DIOPHANTINE REPRESENTATION OF THE SET OF PRIME NUMBERS

JAMES P. JONES, DAIHACHIRO SATO, HIDEO WADA AND DOUGLAS WIENS

1. Introduction. Martin Davis, Yuri Matijasevič, Hilary Putnam and Julia Robinson [4] [8] have proven that every recursively enumerable set is Diophantine, and hence that the set of prime numbers is Diophantine. From this, and work of Putnam [12], it follows that the set of prime numbers is representable by a polynomial formula. In this article such a prime representing polynomial will be exhibited in explicit form. We prove (in Section 2)

THEOREM 1. *The set of prime numbers is identical with the set of positive values taken on by the polynomial*

$$(1)\quad (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2$$
$$-[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2$$
$$-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2$$
$$-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

as the variables range over the nonnegative integers.

(1) is a polynomial of degree 25 in 26 variables, $a, b, c, \ldots, z$. When nonnegative integers are substituted for these variables, the positive values of (1) coincide exactly with the set of all prime numbers 2,3,5,.... The polynomial (1) also takes on negative values, e.g., -76.

In 1971, Yuri Matijasevič [10] outlined the construction of a prime representing polynomial in 24 variables and degree 37, using the Fibonacci numbers. In the addendum to his paper, an improvement to 21 variables and degree 21 was made. (These polynomials were not written out explicitly.) Our construction here yields a polynomial in 19 variables and degree 29. It also yields a polynomial in 42 variables and degree 5. Thus we might ask what is the smallest possible degree and how few variables are actually necessary to represent primes?

Let us consider first the question of the degree. We know that a prime representing polynomial of degree 5 is possible. All that is necessary to reduce the degree to 5 is the Skolem substitution method (cf. [3], p. 263). However, this procedure increases the number of variables (to 42 when applied to (1)). We do not know whether there is a prime representing polynomial of degree < 5.

The question of the minimum number of variables is also open. A simple argument shows that at least 2 variables are necessary. But we do not know the minimum number. The method of proof of Theorem 1 yields a polynomial in 16 variables. To reduce the number of variables below 16 requires an entirely different construction. The best result we were able to obtain is a polynomial in 12 variables. We shall prove

THEOREM 2. *There exists a prime representing polynomial in* 12 *variables.*

This result was reportedly known to Yuri Matijasevič in 1973, although no literature is available concerning this. Our proof uses methods developed by Yuri Matijasevič and Julia Robinson in [11]. The construction is carried out in §3. The polynomial constructed has very large degree.

The proofs of Theorem 1 and 2 are both based on Wilson's Theorem. In each case we show that the set of prime numbers is Diophantine; i.e., that there exists a Diophantine equation solvable only for prime values of a parameter. We construct a polynomial $M(k, x_1, \cdots, x_n)$ with the property that for each nonnegative integer k

$$(3)\qquad k+2 \text{ is prime} \leftrightarrow M(k, x_1, \cdots, x_n) = 0 \text{ is solvable in nonnegative integers.}$$

It will turn out that M is a sum of squares and hence nonnegative. From such a nonnegative polynomial M, satisfying (3), a prime representing polynomial P is constructible by the method of Putnam [12]. We have only to set P equal to

$$(k+2)\{1-M(k, x_1, \cdots, x_n)\}.^{\dagger} \tag{4}$$

The difficulty is of course the construction of M. We shall see that this requires nearly all the techniques invented to solve Hilbert's tenth problem. And there is good reason why this should be so. Several years before Hilbert's tenth problem was solved in the negative by Matijasevič [8], Julia Robinson [16] proved that *if the set of prime numbers was Diophantine, then every recursively enumerable set would be Diophantine.* Hence Theorem 1 and 2 actually imply the unsolvability of Hilbert's tenth problem.

As was mentioned previously, our polynomials take on negative values. Hence it cannot be claimed that they represent primes exactly. This is not an accidental feature of the Putnam construction. It is a limitation inherent in algebraic functions. The reader is probably familiar with the theorem that no polynomial can represent only primes. This theorem is proved in Section 4 and the result is also extended to all algebraic functions of several variables, of which the polynomial is only a special case.

To overcome the inexactness of the polynomial representation, it is necessary to use exponential functions or other transcendental functions. Julia Robinson noticed [4] that we may conveniently employ the function 0^x for this purpose, provided we define $0^0 = 1$. If we take M as in (3) then we can prove

THEOREM 3. *The set of prime numbers is the exact range of a function of the form*

$$2 + k \cdot 0^{M(k, x_1, \cdots, x_n)}$$

in which $M(k, x_1, \cdots, x_n)$ *is a polynomial and* $n \leqq 11$.

Here we used the function 0^x to distinguish between zero and positive integers. We may also use the proper subtraction function, absolute value function, remainder function, signum function or integer part function (but no algebraic function). Define $r(y, x)$ to be the remainder after division of y by x (take $r(y, 0) = y$). Define $y \dot{-} x$ to be $y - x$ for $y \geqq x$ and 0 for $y < x$. Then $y \dot{-} x = (|y - x| + y - x)/2$. Any one of the following six functions may be used in Theorem 3. (The domain is the nonnegative integers.)

$$0^x = 1 \dot{-} x = \frac{|1-x|+1-x}{2} = 1 - r(1, 1+x) = 1 - \operatorname{sgn}(x) = \left[\frac{1}{1+x}\right].$$

Indeed, using these more general functions it is easy to give a short formula for the nth prime, p_n. The following formula is derived in [7].

$$p_n = \sum_{i=0}^{n^2} \left(1 \dot{-} \left(\left(\sum_{j=0}^{i} r((j \dot{-} 1)!^2, j)\right) \dot{-} n\right)\right). \tag{5}$$

The nth prime function may also be represented by a polynomial, though not of course in one variable. We can prove

THEOREM 4. *There exists a polynomial* $P(n, x_1, \cdots, x_k)$ *such that for any positive integers n and m,*

$$p_n = m \leftrightarrow (\exists x_1, \cdots, x_k)\{P(n, x_1, \cdots, x_k) = m\}.$$

---

† Note the apparent paradox. The polynomial P factors! However, the factors are improper, $P = P \cdot 1$.

Proof. The proof is a simple elaboration on Putnam's idea, (due to Yuri Matijasevič [9]). The binary relation $p_n = m$ is recursive and hence Diophantine by [4] [8]. Therefore there exists a polynomial Q such that $p_n = m \leftrightarrow (\exists x_1, \cdots, x_l) Q(n, m, x_1, \cdots, x_l) = 0$.
We have only to put $P = x_{l+1}(1 - Q^2(n, x_{l+1}, x_1, \cdots, x_l))$. (It follows from the central result of [11] that we may take $l = 13$ and hence $k = 14$.)

The Diophantine character of the set of prime numbers has one further consequence which deserves mention. This concerns the problem of *proving* that a number is prime. If p is a composite number, then there is a proof that p is composite consisting of a single multiplication. Julia Robinson remarks in [14] that prior to the solution of Hilbert's tenth problem in 1970, it was not known that there was a similar proof establishing primality in a bounded number of steps. Yet it follows from [4] [8] that this is so. And our construction permits us to compute a bound on this number.

THEOREM 5. *If p is a prime number, then there is a proof that p is prime consisting of only 87 additions and multiplications.*

The number is easily calculated from the equations of Theorem 2.12.

2. Proof of Theorem 1. Throughout this paper, all variables are nonnegative integers, unless the contrary is explicitly stated. We shall use the notation $x = \square$ to indicate that x is a perfect square. $r(a, b)$ denotes the remainder of a upon division by b. $[x]$ denotes the greatest integer $\leqq x$.

We shall be concerned with the solutions of the Pell equation

$$x^2 - (a^2 - 1)y^2 = 1, \qquad \text{for} \qquad 1 \leqq a.$$

It is well known [3], [16] that the solutions of this equation, $x = \chi_a(n)$, $y = \psi_a(n)$, can be generated via Lucas sequences:

$$\chi_a(0) = 1, \qquad \chi_a(1) = a, \qquad \chi_a(n+2) = 2a\chi_a(n+1) - \chi_a(n),$$
$$\psi_a(0) = 0, \qquad \psi_a(1) = 1, \qquad \psi_a(n+2) = 2a\psi_a(n+1) - \psi_a(n).$$

We shall need the following properties of these sequences.

LEMMA 2.1. $(2a-1)^n \leqq \psi_a(n+1) \leqq (2a)^n$.

LEMMA 2.2. $\psi_a(n) \equiv n \pmod{a-1}$.

These properties are immediate consequences of the definition. Proofs may be found in [3] and [11]. The following lemma will be used to force one unknown to be exponentially larger than another.

LEMMA 2.3. *For $2 \leqq e$, the condition*

$$e^3(e+2)(n+1)^2 + 1 = \square \tag{2.3}$$

implies that $e - 1 + e^{e-2} \leqq n$. Conversely, for any positive integers e and t, it is possible to satisfy 2.3 with n such that $t \mid n+1$.

Proof. Put $a = e + 1$. Then (2.3) becomes a Pell equation in $(a-1)(n+1)$, i.e.,

$$(a^2 - 1)(a-1)^2(n+1)^2 + 1 = \square.$$

If n is any solution of (2.3) then $(a-1)(n+1) = \psi_a(j)$ for some j. By Lemma 2.2, $a - 1 \mid j$. Since $0 \neq j$, this implies that $a - 1 \leqq j$. Using Lemma 2.1 we find that

$$(a-2)(a-1) + (a-1)^{a-2} < (2a-1)^{(a-2)} \leqq \psi_a(a-1) \leqq \psi_a(j) = (a-1)(n+1).$$

Hence

$$(a-2) + (a-1)^{a-3} < n + 1,$$

which gives the result. The converse follows easily from the following well-known fact about Pell equations: When $A \neq \square$, the Pell equation $Ay^2 + 1 = x^2$ always has nontrivial solutions, (cf. [**11**] §2).

LEMMA 2.4. *For any numbers p, n and $a \geqq 1$ we have the congruence*

$$\chi_a(n) \equiv p^n + \psi_a(n)(a - p) \pmod{2ap - p^2 - 1}.$$

Furthermore, when $0 < p^n < a$, the right side of the congruence is less than or equal to the left side.

For a proof of the asserted congruence see [**16**] p. 108 or [**3**] p. 242. The asserted inequality is not difficult to derive using $\sqrt{a^2 - 1}\ \psi_a(n) < \chi_a(n)$.

Next we state a Diophantine definition of the sequence $y = \psi_a(n)$. The set of equations is quite economical. It is difficult to assign credit accurately for these equations because they are a synthesis of collective efforts. The equations most resemble those of Julia Robinson (which appear in Theorem 3.1 of Davis [**3**]). However, they are not identical with these and equation V is due to Yuri Matijasevič.

LEMMA 2.5. *For any numbers a, n and y, $(1 \leqq n)$ and $(2 \leqq a)$, in order that $y = \psi_a(n)$ it is necessary and sufficient that there exist numbers b, c, d, r, s, t, u, v and x such that*

(I) $x^2 = (a^2 - 1)y^2 + 1$,

(II) $u^2 = (a^2 - 1)v^2 + 1$,

(III) $s^2 = (b^2 - 1)t^2 + 1$,

(IV) $v = 4ry^2$,

(V) $b = a + u^2(u^2 - a)$,

(VI) $s = x + cu$,

(VII) $t = n + 4dy$,

(VIII) $n \leqq y$.

The proof is virtually identical to that given by Davis in [**3**] so we shall mention only the differences. Davis used positive integer unknowns in [**3**], however this is not essential. We need not replace r by $r + 1$ in equation IV, (to ensure that $0 < v$), since if $v = 0$ then $u = 1$ by II, $b = 1$ by V, $s = 1$ by III, $x = 1$ by I and VI, and $y = 0$ by I, contradicting VIII. Also, the condition V of [**3**] was used only to show that $b \equiv 1 \bmod 4y$ and $b \equiv a \bmod u$. However, these conditions are guaranteed by II, IV and V above. In this connection the proof of sufficiency is slightly different from that given in [**3**]. We need not use the Chinese Remainder Theorem. If we eliminate the unknowns v, b, s and t from I–VIII, by substitution, then we obtain

COROLLARY 2.6. *For any numbers a, n and y, $(1 \leqq n)$ and $(2 \leqq a)$, in order that $y = \psi_a(n)$ it is necessary and sufficient that there exist numbers c, d, r, u and x such that*

(I) $x^2 = (a^2 - 1)y^2 + 1$,

(II) $u^2 = 16(a^2 - 1)r^2y^4 + 1$,

(III) $(x + cu)^2 = ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1$,

(IV) $n \leqq y$.

We shall also require two basic inequalities:

LEMMA 2.7. *If $0 \leqq \alpha < 1/q$, then $1 - q\alpha \leqq (1 - \alpha)^q$.*

LEMMA 2.8 *If $0 \leqq \alpha \leqq \frac{1}{2}$, then $(1 - \alpha)^{-1} \leqq 1 + 2\alpha$.*

The fundamental tool in both constructions is Wilson's theorem which characterizes the primes in terms of the factorial function.

LEMMA 2.9. (Wilson's theorem.) *For any number $k \geqq 1$, $k + 1$ is prime if and only if*

$$k + 1 \mid k! + 1.$$

For a proof see [**6**], p. 68. The next lemma leads to a Diophantine definition of the factorial function. It is stated in [**10**], in slightly different form, without proof.

LEMMA 2.10. *For any positive integer k, if $(2k)^k \leqq n$ and $n^k < p$ then*

$$k! < \frac{(n+1)^k p^k}{r((p+1)^n, p^{k+1})} < k! + 1.$$

Proof. Using the Binomial Theorem we have

$$(p+1)^n = \sum_{i=0}^{k} \binom{n}{i} p^i + p^{k+1} \sum_{i=k+1}^{n} \binom{n}{i} p^{i-k-1}.$$

Now $(np)^{k+1} - 1 = n^k p^k np - 1 \leqq (p-1)p^k np - 1 = pp^k pn - p^k np - 1 < pp^k pn - pp^k = (np-1)pp^k$. Therefore

$$\sum_{i=0}^{k} \binom{n}{i} p^i \leqq \sum_{i=0}^{k} n^i p^i = \frac{(np)^{k+1} - 1}{np - 1} < pp^k$$

so that

(i) $$r((p+1)^n, pp^k) = \sum_{i=0}^{k} \binom{n}{i} p^i \neq 0.$$

First we prove that

(ii) $$k! < \frac{(n+1)^k p^k}{\sum_{i=0}^{k} \binom{n}{i} p^i}.$$

(ii) follows from the inequalities

$$k!\left(\sum_{i=0}^{k} \binom{n}{i} p^i\right) \leqq k!\left(k\binom{n}{k-1} p^{k-1} + \binom{n}{k} p^k\right) \leqq k!\left(k\frac{n^{k-1}}{(k-1)!} p^{k-1} + \frac{n^k}{k!} p^k\right)$$

$$= k!\left(\frac{k^2 n^{k-1}}{k!} p^{k-1} + \frac{n^k}{k!} p^k\right) = k^2 n^{k-1} p^{k-1} + n^k p^k < kn^k p^{k-1} + n^k p^k < kpp^{k-1} + n^k p^k$$

$$= (k + n^k) p^k \leqq (1+n)^k p^k.$$

It remains only to establish

(iii) $$\frac{(n+1)^k p^k}{\sum_{i=0}^{k} \binom{n}{i} p^i} < k! + 1.$$

In consequence of

$$\frac{(n+1)^k p^k}{\sum_{i=0}^{k} \binom{n}{i} p^i} = \frac{(n+1)^k}{\sum_{i=0}^{k} \binom{n}{i} p^{i-k}} < \frac{(n+1)^k}{\binom{n}{k}}$$

we see that (iii) will follow from

(iv) $$\frac{(n+1)^k}{\binom{n}{k}} \leqq k! + 1.$$

To derive (iv) we have only to use Lemmas 2.7 and 2.8, viz.

$$\frac{(n+1)^k}{\binom{n}{k}} < \frac{k!}{\frac{(n+1-k)^k}{(n+1)^k}} = \frac{k!}{\left(1 - \frac{k}{n+1}\right)^k} < \frac{k!}{\left(1 - \frac{k}{n}\right)^k} = k!\left(\left(1 - \frac{k}{n}\right)^k\right)^{-1}$$

$$\leqq k!\left(1 - \frac{k^2}{n}\right)^{-1} \leqq k!\left(1 + \frac{2k^2}{n}\right) \leqq k!\left(1 + \frac{2k^2}{(2k)^k}\right) \leqq k!\left(1 + \frac{1}{k!}\right).$$

Using Lemma 2.10 we may characterize the factorial function in terms of three exponential functions.

LEMMA 2.11. *For any positive integers k and f, in order that $f = k!$ it is necessary and sufficient that there exist nonnegative integers j, h, n, p, q, w and z such that*

$$\text{(I)}\quad q = wz + h + j, \qquad \text{(IV)}\quad p = (n+1)^k,$$

$$\text{(II)}\quad z = f(h+j) + h, \qquad \text{(V)}\quad q = (p+1)^n,$$

$$\text{(III)}\quad (2k)^3(2k+2)(n+1)^2 + 1 = \square, \qquad \text{(VI)}\quad z = p^{k+1}.$$

Proof. Sufficiency. Suppose k, f, j, h, n, p, q, w and z satisfy conditions I–VI. By II and VI, $0 < h + j \leqq z$. If $h + j = z$ then I implies $z \mid q$ contrary to Lemma 2.10. Hence $h + j < z$ and so I implies $r(q, z) = h + j$. From II and Lemma 2.10 we find

$$f \leqq z/(h+j) \leqq f+1 \quad \text{and} \quad k! < z/(h+j) < k! + 1.$$

Hence $f = k!$ since f and $k!$ are integers.

Necessity. Suppose $1 \leqq k$ and $f = k!$ By Lemma 2.3 we may choose n so that $(2k)^k \leqq n$ and III holds. Set $p = (n+1)^k$, $q = (p+1)^n$ and $z = p^{k+1}$. Then IV, V and VI hold. Finally, put $w = (q - r(q, z))/z$, $h = z - fr(q, z)$ and $j = r(q, z) - h$. Then I and II hold. By Lemma 2.10, h and j are nonnegative.

Finally, we are able to give a Diophantine definition of the set of prime numbers.

THEOREM 2.12. *For any number $k \geqq 1$, in order that $k + 1$ be prime it is necessary and sufficient that there exist numbers $a, b, c, d, e, f, g, h, i, j, l, m, n, o, p, q, r, s, t, u, v, w, x, y$ and z such that*

$$\text{(1)}\quad q = wz + h + j,$$

$$\text{(2)}\quad z = (gk + g + k)\cdot(h + j) + h,$$

$$\text{(3)}\quad (2k)^3(2k+2)(n+1)^2 + 1 = f^2,$$

$$\text{(4)}\quad e = p + q + z + 2n,$$

$$\text{(5)}\quad e^3(e+2)(a+1)^2 + 1 = o^2,$$

$$\text{(6)}\quad x^2 = (a^2 - 1)y^2 + 1,$$

$$\text{(7)}\quad u^2 = 16(a^2 - 1)r^2y^4 + 1,$$

$$\text{(8)}\quad (x + cu)^2 = ((a + u^2(u^2 - a))^2 - 1)\cdot(n + 4dy)^2 + 1,$$

$$\text{(9)}\quad m^2 = (a^2 - 1)l^2 + 1,$$

$$\text{(10)}\quad l = k + i(a - 1),$$

$$\text{(11)}\quad n + l + v = y,$$

$$\text{(12)}\quad m = p + l(a - n - 1) + b(2a(n+1) - (n+1)^2 - 1),$$

$$\text{(13)}\quad x = q + y(a - p - 1) + s(2a(p+1) - (p+1)^2 - 1),$$

$$\text{(14)}\quad pm = z + pl(a - p) + t(2ap - p^2 - 1).$$

Proof. Sufficiency. Suppose that numbers $a, b, \cdots, z$ satisfy equations (1)–(14) and that $1 \leqq k$. Equation (3), together with Lemma 2.3, implies that

$$\text{(1')} \qquad 2 \leqq n, \quad \text{and also (2')} \quad k < n.$$

Equations (4) and (5), together with Lemma 2.3, imply that

$$\text{(3')} \qquad p + q + z + 2n - 1 + (p + q + z + 2n)^{p+q+z+2n-2} \leqq a, \quad \text{and also (4')} \quad n < a.$$

According to Corollary 2.6, equations (6), (7), (8) and (11) imply that $y = \psi_a(n)$, and hence also that $x = \chi_a(n)$. Equation (9) implies that $m = \chi_a(k')$ and $l = \psi_a(k')$, for some number k'. Equation (11) asserts that $l < y$ and hence that $k' < n$. Therefore, by (2') and (4') we have $k' < a - 1$ and also $k < a - 1$. By Lemma 2.2, and equation (10), we have $k \equiv k' \pmod{a-1}$. Therefore $k' = k$ so $m = \chi_a(k)$ and $l = \psi_a(k)$.

From (1'), (2'), and (3') it follows that

$$p < a, \ (n+1)^k < a \quad \text{and} \quad a < 2a(n+1) - (n+1)^2 - 1.$$

Using Lemma 2.4 and equation (12) we find that $p \equiv (n+1)^k \pmod{2a(n+1)-(n+1)^2-1}$. This together with the above inequalities implies that

$$p = (n+1)^k. \tag{5'}$$

From (1') and (3') it follows that

$$q < a, \quad (p+1)^n < a \quad \text{and} \quad a < 2a(p+1)-(p+1)^2-1.$$

Using Lemma 2.4 and equation (13) we find that $q \equiv (p+1)^n \pmod{2a(p+1)-(p+1)^2-1}$. This, together with the above inequalities, implies that

$$q = (p+1)^n. \tag{6'}$$

From (1'), (2'), (3') and the fact that $p \neq 0$ (which follows from (5')), it follows that

$$z < a, \quad p^{k+1} < a \quad \text{and} \quad a < 2ap - p^2 - 1.$$

Using Lemma 2.4 and equation (14) we find that $z \equiv p^{k+1} \pmod{2ap-p^2-1}$. This, together with the above inequalities, implies that

$$z = p^{k+1}. \tag{7'}$$

According to Lemma 2.11, conditions (1), (2), (3), (5'), (6') and (7') imply that $gk + g + k = k!$ and hence that $k! + 1 = (g+1)(k+1)$. Thus $k+1$ is prime by Lemma 2.9.

Necessity. Suppose that $1 \leqq k$ and that $k+1$ is prime. By Lemma 2.9 we may find a number g so that $k! = gk + g + k$. According to Lemma 2.11 numbers f, h, j, n, p, q and w may be chosen to satisfy equations (1), (2), (3) and also the conditions

$$p = (n+1)^k, \quad q = (p+1)^n \quad \text{and} \quad z = p^{k+1}. \tag{8'}$$

Choose e so as to satisfy equation (4). By Lemma 2.3 it is possible to choose numbers a and o, $(a \geqq 2)$, satisfying (5). Put $y = \psi_a(n)$. According to Corollary 2.6 we may find numbers c, d, r, u and x satisfying equations (6), (7) and (8). Put $m = \chi_a(k)$ and put $l = \psi_a(k)$. Then (9) holds. By Lemma 2.2 and the fact that $k \leqq \psi_a(k)$ for $2 \leqq a$, we may choose i satisfying equation (10). It is trivial to show (by induction) that for $2 \leqq a$, $n + \psi_a(n-1) \leqq \psi_a(n)$. Using this, and the fact that $k < n$ (which follows from (3)), we find that $n + l \leqq y$. Hence it is possible to choose a number v satisfying (11). Finally, as in the proof of sufficiency, equations (4) and (5) imply that

$$(n+1)^k < a, \quad (p+1)^n < a \quad \text{and} \quad p^k < a.$$

Consequently, by Lemma 2.4 and the equations (8'), numbers b, s and t may be found so that equations (12), (13) and (14) are satisfied. This completes the proof of Theorem 2.12.

Theorem 1 now follows immediately from Theorem 2.12. We have only to replace k by $k+1$ throughout the equations of Theorem 2.12, sum the squares of the equations and employ the device of Putnam [12]. This produces the polynomial (1).

Perhaps some industrious reader will construct a shorter prime representing polynomial.

3. Proof of Theorem 2. Here we show that primes are Diophantine definable in 11 unknowns. In Section 2 we used what might be called the *congruence method.* In this section we shall use what might be called the *ratio method.* This latter technique, developed by Yuri Matijasevič and Julia Robinson in [11], is generally more economical with respect to the number of variables.

LEMMA 3.1. *For* $0 < 2q < \beta$, $\left(\frac{\beta}{\beta-1}\right)^q \leqq 1 + \frac{2q}{\beta}$.

Proof. By Lemmas 2.7 and 2.8.

LEMMA 3.2. *For* $0 < n < M$ *and* $0 \leqq x$, $\left(1-\frac{n}{M}\right) < \left(1-\frac{1}{2M(x+1)}\right)^n$.

Proof. By Lemma 2.7.

LEMMA 3.3. *If* $x > 8 \cdot 2^n$ *and* $n > k$, *then*

(i) $\frac{(x+1)^n}{x^k} - \left[\frac{(x+1)^n}{x^k}\right] < \frac{1}{8}$, (ii) $\left[\frac{(x+1)^n}{x^k}\right] \equiv \binom{n}{k} \bmod x$, (iii) $\binom{n}{k} < \frac{(x+1)^n}{x^k}$.

Proof.

$$\frac{(x+1)^n}{x^k} = \sum_{i=0}^{n} \binom{n}{i} x^{i-k} = \sum_{i=0}^{k-1} \binom{n}{i} x^{i-k} + \sum_{i=k}^{n} \binom{n}{i} x^{i-k},$$

where

$$\sum_{i=0}^{k-1} \binom{n}{i} x^{i-k} \leqq \frac{1}{x} \sum_{i=0}^{k-1} \binom{n}{i} < \frac{2^n}{x} < \frac{1}{8}. \quad \text{Thus} \quad \left[\frac{(x+1)^n}{x^k}\right] = \sum_{i=k}^{n} \binom{n}{i} x^{i-k} \equiv \binom{n}{k} \bmod x.$$

(iii) follows from the assumption $k < n$.

LEMMA 3.4. $n^k \Big/ \binom{n}{k} \leqq k! \left(1 + \frac{2(k-1)^2}{n}\right)$ *for* $n > 2(k-1)^2$.

Proof. As in the proof of Lemma 2.10, condition (iv).

LEMMA 3.5. $a\left(1+\frac{1}{10a}\right)^4 < a + \frac{1}{2}$, (*for* $a \geqq 1$).

LEMMA 3.6. $a\left(1-\frac{1}{4a}\right)^2 > a - \frac{1}{2}$, (*for* $a \geqq 1$).

DEFINITION 3.7. $U(x, y) = (x+2)^3(x+4)(y+1)^2 + 1$.

By Lemma 2.3, if $U(x, y) = \square$ then $x^x < y$. Also, for each x, arbitrarily large numbers y may be found satisfying $U(x, y) = \square$. (This is the same function $U(x, y)$ defined in [**11**].)

LEMMA 3.8. (Matijasevič-Robinson [**11**]) *Suppose* $A > 1$, $B > 1$ *and* $C > 0$. *Then* $\psi_A(B) = C$ *if and only if the following system of conditions can be satisfied.*

(A1) $DFI = \square$, $F \mid H - C$, $B \leqq C$,
(A2) $D = (A^2 - 1)C^2 + 1$,
(A3) $E = 2(i+1)D(k+1)C^2$,
(A4) $F = (A^2 - 1)E^2 + 1$,
(A5) $G = A + F(F - A)$,
(A6) $H = B + 2(j+1)C$,
(A7) $I = (G^2 - 1)H^2 + 1$.

THEOREM 3.9. *For any positive integer* k, *in order that* $k+1$ *be prime, it is necessary and sufficient that the following system of equations has a solution in nonnegative integers*:

(I) $U(2k, n) = \square$,
(II) $U(2n, x) = \square$,
(III) $M = 16nx(w+2) + 1$,
(IV) $A = M(x+1)$,
(V) $B = n + 1$,
(VI) $C = m + B$,
(VII) $DFI = \square$, $F \mid H - C$,
(VIII) $D = (A^2 - 1)C^2 + 1$,
(IX) $E = 2(i+1)DC^2$,
(X) $F = (A^2 - 1)E^2 + 1$,
(XI) $G = A + F(F - A)$,

(XII) $H = B + 2(j+1)C,$

(XIII) $I = (G^2-1)H^2+1,$

(XIV) $$\left\{\frac{R}{\left(\frac{C}{KL}-(w+1)x\right)\left(1-\frac{R}{C}\right)^2 L}-(S+1)\right\}^2 < \tfrac{1}{4},$$

(XV) $(M^2-1)K^2+1=\square,$

(XVI) $(M^2x^2-1)L^2+1=\square,$

(XVII) $(M^2n^2x^2-1)R^2+1=\square,$

(XVIII) $K = n-k+1+p(M-1),$

(XIX) $L = k+1+l(Mx-1),$

(XX) $R = k+1+r(Mnx-1),$

(XXI) $S = (z+1)(k+1)-2.$

Proof of Sufficiency. Let there be given a solution to the system (I)–(XXI). We must show that $k+1$ is prime. By Wilson's Theorem (Lemma 2.9) it is sufficient to show that $k+1 \mid k!+1$. According to the equation (XXI), $k+1 \mid S+2$. Hence it is sufficient to show that $S+1 = k!$. Define real numbers σ and β by

$$\sigma = \frac{C}{KL}, \qquad \beta = \frac{R}{(\sigma-(w+1)x)\left(1-\frac{R}{C}\right)^2 L}.$$

According to (XIV), $|\beta-(S+1)| < \frac{1}{2}$. Hence we need only prove that

(1) $$\beta - k!| < \tfrac{1}{2}.$$

From (I) we have, by Lemmas 2.3 and 3.7,

(2) $$n > (2k)^{2k} > k, \quad \text{and} \quad n \geqq 5.$$

(II) implies that

(3) $$x > (2n)^{2n} > 8n^k.$$

(III) implies that

(4) $$M \geqq 32nx, \quad \text{and} \quad (5) \quad M > 2n, M > 160 \cdot 10^{10}.$$

From (IV), (V) and (VI), $A > 1$, $B > 1$ and $C \geqq B > 1$. So by Lemma 3.8, (VII)–(XIII) imply that

(6) $$C = \psi_{M(x+1)}(n+1).$$

(XV), (XVIII) and Lemma 2.2 imply

(7) $$K = \psi_M(n-k+1+p'(M-1)),$$

where $p' \geqq 0$, since $M-1 > n-k+1$ by (5). (XVI), (XIX) and Lemma 2.2 imply that

(8) $$L = \psi_{Mx}(k+1+l'(Mx-1)),$$

where $l' \geqq 0$ since $Mx-1 > k+1$ by (4) and (2). (XVII), (XX) and Lemma 2.2 imply that

(9) $$R = \psi_{Mnx}(k+1+r'(Mnx-1)),$$

where $r' \geqq 0$ since $Mnx-1 \geqq k+1$.

We now show by contradiction that $p' = l' = 0$. If $p' > 0$ or $l' > 0$ then

$$\sigma \leqq \frac{(2M(x+1))^n}{(2M-1)^{n+M-k-1}(2Mx-1)^k} \quad \text{or} \quad \sigma \leqq \frac{(2M(x+1))^n}{(2M-1)^{n-k}(2Mx-1)^{k+Mx-1}}.$$

In either case,

$$\sigma < \frac{(2M(x+1))^n}{(2M-1)^M} = \frac{(2M)^n}{(4M(M-1)+1)^n} \cdot \frac{(x+1)^n}{(2M-1)^{M-2n}} < \frac{1}{2}.$$

Hence $\beta < 0$ contradicting (XIV) (which implies that $\frac{1}{2} < \beta$).

(10) Thus $p' = l' = 0$, $K = \psi_M(n-k+1)$ and $L = \psi_{Mx}(k+1)$.

We then have

$$\sigma \leqq \frac{(2M(x+1))^n}{(2M-1)^{n-k}(2Mx-1)^k} < \frac{(x+1)^n}{x^k}\left(\frac{2M}{2M-1}\right)^n \leqq \frac{(x+1)^n}{x^k}\left(1+\frac{n}{M}\right),$$

by Lemmas 2.7 and 3.1. Also,

$$\sigma \geqq \frac{(2M(x+1)-1)^n}{(2M)^{n-k}(2Mx)^k} = \frac{(x+1)^n}{x^k}\left(1-\frac{1}{2M(x+1)}\right)^n > \frac{(x+1)^n}{x^k}\left(1-\frac{n}{M}\right)$$

by Lemma 3.2. Thus,

(11) $$\left|\sigma - \frac{(x+1)^n}{x^k}\right| < \frac{n}{M}\cdot\frac{(x+1)^n}{x^k}, \quad \text{and} \quad \sigma > \frac{1}{2}\frac{(x+1)^n}{x^k}.$$

We next derive bounds for $\sigma - (w+1)x$.

Case 1: Suppose $x > \sigma - (w+1)x$. Then $(w+2)x > \sigma$. Put $\epsilon_1 = \left|\sigma - \frac{(x+1)^n}{x^k}\right|$. Then

(12) $$\sigma = \frac{(x+1)^n}{x^k} \pm \varepsilon_1 = \left[\frac{(x+1)^n}{x^k}\right] \pm \varepsilon_1 + \varepsilon_2, \text{ where } 0 < \varepsilon_2 < \frac{1}{8}, \text{ by Lemma 3.3. And}$$

(13) $$\sigma \equiv \binom{n}{k} \pm \varepsilon_1 + \varepsilon_2 \pmod{x}, \quad \text{by Lemma 3.3.}$$

From (11) and (III),

$$0 \leqq \varepsilon_1 < \frac{(x+1)^n}{x^k}\cdot\frac{n}{M} < 2\sigma\cdot\frac{n}{M} < \frac{1}{8}.$$

Since $k+1 \leqq n$, we have

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 2} \geqq \frac{n\cdot k(k-1)\cdots 2}{k(k-1)\cdots 2} = n \geqq 5, \quad \text{and} \quad \binom{n}{k} \leqq n^k < \frac{1}{3}x.$$

Then

$$\sigma - (w+1)x \equiv \sigma \equiv \binom{n}{k} \pm \varepsilon_1 + \varepsilon_2 \pmod{x},$$

where $0 < \binom{n}{k} \pm \varepsilon_1 + \varepsilon_2 < \frac{1}{3}x + \frac{1}{4} < \frac{1}{2}x < x$. By (XIV), $0 < \sigma - (w+1)x$. Hence both sides of the congruence are less than the modulus, so we have

(14) $$\sigma - (w+1)x = \binom{n}{k} \pm \varepsilon_1 + \varepsilon_2 < \tfrac{1}{2}x,$$

and $\sigma - (w+1)x = \binom{n}{k} \pm \varepsilon_1 + \varepsilon_2 \geqq \binom{n}{k} - \frac{1}{8} > 4$, i.e.,

(15) $$4 < \sigma - (w+1)x < \tfrac{1}{2}x.$$

From (9), we have $R = \psi_{Mnx}(k+1+r'(Mnx-1))$, where $r' \geqq 0$. Suppose $r' > 0$. Then

$$R \geqq \psi_{Mnx}(k+Mnx) \geqq (2Mnx-1)^{k+Mnx-1} \geqq (2Mnx-1)^{Mnx}$$

By (6), $C = \psi_{M(x+1)}(n+1) \leqq (2M(x+1))^n < (2Mnx-1)^n$, so $C^3 < R$. Also, $C \geqq (2M(x+1)-1)^n > 9$, so that $C < \frac{1}{3}R^{1/2}$. Thus,

$$R\Big/\left(\frac{R}{C}-1\right)^2 < R/(3R^{1/2}-1)^2 < R/(2R^{1/2})^2 = \tfrac{1}{4}.$$

Since $\frac{1}{2} < \sigma - (w+1)x$ by (15),

$$\beta = \frac{R}{(\sigma-(w+1)x)\left(1-\frac{R}{C}\right)^2 L} < \frac{1}{4(\sigma-(w+1)x)} < \frac{1}{2},$$

contradicting (XIV). Thus

$$r' = 0 \quad \text{and} \quad R = \psi_{Mnx}(k+1). \tag{16}$$

It follows from this, (3) and (4) that

$$\frac{R}{C} = \frac{\psi_{Mnx}(k+1)}{\psi_{M(x+1)}(n+1)} \leqq \frac{(2Mnx)^k}{(2M(x+1)-1)^n} < \frac{(2Mx)^k \cdot n^k}{(2Mx)^n} < \frac{(2Mx)^{k+1}}{(2Mx)^n} \leqq \frac{1}{(2Mx)^2} < \frac{1}{4}. \tag{17}$$

Also,

$$\left(1-\frac{R}{C}\right)^2 > 1-\frac{2R}{C}, \quad \text{so} \quad \frac{1}{\left(1-\frac{R}{C}\right)^2} < \frac{1}{1-\frac{2R}{C}} < 2, \quad \text{by (17).} \tag{18}$$

Case 2: Suppose $\sigma - (w+1)x \geqq x$. Then $\sigma - (w+1)x > \frac{1}{2}$, so $r' = 0$, as in Case 1. Also,

$$\beta = \frac{R}{(\sigma-(w+1)x)\left(1-\frac{R}{C}\right)^2 L} < \frac{2(2Mnx)^k}{x(2Mx-1)^k}, \quad \text{using (18), (16) and (10),}$$

$$= \frac{2n^k}{x}\left(\frac{2Mx}{2Mx-1}\right)^k \leqq \frac{2n^k}{x}\left(1+\frac{k}{Mx}\right) \quad \text{by Lemma 3.1, using (3),}$$

$$< \frac{4n^k}{x} < \frac{1}{2}.$$

Thus $\beta < \frac{1}{2}$, contradicting (XIV). Hence, Case 2 does not hold and Case 1 obtains.

Now it is possible to show that $|\beta - k!| < \frac{1}{2}$. We have, from Case 1, that

$$\sigma - (w+1)x = \binom{n}{k} \pm \varepsilon, \quad \text{where} \quad 0 \leqq \varepsilon = |\pm\varepsilon_1 + \varepsilon_2| < \tfrac{1}{4}. \tag{19}$$

Using (10), (16), (17) and (19) we have

$$\beta = \frac{R}{\left(\binom{n}{k} \pm \varepsilon\right)\left(1-\frac{R}{C}\right)^2 L} < \frac{(2Mnx)^k}{\left(\binom{n}{k}\left(1-\left(\varepsilon\Big/\binom{n}{k}\right)\right)\right)\left(1-\frac{1}{(2Mx)^2}\right)^2 (2Mx-1)^k}$$

$$= \left(n^k\Big/\binom{n}{k}\right)\left(\frac{2Mx}{2Mx-1}\right)^k \left(\frac{1}{1-\left(\varepsilon\Big/\binom{n}{k}\right)}\right)\left(\frac{1}{1-\frac{1}{(2Mx)^2}}\right)^2$$

It is easily seen that

$$\frac{1}{1-\left(\varepsilon\Big/\binom{n}{k}\right)} \leqq 1+\frac{2\varepsilon}{\binom{n}{k}}, \left(\frac{1}{1-\frac{1}{(2Mx)^2}}\right)^2 \leqq 1+\frac{1}{Mx}, \quad \text{and} \quad \left(\frac{2Mx}{2Mx-1}\right)^k \leqq 1+\frac{k}{Mx},$$

using Lemmas 2.7, 2.8 and 3.1. By Lemma 3.4,

$$n^k \Big/ \binom{n}{k} \leqq k! \left(1 + \frac{2(k-1)^2}{n}\right).$$

Thus

$$\beta < k! \left(1 + \frac{2\varepsilon}{\binom{n}{k}}\right)\left(1 + \frac{1}{Mx}\right)\left(1 + \frac{k}{Mx}\right)\left(1 + \frac{2(k-1)^2}{n}\right).$$

We claim

(20) $$\beta < k! + \tfrac{1}{2}.$$

For this, the following inequalities are sufficient, by Lemma 3.5:

(i) $k! \left(2\varepsilon \Big/ \binom{n}{k}\right) < \frac{1}{10}$ (since $10k!k!2\varepsilon < 5(k!)^2 \leqq 5k^{2k} \leqq n < n(n-1)\cdots(n-k+1)$),

(ii) $k! \left(\frac{k}{Mx}\right) < \frac{1}{10}$ (since $10k!\, k \leqq 10k^k < 10n < Mx$),

(iii) $k! \left(\frac{1}{Mx}\right) < \frac{1}{10}$ (by (ii)),

(iv) $k! \left(\frac{2(k-1)^2}{n}\right) < \frac{1}{10}$ (since $20k!(k-1)^2 \leqq 40k^k < (2k)^{2k} < n$, if $k \geqq 2$).

(These inequalities are derived using only (2) and (3).) Thus (20) holds

Also,

$$\beta \geqq \frac{(2Mnx-1)^k}{\binom{n}{k}\left(1 + \left(\varepsilon \Big/ \binom{n}{k}\right)\right)(2Mx)^k} \quad \text{by (16) and (10),}$$

$$= \frac{n^k}{\binom{n}{k}}\left(1 - \frac{1}{2Mnx}\right)^k \left(1 + \frac{\varepsilon}{\binom{n}{k}}\right)^{-1} \geqq \frac{n^k}{\binom{n}{k}}\left(1 - \frac{1}{2Mnx}\right)^k \left(1 - \frac{\varepsilon}{\binom{n}{k}}\right)$$

$$\geqq k! \left(1 - \frac{k}{2Mnx}\right)\left(1 - \frac{\varepsilon}{\binom{n}{k}}\right) \quad \text{by Lemmas 2.7 and 2.8.}$$

We claim that

(21) $$\beta > k! - \tfrac{1}{2}.$$

By Lemma 3.6, the following inequalities are sufficient to establish this.

(i) $1 - \frac{k}{2Mnx} \geqq 1 - \frac{1}{4k!}$ (since $4kk! \leqq 4k^{2k} \leqq 4n < 2Mnx$),

(ii) $1 - \frac{\varepsilon}{\binom{n}{k}} \geqq 1 - \frac{1}{4k!}$ (since $4\varepsilon k!\, k!(n-k)! < k!\, k!(n-k)! \leqq k^{2k}(n-k)! \leqq n(n-k)! \leqq n!$).

Thus (21) holds. Hence (1) holds.

Proof of Necessity. Suppose $k+1$ is a prime number. We must find nonnegative integers satisfying (I)–(XXI). Choose n and x satisfying (I), (II). Let $S = k! - 1$. Then z exists satisfying (XXI), by Wilson's Theorem. Define w by $[(x+1)^n/x^k] = \binom{n}{k} + (w+1)x$. Let M be given by (III), A by (IV), B by (V). Put $C = \psi_A(B)$, and $m = C - B$. Then (VI)–(XIII) may be satisfied by Lemma 3.8. Put $K = \psi_M(n-k+1)$, $L = \psi_{Mx}(k+1)$, $R = \psi_{Mnx}(k+1)$. Then (XV)–(XX) can be satisfied, by Lemma 2.2. It remains only to show that (XIV) holds. Define σ and β as before. Recall that in the proof of sufficiency it was shown that

$$|\beta - k!| < \tfrac{1}{2}. \tag{22}$$

The only assumptions used in the argument establishing (22) were Lemmas 2.7, 2.8, 3.1–3.7, equations (I)–(XIII), the conditions

(i) $$K = \psi_M(n-k+1), \quad L = \psi_{Mx}(k+1), \quad R = \psi_{Mnx}(k+1),$$

(ii) $$\sigma - (w+1)x = \binom{n}{k} \pm \varepsilon, \quad \text{where} \quad 0 \leqq \varepsilon < \tfrac{1}{4},$$

and the inequalities

(iii) $$0 < \sigma - (w+1)x \quad \text{and} \quad \text{(iv)} \quad \sigma - (w+1)x < x.$$

The condition (XIV) was used only to show (i). Now since $S+1 = k!$, (22) is actually equivalent to (XIV). Hence this same argument may be used to establish (XIV). The conditions (i) have already been satisfied by our choice of K, L and R. In Case 1 it was shown how to derive condition (ii) using only conditions (iii) and (iv). Therefore we need only derive (iii) and (iv). (iii) is derived as follows using Lemma 3.3 (i) and (3). First

$$M = 16nx(w+2) = 16n\left(\left[\frac{(x+1)^n}{x^k}\right] - \binom{n}{k} + x\right) > 16n\left(\frac{(x+1)^n}{x^k} - \frac{1}{8} - \binom{n}{k} + x\right) > 16n\frac{(x+1)^n}{x^k}. \tag{23}$$

Hence, using (11) and (23), we see that

$$\sigma - (w+1)x = \sigma - \left[\frac{(x+1)^n}{x^k}\right] + \binom{n}{k} > -\frac{n}{M}\frac{(x+1)^n}{x^k} + \binom{n}{k} > -\frac{1}{16} + \binom{n}{k} \geqq -\frac{1}{16} + 5 > 0.$$

Thus (iii) holds. Next we derive (iv). Using Lemma 3.3 (i), (11), (23) and finally (3) we have

$$\sigma - (w+1)x = \sigma - \left[\frac{(x+1)^n}{x^k}\right] + \binom{n}{k} < \sigma - \frac{(x+1)^n}{x^k} + \frac{1}{8} + \binom{n}{k} < \frac{n}{M}\frac{(x+1)^n}{x^k} + \frac{1}{8} + \binom{n}{k}$$
$$< \frac{1}{16} + \frac{1}{8} + \binom{n}{k} < x.$$

Thus (iv) holds. This completes the proof of Theorem 3.9.

The unknowns $M, A, B, C, D, E, F, G, H, I, K, L, R, S$ eliminate from (I)–(XXI) by substitution. This leaves 10 unknowns, $n, x, w, m, z, i, j, p, l, r$, the parameter k, six square conditions, one divisibility condition and one inequality. These remaining conditions are definable with one unknown, y, by the relation combining theorem of [11]. Thus we obtain a definition M, in 11 unknowns. Replacing k by $k+1$ in M we obtain a prime representing polynomial $P = (k+2)(1-M^2)$ in 12 variables.

A direct calculation, based on [11], shows that $M = M_6$ will have degree 148864. However, Yuri Matijasevič has recently worked out a more efficient version of the relation combining theorem. If we suppose that $1 + |\sqrt{A_i}| \leqq V_i$, then in M_q we may replace W^i by $W_i = V_1 \cdot V_2 \cdots V_i$, $(i = 1, 2, \cdots, q)$.

Thus when a square condition arises from a Pell equation, $(\alpha^2-1)\beta^2+1=\square$, we may choose any $V \geqq |\alpha\beta|+|\beta|+2$. Also, if the quantities B and C of [**11**] are non-negative, as they are here, they need not be squared in M_q. These refinements yield a polynomial M_6 of degree 13376.

Matijasevič also noticed that our first two square conditions, (I) and (II), may be combined into one square condition

$$U(2k,n)[((2U(2k,n)-1)^2-1)(n+1)^2(x+1)^2 4+1]=\square. \tag{24}$$

Observe that the first factor of (24) is prime to the second. This gives a polynomial M_5 of degree 6848. Hence the degree of the 12 variable polynomial P is 13697. (Recently Yuri Matijasević has announced that he has been able to reduce the number of variables still further, from 12 to 10.)

4. Functions not formulas for primes. Many classical theorems are known concerning the impossibility of representing primes with certain sorts of functions. Since these results are negative, they, together with the previous, shed considerable light on the question of the logical complexity of prime representing forms. The oldest result of this type is of course.

THEOREM 4.1. *A polynomial $P(z_1, z_2, \cdots, z_k)$, with complex coefficients, which takes only prime values at nonnegative integers, must be constant.*

Proof. It is not difficult to show that the coefficients of an integer valued polynomial must be rational numbers. Let l be any multiple of the denominators of these coefficients of P. We are assuming that $P(1,1,\cdots,1)=p$ is a prime. Then, if $n_1, n_2, \cdots, n_k$ are integers, $P(1+n_1lp,\ 1+n_2lp, \cdots, 1+n_klp) \equiv P(1,1,\cdots,1) \bmod p$. Hence, for all $n_1, n_2, \cdots, n_k$, $P(1+n_1lp, 1+n_2lp, \cdots, 1+n_klp)=p$. This implies that P is a polynomial of degree 0. The theorem is proved. (Cf. also [**6**], p. 18.)

This result was extended to rational functions by R. C. Buck [**2**]. A rational function is a special case of an *algebraic function*, (cf. [**1**] for the definition of algebraic function). We now proceed to extend the result to all algebraic functions. We shall need

THEOREM 4.2. *An integer valued algebraic function $W(z_1, z_2, \cdots, z_k)$ is a polynomial.*

Proof. We consider first the case of an algebraic function $W=W(z)$ of a single complex variable. Suppose that whenever z is a nonnegative integer, $W(z)$ is also an integer. Let us temporarily restrict z to real values. The point at infinity, $z=\infty$, may or may not be one of the branch points of the function W. However, in any case the function has a Puiseux series expansion around the point at infinity [**19**]. This is the Laurent series expansion of $W=W(t^{-1/h})$, where h is the order of the branch point at infinity and $t=1/z$ is the local parameter. In this Puiseux series

$$W(z)=\sum_{l=0}^{\infty} a_l z^{\alpha-l\delta} \tag{1}$$

α is a fixed rational number and δ is a fixed positive rational number.

Now, if $W=W(z)$ is integer valued, its first, second, $\cdots$, rth differences, defined by $\Delta W(z)=W(z+1)-W(z)$ and $\Delta^{r+1}W(z)=\Delta(\Delta^r W(z))$, are also integer valued algebraic functions of z.

It is easy to prove by induction on r that

$$\Delta^r W(n)=\int_0^1\int_0^1\cdots\int_0^1 W^{(r)}(n+x_1+x_2+\cdots+x_r)dx_1dx_2\cdots dx_r \tag{2}$$

where $W^{(r)}(z)$ denotes the rth derivative of the function $W=W(z)$. Since δ is positive, $W^{(r)}(z)\to 0$ as $z\to\infty$, for all sufficiently large r. Therefore (2) implies that $\Delta^r W(n)\to 0$ as $n\to\infty$, for all sufficiently large r. Since $\Delta^r W(n)$ is integer valued, this implies that $\Delta^r W(n)=0$ for all sufficiently large n and r. Since a nonzero algebraic function cannot have infinitely many zeroes [**17**], it follows that for all z and all sufficiently large r, $\Delta^r W(z)=0$. This implies that $W(z)$ is a polynomial in z, for all real z.

The case of a complex variable z is an immediate consequence of the analytic continuation of the case of the real variable, since an algebraic function is uniquely determined by its values at an infinite number of arguments [17].

The general case, that of an algebraic function of several complex variables, $W(z_1, z_2, \cdots, z_k)$, now follows from the result for one variable. For if we replace all arguments but one with nonnegative integers, we obtain an algebraic function of a single variable

$$W(n_1, \cdots, n_{i-1}, z_i, n_{i+1}, \cdots, n_k). \tag{3}$$

By the preceding proof, (3) is a polynomial in z_i. Since W is algebraic, one can find a polynomial $P(z_i)$ (whose degree is independent of the n_i's) such that $|W(n_1, \cdots, n_{i-1}, z_i, n_{i+1}, \cdots, n_k)| < |P(z_i)|$ for all sufficiently large z_i. This implies that for some fixed d_i

$$\frac{\partial^{d_i} W(n_1, \cdots, n_{i-1}, z_i, n_{i+1}, \cdots, n_k)}{\partial z_i^{d_i}} = 0. \tag{4}$$

Derivatives of algebraic functions are again algebraic. Hence (4) implies that for all $z_1, \cdots, z_k$

$$\frac{\partial^{d_i} W(z_1, \cdots, z_{i-1}, z_i, z_{i+1}, \cdots, z_k)}{\partial z_i^{d_i}} = 0. \tag{5}$$

Now an algebraic function has at most a finite number of branch points. Hence infinitely many k-tuples are not branch points of W. Consider the k variable Taylor series expansion of W about such a point. Plainly, (5) implies that this series terminates. W is a polynomial of degree $\leqq d_1 + d_2 + \cdots + d_k$. The theorem is proved.

COROLLARY 4.3. *An algebraic function $W(z_1, z_2, \cdots, z_k)$, which takes only prime values at nonnegative integers, is constant.*

This corollary follows from Theorems 4.1 and 4.2. It was proved for $k = 1$ by a different, p-adic, method in [18]. Negative results about prime representing *exponential* functions have also been obtained [13] [18] [20]. We shall prove a multivariable result of this type.

THEOREM 4.4. *Suppose $P_i(x_1, \cdots, x_n)$ and $Q_i(x_1, \cdots, x_n) \geqq 0$ are polynomials with integer coefficients and that $a_1, a_2, \cdots, a_m$ are positive integers. Then, if the function*

$$F(x_1, \cdots, x_n) = \sum_{i=1}^{m} P_i(x_1, \cdots, x_n) a_i^{Q_i(x_1, \cdots, x_n)}$$

takes only prime values at nonnegative integers, it is constant.

Proof. It suffices to prove the theorem for the case of a function of a single variable. (For if $F(x_1, \cdots, x_n)$ is constant in each variable separately, then $F(x_1, \cdots, x_n)$ is constant.) Hence we may suppose $n = 1$. Now if $F(x)$ takes on infinitely many prime values p, then we may choose x_1 such that $F(x_1) = p$ is relatively prime to each a_i (since the a_i's are nonzero). By Fermat's theorem we then find that $F(x_1 + kp(p-1)) \equiv p \bmod p$, and hence that for every k

$$F(x_1 + kp(p-1)) = p. \tag{8}$$

(Cf. Reiner [13] or Hardy and Wright [6], p. 66.) On the other hand, if $F(x)$ takes on only a finite number of prime values, then one of these values is taken on infinitely many times. In either case, for some prime p, the equation

$$F(x) = p \tag{9}$$

holds for infinitely many nonnegative integers x. It is not difficult to show that equation (9) must then hold identically. This completes the proof of the Theorem.

It is interesting to compare Theorem 4.4 with Theorem 3 stated in the introduction.

Acknowledgement. The authors wish to thank Martin Davis, Yuri Matijasevič and Julia Robinson for several helpful suggestions made during the course of this work.

References

1. Lars V. Ahlfors, Complex Analysis, McGraw-Hill, New York, 1953, xi + 247 pp.

2. R. C. Buck, Prime representing functions, this MONTHLY, 53 (1946) 265.

3. Martin Davis, Hilbert's tenth problem is unsolvable, this MONTHLY, 80 (1973) 233–269.

4. ———, Hilary Putnam and Julia Robinson, The decision problem for exponential Diophantine equations, Ann. of Math., 74 (1961) 425–436.

5. Underwood Dudley, History of a formula for primes, this MONTHLY, 76 (1969) 23–28.

6. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Fourth Edition, Oxford University Press, 1960, xvi + 421 pp.

7. James P. Jones, Formula for the nth prime number, Canadian Math. Bull., 18 (1975) no. 3.

8. Yuri Matijasevič, Enumerable sets are Diophantine, Doklady Akademii Nauk SSSR, 191 (1970) 279–282. English translation: Soviet Math., Doklady, 11 (1970) 354–358.

9. ———, Diophantine representation of enumerable predicates, Izvestija Akademii Nauk SSSR. Serija Matematičeskaja, 35 (1971) 3–30. English translation: Mathematics of the USSR-Izvestija, 5 (1971) 1–28.

10. ———, Diophantine representation of the set of prime numbers, Doklady Akademii Nauk SSSR, 196 (1971) 770–773. English translation with Addendum: Soviet Math., Doklady, 12 (1971) 249–254.

11. ——— and Julia Robinson, Reduction of an arbitrary Diophantine equation to one in 13 unknowns, Acta Arithmetica, 27 (1975) 521–553.

12. Hilary Putnam, An unsolvable problem in number theory, Journal of Symbolic Logic, 25 (1960) 220–232.

13. Irving Reiner, Functions not formulas for primes, this MONTHLY, 50 (1943) 619–621.

14. Julia Robinson, Hilbert's tenth problem, Proc. Sympos. Pure Math., 20 (1971) 191–194.

15. ———, Existential definability in arithmetic, Trans. Amer. Math. Soc., 72 (1952) 437–449.

16. ———, Diophantine decision problems, M.A.A. Studies in Mathematics, 6 (1969) 76–116 (Studies in Number Theory, W.J. Leveque, editor).

17. Stanislaw Saks and Antoni Zygmund, Analytic Functions, Second Edition Enlarged, Warsaw 1965, p. 276.

18. Daihachiro Sato and E. G. Straus, P-adic proof of non-existence of proper prime representing algebraic functions and related problems, Jour. London Math. Soc., (2), 2 (1970) 45–48.

19. Carl L. Siegel, Topics in Complex Function Theory, Vol. 1, Interscience Tracts in Pure and Applied Mathematics, number 25, Wiley, New York, 1969, ix + 186 pp.

20. E. G. Straus, Functions periodic modulo each of a sequence of integers, Duke Math. Jour., 19 (1952) 379–395.

JAMES P. JONES AND DOUGLAS P. WIENS, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA, CANADA, T2N 1N4.

DAIHACHIRO SATO, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SASKATCHEWAN, REGINA, SASKATCHEWAN, CANADA, S4S 0A2.

HIDEO WADA, DEPARTMENT OF MATHEMATICS, SOPHIA UNIVERSITY, KIOICHO, CHIYODA-KU, TOKYO, JAPAN.