ARITHMETICAL DEFINITIONS IN THE RING OF INTEGERS

RAPHAEL M. ROBINSON

1. **Introduction.** A set of integers is said to be arithmetically definable in the ring of integers if there is a formula containing one free variable and any number of bound variables, involving only the concepts of elementary logic and the operations of addition and multiplication, which is satisfied by the integers in the given set and by no other integers. The logical concepts are $\wedge$ (and), $\vee$ (or), $\sim$ (not), $\rightarrow$ (if $\cdots$ then $\cdots$), $\leftrightarrow$ (if and only if), $\wedge$ (for every), $\vee$(there exists), and $=$ (equals). The range of the quantifiers is to be the set of all integers. For convenience, we shall also allow in our formulas symbols for specific integers, such as 1, 0, -1. These could be eliminated if desired.[1]

We shall be concerned in this note mainly with the following question: What is the simplest possible arithmetical definition of the set of natural numbers in the ring of integers? In particular, what is the smallest number of quantifiers which can occur in such a definition?

According to a theorem of Lagrange,

$$x \geqq 0 \leftrightarrow (\vee y)(\vee z)(\vee u)(\vee v)[x = y^2 + z^2 + u^2 + v^2],$$

and this equivalence furnishes a suitable definition containing four quantifiers. Furthermore, it is well known that an integer can be represented as a sum of three squares if and only if it is not negative and not of the form $4^n(8k+7)$. In particular, positive integers of the form $4x+1$ can be so represented. Hence we may use the definition

$$x \geqq 0 \leftrightarrow (\vee y)(\vee z)(\vee u)[4x + 1 = y^2 + z^2 + u^2],$$

which contains but three quantifiers.

A further reduction in the number of quantifiers may be made by using known results concerning the so-called Pell equation. It is well known that the equation $y^2 - az^2 = 1$ has infinitely many solutions for y and z if a is positive but not a square. On the other hand, if $a < 0$ then $y^2 \leqq 1$, and if $a = b^2$ then $y + bz = y - bz = \pm 1$, hence $y = \pm 1$. Thus

$$x \geqq 0 \wedge \sim (\vee y)[x = y^2] \leftrightarrow (\vee y)(\vee z)[y^2 = 1 + xz^2 \wedge y^3 \neq y].$$

Presented to the Society, April 29, 1950; received by the editors April 2, 1950.

[1] For further discussion of arithmetical definability, see Julia Robinson, *Definability and decision problems in arithmetic*, Journal of Symbolic Logic vol. 14 (1949) pp. 98–114, and R. M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. vol. 70 (1951) pp. 137–159.

It follows that

$$x \geqq 0 \leftrightarrow (\forall y)(\forall z)[x = y^2 \vee (y^2 = 1 + xz^2 \wedge y^3 \neq y)].$$

We have thus found a definition of the set of natural numbers using but two quantifiers. Notice that the symbol 1 can be eliminated without increasing the number of quantifiers. Indeed, we have

$$x \geqq 0 \leftrightarrow (\forall y)(\forall z)[x = y^2 \vee (y^3 = y + xyz^2 \wedge y^3 \neq y)].$$

In §2, we prove a result (Theorem 2) concerning the lattice points on an algebraic curve, which shows that the set of natural numbers is not definable in the form $(\forall y)[F(x, y) = 0]$, where $F(x, y)$ is a polynomial with integer coefficients. This depends on a theorem of Skolem, for which we give a simplified proof.[2] Using Theorem 2, we show in §3 that it is impossible to define the set of natural numbers using a single quantifier.

2. **Lattice points on algebraic curves.** If K is a set of positive integers, then we say that K has density zero if for every $\epsilon > 0$ there is an integer N_0 such that for $N \geqq N_0$ there are at most ϵN elements of K which do not exceed N. A similar definition applies to a set of negative integers. A set of positive and negative integers is said to be of density zero if the integers of each sign form a set of density zero.

LEMMA. *Let K be a set of positive integers. If for every positive integer r, the set of values of x for which both x and $x+r$ belong to K has density zero, then K itself has density zero.*

PROOF. Let K_r consist of those elements x of K for which the next integer in K is exactly $x+r$. The sets K_r together exhaust K. By hypothesis, the set K_r has density zero for each r. Given $\epsilon > 0$, choose an integer $s \geqq 2/\epsilon$, and then choose N_0 so that for $N \geqq N_0$ each of the sets $K_1, K_2, \cdots, K_s$ contains at most $\epsilon N/2s$ elements not exceeding N. We may suppose that $N_0 \geqq s(s+1)$. The union of the remaining sets $K_{s+1}, K_{s+2}, \cdots$ contains at most $N/(s+1)+1$ elements not exceeding N, since each element of one of these sets is followed by at least s integers not belonging to K. Thus for $N \geqq N_0$, the set K contains at most

$$s \cdot \frac{\epsilon N}{2s} + \frac{N}{s+1} + 1 \leqq \frac{\epsilon N}{2} + \frac{N}{s} \leqq \epsilon N$$

[2] Theorem 1 below is equivalent to Satz 10 of Th. Skolem's paper, *Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen*, Skrifter utgit av Videnskapsselskapet i Kristiania, 1921, no. 17, 57 pp.

elements not exceeding N.

THEOREM 1 (Skolem). *Suppose that $f(x)$ is an analytic function, but not a polynomial. Then for any branch of $f(x)$ having an algebraic singularity at ∞, the set of positive integers x at which $f(x)$ is an integer has density zero.*

PROOF. The expansion of $f(x)$ near ∞ has the form

$$f(x) = a_p x^{p/q} + \cdots + a_1 x^{1/q} + a_0 + a_{-1} x^{-1/q} + \cdots ,$$

where, in the branch under consideration, we may suppose that the fractional powers of x are positive for $x > 0$. If $p < 0$, then $f(x)$ vanishes at ∞. Thus $f(x)$ cannot assume integer values infinitely often near ∞; otherwise, it would assume the value zero infinitely often near ∞, and would therefore vanish identically. For $p \geqq 0$, we shall prove the theorem by induction in p, with q fixed.

For every positive integer r, $f(x+r)$ has an expansion at ∞ of the same form as that of $f(x)$, and indeed with the same value of the leading coefficient a_p. Thus $f(x+r) - f(x)$ has a similar expansion with the term involving $x^{p/q}$ missing. Furthermore, $f(x+r) - f(x)$ is not a polynomial, since $f(x+r)$ has the same singularities as $f(x)$, but translated a distance r, so that not all the finite singularities can cancel out when the difference $f(x+r) - f(x)$ is formed. Hence, by the inductive hypothesis, the set of positive integers x at which $f(x+r) - f(x)$ is an integer has density zero. Consequently, the set of positive integers x at which both $f(x)$ and $f(x+r)$ are integers has density zero. Applying the lemma, we find that the set of positive integers x at which $f(x)$ is an integer has density zero.

THEOREM 2. *Suppose that $F(x, y)$ is a polynomial with complex coefficients. Then the set K of integers x for which there is an integer y such that $F(x, y) = 0$ consists of the union of certain residue classes for some modulus and a set of density zero.*

PROOF. Suppose first that $F(x, y)$ is irreducible. Then the equation $F(x, y) = 0$ determines y as an algebraic function $f(x)$.

If $f(x)$ is not a polynomial, then the set of positive or negative integers at which a given branch of $f(x)$ is an integer has density zero by Theorem 1. Hence K also has density zero.

If $f(x)$ is a polynomial of the nth degree and assumes integer values at more than n points, then it has rational coefficients by the Lagrange interpolation formula. In this case, let D be the least common denominator of these coefficients. Then $f(x)$ is an integer if and only if $Df(x) \equiv 0 \pmod{D}$, and the truth of this congruence depends only

on the value of x mod D. Thus a polynomial $f(x)$ assumes integer values at only a finite number of points, or for all values of x in certain residue classes for some modulus.

The general result is obtained by factoring $F(x, y)$ into irreducible factors.

3. **Sets which can be defined using one quantifier.** In order to discuss sets of integers which can be defined using formulas containing one quantifier, we must first find what sets of pairs of integers can be defined by formulas containing no quantifiers.

THEOREM 3. *If $\Phi(x, y)$ is a formula containing no quantifiers (and no free variables except x and y), then either $\Phi(x, y)$ or $\sim\Phi(x, y)$ can be reduced to the form*

$$F(x, y) = 0 \wedge (x, y) \notin S,$$

where $F(x, y)$ is a polynomial with integer coefficients, and S is a finite set of ordered pairs of integers.

PROOF. The formula $\Phi(x, y)$ consists of equations combined by the symbols $\wedge$, $\vee$, $\sim$, $\rightarrow$, and $\leftrightarrow$. It may be reduced to disjunctive normal form; that is, we may find an equivalent formula which is a disjunction of conjunctions of equations and inequations.[3] The equations may be written in the form $A(x, y) = 0$ and the inequations in the form $B(x, y) \neq 0$, where $A(x, y)$ and $B(x, y)$ are polynomials with integer coefficients. Notice that $\alpha = 0 \wedge \beta = 0 \leftrightarrow \alpha^2 + \beta^2 = 0$, and $\alpha \neq 0 \wedge \beta \neq 0 \leftrightarrow \alpha\beta \neq 0$. Thus several equations can be combined into one, and similarly for several inequations. Supplying if necessary the equation $0 = 0$ or the inequation $1 \neq 0$, we may suppose that each conjunction contains one equation and one inequation. Thus

$$\Phi(x, y) \leftrightarrow [A_1(x, y) = 0 \wedge B_1(x, y) \neq 0] \vee \cdots \vee [A_s(x, y) = 0 \wedge B_s(x, y) \neq 0],$$

where $A_1(x, y), \cdots, B_s(x, y)$ are polynomials with integer coefficients.

Each term of the disjunction on the right has the form

$$A(x, y) = 0 \wedge B(x, y) \neq 0.$$

If $A(x, y)$ is identically zero, this becomes simply $B(x, y) \neq 0$. Since $\alpha \neq 0 \vee \beta \neq 0 \leftrightarrow \alpha^2 + \beta^2 \neq 0$, the disjunction of any number of such inequations may be written in a similar form.

[3] We use the term inequation for a formula of the form $\alpha \neq \beta$, reserving the term inequality for formulas such as $\alpha < \beta$ or $\alpha > \beta$.

On the other hand, suppose that $A(x, y)$ is not identically zero. We may then omit from $A(x, y)$ any factor also occuring in $B(x, y)$. Thus we may suppose that $A(x, y)$ and $B(x, y)$ are relatively prime. In this case, the equations $A(x, y) = 0$ and $B(x, y) = 0$ have but a finite number of common solutions (even in complex numbers). Thus the condition $B(x, y) \neq 0$ excludes but a finite number of points allowed by $A(x, y) = 0$. Hence the condition $A(x, y) = 0 \wedge B(x, y) \neq 0$ is equivalent to

$$A(x, y) = 0 \wedge (x, y) \notin S,$$

where S is a finite set of ordered pairs (x, y). Using the fact that $\alpha = 0 \vee \beta = 0 \leftrightarrow \alpha\beta = 0$, we readily see that the disjunction of several such conditions reduces to exactly the same form.

Supplying if necessary the equation $1 = 0$ or the inequation $0 \neq 0$, we conclude that

$$\Phi(x, y) \leftrightarrow [A(x, y) = 0 \wedge (x, y) \notin S] \vee B(x, y) \neq 0,$$

where $A(x, y)$ and $B(x, y)$ are polynomials with integer coefficients, and S is a finite set of ordered pairs of integers.

In a similar way,

$$\sim \Phi(x, y) \leftrightarrow [A'(x, y) = 0 \wedge (x, y) \notin S'] \vee B'(x, y) \neq 0,$$

where $A'(x, y)$ and $B'(x, y)$ are also polynomials with integer coefficients, and S' is also a finite set. It follows that

$$(\wedge x)(\wedge y)[B(x, y) = 0 \vee B'(x, y) = 0],$$

since otherwise, for some x and y, we should have both $\Phi(x, y)$ and $\sim\Phi(x, y)$. Hence one or the other of the two polynomials, $B(x, y)$ and $B'(x, y)$, must vanish identically. Omitting the inequation $0 \neq 0$, we have reduced either $\Phi(x, y)$ or $\sim\Phi(x, y)$ to the required form.

THEOREM 4. *Any set of integers defined arithmetically by a formula containing but one quantifier (or more generally, by any formula in which no quantifier occurs within the scope of another quantifier) consists of certain residue classes for some modulus, augmented and diminished by sets of density zero. Thus the set of natural numbers cannot be so defined.*

PROOF. Formulas containing one quantifier (and just one free variable) may be written either in the form $(\vee y)\Phi(x, y)$ or in the form $(\wedge y)\Phi(x, y)$. The sets defined by formulas of the second kind are the complements of those defined by formulas of the first kind. Any set defined by a formula in which no quantifier occurs within the scope of

another is obtained from sets of the above types by taking finite unions and intersections. Thus it is sufficient to prove the theorem for formulas of the form $(\forall y)\Phi(x, y)$, where $\Phi(x, y)$ is a formula containing no quantifiers.

We now apply Theorem 3. If

$$\Phi(x, y) \leftrightarrow F(x, y) = 0 \wedge (x, y) \notin S$$

then

$$(\forall y)\Phi(x, y) \leftrightarrow (\forall y)[F(x, y) = 0] \wedge x \notin S_0,$$

where S_0 is a finite set of integers. By Theorem 2, this formula defines a set consisting of certain residue classes for some modulus, augmented by a set of density zero, and diminished by a finite set.

On the other hand, if

$$\sim \Phi(x, y) \leftrightarrow F(x, y) = 0 \wedge (x, y) \notin S,$$

then $(\forall y)\Phi(x, y)$ holds for all values of x with a finite number of exceptions, unless $F(x, y)$ vanishes identically, in which case it holds for only a finite number of values of x. Thus we obtain only finite sets and their complements.

Combining the results of the two cases, we see that every set definable by a formula $(\forall y)\Phi(x, y)$, where $\Phi(x, y)$ contains no quantifiers, consists of certain residue classes for some modulus, augmented by a set of density zero and diminished by a finite set.

UNIVERSITY OF CALIFORNIA, BERKELEY