Internat. J. Math. & Math. Sci.
VOL. 20 NO. 3 (1997) 521-528

MULTIPLICATIVE POLYNOMIALS AND FERMAT'S LITTLE THEOREM FOR NON-PRIMES

PAUL MILNES

Department of Mathematics
University of Western Ontario
London, Ontario N6A 5B7, Canada

and

C. STANLEY-ALBARDA

Department of Mathematics
University of Toronto
Toronto, Ontario M5S 1A1, Canada

(Received November 6, 1995)

ABSTRACT. Fermat's Little Theorem states that $x^p = x(\text{mod}\, p)$ for $x \in \mathbf{N}$ and prime p, and so identifies an integer-valued polynomial (IVP) $g_p(x) = (x^p - x)/p$. Presented here are IVP's g_n for non-prime n that complete the sequence $\{g_n \mid n \in \mathbf{N}\}$ in a natural way. Also presented are characterizations of the g_n's and an indication of the ideas from topological dynamics and algebra that brought these matters to our attention.

KEY WORDS AND PHRASES. Fermat's Little Theorem, multiplicative function, polynomials.

1991 AMS SUBJECT CLASSIFICATION CODES: 10A20, 20K30.

Some ideas in topological dynamics (Namioka [6] and Milnes [5]) lead to the consideration of product groups with a group operation that for $\mathbf{Z}^\infty = \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \times \ \dots$ is as follows:

$$(x_1', x_2', x_3', x_4', \ \dots\ ) \otimes (x_1, x_2, x_3, x_4, \ \dots\ ) =$$

$$(x_1' + x_1, x_2' + x_1'x_1 + x_2, x_3' + x_2'x_1 + x_1'x_2 + x_3, x_4' + x_3'x_1 + x_2'x_2 + x_1'x_3 + x_4, \ \dots\ ).$$

The operation is abelian and in fact $(\mathbf{Z}^\infty, \otimes)$ is isomorphic to the direct product group $(\mathbf{Z}^\infty, +)$.

In Namioka [5] a way of defining a class of these seemingly trivial operations $\otimes'$ on $\mathbf{Z}^\infty$ is given. Such operations are basic in the definition of Witt vectors, for which the ring product in $\mathbf{Z}^\infty$ is changed as well, and in an analogous way. (See Lang [4] and Demazure [3]; thanks to J.F. Jardine for these references.)

One property of such an operation is that it makes a certain map E from $\mathbf{Z}^\infty$ into the algebra FP of formal power series with constant term 1 a homomorphism. For $(\mathbf{Z}^\infty, \otimes)$, the map E is

$$E(a) = E(a_1, a_2, a_3, \dots) = 1 + \sum_{n=1}^{\infty} a_n t^n.$$

(For Witt vectors the map is given by $E(a) = \Pi_{n=1}^{\infty}(1 - a_n t^n)$.)

A SEQUENCE OF POLYNOMIALS.

An isomorphism (the obvious one) between $(\mathbf{Z}^\infty, \otimes)$ and $(\mathbf{Z}^\infty, +)$ led to our first sequence of polynomials. Some details of the calculation of this isomorphism are given in the appendix. We computed the first 51 polynomials in 1987, and take this opportunity to thank R. Girgensohn, who using Maple has recently computed the first 100 polynomials (verifying our computations on the way). Here is a sampling of these polynomials.

$$P_1(x) = x, \quad P_2(x) = -(x^2 - x)/2, \quad P_3(x) = (x^3 - x)/3$$
$$P_4(x) = -(x^4 - x)/4 - (x^2 - x)/4, \quad P_5(x) = (x^5 - x)/5$$
$$P_6(x) = -(x^6 - x)/6 + (x^3 - x)/6 + (x^2 - x)/6, \quad P_7(x) = (x^7 - x)/7$$
$$P_8(x) = -(x^8 - x)/8 - (x^4 - x)/8 - (x^2 - x)/4, \quad P_9(x) = (x^9 - x)/9 - (x^3 - x)/9$$
$$P_{20}(x) = -(x^{20} - x)/20 - (x^{10} - x)/20 + (x^5 - x)/10 + (x^4 - x)/20 + (x^2 - x)/20$$
$$P_{31}(x) = (x^{31} - x)/31, \quad P_{39}(x) = (x^{39} - x)/39 - (x^{13} - x)/39 - (x^3 - x)/39$$
$$P_{48}(x) = -(x^{48} - x)/48 - (x^{24} - x)/48 + (x^{16} - x)/48 - (x^{12} - x)/24 + (x^8 - x)/48$$
$$-(x^6 - x)/12 + (x^4 - x)/24 + (x^3 - x)/6 + (x^2 - x)/12$$

The method of construction dictates that the P_n's are integer-valued polynomials (IVP's). Furthermore, for prime p Fermat's Little Theorem (FLT) says that

$$x^p = x (\operatorname{mod} p), \text{ i.e., } (x^p - x)/p \in \mathbf{Z} \text{ for } x \in \mathbf{Z},$$

just the polynomials we are getting for the prime values *except for* $p = 2$ (at least as far as calculations have been done).

We note that $(x^4 - x)/4$ equals $7/2$ at $x = 2$, and furthermore that $n = 561 = 3 \times 11 \times 17$ is the smallest non-prime n such that $(x^n - x)/n$ is an IVP; 561 is called a *Carmichael number.* The infinitude of the set of Carmichael numbers has recently been demonstrated in Alford et al. [1]. (Thanks to Ján Mináč for this reference.)

We view the isomorphism calculation as an algorithm that determines, for each $n \in \mathbf{N}$, in a canonical way, an IVP P_n, such that $P_n(x) = (x^n - x)/n$, the Fermat polynomial, when $n > 2$ is a prime.

There was clearly enough information in the formulae for the P_n's to figure out something to say about these polynomials. The sequence $\{g_n\}$ of the next theorem is observed to agree with $\{nP_n\}$ up to $n = 100$.

THEOREM 1. The following are equivalent ways of defining inductively a sequence $\{g_n\}$ of polynomials starting with $g_1(x) = x$. For $n > 1$

(A) $$g_n(x) = (-1)^{n+1}x^n + \sum_{\substack{1 \le d < n \\ d \mid n}} (-1)^{n/d} g_d(x); \text{ or}$$

(B) $g_n(x) = \sum_{k=1}^{n} b_{n,k}x^k$, where

(a) $b_{n,k} = 0$ if $k \nmid n$,

(b) if $k \mid n$ and $k \neq 1$, $b_{n,k} = (-1)^{k+1} b_{n/k,1}$, and

(c) $b_{n,1} = -\sum_{k=2}^{n} b_{n,k}$ $(= -\sum_{k=2}^{m} b_{n,k}$ for all $m \geq n)$.

PROOF. Proceeding by induction, we note that

$$g_2(x) = x - x^2 = (-1)^3(x^2 - x)$$

satisfies both (A) and (B), and assume that $g_m(x)$, as defined in (A) satisfies the conditions of (B) for all $m < n$. It then suffices to show that

$$g_n(x) = (-1)^{n+1}(x^n - x) + \sum_{\substack{1 < d < n \\ d \mid n}} (-1)^{n/d} g_d(x)$$

(as defined in (A)) also satisfies the conditions (a), (b) and (c) of (B).

With $g_n(x) = \sum_{k=1}^{n} b_{n,k}x^k$, note that the induction hypotheses imply that

★ $$b_{m,k} = \sum_{\substack{1 < d < m \\ d \mid m}} (-1)^{m/d} b_{d,k} \quad (1 < k < m \leq n).$$

(a) If $k \nmid n$, then $k \nmid d$ for any d such that $d \mid n$, so that

$$b_{n,k} = \sum_{\substack{1 < d < n \\ d \mid n}} (-1)^{n/d} b_{d,k} = 0.$$

(c) $$b_{n,1} = (-1)^{n+2} + \sum_{\substack{1 < d < n \\ d \mid n}} (-1)^{n/d} b_{d,1}$$

$$= -b_{n,n} + \sum_{\substack{1 < d < n \\ d \mid n}} (-1)^{n/d} \left(-\sum_{k=2}^{d} b_{d,k} \right)$$

$$= -\left(b_{n,n} + \sum_{\substack{1 < d < n \\ d \mid n}} (-1)^{n/d} \sum_{k=2}^{n-1} b_{d,k} \right) \quad (\text{since } d < n)$$

$$= -\left(b_{n,n} + \sum_{k=2}^{n-1}\left(\sum_{\substack{1<d<n\\ d\mid n}} (-1)^{n/d} b_{d,k}\right)\right) = -\left(b_{n,n} + \sum_{k=2}^{n-1} b_{n,k}\right) \quad (\text{by } \star)$$

$$= -\sum_{k=2}^{n} b_{n,k}.$$

(b) Both (A) and (B) give $b_{n,n} = (-1)^{n+1}$, so let $k\,|\,n$, $1 < k < n$. Then

$$b_{n,k} = \sum_{\substack{1<d<n\\ d\mid n}} (-1)^{n/d} b_{d,k} \quad (\text{by } \star)$$

$$= \sum\left\{(-1)^{n/d} b_{d,k} \mid 1 < d < n,\ d\,|\,n,\ k\,|\,d\right\} \quad (\text{since } k \nmid d \text{ implies } b_{d,k} = 0)$$

$$= \sum\left\{(-1)^{n/d}(-1)^{k+1} b_{d/k,1} \mid 1 < d < n,\ d\,|\,n,\ k\,|\,d\right\} \quad (\text{since } 1 < k).$$

Writing $e = d/k$, we have

$$b_{n,k} = \sum\left\{(-1)^{n/(ek)}(-1)^{k+1} b_{e,1} \mid 1 < ek < n,\ ek\,|\,n,\ k\,|\,ek\right\}$$

$$= (-1)^{k+1}\sum\left\{(-1)^{(n/k)/e} b_{e,1} \mid 1 \le e < (n/k),\ e\,|\,(n/k)\right\}$$

$$= (-1)^{k+1}\left((-1)^{n/k} b_{1,1} + \sum_{\substack{1<e<(n/k)\\ e\mid(n/k)}} (-1)^{(n/k)/e} b_{e,1}\right)$$

$$= (-1)^{k+1}\left((-1)^{n/k} + \sum_{\substack{1<d<(n/k)\\ d\mid(n/k)}} (-1)^{(n/k)/d} b_{d,1}\right),$$

which equals $(-1)^{k+1} b_{n/k,1}$ by (A), and so we have the formula (b) of (B) holding for $g_n(x) = \sum_{k=1}^{n} b_{n,k} x^k$ (as well as (a) and (c)).

The induction proof is complete. ■

We shall get explicit formulae for the g_n's, as well as other information. First we collect preparatory material in some lemmas; the second conclusion of part (a) of the next lemma is well known.

LEMMA 2. (a) For odd prime power p^r, $g_{p^r} = x^{p^r} - x^{p^{r-1}}$, and g_{p^r}/p^r is an IVP.

(b) For powers of 2, we have $g_1 = x$, $g_2 = -x^2 + x$, and for $r > 1$

$$g_{2^r} = -x^{2^r} + \sum_{j=1}^{r} g_{2^{r-j}} = -(x^{2^r} - x^{2^{r-1}}) + 2g_{2^{r-1}} = -x^{2^r} + 2^{r-1}x - \sum_{j=1}^{r-1} 2^{j-1} x^{2^{r-j}};$$

also $g_{2^r}/2^r$ is an IVP.

PROOF. (a) In this case (A) becomes

$$g_{p^r} = x^{p^r} - \sum_{j=1}^{r} g_{p^{r-j}}.$$

The first claim is then easy to show by induction: just write

$$g_{p^r} = x^{p^r} - x^{p^{r-1}} = x^{p^r} - (x^{p^{r-1}} - x^{p^{r-2}}) - (x^{p^{r-2}} - x^{p^{r-3}}) - \ \dots \ - (x^p - x) - x.$$

For the second claim, FLT says that $(x^p - x)/p \in \mathbf{Z}$ for $x \in \mathbf{Z}$, i.e., $x^p = x + kp$; expanding $(x + kp)^{p^{r-1}}$ gives the result.

(b) In this case (A) becomes

$$g_{2^r} = -x^{2^r} + \sum_{j=1}^{r} g_{2^{r-j}} \ ,$$

the first expression for g_{2^r}; the validity of the other 2 forms follows readily by induction. To see that $g_{2^r}/2^r$ is an IVP, apply induction and the proof of (a) to the middle form for g_{2^r}. ■

A function f from $\mathbf{N}$ into an abelian ring is called *multiplicative* if $f(1) = 1$, and $f(mn) = f(m)f(n)$ at least if m and n are relatively prime, $(m, n) = 1$; thus a multiplicative function is determined by its values at the prime powers. Since explicit formulae for the g_n's have been given at the prime powers in the previous lemma, all we need to do to complete the explicit presentation of the g_n's is to show that the function $n \mapsto g_n$, $\mathbf{N} \to FP$, is multiplicative.

We remind the reader of the convolution formula for multiplicative functions f and h,

$$f * h(n) = \sum_{d \mid n} f(d)h(d/n)$$

and that

$f * h$ is also multiplicative,

the operation $*$ is associative, and

the sequence $e = (1, 0, 0, 0, \ \dots)$ is the identity element for the operation $*$.

Furthermore, the Möbius function μ is the multiplicative function that is the inverse of $\rho = (1, 1, 1, \ \dots)$ and is defined by $\mu(1) = 1$, and for $n > 1$

$$\mu(n) = \begin{cases} (-1)^k \text{ if n is the product of } k \text{ distinct primes,} \\ 0 \text{ otherwise.} \end{cases}$$

Then there is the Möbius inversion formula, $h = f * \rho$ if and only if $f = h * \mu$, i.e.,

$$h(n) = \sum_{d \mid n} f(d) \text{ if and only if } f(n) = \sum_{d \mid n} \mu(d)h(n/d).$$

(Baker [2] is a reference for all this.) The next lemma was pointed out to us by R. Girgensohn; the inversion formula that the lemma yields is the key ingredient in the proof of Theorem 4 given here, which is much more elegant than our original proof.

LEMMA 3. The sequence $\rho_1 = (1, -1, 1, -1, 1, -1, \dots)$ is multiplicative and its inverse μ_1 (also multiplicative) is the sequence whose entries are the coefficients of x in the polynomials g_n.

PROOF. Clearly ρ_1 is multiplicative. Rewrite (A) of Theorem 1 as

$$(-1)^{n+1}x^n = -\sum_{\substack{1\leq d\leq n \\ d\mid n}} (-1)^{n/d} g_d(x) \tag{A}$$

and look at the coefficients of x. The resulting equation is just $e(n) = \rho_1 * \mu_1(n)$, the desired conclusion.

Finally, if ν is multiplicative and a sequence ν^{-1} satisfies $\nu * \nu^{-1} = e$, then ν^{-1} is also multiplicative; this is well known (and is readily proved by induction). ■

N.B. We consider the formal polynomials FP to have multiplication

$$\left(\sum_i a_i x^i\right) \cdot \left(\sum_j b_j x^j\right) = \sum_{i,j} a_i b_j x^{ij}, \tag{$\cdot$}$$

so that x is the identity element. (One may consider this multiplication to reflect composition of functions, or to involve a representation of $\ell_1(\mathbf{N}, \times)$.)

Since the g_n's have been identified for prime power n in Lemma 2, the next theorem gives all the g_n's explicitly.

THEOREM 4. The function $G : n \mapsto g_n$, $\mathbf{N} \to FP$, is multiplicative, so the g_n's satisfy $g_n = \Pi\{g_{p^{n(p)}} \mid p \in P\}$ (product using $(\cdot)$) for $n > 1$ with prime factorization $n = \Pi\{p^{n(p)} \mid p \in P\}$.

PROOF. Let FP^∞ denote the set of sequences in FP, which we assume has multiplication $(\cdot)$. Define $X \in FP^\infty$ by $X(n) = (-1)^{n+1}x^n$, and note that X is multiplicative. Then equation (A) in Lemma 3 says that $X = G * \rho_1$, and so $G = X * \mu_1$. Thus G is the convolution of multiplicative functions, and hence is multiplicative. ■

The first corollary is a direct consequence of Lemma 2 and the fact that G is multiplicative; we may view it as extending Fermat's Little Theorem to non-primes.

COROLLARY 5. For all $n \in \mathbf{N}$, g_n/n is an IVP.

We can also identify μ_1 (of Lemma 3) explicitly in terms of the Möbius function μ.

COROLLARY 6. Let $n \in \mathbf{N}$ and write $n = 2^r n'$, where n' is odd. Then $\mu_1(n) = 2^{r-1}\mu(n')$.

PROOF. This follows directly from Theorem 1 and Lemma 2. (Recall that x is the multiplicative identity of FP.) ■

ANOTHER SEQUENCE OF POLYNOMIALS.

The more complicated formulae for the g_{2^r}'s presented an obstacle to the explicit identification of the g_n's. Especially with hindsight we can identify a more tractable related sequence $\{g'_n\} \subset FP$, where $g'_{p^r} = x^{p^r} - x^{p^{r-1}}$ for *all* prime powers (not just the odd ones) and the function $G' : n \mapsto g'_n$, $\mathbf{N} \to FP$, is multiplicative; thus, for $n \in \mathbf{N}$ with prime factorization $\Pi\{p^{n(p)} \mid p \in P\}$

$$g'_n = \Pi_{p\in P}(x^{n(p)} - x^{n(p)-1}),$$

and g'_n/n is an IVP. Computations (up to $n = 50$) indicate that the polynomials $\{g'_n\}$ arise from $(\mathbf{Z}^\infty, \otimes'')$ with multiplication

$$(x'_1, x'_2, x'_3, x'_4, \ \dots\ ) \otimes'' (x_1, x_2, x_3, x_4, \ \dots\ ) =$$

$$(x'_1 + x_1, x'_2 - x'_1x_1 + x_2, x' - x'_2x_1 - x'_1x_2 + x_3, x'_4 - x'_3x_1 - x'_2x_2 - x'_1x_3 + x_4, \ \dots\ )$$

in the same way that the polynomials $\{g_n\}$ arose from $(\mathbf{Z}^\infty, \otimes)$. The corresponding homomorphism $E'' : (\mathbf{Z}^\infty, \otimes'') \to FP$ is given by

$$E''(a) = E''(a_1, a_2, a_3, \ \dots\ ) = 1 - \sum_{n=1}^{\infty} a_n t^n.$$

In this situation, the formulae (A) and (B) of Theorem 1 need to be modified so that 2 is treated in the same way as the other primes. Thus the g'_n's satisfy

$$\text{(A}'\text{)} \qquad x^n = \sum_{\substack{1\le d\le n \\ d \mid n}} g'_d(x).$$

(The corresponding (B′) has the term $(-1)^{k+1}$ omitted from the equation in (b) of (B).) So, if $X' \in FP^\infty$ is defined by $X'(n) = x^n$, then $X' = G' * \rho$ and $G' = X' * \mu$.

APPENDIX. It is from the 'obvious' isomorphism between $(\mathbf{Z}^\infty, \otimes)$ and $(\mathbf{Z}^\infty, +)$ that we get the sequence of polynomials $\{P_n\}$. Here are some details. Consider $s_1 = (1, 0, 0, 0, \ \dots\ ) \in (\mathbf{Z}^\infty, \otimes)$; then

$$s_1^2 = s_1 \otimes s_1 = (2, 1, 0, 0, 0, \ \dots\ ) = \left(2, \binom{2}{2}, 0, 0, 0, \ \dots\ \right),$$

$$s_1^3 = s_1 \otimes s_1 \otimes s_1 = (3, 3, 1, 0, 0, 0, \ \dots\ ) = \left(3, \binom{3}{2}, \binom{3}{3}, 0, 0, 0, \ \dots\ \right), \text{ and}$$

$$s_1^n = \left(n, \binom{n}{2}, \binom{n}{3}, \ \dots\ , \binom{n}{n}, 0, 0, 0, \ \dots\ \right).$$

Also, for $s_2 = (0, 1, 0, 0, 0, \ \dots\ )$ and $s_3 = (0, 0, 1, 0, 0, 0, \ \dots\ )$ in $(\mathbf{Z}^\infty, \otimes)$,

$$s_2^n = \left(0, n, 0, \binom{n}{2}, 0, \binom{n}{3}, 0, \ \dots\ , 0, \binom{n}{n}, 0, 0, 0, \ \dots\ \right), \text{ and}$$

$$s_3^n = \left(0, 0, n, 0, 0, \binom{n}{2}, 0, 0, \binom{n}{3}, 0, 0, \ \dots\ , 0, 0, \binom{n}{n}, 0, 0, 0, \ \dots\ \right),$$

etc. Since the groups are abelian, a homomorphism $\varphi : (\mathbf{Z}^\infty, +) \to (\mathbf{Z}^\infty, \otimes)$ is given by

$$\varphi : x = (x_1, x_2, x_3, \ldots) =$$

$$(x_1, 0, 0, 0, \ldots) + (0, x_2, 0, 0, 0, \ldots) + (0, 0, x_3, 0, 0, 0, \ldots) + \ldots$$

$$\mapsto s_1^{x_1} \otimes s_2^{x_2} \otimes s_3^{x_3} \otimes \text{ (terms with first 3 entries = 0)} =$$

$$\left(x_1, \binom{x_1}{2}, \binom{x_1}{3}, \ldots\right) \otimes \left(0, x_2, 0, \binom{x_2}{2}, 0, \ldots\right) \otimes \left(0, 0, x_3, 0, 0, \binom{x_3}{2}, \ldots\right) \otimes \ldots$$

$$= \left(x_1, x_2 + \binom{x_1}{2}, x_3 + x_1 x_2 + \binom{x_1}{3}, \ldots\right).$$

It is the inverse of φ that gives the desired sequence of polynomials; a few terms of $\varphi^{-1} : (\mathbf{Z}^\infty, \otimes) \to (\mathbf{Z}^\infty, +)$ are easy to calculate by hand,

$$\varphi^{-1} : (x_1, x_2, x_3, x_4, \ldots) \mapsto (\underline{x_1}, x_2 \underline{- (x_1^2 - x_1)/2}, x_3 - x_1 x_2 + \underline{(x_1^3 - x_1)/3},$$

$$x_4 - x_1 x_3 - (x_2^2 - x_2)/2 + x_1^2 x_2 \underline{- (x_1^4 - x_1)/4 - (x_1^2 - x_1)/4}, \ldots).$$

The sequence $\{P_n\}$ can be seen emerging in the x_1 variable; $P_1 - P_4$ are underlined.

We remark that, although φ seems an obvious isomorphism in this context, its analogue for Witt vector addition (which yields an isomorphism of the additive group of Witt vectors and $(\mathbf{Z}^\infty, +)$) is not the Witt vector map and does not yield Witt vector multiplication.

In conclusion, we pose some

QUESTIONS. 1. We have $P_n = g_n/n$ for $n \leq 100$; does this equality hold for all n? (The analogous question can be posed for the g_n''s.) To this end, R. Girgensohn has shown for all n that the coefficient of x in P_n is the same as that in g_n/n.

2. If, as we suspect, question 1 has a positive answer, why does the isomorphism $\varphi : (\mathbf{Z}^\infty, +) \to (\mathbf{Z}^\infty, \otimes)$ yield such a structured sequence of polynomials?

ACKNOWLEDGEMENT. This work was supported in part by NSERC grant A7857.

REFERENCES

[1] ALFORD, W.F., GRANVILLE A. and POMERANCE C., "There are infinitely many Carmichael numbers", *Ann. Math.* **140** (1994), 703-722.

[2] BAKER, A., "A concise introduction to the theory of numbers", *Cambridge U. P.,* Cambridge, 1984.

[3] DEMAZURE, M., "Lectures on p-divisible groups", Lecture Notes in Mathematics #302, *Springer-Verlag,* New York, 1972.

[4] LANG, S., "Algebra", *Addison-Wesley*, Reading, Mass., Revised printing, 1971.

[5] MILNES, P., "Ellis groups and group extensions", *Houston J. Math.* **12** (1986), 87-108.

[6] NAMIOKA, I., "Ellis groups and compact right topological groups", *Amer. Math. Soc. Contemporary Math.* **26** (1984), 295-300.