ON A CONJECTURE OF WILF

STEFAN DE WANNEMACKER, THOMAS LAFFEY, AND ROBERT OSBURN

Abstract. Let n and k be natural numbers and let $S(n,k)$ denote the Stirling numbers of the second kind. It is a conjecture of Wilf that the alternating sum

$$\sum_{j=0}^{n}(-1)^j S(n,j)$$

is nonzero for all $n > 2$. We prove this conjecture for all $n \not\equiv 2$ and $\not\equiv 2944838 \bmod 3145728$ and discuss applications of this result to graph theory, multiplicative partition functions, and the irrationality of p-adic series.

1. Introduction

Let n and k be natural numbers. The Stirling numbers $S(n,k)$ of the second kind are given by

$$x^n = \sum_{k=0}^{\infty} S(n,k)(x)_k,$$

where $(x)_k := x(x-1)(x-2)\dots(x-k+1)$ for $k \in \mathbb{N} \setminus \{0\}$ and $(x)_0 := 1$. $S(n,k)$ is the number of ways in which it is possible to partition a set with n elements into exactly k nonempty subsets. Consider the alternating sum

$$f(n) := \sum_{j=0}^{n}(-1)^j S(n,j).$$

The first few terms in the sequence of integers $\{f(n)\}_{n\geq 0}$ are as follows:

$$1, -1, 0, 1, 1, -2, -9, -9, 50, 267, 413, -2180, -17731, -50533, 110176, \dots$$

This is sequence $A000587$ of Sloane [45]. This sequence appears in Example 5(ii), Section 8, Chapter 3 in Ramanujan's second notebook (see page 53 of [2]) and has been subsequently investigated by Beard [1], Harris and Subbarao [25], Uppuluri and Carpenter [47], Kolokolnikova [32], Layman and Prather [35], Subbarao and Verma [42], Yang [49], Klazar [30], and Murty and Sumner [41].

Wilf has conjectured (see [29]) that $f(n) \neq 0$ for all $n > 2$. So, the only value of n for which $f(n)$ vanishes would be $n = 2$. The best known result in this direction is that of Yang [49]. In [49], the author adapted an approach of de Bruijn [9] concerning the saddle point method and used exponential sum estimates from [33] to show that the number of $n \leq x$ with $f(n) = 0$ is $O(x^{2/3})$ where the implied constant is not explicitly computed. Recently, Murty and Sumner have taken a different approach in proving the non-vanishing of $f(n)$. In [41], the authors use the congruence

Date: January 26, 2007.

2000 *Mathematics Subject Classification.* Primary: 11B73 Secondary: 05C70, 11P83, 11J72.

$$f(n) \equiv \sum_{j=0}^{n} S(n,j) \equiv B_n \bmod 2,$$

properties of the Bell numbers B_n, and of ζ_3, a cube root of unity, to prove the following result.

Theorem 1.1. *If $n \not\equiv 2 \bmod 3$, then $f(n) \neq 0$.*

The purpose of this paper is to extend Theorem 1.1 as follows.

Theorem 1.2. *If $n \not\equiv 2$ and $\not\equiv 2944838 \bmod 3145728$, then $f(n) \neq 0$.*

The paper is organized as follows. In Section 2, we use generating functions and properties of finite fields to prove a general congruence for $f(n)$. This congruence (see Proposition 2.3) combined with computer calculations (see the Appendix) yields a proof of Theorem 1.2. In Section 3, we give a brief discussion of other congruences for $f(n)$. In particular we prove a general congruence for $f(n)$ modulo p where p is a prime (see Proposition 3.1). This result generalizes the congruences given by Lemmas 9 and 10 in [41]. We conclude Section 3 by mentioning another approach to the general congruence for $f(n)$ using a certain set of recursively defined polynomials. We relate these polynomials to $f(n)$ and use this relationship to give an alternative proof of Proposition 2.3. In Section 4, we discuss how Theorem 1.2 has applications in three distinct areas of mathematics, namely graph theory, multiplicative partition functions, and to the irrationality of p-adic series.

2. Proof of Theorem 1.2

The proof of Theorem 1.2 contains two key steps. We first derive the generating function for $f(n)$, then use this expression to determine when $f(n)$ has a period of N modulo m where N and m are positive integers. We first require the following well-known property of Stirling numbers of the second kind, namely (see page 34 in [46])

$$\sum_{n \geq k} S(n,k) x^n = \frac{x^k}{(1-x)(1-2x)\cdots(1-kx)}. \tag{1}$$

For more details and basic results on Stirling numbers of the second kind we refer the reader to [8], [23], or [46]. Recent applications of $S(n,k)$ include computing annihilating polynomials for quadratic forms [11]. Further information on these applications can be found in [12]. Using (1), we derive an expression for the generating function of $f(n)$.

Lemma 2.1. *For any positive integer m, the generating function $F(x)$ of $f(n)$ is the following rational function modulo m.*

$$F(x) := \sum_{n \geq 0} f(n) x^n \equiv \frac{Q(x)}{(1-x)(1-2x)\cdots(1-(m-1)x) - (-1)^m x^m} \bmod m, \tag{2}$$

where $Q(x)$ is a polynomial modulo m given by

$$Q(x) := \left(\sum_{k=0}^{m-1} \frac{(-1)^k x^k}{(1-x)(1-2x)\cdots(1-kx)} \right) (1-x)(1-2x)\cdots(1-(m-1)x).$$

Proof. We begin by multiplying both sides of (1) by $(-1)^k$ and summing over k to obtain

$$F(x) = \sum_{n\geq 0} f(n)x^n = \sum_{k\geq 0} \frac{(-1)^k x^k}{(1-x)(1-2x)\cdots(1-kx)}. \tag{3}$$

Now computing $F(x)$ modulo m yields

$$\begin{aligned} &F(x) \\ &\equiv \left(\sum_{k=0}^{m-1} \frac{(-1)^k x^k}{(1-x)(1-2x)\cdots(1-kx)}\right) \cdot \left(\sum_{i=0}^{\infty} \Big(\frac{(-1)^m x^m}{(1-x)(1-2x)\cdots(1-(m-1)x)}\Big)^i\right) \bmod m \\ &\equiv \left(\sum_{k=0}^{m-1} \frac{(-1)^k x^k}{(1-x)(1-2x)\cdots(1-kx)}\right) \cdot \left(1 - \frac{(-1)^m x^m}{(1-x)(1-2x)\cdots(1-(m-1)x)}\right)^{-1} \bmod m \\ &\equiv \frac{Q(x)}{(1-x)(1-2x)\cdots(1-(m-1)x) - (-1)^m x^m} \bmod m, \end{aligned}$$

where $Q(x)$ is defined as above. □

Remark 2.2. Given a positive integer m, we now explain one way to compute a period N for $f(n)$ modulo m. Consider

$$D(x) := (1-x)(1-2x)\cdots(1-(m-1)x) - (-1)^m x^m,$$

which is the denominator of $F(x)$ via Lemma 2.1. Note that $F(x)$ is proper, i.e., the degree of $Q(x)$ is less than the degree of $D(x)$. Let α be a root of $D(x)$ modulo m and view α as the representative of x in the ring $\mathbb{Z}_m[x]/\langle D(x)\rangle$. Let

$$\Gamma(\alpha) := \{a_0 + a_1\alpha + \cdots a_{m-1}\alpha^{m-1} : a_i \in \mathbb{Z}_m\}.$$

Then $\Gamma(\alpha)$ forms a finite semi-group under multiplication. Define $\Gamma^*(\alpha)$ to be the set of invertible elements in $\Gamma(\alpha)$. Then $\Gamma^*(\alpha)$ forms a finite group. Moreover, let $g(x) = (1 - D(x))/x$ and note that $g(\alpha)$ is a polynomial in α of degree at most $m-1$ and hence belongs to $\Gamma(\alpha)$. Also we have $g(\alpha)\alpha = 1$ and so α belongs to $\Gamma^*(\alpha)$. As the order of α divides $|\Gamma^*(\alpha)|$,

$$\alpha^{|\Gamma^*(\alpha)|} = 1,$$

and so α is a root of $x^{|\Gamma^*(\alpha)|} - 1$. Since this is true for all roots of $D(x)$, we get

$$1 - x^N \equiv D(x)M(x) \bmod m$$

where $M(x) \in \mathbb{Z}_m[x]$ and N is the least common multiple of the $|\Gamma^*(\alpha)|$ as α ranges over the roots of $D(x)$. Now if $1 - x^N \equiv D(x)M(x) \bmod m$, then observe that the proper rational function

$$F(x) \equiv \frac{Q(x)M(x)}{1-x^N} \bmod m$$

has a period of N upon multiplying both sides by $1 - x^N$ and comparing coefficients. This in turn implies that $f(n)$ has a period of N modulo m. For example, if $m = 2$, then

$$F(x) \equiv \frac{1}{x^2 + x + 1} \bmod 2.$$

By multiplying both the numerator and denominator by $x+1$, we obtain

$$F(x) \equiv \frac{x+1}{x^3-1} \bmod 2.$$

Thus $f(n) \equiv f(n+3) \bmod 2$ and so we recover Theorem 1.1 as $f(1)$ and $f(3)$ are odd.

We are now in a position to prove a general congruence for $f(n)$.

Proposition 2.3. *Let n, $h \in \mathbb{N}$. Then*

$$f(n) \equiv f(n + 3 \cdot 4^{h-1}) \bmod 2^h.$$

Proof. We first work over the field $\mathbb{F}_2$. Let $m = 2^h$ with $h \geq 1$. By Remark 2.2, it is sufficient to find a positive integer N such that $\alpha^N \equiv 1 \bmod m$ whenever $D(\alpha) \equiv 0 \bmod m$. Let α be a root of $D(x)$. Then

$$\begin{aligned} D(\alpha) &= (1-\alpha)(1-2\alpha)\dots(1-(2^h-1)\alpha) - (-1)^{2^h}\alpha^{2^h} \\ &\equiv (1-\alpha)^{2^{h-1}} + \alpha^{2^h} \bmod 2 \\ &\equiv 1 + \alpha^{2^{h-1}} + \alpha^{2^h} \bmod 2 \\ &\equiv 0 \bmod 2 \end{aligned}$$

and thus $\alpha^{3\cdot 2^{h-1}} \equiv 1 \bmod 2$. So we have $\alpha^{3\cdot 2^{h-1}} \equiv 1 + 2w \bmod 2^h$ for some $w \in \mathbb{Z}$. Then

$$\alpha^{3\cdot 2^{h-1}\cdot 2^{h-1}} \equiv (1+2w)^{2^{h-1}} \equiv 1 + 2^h w + \binom{2^{h-1}}{2} 2^2 w^2 + \dots + (2w)^{2^{h-1}} \bmod 2^h.$$

As $\binom{2^{h-1}}{t} \equiv 0 \bmod 2^h$ for all $1 \leq t \leq 2^{h-1}$, we deduce

$$\alpha^{3\cdot 4^{h-1}} \equiv 1 \bmod 2^h$$

and thus $3 \cdot 4^{h-1}$ is a period for $f(n)$ modulo 2^h.

□

We can now prove Theorem 1.2

Proof. For every fixed value of $h \geq 1$ one can use Proposition 2.3 to compute the values of n in the interval $[0,\ 3 \cdot 4^{h-1} - 1]$ for which the 2-adic valuation of $f(n)$ is at least h. These values will yield the only possible cases mod $3 \cdot 4^{h-1}$ for which Wilf's conjecture might fail, the so-called "open" cases. For large values of h, the computer program given in the Appendix can be used for this purpose. In particular, take $h = 22$ and consider the set

$$N_{22} := \{l \in \mathbb{N} \ : l < 3 \cdot 4^{21} \text{ and } f(l) \not\equiv 0 \bmod 2^{22}\}.$$

The congruence

$$f(n) \equiv f(n + 3 \cdot 4^{21}) \bmod 2^{22}$$

implies that

$$f(N) \neq 0$$

for all $N \equiv l \bmod 3 \cdot 4^{21}$ where $l \in N_{22}$. In particular, since $f(n) \equiv 0 \bmod 2^{22}$ only for the values $n \equiv 2$ and $\equiv 2944838 \bmod 3145728$ when $n < 3 \cdot 4^{21}$, this implies that if $n \not\equiv 2$ and $\not\equiv 2944838 \bmod 3145728$, then $f(n) \neq 0$ and the result follows. □

In the table below we have listed the "open" cases for values of $h \leq 22$.

h	Open cases	mod
1	2	3
2	2, 11	12
3	2	12
4	2	12
5	2	12
6	2, 38	48
7	2, 38	96
8	2, 134	192
9	2, 326	384
10	2, 326	768
11	2, 326	1536
12	2, 1862	3072
13	2, 1862	6144
14	2, 8006	12288
15	2, 20294	24576
16	2, 44870	49152
17	2, 94022	98304
18	2, 192326	196608
19	2, 192326	393216
20	2, 585542	786432
21	2, 1371974	1572864
22	2, 2944838	3145728

3. Other congruences

The purpose of this section is two-fold. We first discuss how Remark 2.2 can also be used to prove other interesting congruences for $f(n)$. Secondly, we provide an alternative approach to proving congruences for $f(n)$ using a recursively defined set of polynomials. We begin with an immediate application of Remark 2.2.

Proposition 3.1. *Let n, $h \in \mathbb{N}$ and p be an odd prime. Then*

$$f(n) \equiv f(n + 2\tfrac{p^p-1}{p-1}) \bmod p \tag{4}$$

and

$$f(n) \equiv f(n + \tfrac{2p^{2h-2}(p^p-1)}{(p-1)}) \bmod p^h. \tag{5}$$

Proof. We work over the field $\mathbb{F}_p$. By Fermat's Little Theorem for finite fields, the denominator $D(x)$ can be simplified, namely

$$D(x) = (1-x)(1-2x)\cdots(1-(p-1)x) + x^p \equiv 1 - x^{p-1} + x^p \bmod p.$$

By Remark 2.2, we assume that α is a root of $D(x)$ and let $\beta = 1/\alpha$. Note that the period of α is the same as the period of β. One can then check that

$$\beta(\beta-1)(\beta-2)\cdots(\beta-p+1)+1 \equiv \beta^p - \beta + 1 \equiv 0 \bmod p. \tag{6}$$

We now show by induction on i that $\beta^{p^i} \equiv \beta - i \bmod p$. The result holds for $i = 0$ and $i = 1$ by (6). Assume $\beta^{p^i} \equiv \beta - i \bmod p$. Then

$$\beta^{p^{i+1}} \equiv \left(\beta^{p^i}\right)^p \equiv (\beta - i)^p \equiv \beta^p - i \equiv \beta - (i+1) \bmod p.$$

This proves the claim. Now applying this claim and (6), we have

$$\beta^{1+p+p^2+\cdots+p^{p-1}} \equiv \beta(\beta-1)(\beta-2)\cdots(\beta-p+1) \equiv -1 \bmod p.$$

Therefore $\frac{2(p^p-1)}{p-1}$ is a period of β and hence is a period of α. By Remark 2.2, (4) then follows. The proof of (5) is similar to that of Proposition 2.3 and is left to the reader. □

Remark 3.2. One can ask for the minimal periods for $f(n)$ modulo m. In the table below, we compute the minimal periods for $f(n)$ modulo m for small values of m. The values in this table follow from Propositions 2.3, 3.1, and numerical work. Note that $f(n)$ does not have minimal period $3 \cdot 4^{h-1}$ modulo 2^h as can be seen for $h = 3$ (see Remark 3.8). In general, we conjecture that the minimal period for $f(n)$ modulo p^h where $h \geq 1$ is the one given by (5). We would like to point out (thanks to the referee) that the congruences for $f(n)$ are completely analogous to congruences for the Bell numbers. In particular, it is well known that for prime p, the Bell numbers are periodic with minimal period dividing $\frac{p^p-1}{p-1}$ and that this seems to be the minimal period. No one has been able to prove this claim. For further information regarding congruences for Bell numbers, please see [6], [37], and [48].

m	Minimal period	m	Minimal period
2	3	10	398310
3	$3^3 - 1$	11	$\frac{11^{11}-1}{5}$
4	$3 \cdot 4$	12	1560
5	$\frac{5^5-1}{2}$	13	$\frac{13^{13}-1}{6}$
6	390	14	17294382
7	$\frac{7^7-1}{3}$	15	81091300290
8	$\frac{3 \cdot 4^2}{2}$	16	$3 \cdot 4^3$
9	$\frac{2 \cdot 3^2(3^3-1)}{3-1}$		

We now turn to an alternative approach to proving Proposition 2.3. Consider the set of polynomials defined in the following recursive way:

$$P_0(X) := 1$$
$$P_n(X) := XP_{n-1}(X) - P_{n-1}(X+1),\ n \geq 1.$$

Example 3.3.

$$\begin{aligned} P_1(X) &= X - 1, \\ P_2(X) &= X^2 - 2X, \\ P_3(X) &= X^3 - 3X^2 + 1, \\ P_4(X) &= X^4 - 4X^3 + 4X + 1, \\ P_5(X) &= X^5 - 5X^4 + 10X^2 + 5X - 2. \end{aligned}$$

The generating function of the P_n's is given by

$$P(X,t) := \sum_{n\geq 0} P_n(X)t^n = \sum_{j\geq 0} \frac{(-1)^j t^j}{(1-Xt)(1-(X-1)t)\cdots(1-(X-j)t)}. \tag{7}$$

To see this, multiply the recurrence for the P_n's by t^n and sum over n to get the functional equation

$$P(X,t) = \frac{1 - tP(X+1,t)}{1-Xt},$$

which is satisfied by (7). We now relate these polynomials to $f(n)$ and prove a recursive formula. Precisely, we have

Proposition 3.4. *Let $n \in \mathbb{N}$. Then*
(i) $f(n) = P_n(0)$.
(ii) $P_n(X) = \sum_{j=0}^{n} \binom{n}{j} f(n-j)X^j$.
(iii) $-f(n+1) = \sum_{j=0}^{n} \binom{n}{j} f(n-j)$.

Proof. Taking $X = 0$ in (7) and using (3) yields (i). Now (ii) follows from comparing the coefficient of t^n in (7) and using (1). Finally, by (ii), we have

$$P_n(1) = \sum_{j=0}^{n} \binom{n}{j} f(n-j).$$

Then (iii) follows since $f(n+1) = P_{n+1}(0) = -P_n(1)$. We note that observation (iii) was originally made in the context of multiplicative partition functions (see [42]). □

Remark 3.5. It has been numerically verified that $P_n(X)$ is irreducible over $\mathbb{Z}$ for all $5 < n \leq 200$. We believe that $P_n(X)$ is irreducible over $\mathbb{Z}$ for all $n > 5$. It is not immediately clear that the methods of [7], [15], or [44] can be suitably adapted to prove this claim. Note that this claim implies Wilf's conjecture as the constant term of $P_n(X)$ is $f(n)$.

We now prove the following useful properties of the polynomials $P_n(X)$.

Proposition 3.6. *Let k be a positive integer. Let*

$$\begin{aligned} f_k(X,Y) &:= (X-Y)(X+1-Y)\cdots(X+k-1-Y) \\ &= \sum_{r=0}^{k} a_{r,k}(X)Y^r \end{aligned}$$

where $a_{r,k}(X) \in \mathbb{Z}[X]$. Then for all $n \in \mathbb{N}$,

$$P_n(X+k) = \sum_{r=0}^{k} a_{r,k}(X)P_{n+r}(X).$$

Proof. We proceed by induction on k. When $k = 1$, the result states $P_n(X+1) = XP_n(X) - P_{n+1}(X)$ and this is the recurrence relation for the polynomials $P_n(X)$. Assume the result holds for k. Then

$$\begin{aligned} P_n(X+k+1) &= \sum_{r=0}^{k} a_{r,k}(X+1)P_{n+r}(X+1) \\ &= \sum_{r=0}^{k} a_{r,k}(X+1)\left(XP_{n+r}(X) - P_{n+r+1}(X)\right) \\ &= \sum_{r=0}^{k} \left(Xa_{r,k}(X+1)P_{n+r}(X) - a_{r,k}(X+1)P_{n+r+1}(X)\right). \end{aligned}$$

For $0 \le t \le k$, the coefficient of $P_{n+t}(X)$ is

$$Xa_{t,k}(X+1) - a_{t-1,k}(X+1).$$

Thus

$$\begin{aligned} f_{k+1}(X,Y) &= (X-Y)f_k(X+1,Y) \\ &= (X-Y)\sum_{r=0}^{k} a_{r,k}(X+1)Y^r \\ &= \sum_{r=0}^{k} Xa_{r,k}(X+1)Y^r - \sum_{r=1}^{k+1} Xa_{r-1,k}(X+1)Y^r. \end{aligned}$$

So $a_{t,k+1}(X) = Xa_{t,k}(X+1) - a_{t-1,k}(X+1)$ and

$$P_n(X+k+1) \;=\; \sum_{r=0}^{k+1} a_{r,k+1}(X)P_{n+r}(X).$$

□

Corollary 3.7. *Let n, $k \in \mathbb{N}$. Then*

$$f(n) \equiv \sum_{r=1}^{k} a_{r,k}(0)f(n+r) \mod k$$

where

$$(X-Y)(X+1-Y)\cdots(X+k-1-Y)=\sum_{r=0}^{k}a_{r,k}(X)Y^r.$$

Proof. From Proposition 3.6 and $a_{0,k}(0)=0$, it follows that

$$\begin{aligned}P_n(k) &= \sum_{r=1}^{k}a_{r,k}(0)P_{n+r}(0)\\ &= \sum_{r=1}^{k}a_{r,k}(0)f(n+r).\end{aligned}$$

The result now follows from part (i) of Proposition 3.4 and the fact that

$$P_n(k)\equiv P_n(0) \mod k.$$

□

We can now give an alternative proof of Proposition 2.3.

Proof. Corollary 3.7 for $k=2^h$ gives

$$f(n)\equiv\sum_{r=1}^{2^h}a_{r,2^h}(0)f(n+r) \mod 2^h$$

and, in particular,

$$f(n+2^h)\equiv f(n)-\sum_{r=1}^{2^h-1}a_{r,2^h}(0)f(n+r) \mod 2^h.$$

So we have

$$\begin{pmatrix}f(n+2^h)\\ f(n+2^h-1)\\ f(n+2^h-2)\\ \vdots\\ f(n+1)\end{pmatrix}\equiv A\begin{pmatrix}f(n+2^h-1)\\ f(n+2^h-2)\\ f(n+2^h-3)\\ \vdots\\ f(n)\end{pmatrix} \mod 2^h$$

where

$$A=\begin{pmatrix}-a_{2^h-1,2^h}(0) & -a_{2^h-2,2^h}(0) & -a_{2^h-3,2^h}(0) & \cdots & -a_{1,2^h}(0) & 1\\ 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 1 & 0\end{pmatrix}.$$

Note that A is the companion matrix of the polynomial

$$c(Y)=Y(Y-1)\cdots(Y-2^{h+1}+1)-1.$$

Now

$$c(Y)\equiv(Y(Y+1))^{2^{h-1}}+1\equiv(Y^2+Y+1)^{2^{h-1}} \mod 2.$$

Over $\mathbb{F}_2$, A is non-derogatory (see [4], 7.20) and has Jacobson canonical form (see [28], page 72)

$$J = \begin{pmatrix} X & N & & & \\ & X & N & & \\ & & \ddots & \ddots & \\ & & & & N \\ & & & & X \end{pmatrix}$$

where $X = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ is the companion matrix of $Y^2 + Y + 1$ and $N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Let I_s be the $s \times s$ identity matrix where $s \geq 1$. Some calculation shows that

$$c(J) = \begin{pmatrix} 0 & I_2 & & & \\ & 0 & I_2 & & \\ & & \ddots & \ddots & \\ & & & 0 & I_2 \\ & & & & 0 \end{pmatrix}$$

and

$$Z := J^3 - I_{2^h} = (J - I_{2^h})c(J) = \begin{pmatrix} 0 & X^2 & N & & & \\ & 0 & X^2 & N & & \\ & & \ddots & \ddots & \ddots & \\ & & & 0 & X^2 & N \\ & & & & 0 & X^2 \\ & & & & & 0 \end{pmatrix}.$$

The matrix Z has the property that

$$Z^{2^{h-1}} = 0.$$

So over $\mathbb{F}_2$,

$$\begin{aligned} J^{3 \cdot 2^{h-1}} &= (I_{2^h} + Z)^{2^{h-1}} \\ &= I_{2^h} + 2^{h-1}Z + \ldots + Z^{2^{h-1}} \\ &= I_{2^h}. \end{aligned}$$

Hence $A^{3 \cdot 2^{h-1}}$ is similar to a matrix of the form $I_{2^h} + 2W$ for a matrix W over $\mathbb{F}_{2^h}$. So

$$\begin{aligned} A^{3 \cdot 2^{h-1} \cdot 2^{h-1}} &= (I_{2^h} + 2W)^{2^{h-1}} \\ &= I_{2^h} + 2^h W + \binom{2^{h-1}}{2} 4W^2 + \ldots + (2W)^{2^{h-1}}. \end{aligned}$$

Since $\binom{2^{h-1}}{t} 2^t \equiv 0 \mod 2^h$, for all $1 \leq t \leq 2^{h-1}$, we have

$$A^{3 \cdot 2^{2h-2}} \equiv I_{2^h} \mod 2^h.$$

In other words, we have

$$\begin{pmatrix} f(n+2^h) \\ f(n+2^h-1) \\ f(n+2^h-2) \\ \vdots \\ f(n+1) \end{pmatrix} \equiv A \begin{pmatrix} f(n+2^h-1) \\ f(n+2^h-2) \\ f(n+2^h-3) \\ \vdots \\ f(n) \end{pmatrix} \bmod 2^h$$

$$\equiv A^2 \begin{pmatrix} f(n+2^h-2) \\ f(n+2^h-3) \\ f(n+2^h-4) \\ \vdots \\ f(n-1) \end{pmatrix} \bmod 2^h$$

$$\vdots$$

$$\equiv \begin{pmatrix} f(n+2^h-3\cdot 2^{2h-2}) \\ f(n+2^h-3\cdot 2^{2h-2}-1) \\ f(n+2^h-3\cdot 2^{2h-2}-2) \\ \vdots \\ f(n-3\cdot 2^{2h-2}-2^h) \end{pmatrix} \bmod 2^h.$$

Comparing the elements in the matrix yields the desired congruence. □

Remark 3.8. Using this polynomial approach, one can show for instance that $3 \cdot 4^{h-1}$ is not a minimal period modulo 2^h, $h \geq 1$, for $f(n)$. Namely, one can use the definition of the P_n's and Proposition 3.4 to check that

$$P_{n+48}(0) \equiv P_{n+24}(0) \bmod 8$$

or equivalently

$$f(n) \equiv f(n+24) \bmod 8.$$

4. Applications

In this section we consider applications of Theorem 1.2 to graph theory, multiplicative partition functions, and to the irrationality of a p-adic series.

4.1. **Graph Theory.** A *simple graph* G consists of a non-empty finite set $V(G)$ of *vertices* and a finite set $E(G)$ of distinct unordered pairs of distinct elements of $V(G)$ called *edges*. We say that two vertices v, $w \in V(G)$ are *adjacent* if there is an edge $(v, w) \in E(G)$ joining them. A graph for which $E(G)$ is empty is called the *null graph* and is denoted by N_n where n is the number of vertices. A *complete graph* is a simple graph in which each pair of distinct vertices are adjacent. The complete graph on n vertices is denoted by K_n. If the vertex set of a graph G can be partitioned into two disjoint sets A and B so that each edge of G joins a vertex of A and a vertex of B, then G is called a *bipartite graph*. A *complete bipartite graph* is a bipartite graph in which each vertex of A is joined

to each vertex of B by just one edge. The complete bipartite graphs are denoted by $K_{r,s}$ where r and s are the cardinalities of A and B respectively.

Let G be a simple graph with n vertices. One can associate to G many polynomials whose properties yield structure theorems of isomorphism classes of graphs. In the vast literature, one can study, for example, the *chromatic polynomial*, *Tutte polynomial*, *interlace polynomials*, *cover polynomials* of digraphs, and the *matching polynomial* of a graph. In this section we take a closer look at the matching polynomial of certain bipartite graphs.

A *k-matching* in a graph G is a set of k edges, no two of which have a vertex in common. We denote the number of k-matchings in G by $p(G,k)$. We set $p(G,0)=1$ and define the *matching polynomial* of G by

$$\mu(G,X) := \sum_{k\geq 0}(-1)^k p(G,k)X^{n-2k}.$$

Some examples of matchings polynomials are

$$\mu(N_n,X) = X^n,$$

$$\mu(K_n,X) = \sum_{k\geq 0}(-1)^k \frac{n!}{k!(n-2k)!2^k}X^{n-2k},$$

and

$$\mu(K_{n,n},X) = \sum_{k\geq 0}(-1)^k \binom{n}{k}^2 k!X^{n-2k}.$$

The study of matching polynomials has been a focus of research over the last twenty five years. For further details regarding properties of matching polynomials, the reader should consult [3], [13], [14], [18], [19], [20], [21], or [34]. As we are interested in the roots of $\mu(G,X)$, we recall some general results.

Proposition 4.1. *Let G be a graph with n vertices. Then*
(i) The zeros of $\mu(G,X)$ are real.
(ii) The zeros of $\mu(G,X)$ are symmetrically distributed about the origin.

Proof. For (i), see Corollary 1.2 or Lemma 4.3 in [19]. If n is even, then $\mu(G,X)$ can be written as a polynomial in X^2. If n is odd, then $X^{-1}\mu(G,X)$ can be expressed as a polynomial in X^2. Thus (ii) follows. □

Further results on roots of matching polynomials can be found in [16], [17], [20], [21], [24], or [26]. For our purposes, we consider the following bipartite graph. Let $T(n)$ be the graph with vertex set $\{1,\ldots,n\}\cup\{1',\ldots,n'\}$, where i is adjacent to j' if and only if $i>j$. Thus $T(n)$ has $2n$ vertices. For $n=3$, one can check that $p(T(3),1)=3$, $p(T(3),2)=1$, $p(T(3),3)=0$, and thus

$$\mu(T(3),X) = X^2(X^2-X-1)(X^2+X-1).$$

We now relate the matching polynomial of $T(n)$ to Stirling numbers of the second kind $S(n,k)$.

Proposition 4.2. *For the graph $T(n)$, we have*

$$\mu(T(n),X) = \sum_{k=0}^{n}(-1)^k S(n,n-k)X^{2n-2k}.$$

Proof. We briefly sketch the proof as given in [19]. For another proof, see the solution to Problem 4.31 in [36]. The idea is to consider a bijection from the set of k-matchings of $T(n)$ to a certain set of directed graphs. Thus counting the number of such directed graphs yields $p(T(n), k)$ and thus $\mu(T(n), X)$. Each matching in $T(n)$ determines a directed graph with vertex set $N = \{1, \ldots, n\}$ with arc (i, j) for each edge $\{i, j'\}$ in the matching and a loop on each vertex j not in the matching. Now, each vertex component is a directed path with a loop on its last vertex. As there is an arc from i to j in the directed graph only if $i \geq j$, the graph is determined by the vertex set of each component. Thus the number of such directed graphs with c components is $S(n, c)$. Note that c equals the number of loops and decreases by 1 for each edge in the original matching. Hence $c = n - k$ where k equals the number of edges in the matching. □

Each of the polynomials $\mu(T(n), X)$ contains X^2 as a factor and thus is reducible. We thus consider the roots of the polynomial $\dfrac{1}{X^2}\mu(T(n), X)$. This corresponds to removing the vertices 1 and n' in the graph $T(n)$. As a result of Theorem 1.2, we immediately have

Corollary 4.3. *For $n \not\equiv 2$ and $\not\equiv 2944838 \bmod 3145728$, 1 is not a root of $\dfrac{1}{X^2}\mu(T(n), X)$.*

Remark 4.4. We conjecture that 1 is not a root of $\dfrac{1}{X^2}\mu(T(n), X)$ for $n \equiv 2$ and $\equiv 2944838 \bmod 3145728$, and, more generally, that $\dfrac{1}{X^2}\mu(T(n), X)$ is irreducible over $\mathbb{Z}$ for every $n > 3$. This last statement has been numerically verified for all $3 < n \leq 500$. Note that this statement implies Wilf's conjecture.

4.2. **Multiplicative partition functions.** Multiplicative partition functions count the number of representations of a given positive integer m as a product of positive integers. For a well-written survey of techniques for enumerating product representations, please see [31]. Suppose the canonical prime factorization of m is given by

$$m = p_1^{r_1} \ldots p_n^{r_n}.$$

The succession of integers $r_1, r_2, \ldots r_n$, when arranged in descending order of magnitude, specify a multipartite number

$$\overline{r_1 r_2 \ldots r_n}$$

associated to m. These multipartite numbers were first studied by MacMahon in [38]. Let b_m denote the number of multiplicative partitions of m. Note that there is a one-to-one correspondence between b_m and the number of additive partitions of the multipartite number associated to m. MacMahon [39] observed that the infinite product

$$\prod_{k=2}^{\infty}(1 - k^{-s})^{-1}$$

is the generating function of the Dirichlet series

$$\sum_{m=1}^{\infty} b_m m^{-s}.$$

Harris and Subbarao provide a recursion for b_m in [25] while Mattics and Dodd [40] have shown that $b_m \leq m(\log m)^{-\alpha}$ for each fixed $\alpha > 0$ and for all sufficiently large m. This upper bound implies a conjecture of Hughes and Shallit [27]. More precise results of an asymptotic nature on the growth rate of b_m can be found in [5].

In this section we consider the reciprocal Dirichlet series

$$\sum_{m=1}^{\infty} a_m m^{-s}$$

generated by the infinite product $\prod_{k=2}^{\infty}(1-k^{-s})$. The coefficients a_m count the number of (unordered) representations of m as a product of an even number of distinct integers >1 minus the number of representations of m as a product of an odd number of distinct integers >1. Note that for a positive integer $m>1$, a_m depends only on the exponents $r_1, r_2, \ldots, r_n$ in the canonical prime factorization of m. In particular, if m is squarefree, the value of a_m is a function of the number n of prime factors of m. Let $e(n)$ denote this function. Subbarao and Verma [42] studied the asymptotic behavior of $e(n)$ and showed that

$$\frac{\log|e(n)|}{n}$$

is unbounded as $n\to\infty$. In fact, they prove

$$\limsup_{n\to\infty}\frac{\log|e(n)|}{n\log n}=1.$$

Note that if we identify the factors of $m=p_1\ldots p_n$ with subsets of $\{1,2,\ldots,n\}$, then $e(n)$ counts the number of ways to partition a set S of n elements into an even number of non-empty subsets minus the number of ways to partition S into an odd number of non-empty subsets. Thus,

$$e(n)=\sum_{k=1}^{n}(-1)^k S(n,k).$$

As a result of Theorem 1.2, we have the following

Corollary 4.5. *If m is squarefree and contains n prime factors, then $a_m=e(n)\neq 0$ for all $n\not\equiv 2$ and $\not\equiv 2944838 \bmod 3145728$.*

4.3. **p-adic sums.** Let p be a prime. For every $a\in\mathbb{Z}\setminus\{0\}$, put

$$v_p(a)=\max\{m\in\mathbb{Z}: p^m \mid a\}.$$

We extend v_p to $\mathbb{Q}\setminus\{0\}$ by defining $v_p(\alpha)=v_p(a)-v_p(b)$ where $\alpha=\frac{a}{b}$. If we define

$$|\alpha|_p=\begin{cases} p^{-v_p(\alpha)} & \text{if} \quad \alpha\neq 0 \\ \\ 0 & \text{if} \quad \alpha=0, \end{cases}$$

then $|\quad|_p$ is a norm on $\mathbb{Q}$ called the *p-adic norm*. The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\quad|_p$, i.e., p-adic numbers are convergent series of the form

$$\sum_{k=i}^{\infty} a_k p^k,$$

where i, $a_k\in\mathbb{Z}$. Recall that a p-adic number $\alpha\in\mathbb{Q}_p\setminus\mathbb{Q}$ is called a *p-adic irrational*.

It is a well-known result that the series $\sum_{n=1}^{\infty} a_n$ with $a_n\in\mathbb{Q}_p$ converges if and only if $|a_n|_p\to 0$ as $n\to\infty$ (see Corollary 4.1.2 in [22]). Thus the series

$$\alpha := \sum_{n=1}^{\infty} n!$$

converges in $\mathbb{Q}_p$ as $|n!|_p \to 0$. The same is true for the series

$$\alpha_k := \sum_{n=1}^{\infty} n^k n!$$

where k is a non-negative integer. Murty and Sumner [41] investigate the irrationality of α_k. Schikhof [43] was the first to ask whether $\alpha_0 = \alpha$ is a p-adic irrational or not. Murty and Sumner conjecture that it is. They also use the fact that

$$\sum_{n=0}^{m} n \cdot n! = (m+1)! - 1$$

and $|(m+1)!|_p \to 0$ as $m \to \infty$ to deduce that $\alpha_1 = -1$. Moreover, they prove using an inductive argument that

$$\alpha_k = v_k - u_k \alpha,$$

where u_k, $v_k \in \mathbb{Z}$. In fact, they show that if one assumes that α is irrational, then (see Lemma 4 in [41])

$$(-1)^k u_k = \sum_{j=1}^{k+1} (-1)^j S(k+1, j).$$

As a result of this expression for u_k and Theorem 1.2, we can extend Theorem 1 in [41] as follows.

Corollary 4.6. *Let p be a prime. If α is a p-adic irrational and $k+1 \not\equiv 2$ and $\not\equiv 2944838 \bmod 3145728$, then α_k is a p-adic irrational.*

Appendix

The following code provides the possible zeros of $f(n)$ modulo m as well as the minimal period.

```
#include <stdio.h>

#define m 'any number'

long Data1[m + 1]; long Data2[m + 1];

int main() {
        long I;
        long double Steps=0;
        Data1[1] = 1;
        Data2[1] = 0;
        for (I = 2; I < m + 1; ++I) {
                Data1[I]= 0;
                Data2[I]= 0;
        };
        long Sum=0;
        long l=0;
        printf("-------------------------------------------\n");
        printf("Possible zeros for f(n) modulo %i\n",m);
```

```
        printf("-----------------------------------------\n");
cont1:
                ++Steps;
                Sum = 0;
                for (I = m; I > 1 ; --I) {
                        Data2[I] = (m+Data1[I] * (I - 1) - Data1[I - 1]) % m;
                        Sum += Data2[I];
                };
                Data2[1] = (m - Data1[m])%m;
        if (!((Sum + Data2[1] )% m)){
                printf("Possible zero is %Lf  \n ",Steps);
        }
        // Check if minimal period is reached
        if (Sum | (Data2[1]-1)) goto Transfer;
        printf("The minimal period is : %Lf \n", Steps);
        return 0;

Transfer:
        for (I = 1; I < m + 1; ++I){
                Data1[I]=Data2[I];
        }
        goto cont1;
}
```

Acknowledgments

The authors would like to thank Ram Murty for his comments on a preliminary version of this paper, Bruce Berndt for pointing out reference [2], and the referees for their encouragement and insightful comments which shortened our original proof of Theorem 1.2 and improved the exposition. The first author would also like to thank Barbara Verdonck for many productive discussions. The third author would like to mention that this paper owes its existence to a delightful talk given by Professor Murty in the Summer of 2004 at Queen's University in Kingston, Ontario, Canada.

References

[1] R. E. Beard, *On the coefficients in the expansion of e^{e^t} and $e^{e^{-t}}$*, J. Inst. Actuar. **76** (1950), 152–163.
[2] B. Berndt, *Ramanujan's Notebooks*, Part I, Springer–Verlag, New York, 1985.
[3] R. A. Beezer, E. J. Farrell, *The matching polynomial of a regular graph*, Discrete Math. **137** (1995), no. 1-3, 7–18.
[4] W. C. Brown, *Matrices over Commutative Rings*, M. Dekker, New York, 1993.
[5] E. Canfield, P. Erdos, and C. Pomerance, *On a problem of Oppenheim concerning "Factorisatio Numerorum"* J. Number Th. **17** (1983), 1–28.
[6] L. Carlitz, *Congruences for generalized Bell and Stirling numbers*, Duke Math. J. **22** (1955), 193–205.
[7] R. Coleman, *On the Galois group of the exponential Taylor polynomial*, L'Enseignement Math. **33** (1987), 183–189.
[8] L. Comtet, *Advanced Combinatorics*, D. Reidel, 1974.
[9] N. G. de Bruijn, *Asymptotic methods in analysis*, Corrected reprint of the third edition, Dover Publ. Inc., New York, 1981.
[10] S. De Wannemacker, *On 2-adic orders of Striling numbers of the second kind*, INTEGERS, **5(1)** (2005), A21.

[11] S. De Wannemacker, *Annihilating polynomials for quadratic forms and Stirling numbers of the second kind*, to appear in Math. Nachr.
[12] S. De Wannemacker, *Annihilating polynomials and Stirling numbers of the second kind*, Ph.D. thesis, University College Dublin (2006).
[13] P. Diaconis, A. Gamburd, *Random matrices, magic squares, and matching polynomials*, Electron. J. Combin. **11** (2004/06), no. 2, Research Paper 2, 26 pp.
[14] E. J. Farrell, *An introduction to matching polynomials*, J. Combin. Theory Ser. B **27** (1979), no. 1, 75–86.
[15] M. Filaseta, O. Trifonov, *The irreducibility of the Bessel polynomial*, J. Reine Angew. Math. **550** (2002), 125–140.
[16] D. C. Fisher, J. Ryan, *Bounds on the largest root of the matching polynomial*, Discrete Math. **110** (1992), no. 1-3, 275–278.
[17] C. D. Godsil, *Matchings and walks in graphs*, J. Graph Theory **5** (1981), no. 3, 285–297.
[18] C. D. Godsil, *Hermite polynomials and a duality relation for matching polynomials*, Combinatorica **1** (1981), no. 3, 257–262.
[19] C. D. Godsil, *Algebraic Combinatorics*, Chapman & Hall, New York, 1993.
[20] C. D. Godsil, I. Gutman, *On the theory of the matching polynomial*, J. Graph Theory **5** (1981), no. 2, 137–144.
[21] C. D. Godsil, I. Gutman, *On the matching polynomial of a graph*, Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), 241–249, Colloq. Math. Soc. János Bolyai, **25**, North-Holland, Amsterdam-New York, 1981.
[22] F. Q. Gouvêa, *p-adic numbers: An introduction*, Springer-Verlag, Berlin, 1993.
[23] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics, a foundation for computer science*, Addison Wesley, 1989.
[24] I. Gutman, *On some graphic polynomials whose zeros are real*, Publ. Inst. Math. (Beograd) (N.S.) **37(51)** (1985), 29–32.
[25] C. Harris, M. V. Subbarao, *On product partitions of integers*, Canad. Math. Bull. **34** (1991), 474–479.
[26] O. J. Heilmann, E. H. Lieb, *Theory of monomer-dimer systems*, Comm. Math. Phys. **25** (1972), 190–232.
[27] J. Hughes, J. Shallit, *On the number of multiplicative partitions*, Amer. Math. Monthly **90** (1983), 468–471.
[28] N. Jacobson, *Lectures in Abstract Algebra, Vol. II-Linear Algebra*, D. Van Nostrand, 1953.
[29] M. Klazar, *Counting even and odd partitions*, American Math. Monthly, **110** (2003), no. 6, 527–532.
[30] M. Klazar, *Bell numbers, their relatives, and algebraic differential equations*, J. Combin. Theory Ser. A. **102** (2003), no. 1, 63–87.
[31] A. Knopfmacher, M. Mays, *A survey of factorization counting functions*, Inter. J. Number Th. **1** (2005), no. 4, 563–581.
[32] N. A. Kolokolnikova, *Relations between sums of certain special numbers*, in: G.P. Egorycev, M.L. Platonov (Eds.), Asimptoticheskie i perechislitelnye zadachi kombinatornogo analiza (Asymptotic and Enumeration Problems of Combinatorial Analysis), Krasnojarsk. Gos. Univ., Krasnoyarsk. 1976, 117–124.
[33] L. Kuipers, H. Niederreiter, *Uniform distribution of sequences*, Pure and Applied Mathematics, Wiley-Interscience, New York-London-Sydney, 1974.
[34] B. Lass, *The N-dimensional matching polynomial*, Geom. Funct. Anal. **15** (2005), no. 2, 453–475.
[35] J. Layman, C. Prather, *Generalized Bell numbers and zeros of successive derivatives of an entire function*, J. Math. Anal. Appl. **96** (1983), no. 1, 42–51.
[36] L. Lovasz, *Combinatorial Problems and Exercises*, North-Holland, Amsterdam, 1979.
[37] W. Lunnon, P. Pleasants, N. Stephens, *Arithmetic properties of Bell numbers to a composite modulus. I*, Acta. Arith. **35** (1979), no. 1, 1–16.
[38] P. MacMahon, *Memoir on the theory of the compositions of numbers*, Philos. Trans. Roy. Soc. London (A) **184** (1893), 835–901.
[39] P. MacMahon, *Dirichlet series and the theory of partitions*, Proc. London Math. Soc. (2) **22** (1924), 404–411.
[40] L. Mattics, F. Dodd, *Estimating the number of multiplicative partitions*, Rocky Mountain J. Math. **17** (1987), 797–813.

[41] M. Ram Murty, S. Sumner, *On the p-adic series* $\sum_{n=1}^{\infty} n^k \cdot n!$, Number theory, 219–227, CRM Proc. Lecture Notes, **36**, Amer. Math. Soc., Providence, RI, 2004.
[42] M. V. Subbarao, A. Verma, *Some remarks on a product expansion: an unexplored partition function*, F.G. Garvan, M.E.H. Ismail (Eds.), Symbolic Computations, Number Theory, Special Functions, Physics and Combinatorics (Gainesville, FL, 1999), Kluwer, Dordrecht, 2001, pp. 267–283.
[43] W. Schikhof, *Ultrametric Calculus: An Introduction to p-adic Analysis*, Cambridge University Press, 1984.
[44] E. Sell, *On a certain family of generalized Laguerre polynomials*, J. Number Th. **107** (2004), no. 2, 266–281.
[45] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, available at `http://www.research.att.com/~njas/sequences/`
[46] R. P. Stanley, *Enumerative Combinatorics. Vol. 1.*, Cambridge Studies in Advanced Mathematics, **49**, Cambridge University Press, Cambridge, 1997.
[47] V. R. R. Uppuluri, J. A. Carpenter, *Numbers generated by the function* $\exp(1 - e^x)$, Fibonacci Quart. **7** (1969), 437–448.
[48] S. Wagstaff, *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime*, Math. Comp. **65** (1996), no. 213, 383–391.
[49] Y. Yang, *On a multiplicative partition function*, Electron. J. Combin. **8** (2001) R19, 14pp.

Faculty of Applied Economic Sciences, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium
E-mail address: `stefan.dewannemacker@ua.ac.be`

School of Mathematical Sciences, University College Dublin, Belfield, Dublin 4, Ireland
E-mail address: `thomas.laffey@ucd.ie`
E-mail address: `robert.osburn@ucd.ie`