Congruence properties of binary partition functions

Katherine Anders, Melissa Dennison, Jennifer Weber Lansing and Bruce Reznick

Abstract. Let $\mathcal{A}$ be a finite subset of $\mathbb{N}$ containing 0, and let $f(n)$ denote the number of ways to write n in the form $\sum \epsilon_j 2^j$, where $\epsilon_j \in \mathcal{A}$. We show that there exists a computable $T = T(\mathcal{A})$ so that the sequence $(f(n) \bmod 2)$ is periodic with period T. Variations and generalizations of this problem are also discussed.

Mathematics Subject Classification (2010). Primary:11A63,11P81, Secondary: 11B34, 11B50.

Keywords. partitions, digital representations, Stern sequence.

1. Introduction

Let $\mathcal{A} = \{0 = a_0 < a_1 < \cdots\}$ denote a finite or infinite subset of $\mathbb{N}$ containing 0, and fix an integer $b \geq 2$. Let $f_{\mathcal{A},b}(n)$ denote the number of ways to write n in the form

$$n = \sum_{k=0}^{\infty} \epsilon_k b^k, \qquad \epsilon_k \in \mathcal{A}. \tag{1.1}$$

The uniqueness of the standard base-b representation of $n \geq 0$ reflects the fact that $f_{\mathcal{A},b}(n) = 1$ for $\mathcal{A} = \{0, \ldots, b-1\}$. For non-standard bases, the behavior of $f_{\mathcal{A},b}(n)$ has been studied primarily when $\mathcal{A} = \mathbb{N}$ or $b = 2$, in terms of congruences at special values, and also asymptotically. In this paper, we are concerned with the behavior of $f_{\mathcal{A},b}(n) \pmod{d}$, especially when $b = d = 2$, and when $\mathcal{A}$ is finite.

We associate to $\mathcal{A}$ its characteristic function $\chi_{\mathcal{A}}(n)$, and the generating function

$$\phi_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} \chi_{\mathcal{A}}(n) x^n = \sum_{a \in \mathcal{A}} x^a = 1 + x^{a_1} + \cdots . \tag{1.2}$$

Anders and Weber Lansing received support from National Science Foundation grant DMS 0838434 EMSW21MCTP: Research Experience for Graduate Students.

Let

$$F_{\mathcal{A},b}(x) := \sum_{n=0}^{\infty} f_{\mathcal{A},b}(n)x^n \tag{1.3}$$

denote the generating function of $f_{\mathcal{A},b}(n)$. Viewing (1.1) as a partition problem, we find an immediate infinite product representation for $F_{\mathcal{A},b}(x)$:

$$F_{\mathcal{A},b}(x) = \prod_{k=0}^{\infty}\left(1 + x^{a_1 b^k} + \cdots\right) = \prod_{k=0}^{\infty} \phi_{\mathcal{A}}(x^{b^k}). \tag{1.4}$$

Observe that (1.1) implies that $n \equiv \epsilon_0 \pmod b$. Thus, every such representation may be rewritten as

$$n = \sum_{j=0}^{\infty} \epsilon_j b^j = \epsilon_0 + b\left(\sum_{j=0}^{\infty} \epsilon_{j+1} b^j\right). \tag{1.5}$$

Since $f_{\mathcal{A},b}(n) = 0$ for $n < 0$, we see that (1.5) gives the recurrence

$$f_{\mathcal{A},b}(n) = \sum_{\substack{a\in\mathcal{A},\\ n\equiv a \bmod b}} f_{\mathcal{A},b}\left(\tfrac{n-a}{b}\right), \quad \text{for} \quad n \geq 1. \tag{1.6}$$

Alternatively, decompose $\mathcal{A}$ into residue classes mod b and write

$$\mathcal{A} = \bigcup_{i=0}^{b-1} \mathcal{A}_i, \quad \text{where} \quad \mathcal{A}_i := \mathcal{A} \cap (b\mathbb{Z} + i). \tag{1.7}$$

If we write $\mathcal{A}_i = \{bv_{k,i} + i\}$, then for $m \geq 0$ and $0 \leq i \leq b-1$:

$$f_{\mathcal{A},b}(bm + i) = \sum_k f_{\mathcal{A},b}(m - v_{k,i}). \tag{1.8}$$

The initial condition $f_{\mathcal{A},b}(0) = 1$, combined with (1.6) or (1.8), is sufficient to determine $f_{\mathcal{A},b}(n)$ for all $n > 0$.

We say that a sequence (u_n) is *ultimately periodic* if there exist integers $N \geq 0$, $T \geq 1$ so that, for $n \geq N$, $u_{n+T} = u_n$. The *period* of an ultimately periodic sequence is the smallest such T. By extension, we say that the set $\mathcal{A}$ is *ultimately periodic* if the sequence of its characteristic function, $(\chi_{\mathcal{A}}(n))$, is ultimately periodic. Equivalently, $\mathcal{A}$ is ultimately periodic if there exists T, and $k \geq 1$ integers $r_1, \ldots, r_k$, $0 \leq r_i \leq T-1$, so that the symmetric set difference of $\mathcal{A}$ and $\cup(T\mathbb{N} + r_i)$ is finite. In particular, if $\mathcal{A}$ is finite or the complement of a finite set, then $\mathcal{A}$ is ultimately periodic.

Theorem 1.1. *As elements of* $\mathbb{F}_2[[x]]$,

$$F_{\mathcal{A},2}(x)\phi_{\mathcal{A}}(x) = 1. \tag{1.9}$$

This theorem also appears as [5, Lemma 2.2(ii)], although the implications we discuss here for digital representations are not pursued there in detail. Theorem 1.1 has an immediate corollary.

Corollary 1.2.

1. *If $\mathcal{A}$ is finite, then there is a computable integer $T = T(\mathcal{A}) > 0$ so that for all $n \geq 0$, $f_{\mathcal{A},2}(n) \equiv f_{\mathcal{A},2}(n+T) \pmod 2$.*
2. *If $\mathcal{A}$ is infinite, then the following are equivalent:*
   (i) *The sequence $(f_{\mathcal{A},2}(n) \pmod 2)$ is ultimately periodic.*
   (ii) *$\phi_{\mathcal{A}}(x)$ is the power series of a rational function in $\mathbb{F}_2(x)$.*
   (iii) *The set $\mathcal{A}$ is ultimately periodic.*

It will follow from Corollary 1.2(1) that if $\mathcal{A}$ is a finite set, and $T = T(\mathcal{A})$, then there is a *complementary* finite set $\mathcal{A}' = \{0 = b_0 < b_1 < \cdots\}$ so that

$$\begin{aligned} f_{\mathcal{A},2}(n) \quad &\text{is odd} \iff n \equiv b_k \pmod T \quad \text{for some } b_k; \\ f_{\mathcal{A}',2}(n) \quad &\text{is odd} \iff n \equiv a_k \pmod T \quad \text{for some } a_k. \end{aligned} \tag{1.10}$$

Complementary sets needn't look very much alike. If $\mathcal{A} = \{0, 1, 4, 9\}$, then $T = 84$ and $|\mathcal{A}'| = 41$, with elements ranging from 0 to 75 (see Example 4.3).

One instance of Theorem 1.1 in the literature comes from the *Stern sequence* $(s(n))$ (see [13, 8, 11]), which is defined by

$$\begin{gathered} s(0) = 0, \ s(1) = 1; \\ s(2n) = s(n), \ s(2n+1) = s(n) + s(n+1) \quad \text{for } n \geq 1. \end{gathered} \tag{1.11}$$

It was proved in [10] that $s(n) = f_{\{0,1,2\},2}(n-1)$, under which the recurrence (1.11) is a translation of (1.8). It is easy to prove, and has basically been known since [13, p.197], that $s(n)$ is even if and only if n is a multiple of three. A simple application of Theorem 1.1 shows that in $\mathbb{F}_2(x)$,

$$F_{\{0,1,2\},2}(x) = \frac{1}{1+x+x^2} = \frac{1+x}{1+x^3} = 1+x+x^3+x^4+x^6+x^7+\cdots. \tag{1.12}$$

This result was generalized in [10, Th.2.14], using the infinite product (1.4). Here, let $\mathcal{A}_d = \{0, \ldots, d-1\}$. Then $\phi_{\mathcal{A}_d}(x) = \frac{1-x^d}{1-x}$, so in $\mathbb{F}_2(x)$,

$$F_{\mathcal{A}_d,2}(x) = \frac{1+x}{1+x^d} = 1 + x + x^d + x^{d+1} + x^{2d} + x^{2d+1} + \cdots. \tag{1.13}$$

Thus, $f_{\mathcal{A}_d,2}(n)$ is odd if and only if $n \equiv 0, 1 \pmod d$.

We also show that there is no obvious "universal" generalization of Theorem 1.1 to $f_{\mathcal{A},b}(n) \pmod d$, except for the case $b = d = 2$.

Theorem 1.3.

1. *If $(f_{\{0,1,2\},2}(n) \pmod d)$ is ultimately periodic with period T, then $d = 2$ and $T = 3$.*
2. *If $d \geq 2$ and $b \geq 3$, then $(f_{\{0,1\},b}(n) \pmod d)$ is never ultimately periodic.*

Thus, the Stern sequence has no periodicities mod $d \geq 3$ and, there exists a set $\mathcal{A}$ with the property that the number of its representations in any base $b \geq 3$ is never ultimately periodic modulo any $d \geq 2$.

Let $\nu_2(m)$ denote the largest power of 2 dividing m. In 1969, Churchhouse [4] conjectured, based on numerical evidence, that $f_{\mathbb{N},2}(n)$ is even for $n \geq 2$, that $4 \mid f_{\mathbb{N},2}(n)$ if and only if either $\nu_2(n-1)$ or $\nu_2(n)$ is a positive even integer, and that 8 never divides $f_{\mathbb{N},2}(n)$. He also conjectured that, for all even m,

$$\nu_2(f_{\mathbb{N},2}(4m)) - \nu_2(f_{\mathbb{N},2}(m)) = \lfloor \tfrac{3}{2}(3\nu_2(m) + 4) \rfloor. \tag{1.14}$$

This conjecture was proved in the next few years by Rødseth, and by Gupta and generalized by Hirschhorn and Loxton, Rødseth, Gupta, Andrews, Gupta and Pleasants, and most recently by Rødseth and Sellers [12]. We refer the reader to [10, 12] for detailed references. The statements in Theorem 1.3 about the non-existence of recurrences do not apply to formulas such as (1.14). On the other hand, $\phi_{\mathbb{N}}(x) = (1 + x)^{-1}$, so Theorem 1.1 implies that $f_{\mathbb{N},2}(n)$ is even for $n \geq 2$.

The paper is organized as follows. In section two, we review some familiar facts about polynomials and rational functions over $\mathbb{F}_2$. Most of this material can be found in [9], and is included here for the sake of completeness. In section three, we give two proofs of Theorem 1.1 and then prove Corollary 1.2 and Theorem 1.3. In section four, we present several examples and applications of Theorem 1.1.

Portions of the research in this paper were contained in Dennison's UIUC Ph.D. dissertation [6] and in the UIUC Summer 2010 Research Experiences for Graduate Students (REGS) project [1] of Anders and Weber Lansing. These projects were written under Reznick's supervision.

The authors thank Bob McEliece and Kevin O'Bryant for helpful correspondence, and the referee for an insightful report.

2. Background

There is an important relationship between rational functions in $\mathbb{F}_2[[x]]$ and ultimately periodic sequences. (For additional information about most of the material in this section, see [9], especially Chapter 8, "Linear Recurring Sequences".) We first recall some familiar facts about finite fields, identifying $\mathbb{Z}/p\mathbb{Z}$ with $\mathbb{F}_p$ for prime p. The binomial theorem implies that for $a, b \in \mathbb{F}_p$, $(a + b)^p = a^p + b^p$, hence $(\sum a_i)^p = \sum a_i^p$. It follows from this fact and Fermat's Little Theorem that for any polynomial $f \in \mathbb{F}_p[x]$,

$$f(x)^p = f(x^p). \tag{2.1}$$

If $f \in \mathbb{F}_2[x]$ is an irreducible polynomial of degree $d \geq 2$ (so $f(0) \neq 0$), then it is well-known that $f(x) \mid 1 + x^{2^d - 1}$. Repeated application of (2.1) for $p = 2$ shows that $(1 + x^M)^{2^k} = 1 + x^{2^k \cdot M}$, hence if $f \in \mathbb{F}_2[x]$ is irreducible and $j \leq 2^k$, then $f(x)^j \mid 1 + x^{2^k \cdot (2^d - 1)}$. This leads immediately to the following lemma (see [2, Thm.6.21]):

Lemma 2.1. *Suppose $h \in \mathbb{F}_2[x]$, $h(0) \neq 0$ and h can be factored over $\mathbb{F}_2[x]$ as*

$$h = \prod_{i=1}^{s} f_i^{e_i}, \tag{2.2}$$

where the f_i *are distinct irreducible polynomials with* $\deg(f_i) = d_i$*, and suppose* $2^k \geq e_i$ *for all* i *and some* $k \in \mathbb{N}$*. Then*

$$h(x) \mid 1 + x^M, \ \textit{where} \quad M := M(h) = 2^k \cdot \mathit{lcm}(2^{d_1} - 1, \ldots, 2^{d_s} - 1). \quad (2.3)$$

Suppose $h \in \mathbb{F}_2[x]$ and $h(0) = 1$. The *period* of h is the smallest $T \geq 1$ so that $h(x) \mid 1 + x^T$; this definition does not assume that h is irreducible. The period of h can be much smaller than $M(h)$, however it is always a divisor of $M(h)$.

Lemma 2.2. *If* h *has period* T*, then* $h(x) \mid 1 + x^V$ *in* $\mathbb{F}_2[x]$ *if and only if* $T \mid V$*.*

Proof. We first note that $(1 + x^T) \mid (1 + x^{kT})$, proving one direction. For the other, suppose $h(x) \mid 1 + x^V$; then $V \geq T$. Write $V = kT + r$, where $0 \leq r \leq T - 1$. Then $h(x)$ also divides

$$x^r(1 + x^{kT}) + 1 + x^V = 1 + x^r, \quad (2.4)$$

which violates the minimality of T unless $r = 0$. □

If $h \in \mathbb{F}_2[x]$ is irreducible, $\deg h = r$ and the period of h is $2^r - 1$, then h is called *primitive*; see e.g.[9, §3.15]. Primitive trinomials have attracted much recent interest, especially when $2^r - 1$ is a Mersenne prime (see [3]); Lemma 2.1 implies that all such irreducible h are primitive. In coding theory, h is called the *generator* polynomial and

$$q(x) = \frac{1 + x^T}{h(x)} \quad (2.5)$$

is called the *parity-check* polynomial.

Consider a rational function in $\mathbb{F}_2(x)$:

$$\frac{g(x)}{h(x)} = a(x) + \frac{r(x)}{h(x)}, \quad (2.6)$$

where g, h, a, r are polynomials, and $\deg r < \deg h$. We make the additional assumption that $h(0) \neq 0$. Lemma 2.1 leads to an important relationship between rational functions and ultimately periodicity.

Lemma 2.3. *Suppose* $b(x) = \sum b_n x^n \in \mathbb{F}_2[[x]]$ *with* $b_0 = 1$*. Then* $b(x)$ *is a rational function if and only if* $\{n : b_n = 1\}$ *is ultimately periodic.*

Proof. First suppose there exists T, N so that $b_n = b_{n+T}$ for $n \geq N$. Then the coefficient of x^{n+T} in

$$(1 + x^T) \left(\sum_{n=0}^{\infty} b_n x^n \right) \quad (2.7)$$

is $b_{n+T} + b_n = 0$ for $n \geq N$. Hence, $b(x)$ is the quotient of a polynomial of degree less than N and $1 + x^T$, and is thereby a rational function. Conversely, suppose $b = g/h$ is rational and is given by (2.6) with $h(0) = 1$. Then by

Lemma 2.1 and the division algorithm, there exists $q(x) \in \mathbb{F}_2[x]$ and T so that

$$b(x) = a(x) + \frac{r(x)}{h(x)} = a(x) + \frac{r(x)q(x)}{1+x^T}, \tag{2.8}$$

hence $(1+x^T)b(x)$ is a polynomial of degree less than M (say), so $b_n = b_{n+T}$ for $n \ge M$. □

3. Proofs

We start this section with two proofs of Theorem 1.1. The first one is somewhat longer, but yields a recurrence of independent interest.

As in (1.7), write

$$\begin{gathered} \mathcal{A} = \{0 = a_0 < a_1 < \cdots\} = \mathcal{A}_0 \cup \mathcal{A}_1; \\ \mathcal{A}_0 = \{0 = 2b_0 < 2b_1 < \cdots\}, \qquad \mathcal{A}_1 = \{2c_1 + 1 < \cdots\}. \end{gathered} \tag{3.1}$$

We will write $f_{\mathcal{A},2}(n)$ as $f(n)$ when there is no ambiguity. By (1.8), we have:

$$f(2n) = \sum_i f(n-b_i), \qquad f(2n+1) = \sum_j f(n-c_j). \tag{3.2}$$

Theorem 3.1. *For all $n \in \mathbb{Z}$, $n \ne 0$,*

$$\Theta(n) := \sum_k f(n-a_k) \equiv 0 \pmod 2. \tag{3.3}$$

Proof. If $n < 0$, then $f(n) = 0$, so this is immediate; also $\Theta(0) = f(0) = 1$. Suppose $n > 0$. We distinguish two cases: $n = 2m$ and $n = 2m+1$, and put (3.2) back into itself. We then diagonalize the double sums below; for each fixed m, these sums are finite:

$$\begin{aligned} \Theta(2m) &= \sum_k f(2m-a_k) = \sum_i f(2m-2b_i) + \sum_j f(2m-2c_j-1) \\ &= \sum_i \sum_u f(m-b_i-b_u) + \sum_j \sum_v f(m-c_j-1-c_v) \\ &= \sum_i f(m-2b_i) + 2\sum_{i<u} f(m-b_i-b_u) \\ &+ \sum_j f(m-2c_j-1) + 2\sum_{j<v} f(m-c_j-c_v-1) \\ &\equiv \Theta(m) \pmod 2. \end{aligned} \tag{3.4}$$

Similarly,

$$\begin{aligned}\Theta(2m+1) &= \sum_k f(2m+1-a_k) \\ &= \sum_i f(2m+1-2b_i) + \sum_j f(2m-2c_j) \\ &= \sum_i \sum_j f(m-b_i-c_j) + \sum_j \sum_i f(m-c_j-b_i) \\ &= 2\sum_{i,j} f(m-b_i-c_j) \equiv 0 \pmod 2.\end{aligned} \tag{3.5}$$

Since $\Theta(2m) \equiv \Theta(m)$ and $\Theta(2m+1) \equiv 0$, it follows by induction that $\Theta(m) \equiv 0$ for $m \geq 1$. □

We give two proofs of Theorem 1.1. The first uses Theorem 3.1; the second uses the generating function (1.3) and is also [5, Lemma 2.1].

First proof of Theorem 1.1. Write out the product in (1.9) and use Theorem 3.1.

$$F_{\mathcal{A},2}(x)\phi_{\mathcal{A}}(x) = \left(\sum_{n=0}^{\infty} f(n)x^n\right)\left(1+\sum_{i\geq 1} x^{a_i}\right) = \sum_{n=0}^{\infty} \Theta(n)x^n \equiv 1. \tag{3.6}$$

□

Second proof of Theorem 1.1. By repeated use of (1.4) and (2.1),

$$\phi_{\mathcal{A}}(x)F_{\mathcal{A},2}^2(x) \equiv \phi_{\mathcal{A}}(x)F_{\mathcal{A},2}(x^2) = \phi_{\mathcal{A}}(x)\prod_{k=0}^{\infty}\phi_{\mathcal{A}}\left(x^{2^{k+1}}\right) = F_{\mathcal{A},2}(x). \tag{3.7}$$

□

The second proof generalizes to primes $p > 2$ via (2.1).

Theorem 3.2. *If $b = p$ is prime, then $F_{\mathcal{A},p}^{p-1}(x)\phi_{\mathcal{A}}(x) = 1 \in \mathbb{F}_p[x]$.*

Proof. As before, we have

$$\phi_{\mathcal{A}}(x)F_{\mathcal{A},p}^p(x) = \phi_{\mathcal{A}}(x)F_{\mathcal{A},p}(x^p) = \phi_{\mathcal{A}}(x)\prod_{k=0}^{\infty}\phi_{\mathcal{A}}(x^{p^{k+1}}) = F_{\mathcal{A},p}(x). \tag{3.8}$$

□

This result may fail if b is not prime. For example, if $\mathcal{A} = \{0,1\}$ and $b = 4$, then $\phi_A(x) = 1 + x$ and the coefficient of x^2 in $F_{\mathcal{A},4}^3(x)\phi_{\mathcal{A}}(x)$ is $6 \not\equiv 0$ mod 4. Theorem 3.2 implies that $F_{\mathcal{A},p}(x) = \phi_{\mathcal{A}}^{-1/(p-1)}(x)$ as an element of $\mathbb{F}_p[[x]]$.

Proof of Corollary 1.2(1). Suppose $\mathcal{A}$ is finite and T is the period of $\phi_{\mathcal{A}}(x)$. Then by Theorem 1.1, we have in $\mathbb{F}_2[x]$

$$F_{\mathcal{A},2}(x) = \frac{1}{\phi_{\mathcal{A}}(x)} = \frac{q(x)}{1+x^T}, \tag{3.9}$$

where $(1+x^T)F_{\mathcal{A},2}(x) = q(x) = 1+\sum x^{b_k}$ and $\deg q < T$. Since the coefficient of x^{n+T} in q is $f(n+T) - f(n) = 0$, $(f(n) \pmod 2)$ is periodic with period T. □

Let $\mathcal{A}' = \{0 = b_0 < b_1 < \cdots\}$ denote the (finite) set of exponents which occur in q in (3.9); $q(x) = \phi_{\mathcal{A}'}(x)$. It follows from Theorem 1.1 that

$$F_{\mathcal{A}',2}(x) = \frac{1}{\phi_{\mathcal{A}'}(x)} = \frac{1}{q(x)} = \frac{\phi_{\mathcal{A}}(x)}{1+x^T}. \tag{3.10}$$

Equation (1.10) now follows from (3.9) and (3.10). One might hope that $(\mathcal{A}')' = \mathcal{A}$, but that will not be the case if $\mathcal{A}'$ has a smaller period than $\mathcal{A}$. For example, if $\mathcal{A}_d = \{0,\dots,d-1\}$, then $\phi_{\mathcal{A}_d}(x)(1+x) = 1+x^d$, so, regardless of d, $\mathcal{A}'_d = \{0,1\}$. In terms of (1.10), $f_{\mathcal{A}_d,2}(n)$ is odd if and only if $n \equiv 0,1 \pmod d$ (as proved in [10]) and $f_{\mathcal{A}'_d,2}(n)$ is odd if and only if $n \equiv 0,1,\dots,d-1 \pmod d$. That is, $f_{\mathcal{A}'_d,2}(n)$ is odd for all $n \ge 0$, which is true, because it always equals 1.

Since $(f_{\mathcal{A},2}(n) \pmod 2)$ is periodic, it is natural to ask for the proportion of even and odd values. It follows immediately from (1.10) that the density of n for which $f_{\mathcal{A}}(n)$ is odd is equal to $|\mathcal{A}'|/T$. Computations with small examples lead to the conjecture that $|\mathcal{A}'| \le \frac{T+1}{2}$. This conjecture is false. The smallest such example we have found is $\mathcal{A}_0 = \{0,1,5,9,10\}$. It turns out that the period of $\mathcal{A}_0$ is 33 and $|\mathcal{A}'_0| = 18 > \frac{33+1}{2}$. On the other hand, it is well-known that if $\phi_{\mathcal{A}}$ is primitive, then $|\mathcal{A}'| = \frac{T+1}{2}$; see [5, §4] and [9, p.449].

Proof of Corollary 1.2(2). By Lemma 2.3, if $\mathcal{A}$ is infinite, then the sequence $(f_{\mathcal{A},2}(n) \pmod 2)$ is ultimately periodic if and only if $F_{\mathcal{A},2}(x)$ is a rational function, and by Theorem 1.1, this is so if and only if $\phi_{\mathcal{A}}(x)$ is a rational function. Suppose

$$\phi_{\mathcal{A}}(x) = a(x) + \frac{q(x)}{1+x^T} \in \mathbb{F}_2(x), \tag{3.11}$$

where $a, q \in \mathbb{F}_2[x]$, $\deg a < N$ and $\deg q < T$ and $q(x) = 1 + \sum_i x^{b_i}$. Recall that $m \in \mathcal{A}$ if and only if x^m appears in $\phi_{\mathcal{A}}(x)$. By (3.11), this holds for $m > N$ if and only if there exists $b_i \in \mathcal{A}'$ so that $N \equiv b_i \pmod T$. □

We conclude this section with proofs of Theorem 1.3(1) and (2).

Proof of Theorem 1.3(1). Let $f(n) := f_{\{0,1,2\},2}(n)$ and suppose $f(n+T) \equiv f(n) \pmod d$ for all sufficiently large n, where T is minimal. By (1.8),

$$f(2m) = f(m) + f(m-1) \quad \text{and} \quad f(2m+1) = f(m) \tag{3.12}$$

for all m. If $T = 2k$ is even, then for all sufficiently large m,

$$\begin{aligned} f(2m+2k+1) \equiv f(2m+1) \pmod{d} \implies \\ f(m+k) \equiv f(m) \pmod{d}, \end{aligned} \tag{3.13}$$

violating the minimality of T, since $k = T/2$.

If $T = 2k+1$ is odd, then for all sufficiently large m,

$$\begin{aligned} f(2m+2k+2) \equiv f(2m+1) \pmod{d} \implies \\ f(m+k+1) + f(m+k) \equiv f(m) \pmod{d}, \end{aligned} \tag{3.14}$$

and

$$\begin{aligned} f(2m+2k+3) \equiv f(2m+2) \pmod{d} \implies \\ f(m+k+1) \equiv f(m) + f(m+1) \pmod{d}. \end{aligned} \tag{3.15}$$

Together, these imply that for all sufficiently large m,

$$\begin{aligned} f(m+k) \equiv -f(m+1) \pmod{d} \implies \\ f(m+1) \equiv f(m+1+(2k-1)) \pmod{d}, \end{aligned} \tag{3.16}$$

which implies that f has a period of $2k-2$. If $k > 1$, then $0 < 2k-2 < 2k+1$ gives a contradiction. If $k = 1$, then $T = 3$.

We now show that $d = 2$. First, $f(2^r - 1) = f(2^{r-1} - 1)$ and so by induction, $f(2^r - 1) = f(1) = 1$. Thus, $f(2^r) = f(2^{r-1}) + f(2^{r-1} - 1) = f(2^{r-1}) + 1$ and so by induction, $f(2^r) = r + 1$, implying that $f(2^r + 1) = f(2^{r-1}) = r$ and $f(2^r + 2) = f(2^{r-1}) + f(2^{r-1} + 1) = r + r - 1$. Thus, d divides each $f(2^r + 2) - f(2^r - 1) = 2r - 1 - 1$ for sufficiently large r. Therefore, $d = 2$. □

Proof of Theorem 1.3(2). Suppose $\mathcal{A} = \{0, 1\}$ and $b \geq 3$. Then $f(n) := f_{\mathcal{A},b}(n) = 1$ if n is a sum of distinct powers of b, and 0 otherwise. Suppose that for $n > U$,

$$f(n+T) \equiv f(n) \pmod{d} \tag{3.17}$$

and $d \geq 2$. Then, $f(m) \in \{0, 1\}$ implies that $f(n+T) = f(n)$. Choose j so large that $b^j > T, U$ and suppose that f satisfies (3.17). Then $f(b^j) = 1$, hence $f(b^j + T) = 1$, and so $T = \sum_k b^{r_k}$ with distinct $r_k < j$. But then $f(b^j + 2T) = 1$ by periodicity, and so $b^j + 2\sum_k b^{r_k}$ must be also a sum of distinct powers of b, violating the uniqueness of the (standard) base-b representation. □

4. Examples

Example 4.1. The periodicity of $f_{\mathcal{A}_d,2}(n)$ was established in [10], motivated by the interpretation of the Stern sequence. In her dissertation, Dennison [6] studied a variation on the Stern sequence defined by flipping the recurrence (1.11) to a two-parameter family of sequences. The periodicities discovered in [6] for $\mathcal{A} = \{0, 1, 3\}$ and $\mathcal{A} = \{0, 2, 3\}$ led Reznick to suggest that Anders and Weber Lansing look at generalizations as the topic for their 2010 summer research project [1].

For $\alpha, \beta \in \mathbb{C}$, define $b_{\alpha,\beta}(n)$ by

$$\begin{gathered} b_{\alpha,\beta}(1) = \alpha, \qquad b_{\alpha,\beta}(2) = \beta, \\ b_{\alpha,\beta}(2n) = b_{\alpha,\beta}(n) + b_{\alpha,\beta}(n+1) \text{ for } n \geq 2, \\ b_{\alpha,\beta}(2n+1) = b_{\alpha,\beta}(n) \text{ for } n \geq 1. \end{gathered} \tag{4.1}$$

(In order for the recurrence to be unambiguous, it cannot be applied to $b_{\alpha,\beta}(2)$; the value of $b_{\alpha,\beta}(0)$ plays no further role.) It is proved in [6] that $b_{0,1}(n+2) = f_{\{0,2,3\},2}(n)$ for $n \geq 0$. It was also proved there by an argument similar to the proof of Theorem 3.1 that $b_{0,1}(n) \equiv b_{0,1}(n+7) \mod 2$, and is odd when $n \equiv 0, 2, 3, 4 \pmod 7$. This suggested looking at $f_{\{0,1,3\},2}(n)$, which is also periodic with period 7, and is odd when $n \equiv 0, 1, 2, 4 \pmod 7$.

The proofs of these facts are now straightforward in view of Theorem 1.1; we have in $\mathbb{F}_2(x)$:

$$F_{\{0,2,3\}}(x) = \frac{1}{1+x^2+x^3} = \frac{(1+x+x^3)(1+x)}{1+x^7} = \frac{1+x^2+x^3+x^4}{1+x^7};$$
$$F_{\{0,1,3\}}(x) = \frac{1}{1+x+x^3} = \frac{(1+x^2+x^3)(1+x)}{1+x^7} = \frac{1+x+x^2+x^4}{1+x^7}.$$

Thus, $\{0,2,3\}' = \{0,2,3,4\}$ and $\{0,1,3\}' = \{0,1,2,4\}$.

Example 4.2. For $r \geq 2$, define the sets $\mathcal{A}_r = \{0,1,2,\ldots,2^r\}$ and $\mathcal{B}_r = \{0,1,3,\ldots,2^r-1\}$, and let $g_r = \phi_{\mathcal{A}_r}$ and $h_r = \phi_{\mathcal{B}_r}$ for short. Then $g_r(x) = 1 + xh_r(x)$, so in $\mathbb{F}_2[x]$,

$$\begin{gathered} g_r(x)h_r(x) = h_r(x) + xh_r^2(x) = h_r(x) + xh_r(x^2) = \\ 1 + \sum_{\ell=1}^{r} x^{2^\ell-1} + x + \sum_{\ell=1}^{r} x^{2^{\ell+1}-2+1} = 1 + x^{2^{r+1}-1}. \end{gathered} \tag{4.2}$$

This in itself does not establish that $\mathcal{A}_r, \mathcal{B}_r$ are complementary, or that they both have period $2^{r+1}-1$. If either period T were a proper factor of $2^{r+1}-1$, then since T is odd, $T \leq \frac{1}{3}(2^{r+1}-1) < 2^r - 1 < 2^r$, a contradiction. Thus g_r and h_r each have period $2^{r+1}-1$.

We may interpret this result combinatorially: $f_{\mathcal{A}_r,2}(n)$ is the number of ways to write

$$n = \sum_{i=0}^{\infty} \epsilon_i 2^{i+k_i}, \tag{4.3}$$

where $\epsilon_i \in \{0,1\}$ and $0 \leq k_i \leq r$, and $f_{\mathcal{A}_r,2}(n)$ is even, except when there exists $\ell < r$ so that $n \equiv 2^\ell - 1 \pmod{2^{r+1}-1}$. The infinite version of this example can be found in [5, §5].

Example 4.3. We return to $\mathcal{A} = \{0,1,4,9\}$; in $\mathbb{F}_2[x]$,

$$\phi_{\mathcal{A}}(x) = 1 + x + x^4 + x^9 = (1+x)^4(1+x+x^2)(1+x^2+x^3). \tag{4.4}$$

Note that $1+x$ has period 1, $1+x+x^2$ has period 3, and we have already seen that $1+x+x^3$ has period 7. Since the maximum exponent in (4.4) is $\leq 2^2$, Lemma 2.1 implies that the period of $\mathcal{A}$ divides $4 \cdot \mathrm{lcm}(1,3,7) = 84$. Another calculation shows that $\phi_{\mathcal{A}}(x)$ does not divide $1+x^{\frac{84}{p}}$ for $p = 2, 3, 7$, and so 84 is actually the period. A computation shows that $\mathcal{A}' = \{0, 1, 2, 3, \ldots, 70, 75\}$ has 41 terms, as noted earlier. Thus $f_{\mathcal{A}}(n)$ is odd $\frac{41}{84}$ of the time and even $\frac{43}{84}$ of the time. The infinite version of this example can be found in [5, §6.1].

Example 4.4. Although Theorem 1.1 does not generalize to all $\mathcal{A}$ if $(b, d) \neq (2, 2)$, there are a few exceptional cases. Problem B2 on the 1983 Putnam [7] in effect asked for a proof that for $\mathcal{A} = \{0, 1, 2, 3\}$,

$$f_{\mathcal{A},2}(n) = \left\lfloor \frac{n}{2} \right\rfloor + 1. \tag{4.5}$$

This can be seen directly from (1.4), since $\phi_{\mathcal{A},2}(x) = (1 + x)(1 + x^2) = \frac{1-x^4}{1-x}$, hence $F_{\mathcal{A},2}(x)$ telescopes to $\frac{1}{(1-x)(1-x^2)}$. It follows immediately that $f_{\mathcal{A},2}(n+2d) = f_{\mathcal{A},2}(n)+d$, and hence $f_{\mathcal{A},2}$ is periodic mod d with period $2d$, for each $d \geq 2$. A similar phenomenon occurs for $\mathcal{A}_b = \{0, 1, \ldots, b^2 - 1\}$, so that $\phi_{\mathcal{A}_b,b}(x) = \frac{1-x^{b^2}}{1-x}$ and $F_{\mathcal{A}_b,b}(x) = \frac{1}{(1-x)(1-x^b)}$, implying that $f_{\mathcal{A}_b,b}(n) = \lfloor \frac{n}{b} \rfloor + 1$ and $f_{\mathcal{A}_b,b}(n + bd) = f_{\mathcal{A}_b,b}(n) + d$.

Example 4.5. Let $\mathcal{A} = \{0\} \cup (2\mathbb{N} + 1)$ (all non-zero digits in (1.1) are odd). Then

$$\phi_{\mathcal{A}}(x) = 1 + \sum_{i=0}^{\infty} x^{2i+1} = 1 + \frac{x}{1 - x^2} = \frac{1 + x - x^2}{1 - x^2}. \tag{4.6}$$

Working in $\mathbb{F}_2(x)$, we have

$$F_{\mathcal{A},2}(x) = \frac{1 - x^2}{1 + x - x^2} = \frac{(1 + x)^2}{1 + x + x^2} = 1 + \frac{x}{1 + x + x^2} = 1 + \frac{x + x^2}{1 + x^3}. \tag{4.7}$$

Thus, $f_{\mathcal{A},2}(n)$ is odd if and only if $n = 0$ or n is not a multiple of 3.

Example 4.6. Let $\mathcal{A}^{\{k\}} := \mathbb{N} \setminus \{k\}$. By Theorem 1.1,

$$\begin{aligned} \phi_{\mathcal{A}^{\{k\}}} &= \frac{1}{1+x} - x^k = \frac{1 - x^k - x^{k+1}}{1+x} \\ \implies F_{\mathcal{A}^{\{k\}}}(x) &= \frac{1+x}{1 + x^k + x^{k+1}} \\ \implies F_{\mathcal{A}^{\{1\}}}(x) &= \frac{1+x}{1+x+x^2} = \frac{(1+x)^2}{1+x^3} = \frac{1+x^2}{1+x^3}. \end{aligned} \tag{4.8}$$

Thus $f_{\mathbb{N}\setminus\{1\},2}(n)$ is odd precisely when $n \equiv 0, 2 \pmod 3$. This may be contrasted with $f_{\{0,1,2\},2}(n)$, which is odd precisely when $n \equiv 0, 1 \pmod 3$.

References

[1] K. Anders and J. Weber, *The parity of generalized binary representations*, REGS report, Aug. 30, 2010.

[2] E. Berlekamp, *Algebraic coding theory, Revised 1984 edition* Aegean Park Press, Laguna Hills, CA, 1984. MR0238597 (38 #6873) (review of first edition).

[3] R. P. Brent and P. Zimmermann, *The great trinomial hunt*, Trans. Amer. Math. Soc., **58** (2011), 233-239, MR2768116.

[4] R. F. Churchhouse, *Congruence properties of the binary partition function*, Proc. Cambridge Philos. Soc., **66** (1969), 371376, MR0248102 (40 #1356).

[5] J. N. Cooper, D. Eichhorn and K. O'Bryant, *Reciprocals of binary series*, Int. J. Number Theory **2**, (2006), no. 4, 499522, MR2281861 (2007h:11015).

[6] M. Dennison, *A sequence related to the Stern sequence*, Ph.D. dissertation, University of Illinois at Urbana-Champaign, 2010.

[7] L. F. Klosinski, G. L. Alexanderson and A. P. Hillman, *The William Lowell Putnam Mathematical Competition*, Amer. Math. Monthly, **91** (1984), 487495, MR1540495.

[8] D. H. Lehmer, *On Stern's diatomic series*, Amer. Math. Monthly, **36** (1929), 59–67, MR1521653.

[9] R. Lidl and H. Niederreiter, *Finite Fields, 2nd ed.* Encyclopedia of Mathematics and its Applications, **20**. Cambridge University Press, Cambridge, 1997, MR1429394 (97i:11115).

[10] B. Reznick, *Some binary partition functions*, Analytic number theory (Allerton Park, IL, 1989), 451477, Progr. Math., 85, Birkhäuser Boston, Boston, MA, 1990, MR1084197 (91k:11092).

[11] B. Reznick, *Regularity properties of the Stern enumeration of the rationals*, J. Integer Seq. **11** (2008), no. 4, Article 08.4.1, MR2447843 (2009g:11016).

[12] Ø. J. Rødseth and J. A. Sellers, *On m-ary partition function congruences: a fresh look at a past problem*, J. Number Theory, **87** (2001), 270281, MR1824148 (2001m:11177).

[13] M. A. Stern, *Ueber eine zahlentheoretische Funktion*, J. Reine Angew. Math., **55** (1858) 193–220.

Katherine Anders
Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801
e-mail: kaanders@illinois.edu

Melissa Dennison
Department of Math and Computer Science, Baldwin-Wallace College, Berea, OH 44017
e-mail: mdenniso@bw.edu

Jennifer Weber Lansing
Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801
e-mail: jlweber@illinois.edu

Bruce Reznick
Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801
e-mail: reznick@illinois.edu