \boldsymbol{N}$, hence $\prod < \alpha^m$ for some $m > 0$. The existence of a z as required now follows from the number theoretic lemma 4.8 from the previous section. ⊣

Remark. Everything in this section goes through if in the definition in §3 of "group with $\boldsymbol{Z}$-like divisibilities" we had omitted axiom scheme (Div6). The significance (if any) of this fact is unclear. These axioms are only going to be used in §8.

§6. Applications to subdivisibility sets. In this section we derive some of the results on subdivisibility sets mentioned in the Introduction. Given a group $\mathscr{A} = (A, \dots)$ with $\boldsymbol{Z}$-like divisibilities, given a set $U \subseteq A$, and given a bounded induction domain R, a map $\phi : A \to R$ will be called a *weak U-map* if ϕ is an embedding $(A, <) \to (R, <)$ of ordered abelian groups with $\phi(1) = 1$ such that for all $u, v \in U$ we have: $u \operatorname{div} v \Longrightarrow \phi u \mid \phi v$. With this terminology we can state the following user-friendly variant of Proposition 5.2.

COROLLARY 6.1. *Let R be an $\aleph_1$-saturated bounded induction domain, $\mathscr{A} = (A, \dots)$ a finitely generated substructure of R_{div}, B a non-trivial convex subgroup of A, $h \in A$, $h > B$, and let $U \subseteq A$ be finite. Then there is a positive $H \in R$ such that for each sufficiently large $x \in R$ with $x \equiv h \mod H$ there is a weak U-map $A \to R$ that is the identity on B and sends h to x.*

PROOF. We can of course assume that $B = A_i$ is the largest convex subgroup of A that does not contain h, so $1 \leq i < n$, and $h \in A_{i+1}$. We can also assume that our basis $e_1, \dots, e_N$ of A was chosen such that $h = b + te_M$, where $b \in B$, $0 < t \in N$ and $M = r(i) + 1$. It suffices to prove the desired result with e_M instead of h.

To reproduce the situation of §5, we let ϕ_p be the inclusion $(A, \text{div}_p) \to (R, |_p)$, for each prime number p. An easy saturation argument gives a positive $F \in R$ such that $v_p(a) < v_p(F)$ for all p, a such that p is a prime of R, $0 \neq a \in A$, and $p \mid a$. We fix such an F. Then lemma 5.1 holds with $f_1 = e_1, \dots, f_N = e_N$ and with this F.

By enlarging U if necessary, we can assume that U is a full subset of A. The inclusion $B \to R$ is then a $(U \cap B)$-map: clause $(4_{U \cap B})$ is trivially satisfied. So we can apply Proposition 5.2 with $B = A_i$ in the role of A' and A_{i+1} instead of A, with the inclusion map $B \to R$ instead of ϕ. The sets $\mathscr{P}_1$ and $\mathscr{P}_2$ in the proof of that proposition are empty in our case. In the notations of that proof we then have $Q = F$, and one can take $q = e_M$. Thus for all sufficiently large $x \in R$ with $x \equiv e_M \mod F$ there is a $(U \cap A_{i+1})$-map $A_{i+1} \to R$ that is the identity on B and sends e_M to x. We can then apply Proposition 5.2 again, $n - (i + 1)$ -times in succession, to extend each such $(U \cap A_{i+1})$-map to a U-map $A \to R$. This finishes the proof. ⊣

In the proofs of the next two results it will be convenient to fix some $\aleph_1$-saturated elementary extension $^*\boldsymbol{Z}$ of the ring of integers $\boldsymbol{Z}$. First we derive the improvement by Lipshitz [5] of Proposition 1.1.

PROPOSITION 6.2. *Let $E \subseteq N$ be a subdivisibility set. Then*

$$E = E_0 \cup \bigcup_{\sigma} E_\sigma$$

where E_0 is finite, and each $E_\sigma = a_\sigma + Nb_\sigma$ is an infinite arithmetic progression: $a_\sigma, b_\sigma \in N, b_\sigma > 0$.

PROOF. We may reduce to the case that $E = \pi(S)$ for some basic divisibility set $S \subseteq \boldsymbol{Z}^s$ with $s \geq 1$, where $\pi : \boldsymbol{Z}^s \to \boldsymbol{Z}$ is given by $\pi(x_1, \dots, x_s) = x_1$. So

$$S = \{x \in \boldsymbol{Z}^s : \lambda_i(x) \mid \mu_i(x) \text{ for all } i \in I\} \cap \{x \in \boldsymbol{Z}^s : \lambda_j(x) \geq 0 \text{ for all } j \in J\}$$

where I and J are finite index sets, and the polynomials $\lambda_i, \mu_i \in \boldsymbol{Z}[X]$ for $i \in I$ and the polynomials $\lambda_j \in \boldsymbol{Z}[X]$ for $j \in J$ are of total degree at most 1 in $X = (X_1, \dots, X_s)$.

Let $h_1 \in {}^*E$ be positive infinite. It suffices to show that then h_1 is the beginning of a progression $h_1 + {}^*Nb \subseteq {}^*E$ with $0 < b \in {}^*\boldsymbol{Z}$.

Note that $^*S$ contains a point $h = (h_1, h_2, \dots, h_s)$ with first coordinate h_1. Let $A := \boldsymbol{Z} + \boldsymbol{Z}h_1 + \cdots + \boldsymbol{Z}h_s$, an additive subgroup of $^*\boldsymbol{Z}$ containing 1. Let $\mathscr{A}$ be the substructure of $^*\boldsymbol{Z}_{\text{div}}$ with underlying group A. Let

$$U := \{h_1, \dots, h_s\} \cup \{\lambda_i(h) : i \in I\} \cup \{\mu_i(h) : i \in I\}.$$

Any weak U-map $\phi : A \to {}^*\boldsymbol{Z}$ has the property that $\phi(h) := (\phi h_1, \dots, \phi h_s) \in {}^*S$, and hence $\phi h_1 \in {}^*E$. Applying corollary 6.1 with $B = \boldsymbol{Z}$ we see that ϕh_1 can take all values in some arithmetic progression $h_1 + {}^*\boldsymbol{N}b$ with $b \in {}^*\boldsymbol{N}, b > 0$. ⊣

Next we obtain 1.2 in the following equivalent form.

THEOREM 6.3. *Let $E \subseteq \boldsymbol{N}^2$ be an infinite subdivisibility set. Then either there is $a \in \boldsymbol{N}$ such that $E(a)$ is infinite, or there is a real constant $c > 0$ such that for all $(x, y) \in E$ with $x > 0$ we have $y < cx$.*

PROOF. We may reduce to the case that $E = \pi(S)$ for some basic divisibility set $S \subseteq \boldsymbol{Z}^s$ with $s \geq 2$, where $\pi : \boldsymbol{Z}^s \to \boldsymbol{Z}^2$ is given by $\pi(x_1, \dots, x_s) = (x_1, x_2)$. So

$$S = \{x \in \boldsymbol{Z}^s : \lambda_i(x) \mid \mu_i(x) \text{ for all } i \in I\} \cap \{x \in \boldsymbol{Z}^s : \lambda_j(x) \geq 0 \text{ for all } j \in J\}$$

where I and J are finite index sets, and the polynomials $\lambda_i, \mu_i \in \boldsymbol{Z}[X]$ for $i \in I$ and the polynomials $\lambda_j \in \boldsymbol{Z}[X]$ for $j \in J$ are of total degree at most 1 in $X = (X_1, \dots, X_s)$. Suppose there is for each real constant $c > 0$ a point $(x, y) \in E$ with $x > 0$ and $y > cx$. Then ${}^*S$ contains a point $h = (h_1, h_2, \dots, h_s)$ with $0 < h_1 \ll h_2$. Let $A := \boldsymbol{Z} + \boldsymbol{Z}h_1 + \cdots + \boldsymbol{Z}h_s$, an additive subgroup of ${}^*\boldsymbol{Z}$ containing 1. Let $\mathscr{A}$ be the substructure of ${}^*\boldsymbol{Z}_{\text{div}}$ that has underlying group A.

Let $U := \{h_1, \dots, h_s\} \cup \{\lambda_i(h) : i \in I\} \cup \{\mu_i(h) : i \in I\}$. Let B be the smallest convex subgroup of A that contains h_1. Any weak U-map $\phi : A \to {}^*\boldsymbol{Z}$ has the property that $\phi h := (\phi h_1, \dots, \phi h_s) \in {}^*S$, and hence $(\phi h_1, \phi h_2) \in {}^*E$. By corollary 6.1 there is for each $t \in {}^*\boldsymbol{Z}$ a weak U-map $\phi : A \to {}^*\boldsymbol{Z}$ that is the identity on B satisfying $\phi h_2 > t$. Thus ${}^*E(h_1)$ is cofinal in ${}^*\boldsymbol{N}$. It follows that for some $a \in \boldsymbol{N}$ the set $E(a)$ is cofinal in $\boldsymbol{N}$. ⊣

Logical considerations. The results above on subdivisibility sets only used Corollary 6.1 for $R = {}^*\boldsymbol{Z}$. The fact that this corollary holds for arbitrary $\aleph_1$-saturated bounded induction domains has additional consequences for subdivisibility sets, as we shall see.

Let L_{div} be the language of groups with $\boldsymbol{Z}$-like divisibilities, so L_{div} is the language $\{0, 1, -, +, <\}$ of ordered abelian groups with a distinguished element 1, augmented by binary relation symbols div, div$_2$, div$_3, \dots$. Let T_{div} be the theory in the language L_{div} of groups with $\boldsymbol{Z}$-like divisibilities.

Let BI be the theory of bounded induction domains in the language of ordered rings. We extend BI by the defining axioms for the binary relation symbols div, div$_2$, div$_3, \dots$ according to their interpretation in each bounded induction domain R as the relations $|, |_2, |_3, \dots$; see §4. This extension by definitions of BI is also denoted by BI, and its language is just L_{div} augmented by the binary function symbol for multiplication. Note that $BI \vdash T_{\text{div}}$ by Lemma 4.1.

LEMMA 6.4. *Let $\phi(x, y)$ be an existential formula of L_{div} with $x = (x_1, \dots, x_m)$ and y a single variable. Write $|x|'$ for $|x_1| + \cdots + |x_m| + 1$ (for $m = 0$ this is just 1). Then there is an $M \in \boldsymbol{N}$ such that*

$$BI \vdash \exists y(y > M|x|' \wedge \phi(x, y)) \longleftrightarrow \forall y_0 \exists y(y > y_0 \wedge \phi(x, y)).$$

PROOF. To see this, let $c = (c_1, \dots, c_m)$ be a tuple of new constant symbols. Then by compactness the claim above reduces to showing that

$$BI \cup \{\exists y(y > M|c|' \wedge \phi(c, y)) : M \in \boldsymbol{N}\} \vdash \forall y_0 \exists y(y > y_0 \wedge \phi(c, y)).$$

Let $R \models BI \cup \{\exists y(y > M|a|' \wedge \phi(a,y)) : M \in N\}$, with $a = (a_1, \dots, a_m)$, and suppose R is $\aleph_1$-saturated. By saturation there is then an element $b \in R$ such that $b > M|a|'$ for all $M \in N$ and $R \models \phi(a,b)$. We may assume that $\phi(x,y)$ is positive existential, and does not contain any of the symbols $\mathrm{div}_2, \mathrm{div}_3, \dots$. Corollary 6.1 applied to the substructure of R_{div} generated by $a_1, \dots, a_m, b$ and witnesses for the existentially quantified variables of $\phi(a,b)$ yields

$$R \models \forall y_0 \exists y (y > y_0 \wedge \phi(a,y)). \qquad \dashv$$

THEOREM 6.5. *Let $x = (x_1, \dots, x_m)$, $y = (y_1, \dots, y_n)$, $n > 0$, and let $\phi(x,y)$ be an existential L_{div}-formula. Then there is an existential L_{div}-formula $\psi(x)$ such that*

$$BI \vdash \exists^u y \phi(x,y) \longleftrightarrow \psi(x).$$

Here $\exists^u$ is read as "there exist unboundedly many"; formally, $\exists^u y \dots$ abbreviates $\forall y_0 \exists y(|y| > y_0 \wedge \dots)$. In particular, if $S \subseteq \boldsymbol{Z}^{m+n}$ is a subdivisibility set, then $\{a \in \boldsymbol{Z}^m : S(a)$ is infinite$\}$ is a subdivisibility set.

PROOF. The theorem follows easily from the last lemma, as we shall illustrate by just considering the case $n = 2$. By the results above there exist $M_1, M_2 \in N$ such that

$$BI \vdash \exists y_1(|y_1| > M_1|x|' \wedge \exists y_2 \phi(x,y)) \longleftrightarrow \exists^u y_1 \exists y_2 \phi(x,y),$$
$$BI \vdash \exists y_2(|y_2| > M_2|x|' \wedge \exists y_1 \phi(x,y)) \longleftrightarrow \exists^u y_2 \exists y_1 \phi(x,y).$$

Now use that $BI \vdash \exists^u y \phi(x,y) \longleftrightarrow (\exists^u y_1 \exists y_2 \phi(x,y) \vee \exists^u y_2 \exists y_1 \phi(x,y))$. $\dashv$

The lemma and the proof of the theorem provide an algorithm that constructs from each $\phi(x,y)$ as in the hypothesis of the theorem a $\psi(x)$ that satisfies its conclusion. By considering the case $m = 0$ and paying attention to the particular form of the existential sentence ψ in that case we obtain the following interesting consequence.

COROLLARY 6.6. *There is an algorithm that constructs for any given existential formula $\phi(y_1, \dots, y_n)$ of L_{div} a positive integer M such that the set*

$$\{b \in \boldsymbol{Z}^n : \boldsymbol{Z}_{\mathrm{div}} \models \phi(b)\}$$

is infinite or contained in $[-M, M]^n$.

Using the decidability result from [4] it follows that there is an algorithm that takes as inputs existential formulas $\phi(y_1, \dots, y_n)$ of L_{div}, and decides for any such formula whether the set $\{b \in \boldsymbol{Z}^n : \boldsymbol{Z}_{\mathrm{div}} \models \phi(b)\}$ is infinite.

§7. **Polynomial growth.** In this section we prove Theorem 1.5. First some preparations.

Let $\boldsymbol{F}$ be a field of characteristic 0. A *valued $\boldsymbol{F}$-linear space* is a triple (V, v, Γ) where V is an $\boldsymbol{F}$-linear space and $v : V \to \Gamma \cup \{\infty\}$ is a valuation, that is, a map onto a totally ordered set $\Gamma \cup \{\infty\}$ with largest element $\infty \notin \Gamma$, such that for all $x, y \in V$:

1. $vx = \infty \Longleftrightarrow x = 0$,
2. $v(x + y) \geq \min(vx, vy)$,
3. $v(\lambda x) = vx$ for non-zero $\lambda \in \boldsymbol{F}$.

This notion does not fall under the scope of [2], because there the field $\boldsymbol{F}$ comes equipped with a *non-trivial valuation*, and an action of the value group of this valuation on Γ. However, one might consider it as the degenerate case of [2] where the valuation on $\boldsymbol{F}$ is *trivial*. Viewed that way, enough of [2] goes through to yield the lemma below. Given an $\boldsymbol{F}$-linear space (V, v, Γ) we define the divisibility div_v on the additive group V by $x \operatorname{div}_v y \iff vx \leq vy$; we say that (V, v, Γ) is κ-saturated (κ an infinite cardinal), if the one-sorted structure $(V, 0, -, +, (\lambda\cdot)_{\lambda \in \boldsymbol{F}}, \operatorname{div}_v)$ is κ-saturated, where $\lambda\cdot$ is multiplication by the scalar λ.

Given valued $\boldsymbol{F}$-linear spaces (V, v, Γ) and (V', v', Γ') an embedding $(\phi, \theta) : (V, v, \Gamma) \to (V', v', \Gamma')$ is an $\boldsymbol{F}$-linear injective map $\phi : V \to V'$ together with an order preserving injective map $\theta : \Gamma \to \Gamma'$ such that $v'(\phi x) = \theta(vx)$ for all non-zero $x \in V$.

Lemma 7.1. *Let (V, v, Γ) be a valued $\boldsymbol{F}$-linear space, W an $\boldsymbol{F}$-linear subspace of V, and put $\Delta := v(W \setminus \{0\})$, and let $w : W \to \Delta \cup \{\infty\}$ be the restriction of v to W. Let $(\phi_W, \theta_W) : (W, w, \Delta) \to (V', v', \Gamma')$ be an embedding into a κ-saturated valued $\boldsymbol{F}$-linear space (V', v', Γ') where κ is an infinite cardinal $> |V|$. Let $\theta : \Gamma \to \Gamma'$ be an order-preserving injective map that extends θ_W. Then there exists an embedding $(\phi, \theta) : (V, v, \Gamma) \to (V', v', \Gamma')$ such that ϕ extends ϕ_W.*

Let A be a finitely generated additive subgroup of a bounded induction domain R, with $1 \in A$. Let $\mathscr{A} = (A, 1, <, \operatorname{div}, \operatorname{div}_2, \operatorname{div}_3, \dots)$ be the substructure of R_{div} with A as its underlying group. Let $\mathscr{B} = (B, \dots)$ be a convex substructure of $\mathscr{A}$, so $\boldsymbol{Z} \subseteq B$. Put

$$R_0 := \{x \in R : |x| < b^m \text{ for some positive } b \in B \text{ and some } m\},$$

an ordered subring of R, with $R_0 \models BI$, see [8]. Consider the pair (R, R_0) as the ordered domain R with distinguished subset R_0, and take an $\aleph_1$-saturated elementary extension (R', R'_0) of (R, R_0). We have the following diagram of inclusions where the horizontal arrows on the right are elementary embeddings of ordered domains:

$$\begin{tikzcd}
A \arrow[r] & R \arrow[r] & R' \\
B \arrow[r] \arrow[u] & R_0 \arrow[r] \arrow[u] & R'_0 \arrow[u]
\end{tikzcd}$$

Lemma 7.2. *For each finite $U \subseteq A$ there exists a weak U-map $A \to R'_0$ that is the identity on B.*

Proof. Because R_0 is convex in R, the ring R'_0 is a convex in R', so each prime in R'_0 remains prime in R'. In particular we have for each prime p in R'_0 the valuation $v_p : \operatorname{Frac}(R') \to \operatorname{Log}_p(R') \cup \{\infty\}$ with $x \mid_p y \iff v_p(x) \leq v_p(y)$, for all $x, y \in R'$.

Since $B \subseteq R_0 \subseteq R'_0$ we can define

$$\mathscr{P}_B := \{p : p \text{ a prime in } R'_0 \text{ and } v_p(b) > 0 \text{ for some non-zero } b \in B\}.$$

Note that each prime number belongs to $\mathscr{P}_B$.

Let $p \in \mathscr{P}_B$. As $A \subseteq R \subseteq R'$, the divisibility $\mid_p$ on R' restricts to a divisibility on A, which is just div_p if p is a prime number, and which we also denote by div_p if p is infinite. Note that for $a, b \in A$ we have: $a \operatorname{div} b \implies a \operatorname{div}_p b$.

By lemma 4.2 we can choose for each prime number p an embedding $\phi_p : (A, \mathrm{div}_p) \to (R'_0, |_p)$ of groups with divisibility that is the identity on B. An easy saturation argument yields a positive infinite $H \in R'_0$ such that $v_p(\phi_p a) < v_p(H)$ for all prime numbers p and all non-zero $a \in A$. By a further saturation argument we arrange in addition that $v_p(b) < v_p(H)$ for all non-zero $b \in B$ and all $p \in \mathscr{P}_B$.

Suppose now that $p \in \mathscr{P}_B$ is infinite. Then v_p is trivial on $\boldsymbol{Q}$. We are going to apply the previous lemma with $F := \boldsymbol{Q}$, $V := \boldsymbol{Q}A \subseteq \mathrm{Frac}(R')$, $\Gamma := v_p(V \setminus \{0\}) \subseteq \mathrm{Log}_p(R')$, $v := v_p \mid V : V \to \Gamma \cup \{\infty\}$, $W = \boldsymbol{Q}B$ (and w and Δ defined as in Lemma 7.1), $V' := \mathrm{Frac}(R'_0)$, $\Gamma' := \mathrm{Log}_p(R'_0)$ $v' := v_p \mid V' : V' \to \Gamma' \cup \{\infty\}$, with $\phi_W : W \to V'$ and $\theta_W : \Delta \to \Gamma'$ given by the natural inclusions. So we have a diagram of (order-preserving) inclusions of totally ordered sets:

$$\begin{tikzcd}
\Gamma \arrow[r] & \mathrm{Log}_p(R') \\
\Delta \arrow[u] \arrow[r, "\theta_W"] & \Gamma' \arrow[u]
\end{tikzcd}$$

Since the $\boldsymbol{Q}$-linear space V has dimension N, the set Γ has cardinality at most N. Let $\gamma_1 < \cdots < \gamma_k$ be the elements of Γ that are $> \Delta$, so $k < N$. By the properties of H we have $v'(H) \in \Gamma'$ and $v'(H) > \Delta$. Since

$$\{e \in \mathrm{Log}_p(R') : 0 \leq e \leq \gamma' \text{ for some } \gamma' \in \Gamma'\} \subseteq \Gamma',$$

we obtain an order preserving injective map $\theta : \Gamma \to \Gamma'$ with $\theta(\gamma) = \gamma$ whenever $\gamma \leq \delta$ for some $\delta \in \Delta$, and $\theta(\gamma_i) = iv'(H)$ for $i = 1, \dots, k$. Thus θ extends θ_W and $\theta(\Gamma) < Nv'(H) = v_p(H^N)$. Then lemma 7.1 yields an embedding $(\phi, \theta) : (V, v, \Gamma) \to (V', v', \Gamma')$ such that ϕ extends ϕ_W. Next we obtain as in the proof of lemma 4.2 an embedding $\phi_p : (A, \mathrm{div}_p) \to (R'_0, |_p)$ of groups with divisibility that is the identity on B, such that $v_p(\phi_p a) < v_p(H^N)$ for all non-zero $a \in A$.

Put $G := H^N$. Then G is a positive infinite element of R'_0 such that $v_p(\phi_p a) < v_p(G)$ for all $p \in \mathscr{P}_B$ (finite or not) and all non-zero $a \in A$.

Let B have basis $e_1, \dots, e_L$ with $1 \leq L \leq N$. *In the rest of the proof we let p range over primes in R'_0, and given any N-tuple $f = (f_1, \dots, f_N) \in {R'_0}^N$ we let $\phi_f : A \to R'_0$ be the group homomorphism that sends e_i to f_i for $i = 1, \dots, N$.*

Claim. There exists a positive $F \in R'_0$, and a tuple $f = (f_1, \dots, f_N) \in {R'_0}^N$ such that

(i) $p \mid F$ for all $p \in \mathscr{P}_B$, and $e_i = f_i$ for $i = 1, \dots, L$,
(ii) for each $p \mid F$ and non-zero $a \in A$ we have $v_p(\phi_f a) < v_p(F)$,
(iii) for each $p \mid F$ and all $c, d \in A$: $c \,\mathrm{div}\, d \Longrightarrow v_p(\phi_f c) \leq v_p(\phi_f d)$.

Proof of claim. By the Chinese Remainder Theorem and saturation there are $f_1, \dots, f_N \in R'_0$ such that $e_i = f_i$ for $i = 1, \dots, L$ and

$$v_p(f_i - \phi_p e_i) \geq v_p(G) \text{ for } i = 1, \dots, N \text{ and } p \in \mathscr{P}_B.$$

We take such $f_1, \dots, f_N$ and put $f := (f_1, \dots, f_N)$.

Let $p \in \mathscr{P}_B$. Then $v_p(\phi_f a - \phi_p a) \geq v_p(G)$ for $a \in A$, so $v_p(\phi_f a) = v_p(\phi_p a) < v_p(G)$ for $0 \neq a \in A$. Hence for all $c, d \in A$ we have: $c \,\mathrm{div}\, d \Longrightarrow v_p(\phi_f c) \leq v_p(\phi_f d)$.

For $0 \neq b \in B$, $0 \neq a \in A$, and $c, d \in A$ with $c \operatorname{div} d$ we put

$$\begin{aligned} \mathscr{P}_b &:= \{p : p \mid b\}, \\ \mathscr{P}(a) &:= \{p : p \mid G \text{ and } v_p(\phi_f a) < v_p(G)\}, \\ \mathscr{P}(c,d) &:= \{p : p \mid G \text{ and } v_p(\phi_f c) \leq v_p(\phi_f d)\}. \end{aligned}$$

Then $\mathscr{P}_b \subseteq \mathscr{P}(a), \mathscr{P}(c,d)$ for all such a, b, c, d. By saturation there exists a positive divisor F of G such that

- $v_p(F) = v_p(G)$ or $v_p(F) = 0$, for each $p \mid G$,
- for each non-zero $b \in B$ and $p \in \mathscr{P}_b$ we have $v_p(F) = v_p(G)$,
- $\{p : p \mid F\} \subseteq \mathscr{P}(a)$ for each non-zero $a \in A$, and $\{p : p \mid F\} \subseteq \mathscr{P}(c,d)$ for all $c, d \in A$ with $c \operatorname{div} d$.

With these choices of F and f conditions (i), (ii) and (iii) of the claim above are satisfied.

Take F and f with the properties in the claim. To finish the proof of the lemma we can assume that U is a full subset of A, and it suffices to show that then there is a U-map $A \to R'_0$. The inclusion $B \to R'_0$ is a $(U \cap B)$-map, since clause $(4_{U \cap B})$ is trivially satisfied : there is no non-zero $u \in U \cap B$ and prime p in R'_0 such that $v_p(u) > 0$ and $p \nmid F$. Hence by repeated use of Proposition 5.2 we can extend the inclusion $B \to R'_0$ to a U-map $A \to R'_0$. ⊣

We now have everything ready for the proof of Theorem 1.5, which we state here in the following equivalent form.

THEOREM 7.3. *Let $E \subseteq N^2$ be a subdivisibility set. Then there is $K \in N^{>0}$ such that for all $x > 1$ in N, if $E(x) \neq \emptyset$, then there is $y \in E(x)$ with $y < x^K$.*

PROOF. We may reduce to the case that $E = \pi(S)$ for some basic divisibility set $S \subseteq \boldsymbol{Z}^s$ with $s \geq 2$, where $\pi : \boldsymbol{Z}^s \to \boldsymbol{Z}^2$ is given by $\pi(x_1, \dots, x_s) = (x_1, x_2)$. So

$$S = \{x \in \boldsymbol{Z}^s : \lambda_i(x) \mid \mu_i(x) \text{ for all } i \in I\} \cap \{x \in \boldsymbol{Z}^s : \lambda_j(x) \geq 0 \text{ for all } j \in J\}$$

where I and J are finite index sets, and the polynomials $\lambda_i, \mu_i \in \boldsymbol{Z}[X]$ for $i \in I$ and the polynomials $\lambda_j \in \boldsymbol{Z}[X]$ for $j \in J$ are of total degree at most 1 in $X = (X_1, \dots, X_s)$. Suppose a K as in the proposition does not exist. Let $R := {}^*\boldsymbol{Z}$ be an $\aleph_1$-saturated elementary extension of the ring $\boldsymbol{Z}$. Then we can take $(h_1, h_2) \in {}^*E$ such that $h_1 > 1$, $h_2 = \min {}^*E(h_1)$, and $h_2 > h_1^K$ for all $K \in N$. Take a point $h = (h_1, h_2, \dots, h_s) \in {}^*S$. Let $A := \boldsymbol{Z} + \boldsymbol{Z}h_1 + \cdots + \boldsymbol{Z}h_s$, an additive subgroup of R containing 1. Let $\mathscr{A}$ be the substructure of R_{div} that has underlying group A. Let B be the smallest convex subgroup of A that contains h_1, and let $R_0 := \{x \in R : |x| < h_1^m \text{ for some } m\}$, so we are in the situation considered above, in particular, $R_0 \models BI$. As before we take an $\aleph_1$-saturated elementary extension (R', R'_0) of (R, R_0). Let

$$U := \{h_1, h_2, \dots, h_s\} \cup \{\lambda_i(h) : i \in I\} \cup \{\mu_i(h) : i \in I\}.$$

By the previous lemma we have a weak U-map $A \to R'_0$ that is the identity on B, hence we obtain a point $(g_1, \dots, g_s) \in S(R'_0)$ with $g_1 = h_1$. Since $R_0 \prec R'_0$, it follows that there is a point in $S(R_0)$ with first coordinate h_1, and thus second coordinate $< h_1^K$ for some $K \in N$. But clearly $S(R_0) \subseteq {}^*S$, and we have a contradiction with the minimality property of h_2. ⊣

§8. Embedding a group with $\boldsymbol{Z}$-like divisibilities into a bounded induction domain. In this section we prove Theorem 3.1. We start with the same set-up as in §5, and fix a tuple $f = (f_1, \dots, f_N)$ and an F with the properties of lemma 5.1. As in §5 we let p range over the primes of our $\aleph_1$-saturated bounded induction domain R. Let $B = \boldsymbol{Z}e_1 \oplus \cdots \oplus \boldsymbol{Z}e_L$ where $1 \leq L \leq N$, and let U be a full subset of B. A *prime selector on* U is by definition a function $\pi : U \setminus \boldsymbol{Z} \to \{p : p \nmid F\}$ such that for all $u, v \in U \setminus \boldsymbol{Z}$ we have

$$\pi(u) = \pi(v) \iff u^w \operatorname{div} v \text{ and } v^w \operatorname{div} u.$$

(The right hand side in this equivalence means that there are non-zero $k, l \in \boldsymbol{Z}$ such that $ku = lv$.) Given a prime selector π on U we call $\phi : B \to R$ a (U, π)-map if it is a U-map such that for all $u, v \in U \setminus \boldsymbol{Z}$:

(1) $\pi(u) \mid \phi(u)$;
(2) if $u \ll v$, then $\pi(v) \nmid \phi(u)$.

LEMMA 8.1. *Let π be a prime selector on U and $\phi : B \to R$ a (U, π)-map. Then*

(i) *if $u, v \in U \setminus \boldsymbol{Z}$ and $\pi(u) \mid \phi(v)$, then $u^w \operatorname{div} v$;*
(ii) *for all $u, v \in U$ we have: $u \operatorname{div} v \iff \phi(u) \mid \phi(v)$.*

PROOF. Let $u, v \in U \setminus \boldsymbol{Z}$ and $\pi(u) \mid \phi(v)$. As ϕ is a U-map, it follows from clause (4_U) that there exists $u_1 \in U$ such that $u_1{}^w \operatorname{div} u$, $u_1{}^w \operatorname{div} v$ and $\pi(u) \mid \phi(u_1)$. Hence $u_1 \notin \boldsymbol{Z}$, and thus by clause (2) of the definition of "(U, π)-map" we have $u_1 \not\ll u$, that is, u_1 and u have the same archimedean class, so $u^w \operatorname{div} u_1$, and therefore $u^w \operatorname{div} v$. This proves part (i).

Let $u, v \in U \setminus \{0\}$ and $\phi(u) \mid \phi(v)$. We need only derive that then $u \operatorname{div} v$.

Suppose $u \in \boldsymbol{Z}$, and put $m = |u|$, so $m \mid \phi(v)$. By Lemma 3.2 we can take $k \in \boldsymbol{Z}$ such that $m \operatorname{div} v - k$. Hence $m \operatorname{div}_p v - k$ for each prime number p, so $m \mid_p \phi(v - k)$ for each prime number p. It follows that $m \mid \phi(v - k) = \phi(v) - k$, and since $m \mid \phi(v)$ this gives $m \mid k$, hence $m \operatorname{div} k$, so $m \operatorname{div} v$, and thus $u \operatorname{div} v$, as desired.

We assume $u \notin \boldsymbol{Z}$ in the rest of the proof. Since ϕ is an embedding of ordered groups we have $0 < |u| \leq |v|$, hence $v \notin \boldsymbol{Z}$. We have $\pi(u) \mid \phi(u) \mid \phi(v)$, so by part (i) we have $u \operatorname{div} mv$ for some $m > 0$. Suppose $m > 1$, and take a prime factor p of m, and write $m = pm'$. We claim that then $u \operatorname{div} m'v$. Since ϕ embeds $(A, \operatorname{div}_p)$ into $(R, |_p)$ and $\phi(u) \mid \phi(v)$, we have $pu \operatorname{div}_p mv$. Since also $u \operatorname{div} mv$, we can apply the axioms (Div6) for groups with $\boldsymbol{Z}$-like divisibilities to conclude that $pu \operatorname{div} mv$. Hence $u \operatorname{div} m'v$ as claimed. Repeating the same procedure with m' instead of m we eventually obtain $u \operatorname{div} v$. ⊣

Note also that if U is a full subset of A and π is a prime selector on U, then $\pi_B : U_B \setminus \boldsymbol{Z} \to \{p : p \nmid F\}$ is a prime selector on U_B, where $U_B := U \cap B$ and $\pi_B := \pi \mid (U_B \setminus \boldsymbol{Z})$. Given a full subset U of B, a prime selector π on U and a finite set $\mathscr{P}$ of primes, a map $\phi : B \to R$ is said to be a $(U, \pi, \mathscr{P})$-map if ϕ is a (U, π)-map such that $p \nmid \phi u$, for all $p \in \mathscr{P}$ and $u \in U \setminus \boldsymbol{Z}$.

PROPOSITION 8.2. *Let $n > 1$, let U be a full subset of A and $\pi : U \setminus \boldsymbol{Z} \to \{p : p \nmid F\}$ a prime selector on U, and put $A' := A_{n-1}$, $U' := U \cap A'$, and $\pi' := \pi \mid (U' \setminus \boldsymbol{Z})$, so U' is a full subset of A' and π' is a prime selector on U'. Let $\mathscr{P}$ be a finite set of primes not dividing F such that $\pi(U \setminus U') \subseteq \mathscr{P}$. Suppose $\phi : A' \to R$ is a $(U', \pi', \mathscr{P})$-map, and let $M := r(n - 1) + 1$. Then there are $Q, q \in R$ with $Q > 0$ such that for each* *sufficiently large* $x \in R$ *with* $x \equiv q \mod Q$ *there is a* $(U, \pi, \mathscr{P} \setminus \pi(U \setminus U'))$*-map* $A \to R$ *that extends* ϕ *and maps* e_M *to* x.

PROOF. We follow the proof of Proposition 5.2, using its notations, and only indicate the differences. Note that $\mathscr{P}$ is disjoint from $\mathscr{P}_1 \cup \mathscr{P}_2$. We define Q as before except that we include an extra factor $\prod_{p \in \mathscr{P}} p$. We add one more system of congruences to (1), (2) and (3):

$$kx + \phi a \equiv 0 \mod \pi(u) \text{ for } u = ke_M + a \in U \text{ with } 0 \neq k \in \boldsymbol{Z}, a \in A',$$

and one more system of incongruences:

$$kx + \phi a \not\equiv 0 \mod p \text{ for } p \in \mathscr{P} \setminus \pi(U \setminus U'), u = ke_M + a \in U \text{ with } 0 \neq k \in \boldsymbol{Z}, a \in A'.$$

The moduli in these two systems do not belong to $\{p : p \mid F\} \cup \mathscr{P}_1 \cup \mathscr{P}_2$; any two congruences of the first system with the same modulus have the same solutions. There exists $q \in R$ such that each $x \equiv q \mod Q$ satisfies (1), (2) and (3) as well as the two new systems above. We fix such a q in what follows and show that the Proposition holds with these values of Q and q. In *Case 1* we take $D > \phi A'$, and then each $x > D$ with $x \equiv q \mod Q$ has the property that the unique group homomorphism $\phi_x : A \to R$ that extends ϕ and sends e_M to x is a $(U, \pi, \mathscr{P} \setminus \pi(U \setminus U'))$-map.

In *Case 2* we make the inductive assumption that we have a positive $D \in R$ such that for each $x > D$ with $x \equiv q \mod Q$ we can extend ϕ to a $(U_B, \pi_B, \mathscr{P}_B)$-map $\phi_x : B \to R$ with $\phi_x(e_M) = x$, where $\mathscr{P}_B := \mathscr{P} \setminus \pi(U_B \setminus U')$.

We can assume that

$$D > \Bigl(F \cdot \prod_{p \in \mathscr{P}'} p^{v(p)+1} \cdot \prod_{p \in \pi(U \setminus U_B)} p\Bigr)^2.$$

Below we fix any $x > D$ with $x \equiv q \mod Q$. We add one more system of congruences to (i), (ii), (iii) and (iv), namely:

(v) $ky + \phi_x b \equiv 0 \mod \pi(u)$ for $u = ke_N + b \in U$ with $0 \neq k \in \boldsymbol{Z}, b \in B$,

and one more system of incongruences:

(vi) $ky + \phi_x b \not\equiv 0 \mod p$ for $p \in \mathscr{P} \setminus \pi(U \setminus U')$ and $u = ke_N + b \in U$ with $0 \neq k \in \boldsymbol{Z}, b \in B$.

We shall obtain y satisfying (i), (ii), (iii), (iv), (v) and (vi). One checks easily that for any such y the group homomorphism $A = B \oplus \boldsymbol{Z}e_N \to R$ that extends ϕ_x and sends e_N to y is a $(U, \pi, \mathscr{P} \setminus \pi(U \setminus U'))$-map. The moduli of (v) and (vi) lie in $\mathscr{P}_B$, hence do not belong to $\{p : p \mid F\} \cup \mathscr{P}_1' \cup \mathscr{P}_2'$; any two congruences of (v) with the same modulus have the same solutions. Note also that all moduli of (v) lie in $\pi(U \setminus U_B)$, and all moduli of (vi) lie outside $\pi(U \setminus U_B)$. Put

$$G := F \cdot \prod_{p \in \mathscr{P}_1'} p^{v(p)+1} \cdot \prod_{p \in \pi(U \setminus U_B)} p.$$

Note that $D > G^2$. We obtain $r \in R$ with $0 \leq r < G$ such that each $y \equiv r \mod G$ satisfies (i), (ii) and (v). Let z range over R. With $y = Gz + r$, the incongruences of (iii) and (vi) reduce to a system of incongruences (iii)' as in the proof of Proposition 5.2, except that we have finitely many additional incongruences $z \not\equiv \lambda \mod p$ with $p \in \mathscr{P} \setminus \pi(U \setminus U')$ and $\lambda \in R$. Put $\alpha := \frac{m_1 x}{m_2 G}$ and take $\varepsilon > 0$ in $\boldsymbol{Q}$ such that $\alpha + \varepsilon\alpha < \frac{m_3 x}{m_2 G} - \frac{r}{G}$ (any positive rational $< \frac{m_3}{m_1} - 1$ will do). Let $p_1, \ldots, p_\mu, p_{\mu+1}, \ldots, p_{\mu+\nu}$ be the distinct primes that occur as moduli in a given finite set of incongruences of the system (iii)' as augmented above, where $p_1, \ldots, p_\mu$ are $< \alpha^m$ for some m, and $p_{\mu+1}, \ldots, p_{\mu+\nu}$ are $> \alpha^m$ for all m (hence $p_{\mu+1}, \ldots, p_{\mu+\nu} \in \mathscr{P} \setminus \pi(U \setminus U')$). Let $\prod := \prod_{i=1}^{\mu} p_i$, so $\prod < \alpha^m$ for some $m > 0$. By the proof of Lemma 4.8 there exist infinitely many z with $\alpha < z < \alpha + \varepsilon$ that satisfy the incongruences modulo $p_1, \ldots, p_\mu$; all but finitely many of those z will also satisfy the incongruences modulo $p_{\mu+1}, \ldots, p_{\mu+\nu}$. ⊣

COROLLARY 8.3. *There exists an embedding* $\mathscr{A} \to R_{\text{div}}$.

PROOF. Using Lemma 4.2 we choose for each prime number p an embedding $\phi_p : (A, \text{div}_p) \to (R, |_p)$ with $\phi_p(1) = 1$. Next we take F and $f_1, \ldots, f_N$ as in Lemma 5.1 such that in addition $f_1 = 1$. (The proof of that lemma shows this to be possible.) Finally, we choose any function $\pi : A \setminus \boldsymbol{Z} \to \{p : p \nmid F\}$ such that for all $a, b \in A \setminus \boldsymbol{Z}$ we have: $\pi(a) = \pi(b) \iff a^w \text{ div } b$ and $b^w \text{ div } a$.

CLAIM. There is an embedding $\phi : \mathscr{A} \to R_{\text{div}}$ such that $\phi(e_i) \equiv f_i \mod F$ for $i = 1, \ldots, N$ and $\pi(a) \mid \phi(a)$ for all $a \in A \setminus \boldsymbol{Z}$.

Because of saturation this claim holds if for each full subset U of A there exists a (U, π_U)-map $A \to R$, where $\pi_U := \pi \mid (U \setminus \boldsymbol{Z})$. Let U be a full subset of A, and put $U_i := U \cap A_i$, $\pi_i := \pi \mid (U_i \setminus \boldsymbol{Z})$, and $\mathscr{P}_i := \pi(U \setminus U_i)$ for $i = 1, \ldots, n$. The domain of π_1 being empty, the inclusion $\boldsymbol{Z} = A_1 \to R$ is clearly a $(U_1, \pi_1, \mathscr{P}_1)$-map. Using Proposition 8.2, this inclusion map extends successively for $i = 2, \ldots, n$ to a $(U_i, \pi_i, \mathscr{P}_i)$-map $A_i \to R$. For $i = n$ this gives the desired result. ⊣

REMARK. In the proof above we could have fixed an arbitrary positive $H \in R$ and added to the claim the requirement that $|\phi(a)| > H$ for all $a \in A \setminus \boldsymbol{Z}$.

We now have Theorem 3.1:

COROLLARY 8.4. *Each group with* $\boldsymbol{Z}$*-like divisibilities can be embedded into some elementary extension of* $\boldsymbol{Z}_{\text{div}}$*. Hence* T_{div} *axiomatizes the universal part of the elementary theory of* $\boldsymbol{Z}_{\text{div}}$.

The fact that T_{div} axiomatizes the universal part of $\text{Th}(\boldsymbol{Z}_{\text{div}})$ leads to an algorithm that takes as inputs existential sentences of L_{div} and decides for any such sentence whether it is true in $\boldsymbol{Z}_{\text{div}}$. Thus we recover the decidability result from [1] and [4]. Macintyre [6] mentions a special case of the following.

COROLLARY 8.5. *Let* R *be any bounded induction domain of cardinality* κ *and* ${}^*R$ *any* κ^+*-saturated bounded induction domain. Then there exists an embedding* $j : R_{\text{div}} \to {}^*R_{\text{div}}$ *such that* $j(x)$ *is not prime in* ${}^*R$ *for all positive infinite* $x \in R$.

PROOF. By saturation it suffices to show that for each finitely generated substructure $\mathscr{A}$ of R_{div} there exists an embedding $j_{\mathscr{A}} : \mathscr{A} \to {}^*R_{\text{div}}$ such that $j_{\mathscr{A}}(x)$ is not prime in ${}^*R$ for all positive infinite $x \in A$. The proof of Corollary 8.3 produces for any such $\mathscr{A}$ an embedding with those properties, taking into account also the remark following that proof. ⊣

Postscript. In preparing a final version of the manuscript we noticed an easy example showing that the power lower bound in Corollary 1.6 cannot be replaced by something better, in particular not by a linear lower bound. This gives a negative answer to a question formulated towards the end of the introduction.

Define $f : \boldsymbol{N}^2 \to \boldsymbol{N}$ by $f(x, y) = x$ if $x, y > 0$, $x \mid y$ and $x + 1 \mid y$, and put $f(x, y) = 0$ otherwise. Then f is unbounded and its graph is a divisibility set in $\boldsymbol{Z}^3$. For each positive real constant $c < 1/2$ we have $f(x, y) > (x + y)^c$ for infinitely many $(x, y) \in \boldsymbol{N}^2$, but this fails for $c = 1/2$.

REFERENCES

[1] A. P. Bel'tyukov, *Decidability of the universal theory of natural numbers with + and |*, ***Seminars of Steklov Mathematical Institute (Leningrad)***, vol. 60 (1976), pp. 15–28.

[2] L. van den Dries, *Quantifier elimination for linear formulas over ordered and valued fields*, ***Bulletin de la Société Mathématique de Belgique***, vol. 33 (1981), pp. 19–33.

[3] H. Groemer, *On the extension of additive functionals on classes of convex sets*, ***Pacific Journal of Mathematics***, vol. 75 (1978), pp. 397–410.

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

[5] ———, *Some remarks on the diophantine problem for addition and divisibility*, ***Bulletin de la Société Mathématique de Belgique***, vol. 33 (1981), pp. 41–52.

[6] A. Macintyre, *A theorem of Rabin in a general setting*, ***Bulletin de la Société Mathématique de Belgique***, vol. 33 (1981), pp. 53–63.

[7] Y. Moschovakis, *On primitive recursive algorithms and the greatest common divisor function*, ***Theoretical Computer Science***, to appear.

[8] A.J. Wilkie, *Modèles non standard de l'arithmétique, et complexité algorithmique*, ***Modèles non standard en arithmétique et theorie des ensembles***, Publications Mathématiques de l'Université Paris VII, 1984, pp. 5–45.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
URBANA, IL 61801, USA
E-mail: vddries@math.uiuc.edu

MATHEMATICAL INSTITUTE
UNIVERSITY OF OXFORD
24–29 ST. GILES, OXFORD OX1 3LB, UK
E-mail: wilkie@maths.ox.ac.uk