ON THE POLYNOMIALS WHOSE DERIVATIVES HAVE INTEGRAL VALUES AT THE INTEGERS

ERNST G. STRAUS

It is well known that the polynomials, which together with their derivatives have integral values at a fixed point $x = x_0$, have the basis

$$(x - x_0)^n/n!, \qquad n = 0, 1, 2, \cdots,$$

over the integers. That is to say every polynomial with that property is of the form $\sum_{k=0}^{n} c_k(x-x_0)^k/k!$ where $c_0, c_1, \cdots, c_n$ are integers. Similarly it is known that a basis over the integers for those polynomials whose values are integral at all integers is given by

$$1, x(x - 1) \cdots (x - n + 1)/n!, \qquad n = 1, 2, \cdots.$$

It is the purpose of this note to construct a basis over the integers for the polynomials which together with all their derivatives have integral values at all integers. We shall call such polynomials *I-polynomials*.

In order to construct this basis we prove a few introductory lemmas:

LEMMA 1. *Let D_n be the greatest integer such that there exists an I-polynomial of the form*

$$f_n(x) = x^n/D_n + \textit{lower powers},$$

and let

$$f(x) = (a/b)x^n + \textit{lower powers}, \qquad (a, b) = 1,$$

be any I-polynomial; then $b \mid D_n$.

PROOF. Let m be the least common multiple of D_n and b and let $k_1 = m/D_n$, $k_2 = m/b$; then $(k_1, k_2) = (k_1, a) = 1$. Hence there exist two integers c_1, c_2 such that $c_1 k_1 + c_2 k_2 a = 1$ and $c_1 f_n(x) + c_2 f(x) = x^n/m +$ lower powers.

From the definition of D_n it follows that $m \leq D_n$; but since m is a multiple of D_n we have $m = D_n$ or $b \mid D_n$.

LEMMA 2. *The I-polynomials*

$$f_n(x) = x^n/D_n + \textit{lower powers}, \qquad n = 0, 1, 2, \cdots,$$

where D_n is as in Lemma 1, form a basis over the integers of the I-polynomials.

PROOF. We proceed by induction. The lemma is obviously true for polynomials of degree 0. Assume the lemma true for all polynomials of degree $< n$. Let

$$f(x) = (a/b)x^n + \text{lower powers}$$

be an I-polynomial; then according to Lemma 1, $c_n = aD_n/b$ is an integer. Thus $f(x) - c_n f_n(x)$ is an I-polynomial of degree $< n$ and

$$f(x) - c_n f_n(x) = c_0 f_0(x) + \cdots + c_{n-1} f_{n-1}(x)$$

or $\quad f(x) = c_0 f_0(x) + \cdots + c_n f_n(x).$

LEMMA 3. *If $m < n$, then $D_m \big| D_n$.*

PROOF. If $f_m(x) = x^m/D_m + \cdots$ is an I-polynomial, then so is $x^{n-m} f_m(x) = x^n/D_m + \cdots$ and hence according to Lemma 1 we have $D_m \big| D_n$.

LEMMA 4. *If p is a prime and $p^k \big| D_n$, then $p^k \big| [n/p]!$ or, in other words,*

$$k \leq [n/p^2] + [n/p^3] + \cdots.$$

PROOF. Let $f(x)$ be a polynomial with integral coefficients of least degree such that $f(x)/p^k$ is an I-polynomial, and let j be any one of the numbers $0, 1, \cdots, p-1$. Let m be the multiplicity of j as a root of the congruence $f(x) \equiv 0 \pmod{p}$, that is to say

$$f(x) = (x - j)^m g(x) + p h(x)$$

where $g(x)$, $h(x)$ are polynomials with integral coefficients and $g(j) \not\equiv 0 \pmod{p}$.

Differentiating m times we obtain

$$f^{(m)}(x) = m! g(x) + (x - j) k(x) + p h^{(m)}(x)$$

where $k(x)$ is a polynomial with integral coefficients. We have $h^{(m)}(x) = m! l(x)$ where $l(x)$ has integral coefficients and hence:

$$f^{(m)}(x) = m! g(x) + (x - j) k(x) + p m! l(x).$$

Let p^r be the highest power of p which divides $m!$; then we obtain

$$f^{(m)}(j) \equiv m! g(j) \pmod{p^{r+1}}$$

and hence unless $r \geq k$ we cannot have $f^{(m)}(j)/p^k = \text{integer}$.

Since j was chosen as any one of the numbers $0, 1, \cdots, p-1$ we see that, mod p, $f(x)$ must be divisible by $x^m(x-1)^m \cdots (x-p+1)^m$, where m is such that $p^k \big| m!$. But the degree of $f(x)$ is then greater than or equal to pm.

If we introduce the symbol $(n)_p$ for the greatest exponent, m, such that $p^m \mid n$, then we can state

LEMMA 5. $D_n \leqq \prod_{p=\text{prime}} p^{([n/p]!)_p} = n! / \prod_{p=\text{prime}} p^{[n/p]}$.

The proof is an immediate consequence of Lemmas 3 and 4. We now can prove the following theorem.

THEOREM. *The polynomials*

$$f_n(x) = \prod p^{[n/p]} x(x-1) \cdots (x-n+1)/n!$$

form a basis over the integers of the I-polynomials.

PROOF. According to Lemmas 5 and 2 it suffices to show that the $f_n(x)$ are I-polynomials. Since $f_n(x)$ is an integral multiple of $x(x-1) \cdots (x-n+1)/n!$, it is integral-valued. We now proceed by induction and show that if $f_k(x)$ is an I-polynomial for $k < n$, then $f_n'(x)$, and hence $f_n(x)$, is an I-polynomial.

We have

$$f_n'(x) = \frac{\prod p^{[n/p]}}{n!} \sum_{i=0}^{n-1} \frac{x(x-1) \cdots (x-n+1)}{x-i}$$

and since

$$\frac{x(x-1) \cdots (x-n+1)}{x-i}$$

$$= \sum_{k=0}^{n-i-1} (-1)^k \frac{(n-i-1)!}{(n-i-k-1)!} x(x-1) \cdots (x-n+2+k)$$

we have

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

$$= \sum_{k=0}^{n-1} (-1)^k \frac{n(n-1) \cdots (n-k)}{k+1} x(x-1) \cdots (x-n+2+k)$$

or

$$f_n'(x) = \prod p^{[n/p]} \sum_{k=1}^{n} (-1)^{k+1} \frac{1}{k(n-k)!} x(x-1) \cdots (x-n+k+1)$$

$$= \sum_{k=1}^{n} (-1)^{k+1} \frac{1}{k} \prod p^{[n/p]-[(n-k)/p]} f_{n-k}(x).$$

We now show that

$$\prod_{p=\text{prime}} p^{[n/p]-[(n-k)/p]}/k = A_k$$

is an integer. A_k is certainly an integer modulo p if k is not divisible by p. If k is divisible by p then $[(n-k)/p] = [n/p] - k/p$ and

$$p^{[n/p]-[(n-k)/p]} = p^{k/p}$$

and since obviously

$$k/p \geqq (k)_p$$

we have again that A_k is an integer modulo p. Thus A_k is an integer for

$$k = 1, \cdots, n-1; \quad \text{and} \quad f_n'(x) = \sum_{k=1}^{n} (-1)^{k+1} A_k f_{n-k}(x)$$

is an I-polynomial.

In conclusion we should like to pose a number of problems:

(1) Instead of considering those polynomials whose values at the rational integers are rational integers, we consider the polynomials whose values at the algebraic integers of a certain field are algebraic integers of the same field. Find a basis for the polynomials which are integral-valued in this generalized sense, and for the polynomials which together with all their derivatives are integral-valued in the generalized sense. It may be conjectured that there exist bases of the form $(\alpha_n/n!)x(x-1) \cdots (x-n+1)$ where the α_n are algebraic integers.

(2) Show that the only (entire) analytic functions which have integral (Gaussian integral) derivatives at all (infinitely many) integers (Gaussian integers) are polynomials. We have shown in another paper that a transcendental entire function with integral derivatives of all orders at infinitely many integral points would have to be of infinite order.

(3) Our problem can be generalized in many other directions. For example, if instead of considering a basis for the I-polynomials, we look for a basis of those polynomials which have integral derivatives of all orders, not at all integral points, but only at the points $0, 1, \cdots, m-1$, then we obtain a basis $f_{mn}(x)$; $n = 0, 1, 2, \cdots$ with the denominators

$$D_{mn} = \prod_{p<m} p^{([n/p]!)_p} \prod_{p \geqq m} p^{([n/m]!)_p}$$

and the numerators

$$\{x(x-1) \cdots (x-m+1)\}^{[n/m]} x(x-1) \cdots (x-n+m[n/m]+1).$$

UNIVERSITY OF CALIFORNIA, LOS ANGELES