Some classes of integer-valued functions

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN – AMSTERDAM
Reprinted from Proceedings, Series A, **58**, No. 3 and Indag. Math., **17**, No. 3, 1955

MATHEMATICS

SOME CLASSES OF INTEGER-VALUED FUNCTIONS

BY

N. G. DE BRUIJN

(Communicated by Prof. H. D. KLOOSTERMAN at the meeting of March 26, 1955)

1. The following problem was proposed to me by L. HENKIN. Let an integer-valued function $f(x)$, defined for $x=0, 1, 2, \ldots$ be called *universal* if it has the property that

$$(1) \qquad f(x+m)-f(x) \equiv 0 \pmod m$$

for all x and all m ($x=0, 1, 2, 3, \ldots$; $m=1, 2, 3, \ldots$). Obviously every polynomial with integer coefficients is universal. Are there any other universal functions?

There are indeed, and all universal functions will be determined here. One of the simplest is the following polynomial with non-integer coefficients: $f(x)=\frac{1}{2}x^4+\frac{1}{2}x^2$. In that case we have

$$f(x+m)-f(x)=2mx^3+3m^2x^2+2m^3x+mx+f(m),$$

and it is easily seen that m divides $f(m)$.

The question about all universal functions is analogous to the question about all integer-valued functions, to which the answer is well-known (cf. G. PÓLYA and G. SZEGÖ, *Aufgaben und Lehrsätze aus der Analysis*, Vol. 2, Abschnitt VIII, Kap. 2, nr. 84–85): Any function $f(x)$ defined and integer-valued for $x=0, 1, 2, \ldots$ can be uniquely written in the form

$$(2) \qquad f(x) = b_0 + b_1\binom{x}{1} + b_2\binom{x}{2} + \ldots \qquad \left(\binom{x}{k} = \frac{x(x-1)\ldots(x-k+1)}{k!}\right),$$

where $b_0, b_1, \ldots$ are integers. Conversely, any function of this form is integer-valued.

The second statement follows from the fact that the binomial coefficients are integers, and that $\binom{x}{k}=0$ if $k > x$ (hence, for each x, the series (2) contains only a finite number of terms $\neq 0$).

In order to show the first statement, consider (2) as a set of equations in the unknowns $b_0, b_1, \ldots$. The matrix is of triangular type and the diagonal coefficients are 1, so that there is a uniquely determined solution in the b_k's and the b_k's turn out to be integers.

The binomial coefficients are obviously polynomials in x. The sum of the first $n+1$ terms of the series (2) is a polynomial of degree $\leqslant n$, which equals $f(x)$ for $x=0, \ldots, n$. Therefore, if $f(x)$ is an integer-valued polynomial of degree $\leqslant n$, then in the representation (2) the coefficients $b_{n+1}, b_{n+2}, \ldots$ vanish identically.

Turning our attention to universal functions, we find a similar situation. Let s_k denote the least common multiple of the numbers $1, 2, \ldots, k$. Then we have

Theorem 1: $f(x)$ is universal if and only if it has the form

$$f(x) = c_0 + s_1 c_1 \binom{x}{1} + s_2 c_2 \binom{x}{2} + s_3 c_3 \binom{x}{3} + \ldots, \tag{3}$$

where the c's are integers. If $f(x)$ is given, then the c_k's are uniquely determined. $f(x)$ is a universal polynomial of degree $\leqslant n$ if and only if, moreover, $c_{n+1} = c_{n+2} = \ldots = 0$.

Proof: After what was said above it suffices to show the following facts:

(i) $s_k \binom{x}{k}$ is a universal function.

(ii) If $f(x)$ is given in the form (2), and $f(x)$ is universal, then b_k is a multiple of s_k $(k=0, 1, 2, \ldots)$.

We first prove a simple lemma. If p is any prime number, and k an integer $\geqslant 1$, then by $\lambda = \lambda(p, k)$ we denote the largest integer such that $p^\lambda \leqslant k$. Denoting by $\Omega(p, k)$ the number of factors p dividing $k!$, we have Legendre's formula

$$\Omega(p, k) = [k/p] + [k/p^2] + \ldots + [k/p^\lambda].$$

If $\lambda(p, k) = 0$, this sum is understood to be zero.

Lemma: Let $a_1, \ldots, a_s$ be s distinct numbers taken from a set of k consecutive integers $(0 \leqslant s \leqslant k)$. Then the product $p^{(k-s)\lambda} a_1 \ldots a_s$ is divisible by p^Ω (if $s=0$, the product $a_1 \ldots a_s$ is understood to be 1).

Proof: Let σ_r, for $r = 1, 2, 3, \ldots$, denote the number of multiples of p^r among $a_1, \ldots, a_s$. Among k consecutive integers there are at least $[k/p^r]$ multiples of p^r, and therefore $\sigma_r \geqslant [k/p^r] - (k-s)$.

Obviously $p^{(k-s)\lambda} a_1 \ldots a_s$ is divisible by p^η, where

$$\eta = \sigma_1 + \ldots + \sigma_\lambda + (k-s)\lambda = \Sigma_{r=1}^{\lambda} (\sigma_r + k - s) \geqslant \Sigma_{r=1}^{\lambda} [k/p^r] = \Omega.$$

This proves the lemma.

We next prove (i). Abbreviate

$$f_k(x) = s_k \binom{x}{k} = \frac{s_k}{k!} x(x-1)\ldots(x-k+1). \tag{4}$$

It suffices to show that, for each prime p and for all integers x, α, k $(\alpha \geqslant 1, k \geqslant 1)$, we have

$$f_k(x + p^\alpha) \equiv f_k(x) \pmod{p^\alpha}. \tag{5}$$

First assume $\alpha > \lambda$. We have

$$k!\, s_k^{-1} \{f_k(x + p^\alpha) - f_k(x)\} = p^{k\alpha} \Sigma_0 + p^{(k-1)\alpha} \Sigma_1 + \ldots + p^\alpha \Sigma_{k-1}, \tag{6}$$

where Σ_s is the s-th elementary symmetrical function of the numbers $x, x-1, \ldots, x-k+1$; and $\Sigma_0 = 1$. By the lemma, $p^{(k-s)\alpha} \Sigma_s$ is divisible by at least $\Omega + (k-s)(\alpha - \lambda)$ factors p, and so, for $0 \leqslant s \leqslant k-1$, by at least

$\Omega+\alpha-\lambda$ factors p. As $k!$ and s_k contain exactly Ω and λ factors p, respectively, we now find that (6) leads to (5).

Next assume $\alpha \leqslant \lambda$. Then we simply use the fact that $f_k(x)$ is always divisible by s_k (as $\binom{x}{k}$ is an integer). And, s_k contains λ factors p, so that both members of (5) are multiples of p^λ, and therefore multiples of p^α.

We proceed to the proof of (ii). Let $f(x)$ be given by (2), and assume that $f(x)$ is universal. As $f(x)$ is integer-valued, b_1 is an integer, and therefore it is a multiple of s_1. Now take $k>1$, and suppose that it has already been proved that s_j divides b_j if $j=1, \ldots, k-1$.

By (i) we know that $b_0+b_1\binom{x}{1}+\ldots+b_{k-1}\binom{x}{k-1}$ is a universal function. Subtracting this one from $f(x)$, we obtain a new universal function $g(x)$, given by

$$g(x) = b_k\binom{x}{k} + b_{k+1}\binom{x}{k+1} + \ldots.$$

Clearly $g(0)=\ldots=g(k-1)=0$, $g(k)=b_k$. As $g(x)$ is universal, we have

$$g(k) \equiv g(k-m) \pmod{m} \qquad (1 \leqslant m \leqslant k),$$

and so $g(k)$ is a multiple of m for $m=1, \ldots, k$. Hence $g(k)$ is a multiple of their least common multiple, i.e. s_k. This proves that s_k divides b_k.

2. By a slight modification of the definition of universal functions we arrive at a class of functions which we shall call, for the moment, *modular*. An integer-valued function $f(x)$, defined for both non-negative and negative integers x, is called modular if (1) holds for all m, without the restriction $x \geqslant 0$.

The polynomials with integer coefficients are obviously modular. Furthermore, the functions (4) are modular as in proving (5) we did not make the restriction $x \geqslant 0$.

Any modular function is universal. Furthermore, if a polynomial is universal, then it is also modular. For if it is modular, it is, for $x \geqslant 0$, represented by a finite series (3). This clearly represents it for $x < 0$ as well. Each term is modular, hence the polynomial is modular.

On the other hand a universal function which is not a polynomial cannot always be extended to a modular function.

We shall construct a counter-example by suitable definition of the integers c_k in (3). For each prime p we choose an integer R_p such that $\frac{1}{3}p \leqslant R_p \leqslant \frac{2}{3}p$. We take $c_k=0$ if $k+1$ is not a prime, and the others will be defined by induction. Let p be any prime, and assume that c_k has already been chosen for $k<p-1$.

Obviously,

$$f(p-1) = c_0 + s_1 c_1\binom{p-1}{1} + \ldots + s_{p-1} c_{p-1}\binom{p-1}{p-1},$$

as all further terms vanish. The number s_{p-1} is not a multiple of p. Therefore, we can and do choose c_{p-1} such that $f(p-1) \equiv R_p \pmod{p}$.

Thus we have constructed a universal function $f(x)$ such that $f(p-1) \equiv R_p \pmod{p}$ for all p. If $f(x)$ could be extended to a modular function, we would have $f(-1) \equiv R_p \pmod{p}$ for all p. Taking $p > 3\,|f(-1)|$ we obtain a contradiction.

Therefore, modular continuation of a universal function is not always possible. If it is possible, it is unique. For, a modular function which vanishes for $x < 0$, is easily seen to vanish identically (if $a \geqslant 0$, we infer that $f(a) \equiv f(a-am) \equiv 0 \pmod{m}$ for all $m > 1$, and this implies $f(a) = 0$).

Unless $f(x)$ is a polynomial, formula (3) cannot be used for negative values of x, as it is divergent. But modular functions can easily be represented in a slightly different way.

Theorem 2: $f(x)$ is modular if and only if it has the form

$$f(x) = c_0 + \sum_{k=1}^{\infty} s_k\, c_k \binom{x+[\frac{1}{2}k]}{k},$$

where the c_k's are integers. If $f(x)$ is given, then the c_k's are uniquely determined.

Theorem 2 can be proved along the same lines as Theorem 1.

Instead of $[\frac{1}{2}k]$ we can take any other non-decreasing sequence of integers t_k, provided that $t_{k+1} - t_k$ is always 0 or 1, and infinitely often 0, infinitely often 1. The c_k's of course depend on the choice of the t_k's.

3. A further generalization is to universal functions of several variables, a question also proposed by Mr. HENKIN. $f(x_1, \ldots, x_n)$ is called universal if it is defined for all non-negative integers $x_1, \ldots, x_n$ and if, for each integer $m \geqslant 1$

$$x_1' \equiv x_1 \pmod{m}, \ldots, x_n' \equiv x_n \pmod{m} \quad (x_i \geqslant 0,\, x_i' \geqslant 0)$$

implies

$$f(x_1', \ldots, x_n') \equiv f(x_1, \ldots, x_n) \pmod{m}.$$

We first remark that any integer-valued function $f(x_1, \ldots, x_n)$, defined for $x_1 \geqslant 0, \ldots, x_n \geqslant 0$, can be uniquely represented as

$$f(x_1, \ldots, x_n) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} b(k_1, \ldots, k_n) \binom{x_1}{k_1} \cdots \binom{x_n}{k_n}, \tag{7}$$

where the $b(k_1, \ldots, k_n)$ are integers, and that any such series represents an integer-valued function.

The second statement is trivial, as for each set $x_1, \ldots, x_n$ the series contains only a finite number of terms $\neq 0$. The first one can be proved as follows. f is an integer-valued function of x_n and hence it can be written as a series of the type (2), with integer coefficients. That means that the coefficients are integer-valued functions of $x_1, \ldots, x_{n-1}$. Next consider these as functions of x_{n-1}, again apply (2), etc. In this way we obtain (7). In each step of this process, the coefficients are uniquely determined, and therefore the same holds for (7).

Theorem 3: $f(x_1, \ldots, x_n)$ is universal if and only if in the representation (7) each $b(k_1, \ldots, k_n)$ is a multiple of s_t, where

$$t = \max(k_1, \ldots, k_n),$$

and s_t is, as before, the l.c.m. of the numbers $1, \ldots, t$ $(s_0 = 1)$.

Proof: Considering f as a function of x_n only, we obtain: $f(x_1, \ldots, x_n)$ is a universal function of x_n if and only if it has the form

$$f(x_1, \ldots, x_n) = \sum_{k=1}^{\infty} s_k \, c_k(x_1, \ldots, x_{n-1}) \binom{x_n}{k},$$

where the $c_k(x_1, \ldots, x_n)$ are integer-valued. Expanding $c_k(x_1, \ldots, x_{n-1})$ in a series of the type (7) (with $n-1$ instead of n) we obtain, in connection with the uniqueness of the development of $f(x_1, \ldots, x_n)$: (7) represents a universal function of x_n if and only if each $b(k_1, \ldots, k_n)$ is a multiple of s_{k_n}. A similar thing holds, of course, for universal functions of x_j $(1 \leqslant j \leqslant n)$.

Further, $f(x_1, \ldots, x_n)$ is a universal function of $x_1, \ldots, x_n$, if and only if it is a universal function of x_j for each j. Therefore, a necessary and sufficient condition that f be modular, is that the following n conditions hold simultaneously:

$$(8) \qquad b(k_1, \ldots, k_n) \equiv 0 \pmod{s_{k_j}} \quad (j = 1, \ldots, n).$$

As the l.c.m. of $s_{k_1}, \ldots, s_{k_n}$ equals s_t, (8) is equivalent with

$$b(k_1, \ldots, k_n) \equiv 0 \pmod{s_t}.$$

Needless to say, a similar result holds if in Theorem 3, the word "universal" is replaced by "modular" (cf. Theorem 2).

University of Amsterdam