EXISTENTIAL DEFINABILITY IN ARITHMETIC

BY

JULIA ROBINSON

1. **Introduction.** A relation $\rho(x_1, \cdots, x_n)$ among natural numbers is said to be *arithmetically definable* if there is a formula containing the free variables $x_1, \cdots, x_n$, any number of bound variables, and symbols for particular natural numbers, involving only the mathematical symbols $+$ and $\cdot$, and the logical symbols: $\bigwedge$ (for every), $\bigvee$ (there exists), $\wedge$ (and), $\vee$ (or), $\sim$ (not), and $=$ (equals), which holds if and only if the relation $\rho(x_1, \cdots, x_n)$ is satisfied.

A relation $\rho(x_1, \cdots, x_n)$ is said to be *existentially definable* if there is a formula of the type described above which does not contain either of the logical symbols $\bigwedge$ or $\sim$. We shall consider the existential definability of certain relations, e.g. $x=y^z$, $x=y!$, and "x is a prime," which are known to be arithmetically definable by a general theorem of Gödel (see §6)(1).

It can easily be seen that a relation $\rho(x_1, \cdots, x_n)$ is existentially definable if and only if there is a polynomial $P(x_1, \cdots, x_n, u_1, \cdots, u_k)$ with (positive or negative) integer coefficients such that

$$\rho(x_1, \cdots, x_n) \leftrightarrow \bigvee_{u_1, \cdots, u_k} P(x_1, \cdots, x_n, u_1, \cdots, u_k) = 0.$$

Thus, a set of natural numbers is existentially definable if and only if it is the set of values of a parameter for which a certain diophantine equation is solvable in natural numbers.

Solving the diophantine equation $P(x)=0$ in integers is equivalent to solving $P(x)P(-x)=0$ in natural numbers. Also solving $P(x)=0$ in natural numbers is equivalent to solving $P(u^2+v^2+w^2+z^2)=0$ in integers. Hence we see that sets of natural numbers which are existentially definable are also existentially definable if we allow the variables to range over the integers.

A simple example of an existentially definable set is the set of perfect squares. The complementary set is also existentially definable, since

$$\sim \bigvee_y x = y^2 \leftrightarrow \bigvee_{u,v,w} [(u^2 + v + 1 = x \wedge (u+1)^2 = x + w + 1)].$$

The tenth problem in Hilbert's famous list is to find an effective method for deciding if a given diophantine equation is solvable. Since there are many classical diophantine equations with one parameter for which no effective

Presented to the International Congress of Mathematicians, September 4, 1950; received by the editors March 30, 1951.

(1) Professor Alfred Tarski suggested the study of existentially definable relations to me.

method is known to determine the solvability for an arbitrary value of the parameter, it is very unlikely that a decision procedure can be found. For example, no way is known to determine the values of a for which the diophantine system,

$$x^2 + ay^2 = s^2, \qquad x^2 - ay^2 = t^2,$$

is solvable. (This problem was first studied by the Arabs in the Middle Ages.) If there is some non-recursive set which is existentially definable, then we could conclude that there is no effective method for determining the solvability of an arbitrary diophantine equation.

A relation $\rho(x_1, \cdots, x_n)$ is said to be existentially definable in terms of the relations $\phi_1, \cdots, \phi_k$ if there is a defining formula of the type described in the definition of existential definability except that it may also contain the relations $\phi_1, \cdots, \phi_k$. Clearly, if ρ is existentially definable in terms of certain existentially definable relations, then ρ itself is existentially definable.

The main result of this paper is that the relation $x=y^z$ is existentially definable in terms of any relation of roughly exponential growth. Let the "nth super power of x," $x*n$, be defined recursively by

$$x*0 = 1, \quad x*(n+1) = x^{(x*n)}.$$

We shall prove that the relation $x=y^z$ is existententially definable in terms of any relation $\phi(u, v)$ such that

$$\bigvee_n \bigwedge_{u,v} [\phi(u, v) \rightarrow v < u*n], \tag{1.1}$$

and

$$\sim \bigvee_n \bigwedge_{u,v} [\phi(u, v) \rightarrow v < u^n]. \tag{1.2}$$

It is not known whether any ϕ satisfying these conditions is existentially definable. At present, very little is known about the size of solutions of diophantine equations with a finite number of solutions. However, it seems to me very likely that some such relation ϕ is existentially definable. If this is the case, then we could conclude that $x=y^z$ is existentially definable. In particular, this would mean that there is a polynomial $P(x, y, z, n, u_1, \cdots, u_k)$ with integer coefficients such that

$$x^n + y^n = z^n \leftrightarrow \bigvee_{u_1, \cdots, u_k} P(x, y, z, n, u_1, \cdots, u_k) = 0.$$

In other words, we could reduce Fermat's equation (or any exponential equation) to a polynomial equation in more variables. On the other hand, if it should be shown that $x=y^z$ is not existentially definable, then we could conclude that no relation satisfying (1.1) and (1.2) is existentially definable.

Various properties of solutions of the Pell equation $x^2-(a^2-1)y^2=1$ are

listed in §2. These are needed in §§3 and 4. §3 contains the main result of the paper. In §4, we show that $x=y^z$ is existentially definable in terms of the relation x Pow y (x is a power of y). It is not known whether Pow is existentially definable or not. However we show that the relation $\sim x$ Pow y is existentially definable. In §5, we investigate existential definability in terms of exponentiation. The relations $x=y!$ and "x is a prime" are shown to be existentially definable in terms of exponentiation. In §6, there is a discussion of the relation of recursive enumerability and existential definability.

2. **Pell's equation.** In this section, we give various lemmas concerning solutions of the equation $x^2-(a^2-1)y^2=1$ in natural numbers. The first lemma is a special case of the well known theorem on Pell's equation, $x^2-ay^2=1$. [See Landau, *Vorlesungen über Zahlentheorie*, vol. 1, pp. 57–64.] The remaining lemmas can be proved easily. In all of the lemmas, a is any natural number greater than 1 and the other free variables are any natural numbers.

LEMMA 1.

$$x^2-(a^2-1)y^2=1 \leftrightarrow \bigvee_n x + y(a^2-1)^{1/2} = (a+(a^2-1)^{1/2})^n.$$

LEMMA 2. *If a_n and a_n' are defined by the equation*

$$a_n + a_n'(a^2-1)^{1/2} = (a+(a^2-1)^{1/2})^n,$$

then

$$a_0 = 1, \qquad a_0' = 0,$$
$$a_1 = a, \qquad a_1' = 1,$$
$$a_{n+2} = 2a\cdot a_{n+1} - a_n, \qquad a_{n+2}' = 2a\cdot a_{n+1}' - a_n'.$$

LEMMA 3. $a_{n+1}=a\cdot a_n+a_n'(a^2-1)$.

LEMMA 4. $a^n \leqq a_n \leqq (2a)^n$. *The equality holds on the right only for $n=0$.*

LEMMA 5. $a_n-a_n'(a-y)\equiv y^n \pmod{2ay-y^2-1}$.

This follows easily by induction from Lemma 2.

LEMMA 6.

$$a_n = \sum_{k=0,\ k \text{ even}}^{n} \binom{n}{k} a^{n-k}(a^2-1)^{k/2}$$

and

$$a_n' = \sum_{k=1,\ k \text{ odd}}^{n} \binom{n}{k} a^{n-k}(a^2-1)^{(k-1)/2}.$$

LEMMA 7.

$$a_n' \equiv na^{n-1} \pmod{a^2 - 1},$$

hence

$$a_n' \equiv n \pmod{a - 1}.$$

This follows immediately from Lemma 6.

LEMMA 8. *Let $\psi(a, u)$ be the relation defined by the following equivalence,*

$$\psi(a, u) \leftrightarrow \bigvee_{x,y} [x^2 - (a^2 - 1)(a - 1)^2y^2 = 1 \wedge x > 1 \wedge a > 1 \wedge u = ax].$$

Then

$$\psi(a, u) \rightarrow u \geqq a^a$$

and

$$a > 1 \rightarrow \bigvee_{u} (\psi(a, u) \wedge u < a^{2a}).$$

Proof. By Lemma 7, $u = ax \geqq a \cdot a_{a-1}$. Hence we obtain the first conclusion by Lemma 4. On the other hand, $u = a \cdot a_{a-1}$ satisfies $\psi(a, u)$ and by Lemma 4, $a \cdot a_{a-1} \leqq a \cdot (2a)^{a-1} < a^{2a}$.

LEMMA 9. *If $x > 1$ and $a > x^n$, then*

$$a_n x^n \leqq (ax)_n < a_n(x^n + 1).$$

Proof. By Lemma 6,

$$a_n x^n = \sum_{k=0,\ k \text{ even}}^{n} \binom{n}{k} (ax)^{n-k}(a^2x^2 - x^2)^{k/2}$$

and

$$(ax)_n = \sum_{k=0,\ k \text{ even}}^{n} \binom{n}{k} (ax)^{n-k}(a^2x^2 - 1)^{k/2}.$$

Hence $a_n x^n \leqq (ax)_n$. Also,

$$(ax)_n/(a_n x^n) \leqq \{(a^2x^2 - 1)/(a^2x^2 - x^2)\}^{n/2} \leqq (1 - 1/a^2)^{-n},$$

and

$$(1 - 1/a^2)^n > 1 - n/a^2 > 1 - 1/a \geqq 1 - 1/(x^n + 1).$$

Therefore,

$$a_n x^n \leqq (ax)_n < a_n(x^n + 1).$$

LEMMA 10. *If $x > 1$ and $a > x^n$, then*

$$a_n \leqq (ax)_m \leqq a \cdot a_n \leftrightarrow m = n.$$

Proof. From Lemma 9 and $a > x^n$, we have

$$a_n \leqq (ax)_n \leqq a \cdot a_n.$$

Since $(ax)_m$ is an increasing function of m, it is sufficient to show that

$$(ax)_{n-1} < a_n$$

and

$$(ax)_{n+1} > a \cdot a_n.$$

Applying Lemma 9 with n replaced by $n-1$, we obtain

$$(ax)_{n-1} < a \cdot a_{n-1} \leqq a_n.$$

Also,

$$(ax)_{n+1} > ax \cdot (ax)_n > a \cdot a_n.$$

3. **Exponentiation.** In this section, we shall show that the relation $x = y^z$ is existentially definable in terms of any relation of roughly exponential growth.

LEMMA. *There is an existential definition of a relation* $\rho(x, y)$ *satisfying*

$$\rho(x, y) \rightarrow y < x^x \tag{3.1}$$

and

$$\sim \bigvee_n \bigwedge_{x,y} (\rho(x, y) \rightarrow y < x^n), \tag{3.2}$$

in terms of any relation $\phi(u, v)$ *satisfying* (1.1) *and* (1.2).

Proof. Case 1. There is a k such that $\phi(u, v) \rightarrow v < u^{ku}$. Clearly, if we let ρ be defined by the equivalence:

$$\rho(x, y) \leftrightarrow \bigvee_v (\phi(x, v) \wedge y^k \leqq v),$$

then $\rho(x, y)$ satisfies (3.1) and (3.2).

Case 2. $\phi(u, v) \rightarrow v < u * n$ and there is no k such that $\phi(u, v) \rightarrow v < u^{ku}$. In this case, we shall show that we can define existentially in terms of ϕ, a relation $\phi_1(u, v)$ such that

$$\phi_1(u, v) \rightarrow v < u * (n - 1) \tag{3.3}$$

and

$$\sim \bigvee_m (\phi_1(u, v) \rightarrow v < u^m). \tag{3.4}$$

Then, either ϕ_1 satisfies the condition of Case 1 or, by Case 2, we can define ϕ_2 satisfying

$$\phi_2(u, v) \rightarrow v < u * (n - 2)$$

and

$$\sim \bigvee_m (\phi_2(u, v) \rightarrow v < u^m).$$

By continuing this process, we must eventually obtain a relation ϕ_r satisfying the condition of Case 1. Hence a relation ρ satisfying (3.1) and (3.2) can be existentially defined in terms of a relation ϕ satisfying (1.1) and (1.2).

It remains to prove that given ϕ satisfying the conditions of Case 2, we can define existentially in terms of ϕ a relation ϕ_1 satisfying (3.3) and (3.4). Let ϕ_1 be defined by the equivalence

$$\phi_1(u, v) \leftrightarrow \bigvee_a [\psi(a, u) \wedge \phi(a, v)],$$

where ψ is the relation of Lemma 8. Clearly, $\phi_1(u, v) \rightarrow v < u * (n-1)$, since $\psi(a, u) \rightarrow u \geqq a^a$ and $\phi(a, v) \rightarrow v < a * n < (a^a) * (n-1) \leqq u * (n-1)$. Also, there is no m with $\phi_1(u, v) \rightarrow v < u^m$, since for each m, there exist a, u, and v such that

$$\phi(a, v) \wedge v \geqq a^{2ma}$$

and

$$\psi(a, u) \wedge u < a^{2a},$$

so that $v \geqq (a^{2a})^m > u^m$. This completes the proof of the lemma.

We now turn to the proof of our main result. We wish to show that the relation $x = y^z$ can be defined existentially in terms of any relation ϕ satisfying (1.1) and (1.2). In view of the lemma, it is sufficient to show that $x = y^z$ can be defined existentially in terms of any relation ρ satisfying (3.1) and (3.2).

By Lemma 9, we have

$$(3.5) \quad (y > 1 \wedge a > y^z) \rightarrow [x = y^z \leftrightarrow a_z x \leqq (ay)_z < a_z(x + 1)].$$

Furthermore, by Lemma 10,

$$(3.6) \quad \begin{aligned} &(y > 1 \wedge a > y^z) \\ &\quad \rightarrow [u = (ay)_z \leftrightarrow \bigvee_v (u^2 - (a^2y^2 - 1)v^2 = 1 \wedge a_z \leqq u \leqq a \cdot a_z)]. \end{aligned}$$

Hence,

$$(3.7) \quad \begin{aligned} &(1 < x < a \wedge y > 1 \wedge a > y^z) \\ &\quad \rightarrow [x = y^z \leftrightarrow \bigvee_{u,v} \{u^2 - (a^2y^2 - 1)v^2 = 1 \wedge a_z x \leqq u < a_z(x + 1)\}]. \end{aligned}$$

We can replace the requirement $a > y^z$ in the hypothesis of (3.7) by the stronger condition

$$\bigvee_{b,c} [b > y \wedge b > z \wedge a > c \wedge \psi(b, c)],$$

where ψ is the existentially definable relation of Lemma 8. Hence from (3.7) we can obtain an existential definition of $x = y^z$ in terms of the relation $r = a_z$, namely,

$$\begin{aligned} x = y^z \leftrightarrow [&(z = 0 \wedge x = 1) \vee (z > 0 \wedge y < 2 \wedge x = y) \\ &\vee (y > 1 \wedge x > 1 \wedge z > 0 \wedge \bigvee_{a,b,c,u,v} \{x < a \wedge b > y \wedge b > z \\ &\wedge a > c \wedge \psi(b, c) \wedge u^2 - (a^2y^2 - 1)v^2 = 1 \wedge a_z x \leqq u < a_z(x + 1)\})]. \end{aligned} \tag{3.8}$$

Consequently, it would be sufficient to give an existential definition of the relation $r = a_z$ in order to obtain an existential definition of $x = y^z$. But at present I am unable to do exactly this. However, by Lemma 7,

$$\begin{aligned} &(1 < r < a_a \wedge 0 < z < a) \\ &\qquad \rightarrow [r = a_z \leftrightarrow \bigvee_{s} r^2 - (a^2 - 1)(z + s(a - 1))^2 = 1]. \end{aligned} \tag{3.9}$$

Here we see how we can make use of ρ. In order that (3.9) can be used to define $r = a_z$, we must limit the size of r. This can be done by means of ρ (for some values of a). Namely,

$$[r \leqq d \wedge \rho(a, d)] \rightarrow r < a^a < a_a.$$

On the other hand, there are infinitely many values of a for which there is a d satisfying $\rho(a, d) \wedge d > a_z$. Fortunately, in (3.8), we need only define a_z for a sufficiently large value of a. Hence we obtain

$$\begin{aligned} &(x > 1 \wedge y > 1 \wedge z > 0) \rightarrow \\ &[x = y^z \leftrightarrow \bigvee_{a,b,c,d,u,v,r,s} \{x < a \wedge b > y \wedge b > z \wedge \psi(b, c) \\ &\wedge r > 1 \wedge a > c \wedge r \leqq d \wedge \rho(a, d) \wedge u^2 - (a^2y^2 - 1)v^2 = 1 \\ &\wedge rx \leqq u < r(x + 1) \wedge r^2 - (a^2 - 1)(z + s(a - 1))^2 = 1\}]. \end{aligned}$$

Therefore, $x = y^z$ is existentially definable in terms of any relation ρ satisfying (3.1) and (3.2). Consequently, it is existentially definable in terms of any relation ϕ satisfying (1.1) and (1.2).

4. **Powers and non-powers.** We shall show first that exponentiation can be defined in terms of the relation x Pow y. Let $R(a, b, c, d)$ be the relation which holds if and only if $b > 1$, $d > 1$, and there is an n, such that $a = b^n$ and $c = d^n$. We shall show that R is existentially definable in terms of Pow and, then, that $x = y^z$ is existentially definable in terms of R. The following equivalence gives an existential definition of R in terms of Pow:

$$R(a, b, c, d) \leftrightarrow \{b > 1 \wedge d > 1 \wedge a \text{ Pow } b \wedge c \text{ Pow } d$$
$$\wedge \bigvee_e [e \text{ Pow } (bd + 1) \wedge ae \text{ Pow } b(bd + 1)$$
$$\wedge ce \text{ Pow } d(bd + 1)]\}. \tag{4.1}$$

If $b>1$, $d>1$, $a=b^n$, and $c=d^n$, then $e=(bd+1)^n$ satisfies the right side of the equivalence. If the right side holds, then there are k, l, m, s, and t so that $a=b^k$, $c=d^l$, $e=(bd+1)^m$, $ae=\{b(bd+1)\}^s$, and $ce=\{d(bd+1)\}^t$. Hence

$$ae = b^k(bd + 1)^m = b^s(bd + 1)^s,$$
$$ce = d^l(bd + 1)^m = d^t(bd + 1)^t.$$

Therefore, all the exponents are equal and $R(a, b, c, d)$ holds.

Now, notice that if $u=2^z$, then

$$u + z \leqq u(u + 1)^z/u^z \leqq u + z + (2^z - 1)/2^z < u + z + 1. \tag{4.2}$$

This inequality provides a way to determine the exponent corresponding to a given power of y. Thus,

$$x = y^z \leftrightarrow \{(z = 0 \wedge x = 1) \vee (y = 0 \wedge z > 0 \wedge x = 0)$$
$$\vee (y = 1 \wedge x = 1) \vee (y > 1 \wedge \bigvee_{u,v,w} [R(u, 2, x, y)$$
$$\wedge R(v, u, x, y) \wedge R(w, u + 1, x, y)$$
$$\wedge v(u + z) \leqq uw < v(u + z + 1)]\}. \tag{4.3}$$

Clearly, if $x=y^z$, the right side is satisfied by (4.2). Suppose that the right side holds, then x Pow y, say $x=y^t$. It remains to show that $t=z$. But by (4.2), $v(u+t)\leqq uw<v(u+t+1)$. By hypothesis,

$$v(u + z) \leqq uw < v(u + z + 1),$$

hence $t=z$. Since R is existentially definable in terms of Pow, we have shown that $x=y^z$ is existentially definable in terms of Pow.

I have been unable to find an existential definition of the set of powers of 2. However some sets of logarithmic density can be defined existentially. For example, let T be the set of values of x for which the equation $x^2-3y^2=1$ is solvable. Then, by Lemma 1, elements of T are roughly powers of $(2+3^{1/2})$.

There is a simple existential definition of the set of natural numbers which are not power of 2, namely,

$$\sim x \text{ Pow } 2 \leftrightarrow \bigvee_{u,v} x = (2u + 3)v.$$

It is not so easy to give an existential definition of the non-powers of 6. However, we shall now give an existential definition of the relation $\sim x$ Pow y.

Let x Pow y (mod z) be the relation which holds if and only if there exists an n such that $x \equiv y^n \pmod{z}$. We first check the following formula,

$$(4.4)\quad \begin{aligned}&(x > 1 \wedge y > 1 \wedge y \mid x)\\ &\to \{\sim x \text{ Pow } y \leftrightarrow \bigvee_{u,v} (u \text{ Pow } y \pmod{x-1} \wedge v \text{ Pow } y \pmod{x-1}\\ &\wedge 0 < u < v < yu \wedge v < x)\}.\end{aligned}$$

Here $y \mid x$ (y divides x) is existentially definable, since

$$y \mid x \leftrightarrow \bigvee_{u} x = yu.$$

Suppose $x>1 \wedge y>1 \wedge y \mid x \wedge \sim x$ Pow y. Choose n so that $y^n < x < y^{n+1}$. Then there are v and k so that $y^{n+1} = v + k(x-1)$ with $0 \leqq v < x-1$ and $0 < k \leqq y$. By using divisibility arguments, we see that actually $1 < v < x-1$, $0 < k < y$, $y \nmid v$. Hence v is not a power of y, so there is an l with $y^l < v < y^{l+1}$. Let $u = y^l$. Then for this u and v, the right side of the equivalence in (4.4) is satisfied.

Suppose $x>2 \wedge y>1 \wedge y \mid x \wedge x$ Pow y. If $z<x$, then z Pow y (mod $x-1$) if and only if z Pow y. Hence the right side of the equivalence in (4.4) does not hold. The case $x=2$ and $y=2$ can be treated separately. Thus (4.4) is verified.

We shall now show that the relation u Pow v (mod m) is existentially definable provided v and m are relatively prime. From Lemma 5, we have for $a>1$,

$$u \text{ Pow } v \pmod{2av - v^2 - 1} \leftrightarrow$$
$$\bigvee_{x,y,r} [x^2 - (a^2-1)y^2 = 1 \wedge u = x - y(a - v) \pm r(2av - v^2 - 1)].$$

Now if $(m, v) = 1$, i.e. m and v are relatively prime, then there is an $a>1$ such that $m \mid (2av - v^2 - 1)$. Hence

$$(u \text{ Pow } v \pmod{m} \wedge (m, v) = 1) \leftrightarrow$$
$$\bigvee_{a,w,k} [a > 1 \wedge w \text{ Pow } v \pmod{2av - v^2 - 1} \wedge m \mid (2av - v^2 - 1) \wedge u = w + km].$$

Finally, we give an existential definition of the relation $\sim x$ Pow y,

$$(4.5)\quad \begin{aligned}\sim x \text{ Pow } y \leftrightarrow [&(x = 0 \wedge y > 0) \vee (x > 1 \wedge y \nmid x)\\ &\vee (x > 1 \wedge y = 1)\\ &\vee (x > 1 \wedge y > 1 \wedge y \mid x \wedge \sim x \text{ Pow } y)].\end{aligned}$$

The relation $x \nmid y$ is existentially definable since

$$x \nmid y \leftrightarrow \bigvee_{u,v} (y = ux + v \wedge 0 < v < x).$$

Hence we see that each of the alternatives in (4.5) is existentially definable, so the relation $\sim x$ Pow y is existentially definable.

5. **Existential definability in terms of exponentiation.** We shall show that the relations $r=\binom{n}{k}$, $y=x!$, and "p is a prime" are all existentially definable in terms of exponentiation.

In order to see that $r=\binom{n}{k}$ is existentially definable in terms of exponentiation, we first establish the following identity:

$$\binom{n}{k} = [2^{nk}(1+2^{-n})^n] - 2^n[2^{n(k-1)}(1+2^{-n})^n] \qquad \text{for } n,\ k>0. \tag{5.1}$$

If $0<k\leqq n$, then

$$2^{nk}(1+2^{-n})^n = 2^{nk}\sum_{\nu=0}^{n}\binom{n}{\nu}2^{-n\nu} < \sum_{\nu=0}^{k}\binom{n}{\nu}2^{n(k-\nu)} + (2^n-1)/2^n.$$

Hence

$$[2^{nk}(1+2^{-n})^n] = \sum_{\nu=0}^{k}\binom{n}{\nu}2^{n(k-\nu)}.$$

Similarly,

$$2^n[2^{n(k-1)}(1+2^{-n})^n] = \sum_{\nu=0}^{k-1}\binom{n}{\nu}2^{n(k-\nu)}.$$

Thus, we see that (5.1) holds provided that $0<k\leqq n$. It can be readily verified in the remaining cases.

From (5.1), we obtain the following existential definition of the binomial coefficient in terms of exponentiation (and less than):

$$\begin{aligned} r=\binom{n}{k} \leftrightarrow \{&(n=0 \wedge k>0 \wedge r=0) \vee (k=0 \wedge r=1) \\ &\vee (n>0 \wedge k>0 \wedge \bigvee_{u,v}(r=u-2^nv \\ &\wedge 2^{n^2}u \leqq 2^{nk}(1+2^n)^n < 2^{n^2}(1+u) \\ &\wedge 2^{n^2}v \leqq 2^{n(k-1)}(1+2^n)^n < 2^{n^2}v)\}. \end{aligned} \tag{5.2}$$

Next we show that the relation $y=x!$ is existentially definable in terms of exponentiation and the binomial coefficient. In fact,

$$x! = \left[r^x \Big/ \binom{r}{x}\right] \qquad \text{for any } r>(2x)^{x+1}. \tag{5.3}$$

The following chain of inequalities will establish (5.3) for $x>0$. In deriving them, we use the elementary inequalities,

$$1/(1-\theta) < 1+2\theta \qquad \text{for } 0<\theta<1/2,$$

$$(1+\theta)^x < 1+2^x\theta \qquad \text{for } 0<\theta<1.$$

$$r^x \Big/ \binom{r}{x} = x! \Big/ \left\{\left(1-\frac{1}{r}\right)\left(1-\frac{2}{r}\right)\cdots\left(1-\frac{x-1}{r}\right)\right\}$$

$$< x! \Big/ \left(1-\frac{x}{r}\right)^x < x!\left(1+\frac{2x}{r}\right)^x$$

$$< x!(1+2^x\cdot 2x/r) < x!+1 \qquad \text{for } r > (2x)^{x+1}.$$

The existential definition of the relation $y=x!$ in terms of exponentiation can be written down easily from (5.2) and (5.3).

Finally, to see that the set of primes is existentially definable in terms of exponentiation, we use the fact that p is a prime if and only if $p>1$ and p is relatively prime to $(p-1)!$. Hence

$$(5.4) \qquad \begin{aligned} &\sim \bigvee_{x,y}[p=(x+2)(y+2) \vee p=0 \vee p=1] \\ &\leftrightarrow \bigvee_{u,v}[pu+(p-1)!v=1 \wedge p>1]. \end{aligned}$$

6. **Recursively enumerable relations.** In this section, we shall discuss some results concerning recursively enumerable relations. (It is assumed that the reader is familiar with this concept. For a good account of the theory together with references to earlier papers, see Kleene [3].)

Gödel [2, p. 191] proved that every primitive recursive relation is arithmetically definable. Hence all recursively enumerable relations are arithmetically definable. All of the relations which we have considered are primitive recursive relations and, so, arithmetically definable.

Clearly, every existentially definable relation is recursively enumerable. It is not known whether the converse is true. Davis [1] has shown that every recursively enumerable relation $\phi(x_1, \cdots, x_n)$ can be put in the form

$$(6.1) \qquad \bigvee_u \bigwedge_{v\leqq u} \rho(x_1, \cdots, x_n, u, v)$$

where ρ is an existentially definable relation. (Here the inequality under the quantifier restricts the variable, thus

$$\bigwedge_{v\leqq u}\phi \leftrightarrow \bigwedge_v [v\leqq u \rightarrow \phi], \qquad \bigvee_{v\leqq u}\phi \leftrightarrow \bigvee_v [v\leqq u \wedge \phi].)$$

We shall show that ρ can also be taken to be primitive recursive. Let ϕ be written in the form (6.1),

$$\phi(x_1, \cdots, x_n) \leftrightarrow \bigvee_u \bigwedge_{v\leqq u} \bigvee_{y_1,\cdots,y_k} P(x_1, \cdots, x_n, u, v, y_1, \cdots, y_k) = 0.$$

Then

$$\phi(x_1, \cdots, x_n) \leftrightarrow \bigvee_{u,s} \bigwedge_{v \leqq u} \bigvee_{y_1, \cdots, y_k \leqq s} P = 0.$$

The relation

$$\bigvee_{y_1, \cdots, y_k \leqq s} P = 0$$

is primitive recursive as well as existentially definable, since Gödel [2, p. 180] proved that if, in an arithmetical definition of a given relation, all of the bound variables are bounded by primitive recursive functions, then the relation is primitive recursive. Also,

$$\bigvee_{u,s} \bigwedge_{v \leqq u} \bigvee_{y_1, \cdots, y_k \leqq s} P = 0 \leftrightarrow \bigvee_{z} \bigwedge_{v \leqq z} \{ \bigvee_{u,s \leqq z} \bigvee_{y_1, \cdots, y_k \leqq s} [z = (u + s)^2 + u \wedge (P = 0 \vee v > u)] \}.$$

Here we use the fact that the function $(u+s)^2+u$ is univalent. The expression in braces is both primitive recursive and existentially definable. Hence every recursively enumerable relation can be expressed in the form (6.1) where ρ is an existentially definable primitive recursive relation.

The complement of an existentially definable relation is not necessarily existentially definable, for otherwise every arithmetically definable relation would also be existentially definable and hence recursively enumerable, which is not the case(2). However if the complement of every existentially definable primitive recursive relation is existentially definable, then every recursively enumerable relation is existentially definable. To see this, let ϕ be put in the form (6.1) with ρ a primitive recursive existentially definable relation. Then,

$$\phi(x_1, \cdots, x_n) \leftrightarrow \bigvee_{u} \sim \bigvee_{v \leqq u} \sim \rho(x_1, \cdots, x_n, u, v).$$

By hypothesis $\sim\rho$ is existentially definable and primitive recursive. Hence

$$\bigvee_{v \leqq u} \sim \rho$$

is existentially definable and primitive recursive. Consequently,

$$\sim \bigvee_{v \leqq u} \sim \rho$$

is existentially definable. Therefore ϕ is existentially definable.

Several years ago, Tarski proved that the complement of every set of the form

$$\bigvee_{u} P(x, u) = 0$$

(2) I am indebted to Martin Davis for pointing this out to me.

is existentially definable. (Here P is a polynomial with integer coefficients. In this theorem, it will be more convenient to let the variables range over the integers instead of the natural numbers.) Since this result has not been published, we shall sketch the proof.

THEOREM (TARSKI). *Let* $P(x)=a_nx^n+\cdots+a_0$ *be a polynomial and let* $\phi(a_0, \cdots, a_n)$ *be the relation which holds if and only if* $P(x)=0$ *has an integral root, i.e.*

$$\phi(a_0, \cdots, a_n) \leftrightarrow \bigvee_x a_nx^n + \cdots + a_0 = 0.$$

Then the relation $\sim\phi$ *is also existentially definable.*

Proof. From Tarski's generalization of Sturm's theorem (see [4, p. 51]), it is possible to give a system $\mathfrak{S}(a_0, \cdots, a_n, b, c)$ of inequalities and equations with integer coefficients such that there is no real root of $P=0$ in the closed interval $\langle b, c\rangle$, if and only if $\mathfrak{S}(a_0, \cdots, a_n, b, c)$. We see that for integral $a_0, \cdots, a_n, b$, and $c, \mathfrak{S}(a_0, \cdots, a_n, b, c)$ is an existentially definable relation among integers. If $b=-\infty$ or $c=+\infty$, then the corresponding $\mathfrak{S}$ is still existentially definable. The following equivalence gives an existential definition of the relation $\sim\phi$,

$$\begin{aligned}\sim\phi(a_0, \cdots, a_n) \leftrightarrow \bigvee_{r_1, \cdots, r_n} [&\mathfrak{S}(a_0, \cdots, a_n, -\infty, r_1)\\ &\wedge \mathfrak{S}(a_0, \cdots, a_n, r_1+1, r_2) \wedge \cdots\\ &\wedge \mathfrak{S}(a_0, \cdots, a_nr_{n-1}+1, r_n)\\ &\wedge \mathfrak{S}(a_0, \cdots, a_n, r_n+1, +\infty)].\end{aligned}$$

To see that this is a valid equivalence, notice that:

(1) Every integer is included in one of the closed intervals in which there are no real solutions.

(2) Since there are not more than n real roots, these can be isolated in the n open intervals, (r_i, r_{i+1}) with $i=1, \cdots, n$.

BIBLIOGRAPHY

1. M. Davis, *Arithmetical problems and recursively enumerable predicates* (abstract), Journal of Symbolic Logic vol. 15 (1950) pp. 77–78.

2. K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* I, Monatshefte für Mathematik und Physik vol. 38 (1931) pp. 173–198.

3. S. C. Kleene, *Recursive predicates and quantifiers*, Trans. Amer. Math. Soc. vol. 53 (1943) pp. 41–73.

4. A. Tarski, *A decision method for elementary algebra and geometry*, Rand Corporation, Santa Monica, Calif., 1948. Reprinted by the University of California Press, Berkeley, Calif., 1951.

BERKELEY, CALIF.