TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 235, January 1978

THE DIOPHANTINE PROBLEM FOR ADDITION AND DIVISIBILITY

BY
L. LIPSHITZ[1]

ABSTRACT. An algorithm is given for deciding existential formulas involving addition and the divisibility relation over the natural numbers.

In this paper it will be shown that there is an algorithm for deciding formulas of the form

$$\exists x_1, \ldots, \exists x_{n \in \mathbf{N}} \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) | g_i(x_1, \ldots, x_n) \tag{1}$$

in $\mathbf{N}$ (the natural numbers), where the f_i and g_i are linear polynomials with integer coefficients. ($a|b$ means "a divides b".) This is a generalization of the Chinese Remainder Theorem (C.R.T.) which states that

$$\bigwedge_{i=1}^{k} m_i|(x - r_i)$$

has a solution for $x \in \mathbf{N}$ if and only if $(m_i, m_j)|(r_i - r_j), i, j = 1, \ldots, k$, where $(a, b) = \text{g.c.d.}(a, b)$, cf. [2]. The corresponding problem where the f_i and g_i are second degree polynomials is undecidable. This follows immediately from the undecidability of Hilbert's Tenth Problem. We get as a corollary that formulas of the form $\exists x_1 \ldots \exists x_n\, \Delta(x_1, \ldots, x_n)$, where Δ is an open formula in the language $\langle +, |, 0, 1\rangle$ are decidable. This result is also the best possible in the following sense. Using the undecidability of Hilbert's Tenth Problem and standard techniques (cf. [3], [4] and the references therein) for defining multiplication from $+$ and $|$ one can show that formulas of the form $\exists x_1 \ldots \exists x_n\, \forall y\, \Delta(x_1, \ldots, x_n, y)$, with Δ an open formula in the language $\langle +, |, 0, 1\rangle$ are undecidable. Similar results have been obtained by A. P. Bel'tyukov (personal communication from Julia Robinson).

We shall also show (in §3) that if R is the ring of integers of an imaginary quadratic extension of the rationals ($\mathbf{Q}$) then there is an algorithm for

Received by the editors August 19, 1975 and, in revised form, June 11, 1976.
AMS (MOS) subject classifications (1970). Primary 02E10, 02F47, 10A10, 10N05.

[1]Supported in part by N.S.F. grant GP 43749 and a grant from the Purdue Research Foundation.

deciding formulas of the form

$$(2) \qquad \exists x_1 \ldots \exists x_{n \in \mathbf{N}} \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) | g_i(x_1, \ldots, x_n)$$

where the f_i and g_i are linear polynomials with coefficients from R. Consequently there is also an algorithm for deciding formulas of the form

$$(3) \qquad \exists x_1 \ldots \exists x_{n \in \mathbf{R}} \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) | g_i(x_1, \ldots, x_n)$$

with the f_i and g_i as above.

In a subsequent paper we shall show that if R is the ring of integers of a real quadratic extension of the rationals then both (2) and (3) are undecidable; and that if R is the ring of integers in any proper algebraic extension of the rationals other than imaginary quadratic, then (2) is undecidable.

I would like to thank A. P. Bel′tyukov and Ju. Matijasevič for helpful criticisms of an earlier verison of this paper and especially Julia Robinson for helpful and encouraging suggestions during the preparation of this paper.

The plan is to reduce the problem to formulas of a special form where, among other things, all the coefficients are from **N** and the variables are ordered in some way and then use the C.R.T. to eliminate the largest variable. x will denote the variables $x_1, \ldots, x_n$ and $\phi(x)$, $\phi_i(x)$, $\psi(x)$ etc. will denote the formulas of the form $\bigwedge_{i=1}^{k} f_i(x) | g_i(x)$ where the f_i and g_i are linear polynomials with integer coefficients. We shall call such a formula *positive* if its coefficients are from **N**. We shall assume that if a formula can be made positive by replacing some of the f_i's and g_j's by $-f_i$ and $-g_j$ then this is always automatically done. The resulting formula is of course equivalent to the original formula.

1. In this section we shall show how to reduce the problem to the case of formulas of a very convenient form.

Let $P_n = \{x \in \mathbf{Q}^n\colon x_i \geqslant 0,\ i = 1, \ldots, n\}$ and let $R = P_n \cap \{x \in \mathbf{Q}^n\colon l_i(x) \geqslant 0,\ i = 1, \ldots, m\}$ where the $l_i(x)$ are linear polynomials. A positive cone in $\mathbf{Q}^n$ is the image of P_n under a mapping of the form $x = Au + b$ where A is an $n \times n$ matrix and b an $n \times 1$ vector, both with coefficients from $\mathbf{Q}$. If B is a region in $\mathbf{Q}^n$ then ${}^IB$ denotes the set of integral points in B.

LEMMA 1. *Let R be a convex set in $\mathbf{Q}^n$ as above. Then one can constructively find a finite set of positive cones C_i: $x = A_i u + b_i$, $i = 1, \ldots, J$, such that*

(i) *each $C_i \subset R$ and ${}^IR = \bigcup_{i=1}^{J} {}^IC_i$,*

(ii) *if $x_0 \in {}^IR$ then there exist i_0 and $u_0 \in {}^IP_n$ such that $x_0 = A_{i_0}u_0 + b_{i_0}$.*

The lemma is geometrically reasonably clear, cf. [1]. Since the proof is not relevant to the rest of the paper we present it in the appendix at the end of the paper.

Let $\phi(x)$ be a formula and let $x = Au + b$ be a change of variables, where the entries of A and b are from Q. Let $\alpha \in \mathbf{N}$ be the l.c.m. of the denominators of all these entries. When we say $\phi'(u) = \phi(Au + b)$ results from $\phi(x)$ by the change of variables $x = Au + b$ we mean that $\phi'(u)$ is obtained from $\phi(x)$ by substituting $Au + b$ for x and then multiplying right through (all the terms) by α and adjoining some divisibilities of the form $\beta | h(u)$ ($\beta \in \mathbf{N}$) to ensure that if $u \in \mathbf{N}^n$ satisfies ϕ', then $x = Au + b$ is an integral point. (The coefficients of $h(u)$ will be positive multiples of some of the entries of A and b.) Then $\phi'(u)$ is a formula of the type we are considering.

LEMMA 2. *Let $\phi(x)$ have coefficients from $\mathbf{Z}$ and let $\chi(x)$ be a partial ordering of the variables together with some linear inequalities of the form $l(x) \geq 0$. There exists a finite set of changes of variables $x = A_i u + b_i$ with the A_i and b_i having positive rational entries such that the resulting formulas $\phi_i(u)$, $i = 1, \ldots, J$, are positive and*

$$\exists x_{\in \mathbf{N}}(\phi(x) \wedge \chi(x)) \leftrightarrow \bigvee_{i=1}^{J} \exists u_{\in \mathbf{N}} \phi_i(u).$$

PROOF. Let $\phi(x) = \bigwedge_i f_i(x) | g_i(x)$ and let $\chi_j(x)$ run through all possible combinations $(\bigwedge_i \pm f_i(x) \geq 0) \wedge (\bigwedge_i \pm g_i(x) \geq 0)$ where only those f_i and g_i are considered which contain both positive and negative coefficients. Then

$$\exists x(\phi(x) \wedge \chi(x)) \leftrightarrow \bigvee_j \exists x(\phi(x) \wedge \chi(x) \wedge \chi_j(x)).$$

Hence it is sufficient to show that there are positive formulas $\phi_i(u)$ such that

$$\exists x(\phi(x) \wedge \chi(x) \wedge \chi_j(x)) \leftrightarrow \bigvee_i \exists u \phi_i(u)$$

where χ_j is as above. Let $R = P_n \cap \{x \in \mathbf{Q}^n\colon \chi(x) \wedge \chi_j(x)\}$. Let the C_i: $x = A_i u + b_i$ be as in Lemma 1, and let $\phi_i(u)$ result from $\phi(x)$ by making the change of variables $x = A_i u + b_i$. Recall that in $\phi_i(u)$ we have adjoined some divisibilities of the form $\alpha | h(u)$ ($\alpha \in \mathbf{N}$) if necessary to ensure that if $\phi_i(u)$ holds for $u \in \mathbf{N}^n$ then $x = A_i u + b_i$ is an integral point. Since $x = A_i u + b_i \in P_n$ for all $u \in P_n$ it is clear that all the entries in the A_i and b_i are nonnegative. We claim that $\phi_i(u)$ is positive (recall our convention that if f_j or g_j has all negative coefficients then it is replaced by $-f_j$ or $-g_j$). Notice that for all $u \in P_n$ we have that if $x = A_i u + b_i$ then $x \in P_n$ and $\chi(x)$ and $\chi_j(x)$ hold. If $\phi_i(u)$ were not positive then for some k $f_k(A_i u + b_i)$ or $g_k(A_i u + b_i)$ would assume both positive and negative values as u varies over P_n. Call it $h(A_i u + b_i)$. h does not occur in χ_j since if it did then for all $u \in P_n$ $h(x) = h(A_i u + b_i)$ satisfies the inequality in χ_j. If h does not occur in χ_j then all its coefficients are positive (by our convention the case when all are negative is eliminated). Since A_i and b_i have nonnegative entries it follows that all the coefficients of $h(A_iu + b_i)$ are positive. Hence $\phi_i(u)$ is positive. By conditions (i) and (ii) of Lemma 1 it is clear that

$$\exists x_{\in \mathbf{N}}(\phi(x) \wedge \chi(x) \wedge \chi_j(x)) \leftrightarrow \bigvee_i \exists u_{\in \mathbf{N}} \phi_i(u).$$

This completes the proof of Lemma 2.

Let $\phi(x)$ be positive and let an ordering $\chi(x)$ of the variables be specified. Suppose that no atomic formula of the form $f(z, y) | g(z, y)$ with $y > x_i$ (w.r.t. χ) for all the x_i in z and with y having nonzero coefficient in f, occurs in $\phi(x)$. Then we call $\phi(x)$ *increasing* w.r.t. χ.

LEMMA 3. *Let $\phi(x)$ have coefficients from $\mathbf{Z}$. Then there exists a finite set of positive formulas $\phi_i(x)$ and orderings $\chi_i(x)$ such that $\phi_i(x)$ is increasing w.r.t. $\chi_i(x)$ and*

$$\exists x \phi(x) \leftrightarrow \bigvee_i \exists x(\phi_i(x) \wedge \chi_i(x)).$$

PROOF. Induction on the number of variables. By Lemma 2 it is sufficient to consider the case of ϕ positive. Let $\chi_i(x)$ vary over all possible orderings of the variables in ϕ. Then $\exists x\phi(x) \leftrightarrow \bigvee_i \exists x(\phi(x) \wedge \chi_i(x))$. If ϕ is not increasing w.r.t. χ_i then $f(y, z) | g(y, z)$ occurs in ϕ with $y \geqslant x_i$ for all $x_i \in z$ (w.r.t. χ_i) and y occurs in f with nonzero coefficient. Let M be the sum of the coefficients of g. It is clear that $\chi_i(x) \wedge f(x) | g(x) \leftrightarrow \chi_i(x) \wedge (\bigvee_{\alpha=1}^{M} \alpha f = g)$. Replace $f | g$ by $\bigvee_{\alpha=1}^{M}(\alpha f = g)$ in ϕ, return to disjunctive normal form and in each disjunct use the equation $(\alpha f = g)$ to eliminate one of the variables and then use Lemma 2 and the induction hypothesis. (If $\alpha f = g$ formally we cannot use this equation to eliminate a variable. In this case just delete the atomic formula $f | g$ from the original formula.)

Let ϕ be a positive increasing formula w.r.t. χ and let x_0 be the largest variable. The other variables are $(x_1, \ldots, x_n) = x$. Let $f_i(x) | g_i(x, x_0) = h_i(x) + a_i x_0, i = 1, \ldots, k,$ be all the atomic formulas of ϕ containing x_0. Let $\bar{\phi}(x)$ result from ϕ by deleting all the atomic formulas containing x_0. Let (α, β) denote the g.c.d. of α and β. Then for fixed $x \in \mathbf{N}$

$$(*)\ \exists x_0 \phi(x, x_0) \leftrightarrow \bar{\phi}(x) \wedge \bigwedge_{i<j\leqslant k} (a_j f_i(x), a_i f_j(x)) | h_{ij}(x) \wedge \bigwedge_i (f_i(x), a_i) | h_i(x)$$

where $h_{ij}(x) = a_j h_i(x) - a_i h_j(x)$. This follows immediately from the C.R.T. mentioned above. Our plan is to reduce the problem of determining if ϕ has a solution to the problem of determining if $\bar{\phi}$ has a solution. We need however to adjoin certain divisibilities involving the variables x which are implicit in ϕ but not implicit in $\bar{\phi}$, e.g. if $f | f_i$ and $f | f_j$ occur in ϕ then from $(*)$ it follows that we must have $f | h_{ij}$. We shall want the formula ϕ to satisfy the conditions (a)–(d) below. The conditions $(f_i, a_i) | h_i$ are of no problem since they involve congruences w.r.t. factors of the a_i's and the a_i's occur in ϕ. Hence $(f, a)|h$ can be replaced by a disjunction of the formulas of the form $\alpha|f$ and $\alpha|h$. In the statement of these conditions we shall understand that when we write αf (or βg, $\alpha_i g_i$ etc.) that $\alpha \in \mathbf{N}$ and that the g.c.d. of the coefficients of f (g, g_i, etc.) is 1.

(a) If $\alpha f|\beta g$ occurs in ϕ then $1|f$ and $1|g$ occur in ϕ.

(b) If $\alpha f|\beta g$ and $\gamma g|\delta h$ occur in ϕ then $f|\varepsilon h$ occurs in ϕ for some $\varepsilon \in \mathbf{N}$ with $\varepsilon|\beta\delta$.

(c) If $\alpha_1 f|\beta_1 g_1, \ldots, \alpha_k f|\beta_k g_k$ and g occur in ϕ and $g_1, \ldots, g_k$ are linearly independent and $\beta g = \sum \gamma_i g_i$ with $\beta, \gamma_i \in \mathbf{Z}$ and g.c.d. $(\beta, \gamma_1, \ldots, \gamma_k) = 1$ then $f|\delta g$ occurs in ϕ for some $\delta \in \mathbf{N}$.

(d) If $\alpha_1 f|g_1$ and $\alpha_2 f|g_2$ occur in ϕ and the largest (w.r.t. χ) variable in g_1 (with nonzero coefficient) is the same as that in g_2 ($= x_0$ say) and the coefficient of x_0 in g_1 in a_1 and in g_2 is a_2 and α is the g.c.d. of the coefficients of $(a_1 g_2 - a_2 g_1)$ then $f|(\beta/\alpha)(a_1 g_2 - a_2 g_1)$ occurs in ϕ for some $\beta \in \mathbf{N}$.

If ϕ is positive, increasing w.r.t. χ and satisfies (a)–(d) above we shall call ϕ totally positive increasing w.r.t. χ.

We say that $\chi(x)$ is a generalized ordering of the variables x if $\chi(x)$ is the conjunction of an ordering $\chi'(x)$ of the variables with some linear inequalities of the form $x_i \geqslant l(z)$ where for all $x_j \in z$ $x_i > x_j$ w.r.t. χ'. If $\chi(x)$ is a generalized ordering as above then we call $\phi(x)$ totally positive increasing w.r.t. $\chi(x)$ if $\phi(x)$ is totally positive increasing w.r.t. $\chi'(x)$ (the ordering in $\chi(x)$).

Lemma 4. *Let $\phi(x)$ be a formula. One can construct a finite set $\phi_i(x)$, $\chi_i(x)$ ($i = 1, \ldots, J$) of formulas and generalized orderings such that $\phi_i(x)$ is totally positive increasing w.r.t. $\chi_i(x)$ and*

$$\exists x\phi(x) \leftrightarrow \bigvee_{i=1}^{J} \exists x(\phi_i(x) \wedge \chi_i(x)).$$

Proof. By Lemma 3 we can assume that $\phi(x)$ is positive and increasing w.r.t. $\chi(x)$, say. We shall prove the lemma by induction on the number of variables.

Of (a)–(d) above, only (d) leads to the introduction of new atomic formulas which may alter the fact that ϕ is positive. We shall look ahead and introduce all of these first, at the same time using Lemma 2 to get positive formulas. Then we shall close up under (a)–(d). The worst that can happen here is that we get a formula which is not increasing. But this leads to the elimination of a variable and then we can use Lemma 2 to get rid of the generalized ordering and then use the induction hypothesis.

(1) Let the largest variable be x_0 (others are $(x_1 \ldots x_n) = x$). Let the atomic formulas containing x_0 be $f_i(x)|g_i(x_0, \dot{x})$, $i = 1, \ldots, k$, (since ϕ is

positive increasing x_0 occurs only on the right-hand side) let $g_i(x_0, x) = h_i(x) + a_i x_0$ and let $h_{ij}(x) = a_j h_i - a_i h_j$, $i < j \leqslant k$. Adjoin the formulas $1|h_{ij}$, $i < j \leqslant k$, to get formula ϕ'. If ϕ' is positive, go to (3) below. If ϕ' is not positive then go to (2).

(2) Let ϕ'' result from ϕ' by deleting all the atomic formulas containing x_0. Find changes of variables $x = A_i u + b_i$ as in Lemma 2 corresponding to ϕ''. Let each $\phi_i'(x_0, A_i u + b_i)$ result from ϕ' by the change of variables $(x_0, x) = (x_0, A_i u + b_i)$. Then ϕ_i' is positive since there were no minus signs in the atomic formulas we deleted and all the entries in A_i, b_i are nonnegative. Let α_i be the l.c.m. of the denominators in A_i, b_i. Then in $\phi_i'(x_0, u)$ we have multiplied right through by α_i. Let $\phi_i(y, u)$ result from ϕ_i' by replacing $\alpha_i x_0$ by the new variable y_0 and adjoining the divisibility $\alpha_i | y_0$. Let $A_i = (a_{kj})$, $b_i = (b_k)$. Then $x_k = \sum a_{kj} u_j + b_k$. Let $\chi_i(y_0, u)$ be the conjunction of the inequalities

$$y_0 > \sum_j \alpha_i a_{kj} u_j + \alpha_i b_k$$

(each $\alpha_i a_{kj}$ and each $\alpha_i b_k \in \mathbf{N}$). We certainly have

$$\exists x_0 x \phi(x_0, x) \leftrightarrow \bigvee_i \exists y_0 \exists u (\phi_i(y_0, u) \wedge \chi_i).$$

(3) Extend $\chi_i(y_0, u)$ to an ordering of the variables y_0, u in all possible ways with $y_0 > u_i$ ($i = 1, \ldots, n$). (These inequalities follow from the inequalities $y_0 > \sum \alpha_i a_{kj} u_j + \alpha_i b_k$ if all of $u_1, \ldots, u_n$ are used in the change of variables. If one is missing, we have reduced the number of variables and we can apply Lemma 3 and the induction hypothesis to each $\phi_i \wedge \chi_i$.) If we are coming from (1), then there is only one i and χ is vacuous. By abuse of notation we still call the resulting formulas and generalized orders $\phi_i(x_0, u)$ and $\chi_i(x_0, u)$. Then certainly we have $\exists x_0 x \phi(x_0, x) \leftrightarrow \bigvee_i \exists y_0 \exists u (\phi_i(y_0 u) \wedge \chi_i(y_0, u))$.

(4) Consider each $\phi_i \wedge \chi_i$ separately. If ϕ_i, χ_i is not increasing, eliminate a variable and apply the induction hypothesis. If it is increasing, let u_1 be the largest of the u_j (i.e. the second largest variable w.r.t. χ_i) and let $f_{ij} | g_{ij} = h_{ij} + a_{ij} u_1$ be the atomic formulas in which u_1 is the largest variable. Let $h_{ijk} = a_{ij} h_{ik} - a_{ik} h_{ij}$ and adjoin $1 | h_{ijk}$ to ϕ_i. By abuse of notation, we still call it ϕ_i. If the resulting formula is not positive, let $\bar{\phi}_i$, $\bar{\chi}_i$ result from ϕ_i, χ_i by deleting all the atomic formulas in which y_0 or u_1 occur. Let $v = (v_2, \ldots, v_n)$ and make changes of variables $(u_2, \ldots, u_n) = A_{ij} v + b_{ij}$ as in Lemma 2. Let $\phi_{ij}(y_0, u_1, v)$, $\chi_{ij}(y_0, u_1, v)$ result from ϕ_i, χ_i by making this change of variables. Let the l.c.m. of the denominators be α_{ij} and replace $\alpha_{ij} y_0$ by z_0, $\alpha_{ij} u_1$ by z_1 and adjoin the divisibility $\alpha_{ij} | z_1$. Extend χ_{ij} to an ordering in all possible ways with $z_0 > z_1 > v_k$, $k = 2, \ldots, n$. Call the resulting formulas $\phi_{ij}(z_0, z_1, v)$, $\chi_{ij}(z_0, z_1, v)$. Then certainly the ϕ_{ij} with χ_{ij} are positive and

$$\exists x_0 x \phi(x_0, x) \leftrightarrow \bigvee \exists z_0 z_1 v \phi_{ij}(z_0, z_1, v) \wedge \chi_{ij}(z_0, z_1, v)$$

and each χ_{ij} is a generalized ordering.

(5) Repeat the above process with respect to the 3rd largest, 4th largest variables etc. Eventually we obtain ψ_i and generalized orderings χ_i such that

$$\exists x_0, x\phi(x) \leftrightarrow \bigvee \exists x_0 x(\psi_i(x_0, x) \wedge \chi_i(x_0, x))$$

and each ψ_i is positive increasing w.r.t. χ_i and whenever $h(y, z)$, $k(y, z)$ occur in ψ_i with $y >$ all the variables in z (w.r.t. χ_i) and y having coefficient a in h and b in k, then $1|bh - ak$ occurs in ψ_i. In other words, the terms which need to be adjoined by (d) above are present.

(6) Close up under (a)–(b), using the proviso that at any time that we have atomic formulas $\alpha f | \beta g$ and $\alpha f | \gamma g$ both occurring, then we replace these two formulas by $\alpha f|\text{g.c.d.}(\beta, \gamma) g$. (Choose the ε, δ and β in (a), (b) and (c) respectively in the natural way.) We must see that the process terminates. We can certainly check constructively whether the formula satisfies (a)–(d). Notice that if it does not, then we must adjoin an atomic formula of the form $\alpha f | \beta g$. Notice that if the original formula contained K atomic formulas then we can adjoin such formulas at most $4K^2$ times without the proviso being applicable and that each time we apply the proviso we get a shorter formula. Hence the process terminates. If the resulting formula is increasing, then it is totally positive increasing. If it is not, then eliminate one of the variables and apply Lemma 2 and the induction hypothesis.

2. Let $\phi(x) = \bigwedge_{i=1}^{K} f_i(x)| g_i(x)$ and let n be the number of variables in $\phi(x)$, m the maximum of absolute values of the coefficients of $\phi(x)$, $\alpha_p = [\log_p(m \cdot n)] + 2$ and $k(\phi, p) = (p + 1)^{4(n+2)\alpha_p K}$, for primes p. In the following by $a|b \pmod{p^k}$ we mean that for some c $ac \equiv b \pmod{p^k}$.

Lemma 5. *If for some k $\phi(x)$ has a solution* mod p^k *with all the $f_i(x) \not\equiv 0$* mod p^k, *then $\phi(x)$ has such a solution* mod $p^{k(\phi,p)}$.

Proof. Think of $x_i = x_{i0} + x_{i1}p + x_{i2}p^2 + \dots$ as a p-adic integer with the $x_{ij} \in \{0, 1, \dots, p - 1\}$ to be determined. Let $x_i^{(j)} = \sum_{m=0}^{j} x_{im}p^m \in \mathbf{N}$, once the x_{im} for $m = 0, \dots, j$ are determined; and let

$$f_i^{(j)} = f_i(x_1^{(j)}, \dots, x_n^{(j)}).$$

Then $f_i^{(j)} = \sum_{k=1}^{j+\alpha_p} a_{ik}p^k$ where α_p is as above, and the $a_{ik} \in \{0, 1, \dots, p - 1\}$.

We shall successively determine the x_{ij}, $j = 0, 1, 2, \dots$, in all possible ways. We shall see that this process finally becomes cyclic.

Suppose that the x_{ij} have been determined for $j < k$ so that $\phi(x)$ is satisfied mod p^k. Then the x_{ik} must be chosen so that $f_i^{(k)}| g_k^{(k)}$ mod p^{k+1}. We need only consider those f_i, g_i such that

$$f_i^{(k-1)} \equiv 0 \bmod p^k,$$

(and hence $g_i^{(k-1)} \equiv 0 \bmod p^k$). We have

$$f_i^{(k)} = \sum_{m=0}^{\alpha_p} a_{imk} p^{m+k} + \sum_{i=1}^{n} c_i x_{ik} p^k$$

where the c_i, $i = 1, \ldots, n$, are fixed and the a_{ijk} depend on the x_{jm} for $m < k$. Similarly

$$g_i^{(k)} = \sum_{m=0}^{\alpha_p} b_{imk} p^{m+k} + \sum_{i=1}^{n} d_i x_{ik} p^k.$$

(Recall that $f_i^{(k-1)}, g_i^{(k-1)} \equiv 0 \bmod p^k$.) Then the x_{ik} must be chosen so that if

$$f_i^{(k)} \equiv 0 \bmod p^{k+1} \quad \text{then} \quad g_i^{(k)} \equiv 0 \bmod p^{k+1}.$$

The possibility (and the ways) of doing this depend only on the c_i, d_i, $i = 1, \ldots, n$, and the a_{imk}, b_{imk}, $m = 0, \ldots, \alpha_p$. Call a set of values of the x_{ik}, $i = 1, \ldots, n$, acceptable (for fixed values of the x_{ij}, $i = 1, \ldots, n, j < k$) if the above conditions are satisfied. Start making a list of all the acceptable values of the x_{ij}, $i = 1, \ldots, n$, $j = 0, 1, 2, \ldots,$ i.e. start writing down the following tree:

Stage 0: all acceptable values of x_{i0},

Stage 1: all acceptable values of x_{i1} which follows from these values of x_{i0}, etc.

A path through this tree would give us p-adic integers x_i which satisfy $\phi(x)$ and a path up to stage k would give us integers $x_i^{(k)}$ which satisfy $\phi(x)$ mod p^{k+1}.

At each node in this tree also write down the corresponding values of the a_{imk}, b_{imk} for $m = 0, \ldots, \alpha_p$. (k = stage of the node.)

Let a branch terminate at stage $k + \gamma$ if

$$a_{im\gamma} = a_{im\gamma+k} \quad \text{and} \quad b_{im\gamma} = b_{im\gamma+k}$$

for $m = 0, \ldots, \alpha_p$ and $i = 1, \ldots, K$ and

$$x_{i\gamma} = x_{i\gamma+k}, \qquad i = 1, \ldots, n.$$

This just means that the branch has become cyclic. The whole process now terminates in $< (p+1)^{4(n+2)\alpha_p K}$ stages.

Hence if for some k, ϕ has a solution mod p^k with all the $f_i \not\equiv 0 \bmod p^k$ then it has such a solution mod $p^{(p+1)^{4(n+2)\alpha_p K}}$.

Let $\psi(x, y)$ be totally positive increasing w.r.t. generalized order χ. Let m = max(coefficients of ψ), k = number of atomic formulas in ψ (i.e. $\psi = \bigwedge_{i=1}^{k} f_i | g_i$) and let $M_\psi = \max(m, k)$. Let n = the number of variables in ψ, $\alpha_p = [\log_p(m, n)] + 2$ and $k(\psi, p) = (p+1)^{4(n+2)\alpha_p k}$.

LEMMA 6. *Let ψ, χ be as above and let $K > M_\psi$ and for each prime $p < K$ let $k_p > k(\psi, p)$ and let a solution of ψ* mod p^{k_p}, *with $f_i \not\equiv 0$* mod p^{k_p} *(i =*

$1, \ldots, k$) *be specified. Then* ψ, χ *has a solution in* $\mathbf{N}$ *with these specified residues* mod p^{k_p} *for* $p < K$, *and except for primes* $p < K$ *the* f_i *and* g_j *have no common factors except as specified by divisibilities occurring in* ψ *and further if* h, k *occurs in* ψ *and* $p > K$ *and* $p|h$ *and* $p|k$ *then the same power of* p *divides both* h *and* k. (*Call such a solution as mutually prime as possible.*)

PROOF. Let $\bar{\bar{\psi}}, \bar{\bar{\chi}}$ result from ψ, χ by deleting all the atomic formulas which contain the largest variable y. Then we certainly have $K > M_{\bar{\bar{\psi}}}$ and $k_p > \underline{k}(\bar{\bar{\psi}}, p)$ for $p < K$. By induction we assume x chosen to satisfy the lemma for $\bar{\bar{\psi}}, \bar{\bar{\chi}}$. Let

$\alpha = \Pi\{p^{k_p}: p < K\}$,

$\beta = \text{l.c.m. } \{f(x): f(x) | g_i(x, y) \text{ occurs in } \psi, \text{ for some } i\}$,

$\gamma = \text{l.c.m. } \{f(x): f(x) \text{ occurs in } \bar{\bar{\psi}}\}$.

Let y_0 be chosen as follows:

(i) y_0 has the specified residue mod α.

(ii) If $p^s | \beta, p^{s+1} \nmid \beta, p \nmid \alpha$ then y_0 satisfies $\psi(x, y)$ mod p^s and each $g_i(x, y_0) \not\equiv 0 \bmod p^{s+1}$.

(iii) If $p|\gamma$ and $p \nmid \alpha\beta$ (p prime) then y_0 is such that $g_i(x, y_0) = h_i(x) + a_i y_0 \not\equiv 0 \bmod p$ for each i.

(iv) y_0 satisfies the inequalities in χ. (Those in $\bar{\bar{\chi}}$ are satisfied by assumption.)

(i) is possible by assumption. (iii) is possible because if $p|\gamma$ and $p \nmid \alpha$ then $p > |a_i|$ for all coefficients a_i occurring in $\psi, p > k >$ the number of g_i's in which y occurs so all the noncongruences in (iii) can be simultaneously satisfied (we see this by a counting argument). The first part of (ii) is possible by the C.R.T. and the fact that ψ and hence $\bar{\bar{\psi}}$ satisfy conditions (a)–(d), and that the solution x of $\bar{\bar{\psi}}$ is as mutually prime as possible. Condition (d) guarantees that if $p^t | \beta, p \nmid \alpha$ and $p^t | f_i$ and $p^t | f_j$ then $p^t | h_{ij}$. The case of primes $p < K$ is taken care of by (i). The second part of (ii) viz. $g_i(x, y_0) \not\equiv 0$ mod p^{s+1} can be taken care of in the same way that (iii) was taken care of. (i), (ii) and (iii) just involve congruences and noncongruences (w.r.t. different primes) and since they can be satisfied separately they can be satisfied simultaneously by arbitrarily large values of y. Choose y_0 large enough to satisfy the inequalities in (iv). We must now show that $\psi(x, y_0)$ has the required mutual primeness.

Suppose that $p \nmid \alpha$ and $p | g_i(x, y_0)$ and $p | g_j(x, y_0)$. Then $p | h_{ij}$ and so $p | \gamma$. But $g_i(x, y_0) \equiv 0 \bmod p$ so by (iii) $p | \beta$. Let $p^s \nmid \beta, p^{s+1} \nmid \beta$. Then if h occurs in $\bar{\bar{\psi}}$ and $p|h, p^s|h$ and $p^{s+1} \nmid h$. Since $p|\beta$, for some $f(x)$ in $\bar{\bar{\psi}}$ $p^s | f(x)$ and $f | g_k(x, y)$ occurs in ψ for some k. Hence $p | h_{ik}$ and hence from the mutual primeness of the solution x of $\bar{\bar{\psi}}, f' | f$ and $f' | h_{ik}$ occur in $\bar{\bar{\psi}}$ for some $f'(x)$ with

$p^s|f'(x)$ (perhaps $f' = f$ or $f' = h_{ik}$ in which case one of these divisibilities is trivial and need not occur). From $f'|f, f|g_k$ and $f'|h_{ik}$ and the fact that ψ is closed under (c) we have $f'|ag_i$ occurs in ψ ($\underline{a}$ is some factor of a_k). Hence $p^s|g_i$. Similarly we have that for some f'' in $\bar{\psi}$, $p^s|f''$ and $f''|bg_i$ occurs in ψ. Hence $p^s|g_j$ and from the mutual primeness of $\bar{\psi}(x)$ there is a f''' in $\bar{\psi}$ such that $p^s|f'''$ and $f'''|f'$ and $f'''|f''$ occur in $\bar{\psi}$. Hence $f'''|ag_i$ and $f'''|bg_i$ occur in ψ (for some a, b). This establishes the mutual primeness of $\psi(x, y_0)$. If $p^s|\beta, p^{s+1}\nmid\beta$ and $p\nmid\alpha$, then we have $f_i(x)|g_i(x, y_0) \bmod p^s$ and $f_i(x) \not\equiv 0 \bmod p^{s+1}$. If $p|\alpha$ then we have $f_i(x)|g_i(x, y_0) \bmod p^{k_p}$ and $f_i(x) \not\equiv 0 \bmod p^{k_p}$. Hence x, y_0 satisfy ψ, χ and the lemma is proved.

Lemma 7. *Let ψ be totally positive increasing, w.r.t. generalized order χ. Then ψ, χ has a solution in* N *if and only if ψ has one* mod $p^{k(p,\psi)}$ (*with all the* $f_i(x) \not\equiv 0 \bmod p^{k(p,\psi)}$) *for all $p \leqslant M_\psi$.*

Proof. One direction is trivial (Lemma 5). The other follows from Lemma 6 by induction. Suppose ψ has such a solution mod $\underline{p}^{k(p,\psi)}$ for $p < M_\psi$. Then it has a solution mod $p^{k(p,\psi)}$ for $p \leqslant M_{\bar{\psi}}$. Then $\bar{\psi}, \bar{\chi}$ has a solution (by induction on the number of variables). Hence $\bar{\psi}$ has a solution which is as mutually prime as possible as in Lemma 6. Hence ψ has a solution by the CRT, and since y occurs only on the right-hand sides of atomic formulas, y can be chosen large enough to satisfy the inequalities in χ.

Let $\phi(x) = \bigwedge_{i=1}^{k} f_i(x)|g_i(x)$ where the $f_i(x)$ and $g_i(x)$ are linear polynomials in $x_1, \ldots, x_n$ with integer coefficients.

Theorem 1. *Let $\phi(x)$ be as above. There is an algorithm for deciding formula of the form $\exists x_{\in \mathbf{N}}\phi(x)$.*

Proof. Lemma 4 shows how to find formulas ϕ_i and generalized orderings χ_i so that ϕ_i is totally positive increasing w.r.t. χ_i and

$$\exists x\phi(x) \leftrightarrow \bigvee_i \exists x(\phi_i(x) \wedge \chi_i(x)).$$

Lemma 7 shows that to decide if $\phi_i(x) \wedge \chi_i(x)$ has a solution it is sufficient to check if ϕ_i has a solution mod $p^{k(p,\psi_i)}$ for $p \leqslant M_{\psi_i}$ with all the $f(x)$'s in $\phi_i \not\equiv 0$.

Using the above ideas, especially Lemma 6 it is not hard to generalize this to get

Theorem 2. *There is an algorithm for deciding formulas of the form $\exists x\Delta(x)$ in* N, *where $\Delta(x)$ is an open formula in the language* $\langle +, |, 0, 1\rangle$.

Proof. Since this seems to have little interest on its own, we leave the details to the reader.

Remarks. (1) §1 shows that the corresponding problems for **Z** instead of **N** are decidable.

(2) Theorem 2 shows that there is no existential definition of multiplication from $+$ and $|$.

(3) It may have been hoped that one could prove that $\exists x_{\in \mathbf{N}}\phi(x)$ if and only if $\phi(x)$ is satisfiable mod p^k for some suitable finite set of prime powers thus giving a result closer in spirit to the CRT. This is not possible for arbitrary ϕ as the following example shows: for each prime power $x + 2|x + 1$ has a solution with $x + 2 \not\equiv 0$, but $x + 2|x + 1$ has no solution in $\mathbf{N}$.

3. In this section we indicate (briefly) how the above algorithm extends to the ring of integers R in an imaginary quadratic extension of the rationals, say $\mathbf{Q}(\alpha)$ with $\alpha^2 = -a$, $a \in \mathbf{N}$.

There are only finitely many units in R–the roots of unity. Our formula ψ will be of the form

$$\bigwedge_i f_i(x) + \alpha h_i(x) | g_i(x) + \alpha k_i(x)$$

where the f_i, h_i, g_i, k_i have coefficients from $\mathbf{Z}$. Using the method of §1 we can reduce this to the case

$$\bigwedge_i f_i(x) \pm \alpha h_i(x) | g_i(x) \pm \alpha k_i(x)$$

where the f_i, h_i, g_i, k_i have coefficients from $\mathbf{N}$. As above, suppose that we have an ordering χ of the variables and suppose that $y > x_i$ for $x_i \in z$ and that

$$f_i(z, y) \pm \alpha h_i(z, y) | g_i(z, y) \pm \alpha k_i(z, y)$$

occurs in ψ with y appearing on the left-hand side. Let $m = \max$ of the coefficients of g_i, k_i. Then $f_i \pm \alpha h_i | g_i \pm \alpha k_i$ implies that $f_i^2 + ah_i^2 | g_i^2 + ak_i^2$ (in $\mathbf{N}$). We also have $y^2 \leqslant f_i^2 + ah_i^2$ and $g_i^2 + ak_i^2 \leqslant m^2n^2ay^2$. So $f_i \pm \alpha h_i | g_i \pm \alpha k_i$ if and only if $c, d_{\in Z}(c^2 + ad^2 \leqslant m^2n^2a$ and $g_i \pm \alpha h_i = (c \pm \alpha d)(f_i \pm \alpha k_i))$. Since there are only finitely many such c's and d's we can rewrite this as a finite disjunction as above (§1).

In this way we can ensure that the largest variable occurs only on the right-hand side of the divisibilities as in §2.

The rest of the algorithm is essentially the same as the above algorithm for the integers, with "prime p" replaced by "prime ideal p" as necessary. We omit the details.

REMARK. The above argument depends heavily on the fact that there are only finitely many units in R (i.e. elements with norm ± 1). We shall show in a subsequent paper that if there are infinitely many units in R (which is true for all proper algebraic extensions except imaginary quadratic ones) then the corresponding problem is unsolvable.

APPENDIX. In this appendix we give a proof of Lemma 1. The results in [1] made the lemma geometrically clear. One could just check that the proof can be made constructive. We shall however give another proof. The proof is by induction on the number of inequalities defining the convex set R and on the number of variables. We need only consider the one case that $R = P_n \cap \{x \in \mathbf{Q}^n: l(x) > 0\}$ since each positive cone is either isomorphic with P_n or of lower dimension.

Let $l(x) = \Sigma a_i x_i - b$, and let $H = \{x \in \mathbf{Q}^n: \Sigma a_i x_i = b\}$, $H^+ = \{x \in \mathbf{Q}^n: \Sigma a_i x_i \geqslant b\}$. Then $R = P_n \cap H^+$. We shall show that there is a finite set of positive cones $C_i = x = A_i u + b_i$ and a finite set of $n - 1$ dimensional convex sets R_i such that

$$IR = \bigcup_i {}^I C_i \cup \bigcup_i {}^I R_i.$$

This will satisfy (i) of the lemma. In order to guarantee that (ii) is satisfied we can replace A_i by $(1/\beta_i)A_i$ for suitable $\beta_i \in \mathrm{N}$ (e.g. β_i = l.c.m. (numerators occurring in A_i, b_i)). Consider three cases. (The proof will be clearer if one draws the corresponding 2 dimensional pictures.)

Case 1. All the $a_i > 0$ (none zero). Consider the cones C_i: $x = u + \alpha_i e_i$ where $\alpha_i = b/a_i$. Then

$$R - \bigcup_i C_i \subset P \cap \{x | x_i < a_i, i = 1, \ldots, n\}$$

which contains only a finite set ($< \Pi_{i=1}^n (a_i + 1)$) of integral points.

Case 2. Not all the $a_i > 0$ and $\underline{0} \in R$ and hence $b \leqslant 0$. Consider the hyperplanes K_j: $\Sigma a_i x_i = b_j$, where b_j varies over all integers between 0 and b which are divisible by $(a_1, \ldots, a_n)$ (= g.c.d. $(a_1, \ldots, a_n)$) (notice that the hyperplane $\Sigma a_i x_i = c$ contains an integral point just exactly when $(a_1, \ldots, a_n)|c$). Let $R' = P \cap \{x: \Sigma a_i x_i \geqslant 0\}$. Then ${}^I R = {}^I R' \cup \bigcup_j^I (K_j \cap R')$ and each $K_j \cap R'$ is a convex polyhedral set of dimension $n - 1$. Let f_i ($i = 1, \ldots, k$) be all the unit vectors with positive entries contained in $H'^+ = \{x: \Sigma a_i x_i \geqslant 0\}$ which are contained in the maximal nonempty intersections of the hyperplanes $\{H_i, i = 1, \ldots, n\} \cup \{H'\}$ where $H_i = \{x \in P_n: x_i = 0\}$ and $H' = \{x \in P_n: \Sigma a_i x_i = 0\}$. Each subset of n of these f_i defines a positive cone in R' and these cones exhaust R'.

Case 3. $0 \not\in R$ and not all the $a_i > 0$. Then for some i_0 βe_{i_0} lies on H for some $\beta > 0$. The e_i are the unit coordinate vectors. Consider the hyperplanes $H_i' = H_i$ for $i \neq i_0$ and $H_{i_0}' = H$, and the half spaces $H_i'^+$. Since $a = (a_1, \ldots, a_n)$ is not a linear combination of the vectors e_i, $i \neq i_0$ (since $a_{i_0} \neq 0$) these half spaces define a new coordinate system $\{f_i, i = 1, \ldots, n\}$ with positive part $P_n' = \{u: f_i \cdot u \geqslant 0, i = 1, \ldots, n\}$. Let $H' = H_{i_0}$ and $H'^+ = H_{i_0}^+$ then $R' = P_n' \cap H'^+$ and $0'$ $(\in P_n') \in R'$ thus reducing this case to Case 2. This completes the proof of the lemma.

Since any n-dimensional positive cone is isomorphic with P_n the lemma applied to the first inequality defining R reduced R to a finite number of similar cases each of which is of lower dimension, or is defined by less inequalities. The desired conclusion now follows by induction on the dimension (n) and the number of inequalities defining R.

References

1. A. J. Goldman, *Resolution and separation theorems for polyhedral convex sets*, Linear Inequalities and Related Systems, Ann. of Math. Studies, no. 38, Princeton Univ. Press, Princeton, N. J., 1956, pp. 41–51. MR **19**, 621.

2. K. Mahler, *On the Chinese remainder theorem*, Math. Nachr. **18** (1958), 120–122. MR **20** #3048.

3. Ju. V. Matijasevič, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 = Soviet Math. Dokl. **11** (1970), 354–358. MR **41** #3390.

4. J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114. MR **11**, 151.

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907

Current address: School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540