CONGRUENCES FOR WEIGHTED NUMBER OF LABELED FORESTS

Arun P. Mani[1]
School of Mathematics and Statistics, The University of Melbourne, Australia
arunpmani@gmail.com

Rebecca J. Stones[2]
Faculty of Information Technology, Monash University, Australia
School of Mathematical Sciences, Monash University, Australia
Department of Mathematics and Statistics, Dalhousie University, Canada
College of Computer and Control Engineering, Nankai University, China
rebecca.stones82@gmail.com

Received: 5/12/15, Accepted: 2/28/16, Published: 3/11/15

Abstract

Let f_n be the number of vertex labeled forests (acyclic graphs) on n vertices. In this paper we study the number-theoretic properties of the sequence $(f_n : n \geq 1)$. First, we find recurrence congruences that relate f_{n+p^k} to f_n, for all positive integers n and prime powers p^k. We deduce that this sequence is ultimately periodic modulo every positive integer, and that every positive integer divides infinitely many terms of this sequence. More generally, we state and prove these results for sequences defined by a weighted generalization of f_n, or equivalently, by a special evaluation of the Tutte polynomial of the complete graph K_n.

1. Introduction

Let $\mathcal{F}_n$ be the set of labeled forests on the vertex set $\{1, 2, \ldots, n\}$. In this work, we will find congruences satisfied by evaluations at integer points of the *forest polynomial* $F_n(x)$, defined by

$$F_n(x) \stackrel{\text{def.}}{=} \sum_{A \in \mathcal{F}_n} x^{n-1-|A|}, \tag{1}$$

[1]Mani supported in part by an Australian Research Council DECRA grant.
[2]Stones supported in part by an ARC grant, NSFC grant 61170301, and NSF China Research Fellowship for International Young Scientists (grant numbers: 11450110409, 11550110491). Stones also thanks AARMS for partially supporting this work.

where $|A|$ denotes the number of edges of forest A. These evaluations include as special cases, the number of n-vertex labeled trees when $x = 0$ ($= n^{n-2}$ by Cayley's Formula [5]), and the number of n-vertex labeled forests when $x = 1$. For $a \in \mathbb{Z}$, we can think of $F_n(a)$ as counting the n-vertex labeled forests $A \in \mathcal{F}_n$, each with weight $a^{n-1-|A|}$. The first few forest polynomials are given in Table 2.

The forest polynomial is also a partial evaluation of the *Tutte polynomial* of K_n, the complete graph on n vertices. The Tutte polynomial of K_n is a two-variable polynomial given by

$$T_n(x, y) \stackrel{\text{def.}}{=} \sum_{G \in \mathcal{G}_n} (x-1)^{c(G)-1}(y-1)^{c(G)+|G|-n},$$

where $\mathcal{G}_n$ is the the set of all labeled graphs on n vertices and $c(G)$ is the number of connected components of graph G. The forest polynomial $F_n(x)$ is the same as $T_n(1 + x, 1)$.

The aim of this paper is to prove the following proposition which gives a recurrence congruence for $F_n(a)$ whenever $a \in \mathbb{Z}$.

Proposition 1. *Let p be a prime, $n \geq 0$, $k \geq 1$ and $a \in \mathbb{Z}$. Then*

$$F_{n+p^k}(a) \pmod{p^k} \equiv \begin{cases} (n+a)^{p^k} F_n(a) & \text{if } p \geq 3 \text{ and } n \geq 1 \\ a^{p^k-1} & \text{if } p \geq 3 \text{ and } n = 0 \\ F_n(a) & \text{if } p = 2, k \neq 2 \text{ and } n \text{ is odd} \\ (-1)^a F_n(a) & \text{if } p = 2, k = 2 \text{ and } n \text{ is odd} \\ 1 & \text{if } p = 2, k = 1, n = 0 \text{ and } a \text{ is even} \\ 2 & \text{if } p = k = 2, n = 0 \text{ and } a \not\equiv 0 \pmod 4 \\ 4 & \text{if } p = 2, k = 3, n = 0 \text{ and } a \text{ is odd} \\ 0 & \text{otherwise.} \end{cases}$$

We give a proof in Section 2. Proposition 1 implies that for $a \in \mathbb{Z}$, prime p and $k \geq 1$, every term of the infinite integer sequence $(F_n(a) : n \geq 1)$ modulo p^k is fully determined by its first p^k terms. A standard number-theoretic tool, the Chinese Remainder Theorem [2, Th. 5.4], readily extends this observation to modulo any positive integer as shown in Section 3.1.

Proposition 1 also helps us identify small prime factors of $F_n(a)$, in particular, factors p^k such that $p^k \leq n$. Indeed we give a complete characerization of all such small prime factors of $F_n(a)$ in Section 3.2. As a consequence, we show that for all $a \in \mathbb{Z}$, every positive integer divides infinitely many terms in the sequence $(F_n(a) : n \geq 1)$.

Lastly, in Section 3.3, we use Proposition 1 to show that for all $a \in \mathbb{Z}$ and positive integers m, the sequence $\big(F_n(a) : n \in \mathbb{Z}_{\geq 1}\big)$ is ultimately periodic modulo m. Such sequences were called *modularly C-finite* (MC-finite) by Fischer, Kotek,

and Makowsky [6], who showed that the sequence $(f_n = F_n(1) : n \geq 1)$ is MC-finite. We generalize this observation to $(F_n(a) : n \geq 1)$ for every $a \in \mathbb{Z}$, and our proof can also be used to compute the period, unlike the proof of periodicity of $(f_n : n \geq 1)$ in [6].

1.1. Notation

The notation in Table 1 is consistent throughout this paper and, for brevity, we will not restate these definitions for each subsequent result.

n	an arbitrary non-negative integer
p	an arbitrary prime
k	an arbitrary positive integer
a	an arbitrary integer
$\lvert G\rvert$	the number of edges in the graph G
N	the set $N = \{1, 2, \ldots, n\}$
α	the permutation $(n+1, n+2, \ldots, n+p^k)$
β	the permutation $(n+1, n+2, \ldots, n+p)(n+p+1, n+p+2, \ldots, n+2p)\cdots(n+p^k-p+1, n+p^k-p+2, \ldots, n+p^k)$
P_i	the block $P_i = \{n+p(i-1)+1, n+p(i-1)+2, \ldots, n+p(i-1)+p\}$ formed by the i-th non-trivial cycle of β
Γ	the permutation group generated by α
$\mathcal{C}$	the set of labeled forests on the vertex set $\{1, 2, \ldots, n+p^k\}$
$\mathcal{A}$	the set $\mathcal{A} = \{G \in \mathcal{C} : \beta G = G\}$
$\mathcal{S}$	the set of partitions of the set $\{1, 2, \ldots, p^{k-1}\}$
Q	a partiton in $\mathcal{S}$
q	a part in Q (which will be a subset of $\{1, 2, \ldots, p^{k-1}\}$)
π	a partition of the number p^{k-1}
$\mathcal{S}_\pi$	the set of partitions of the set $\{1, 2, \ldots, p^{k-1}\}$ whose cardinalities induce the partition π
Q_π	an arbitrary representative of $\mathcal{S}_\pi$
π_0	the partition $\{\overbrace{1, 1, \ldots, 1}^{p^{k-1}}\}$ of p^{k-1}
π_1	the partition $\{\overbrace{1, 1, \ldots, 1}^{2^{k-1}-2}, 2\}$ of 2^{k-1} (we require $k \geq 2$)
π_2	the partition $\{\overbrace{1, 1, \ldots, 1}^{2^{k-1}-4}, 2, 2\}$ of 2^{k-1} (we require $k \geq 3$)

Table 1: Table of notation.

2. Proof of Proposition 1

We begin the proof of Proposition 1 with the following lemma. Importantly, it allows us to study the set $\mathcal{A}$ defined in Table 1, whose members admit a non-trivial symmetry (instead of the set $\mathcal{C}$).

Lemma 1.

$$F_{n+p^k}(a) \equiv \sum_{G \in \mathcal{A}} a^{n+p^k-|G|-1} \pmod{p^k}. \tag{2}$$

Proof. Rephrasing (1), we have

$$F_{n+p^k}(a) = \sum_{G \in \mathcal{C}} a^{n+p^k-|G|-1}. \tag{3}$$

The action of Γ (defined in Table 1) on $\mathcal{C}$ partitions $\mathcal{C}$ into orbits.

- All graphs within a single orbit are isomorphic to each other, and make the same contribution to (3).
- By the Orbit-Stabilizer Theorem [3, Th. 17.2], an orbit has size p^k unless it contains a forest G whose stabilizer has cardinality divisible by p, whence $\alpha^{p^{k-1}}$ is an automorphism of G.
- If we define $\mathcal{B} = \{G \in \mathcal{C} : \alpha^{p^{k-1}} G = G\}$, then $\mathcal{B}$ (and hence $\mathcal{C} \setminus \mathcal{B}$) is closed under the action of Γ. Further, the action of Γ partitions $\mathcal{C} \setminus \mathcal{B}$ into orbits of size $|\Gamma| = p^k$.

Hence we have

$$F_{n+p^k}(a) \equiv \sum_{G \in \mathcal{B}} a^{n+p^k-|G|-1} \pmod{p^k}.$$

Since $\alpha^{p^{k-1}}$ and β (defined in Table 1) have the same cycle structure, there exists a permutation χ such that $\beta = \chi \alpha^{p^{k-1}} \chi^{-1}$. Hence, $\alpha^{p^{k-1}}$ is an automorphism of G if and only if β is an automorphism of $\chi(G)$. The permutation χ gives a bijection between $\mathcal{B}$ and $\chi(\mathcal{B}) = \mathcal{A}$ which preserves the contribution to (3), and the lemma follows. □

We are now ready to start proving cases of Proposition 1. As we will see, the forests in $\mathcal{A}$ are structurally different in the $p = 2$ and $p \geq 3$ cases, and the $n \geq 1$ and $n = 0$ cases, which results in four cases we will study (Theorems 1, 2, 3, and 4).

Each case, however, has a similar theme: we give a description of how to construct forests in $\mathcal{A}$, which we then use to split (2). In each case, we partition the vertices of the forests in $\mathcal{A}$ into the blocks N and P_i for $1 \leq i \leq p^{k-1}$ (see Table 1). Vertices in N are fixed by the automorphism β, whereas vertices in each P_i are simultaneously cyclically permuted by β. An example is given in Figure 1; the dotted arrows indicate that action of β.

Theorem 1. *If $p \geq 3$ and $n \geq 1$ then*

$$F_{n+p^k}(a) \equiv (n+a)^{p^k} F_n(a) \pmod{p^k}.$$

Proof. We make the following two observations, valid for arbitrary $G \in \mathcal{A}$ (illustrated in Figure 2).

Observation 1. Suppose w and x are two distinct vertices in N and $y \in P_j$. Then G cannot have both edges wy and xy. *Proof*: Otherwise $\{wy, yx, x\beta(y), \beta(y)w\}$ is a 4-cycle in G.

Observation 2. Suppose w and x are two distinct vertices in N and $y \in P_i$, $z \in P_j$ where $i \neq j$. Then G cannot have edges wy and xz and any path T from y to z contained in the subgraph induced by $\cup_r P_r$. *Proof*: Otherwise $\{\beta(y)w, wy\} \cup T \cup \{zx, x\beta(z)\} \cup \beta(T)$ is a cycle.

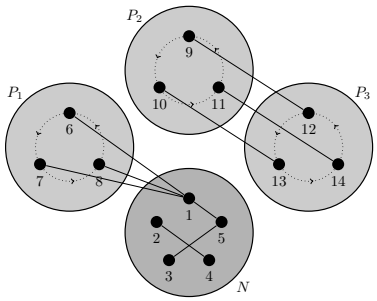
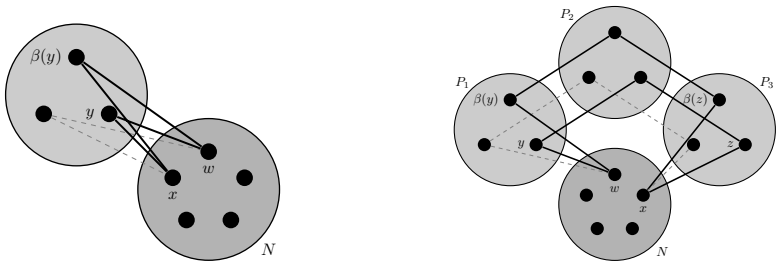


Figure 1: An example of a graph in $G \in \mathcal{A}$ when $p = 3$, $k = 2$ and $n = 5$.



(a) Observation 1 (b) Observation 2

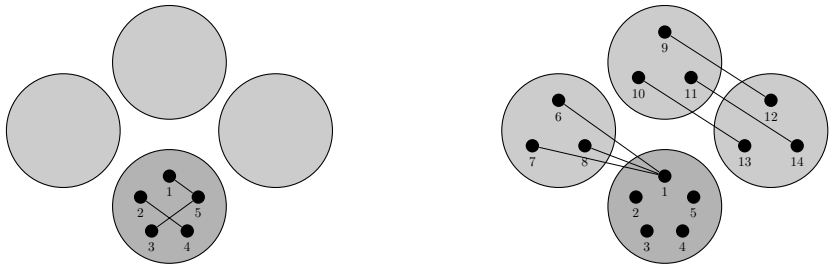
Figure 2: Illustrating how cycles arise in Observations 1 and 2.

We can decompose any $G \in \mathcal{A}$ into two components: the subgraph $J = J(G)$ induced by the vertices in N, and $H = H(G)$ formed from G by deleting the edges in J. For the example in Figure 1, J and H are given in Figure 3.

Importantly, Observations 1 and 2 imply that, regardless of the structure of G, we can delete the edges in J and replace them by the edges from any other forest on the vertex set N to obtain another forest in $\mathcal{A}$; i.e., this replacement (a) does not introduce any cycles and (b) preserves the automorphism β. Let $\mathcal{J}$ and $\mathcal{H}$ respectively be the sets of possible subgraphs J and H that arise in any $G \in \mathcal{A}$ (i.e., the range of J and H). Hence

$$\mathcal{A} = \{J \cup H : J \in \mathcal{J} \text{ and } H \in \mathcal{H}\}$$

and each $J \cup H$ is unique. Moreover, $\mathcal{J}$ is the set of spanning forests on the vertex



(a) J, the subgraph induced by $N = \{1, 2, \ldots, 5\}$.

(b) H, formed from G by deleting the edges in J.

Figure 3: Illustrating how the forest G in Figure 1 decomposes into J and H.

set N. Consequently, we may split (2) as follows:

$$\begin{aligned} F_{n+p^k}(a) \pmod{p^k} &\equiv \sum_{G\in\mathcal{A}} a^{n+p^k-|G|-1} \\ &\equiv \sum_{J\in\mathcal{J}} \sum_{H\in\mathcal{H}} a^{n-|J|-1}\ a^{p^k-|H|} \qquad [\text{since } n \geq 1] \\ &\equiv \left(\sum_{J\in\mathcal{J}} a^{n-|J|-1}\right)\left(\sum_{H\in\mathcal{H}} a^{p^k-|H|}\right) \\ &\equiv F_n(a) \sum_{H\in\mathcal{H}} a^{p^k-|H|}. \end{aligned} \tag{4}$$

Remark. Note that (4) is not valid when $n = 0$, so this case will need to be resolved separately; see Theorem 3.

The next step in this proof is therefore to classify which H are in $\mathcal{H}$. Each $H \in \mathcal{H}$ induces a partition $Q \in \mathcal{S}$ (defined in Table 1) and a subset $R \subseteq Q$, wherein:

(i) Integers i and j belong to the same part in Q whenever there is a path in H between a vertex in P_i to a vertex in P_j $(i \neq j)$.

(ii) A part $q \in Q$ belongs to R whenever there is some $i \in q$ such that there is an edge in H between a vertex in P_i and a vertex in N.

For example, the graph in Figure 1 induces the partition $Q = \big\{\{1\}, \{2, 3\}\big\}$ and the subset $R = \big\{\{1\}\big\} \subseteq Q$.

We will use Q to account for the possible ways that the vertices in the various P_i's might be connected to each other, and similarly we will use R to account for the possible ways that the vertices in P_i might be connected to those in N. We partition $\mathcal{H}$ into the sets

$$\mathcal{H}(Q, R) = \{H \in \mathcal{H} : H \text{ induces partition } Q \text{ and subset } R \subseteq Q\}.$$

Hence (4) splits as

$$F_{n+p^k}(a) \equiv F_n(a) \sum_{Q \in \mathcal{S}} \sum_{R \subseteq Q} \sum_{H \in \mathcal{H}(Q,R)} a^{p^k - |H|} \pmod{p^k}. \tag{5}$$

Thus we will now classify which H are in $\mathcal{H}(Q,R)$. Note that Observations 1 and 2 are also valid for all $H \in \mathcal{H}$. Next, we make two additional observations about the graphs in $\mathcal{H}$.

Observation 3. Suppose w and x are two distinct vertices in P_i, and $y \in P_j$, where $i \neq j$. Then H cannot have edges wy and xy. *Proof*: Otherwise $\{\beta(w)^r\beta(y)^r : 0 \leq r \leq p-1\} \cup \{\beta(x)^r\beta(y)^r : 0 \leq r \leq p-1\}$ are the edges of a 2-regular bipartite subgraph, which must contain a cycle. (In fact, since p is prime, it would be a $2p$-cycle.)

Observation 4. We cannot have an edge yz for distinct $y, z \in P_i$. *Proof*: Otherwise, since $p \geq 3$, the induced subgraph on the vertices P_i contains a p-cycle.

Remark. Observation 4 is false when $p = 2$, and is where the $p = 2$ and $p \geq 3$ cases first deviate.

Now, given $Q \in \mathcal{S}$ and $R \subseteq Q$, we can construct forests $H \in \mathcal{H}(Q,R)$ in the following way:

(a) We begin with H as the null graph on the vertex set $\{1, 2, \ldots, n + p^k\}$.

(b) For each part $q \in Q$ we choose one of the $|q|^{|q|-2}$ spanning trees T_q on the vertex set q.

(c) For each edge ij in T_q, we choose a vertex y in P_i and a vertex z in P_j, and add the edges $\{\beta^r(y)\beta^r(z) : 0 \leq r \leq p-1\}$ to H. This can be achieved in p ways per edge in T_q, and hence $p^{|q|-1}$ ways in total for a given T_q. In this step, we add $(|q|-1)p$ edges to the graph H for each part $q \in Q$.

(d) For each part $r \in R$, we choose an $i \in r$ and an $x \in N$, and add to H the p edges from each vertex in P_i to x. Clearly, this can be achieved in $|r|n$ ways for each $r \in R$. This step adds a further $|R|p$ edges to the graph H.

Observations 1–4 imply that we can construct all $H \in \mathcal{H}(Q,R)$ this way. Specifically, if we attempt to add edges in a manner not accounted for above, we will introduce a cycle: Observations 1 and 2 preclude having P_i-to-N edges in any other way; Observation 3 precludes having additional P_i-to-P_j edges in step (c); Observation 4 precludes adding P_i-to-P_i edges. By definition, there are no N-to-N edges in H.

From the above construction we find, for a given $Q \in \mathcal{S}$ and an $R \subseteq Q$, we have $|H| = |R|p + \sum_{q\in Q}(|q|-1)p = p^k - (|Q|-|R|)p$ for all $H \in \mathcal{H}(Q,R)$. Hence,

$$\sum_{H\in\mathcal{H}(Q,R)} a^{p^k-|H|} = |\mathcal{H}(Q,R)|\ a^{(|Q|-|R|)p}$$
$$= \Big(\prod_{q\in Q} |q|^{|q|-2}p^{|q|-1}\Big)\Big(\prod_{r\in R} |r|\ n\Big)\ a^{(|Q|-|R|)p}. \tag{6}$$

When R is empty, step (d) can be performed in exactly one way (i.e., do nothing), in which case we define $\prod_{r\in R} |r|\ n = 1$. Defining

$$h(Q) = \sum_{R\subseteq Q} \Big(\prod_{q\in Q} |q|^{|q|-2}p^{|q|-1}\Big)\Big(\prod_{r\in R} |r|\ n\Big)\ a^{(|Q|-|R|)p},$$

and substituting (6) into (5) gives

$$F_{n+p^k}(a) \equiv F_n(a)\sum_{Q\in\mathcal{S}} h(Q) \pmod{p^k}. \tag{7}$$

We will split (7) according to which number partition is induced by the cardinalities of the sets in Q. From any set partition $Q \in \mathcal{S}$ we can generate a multiset $\pi(Q) = \{|q| : q \in Q\}$ that forms an integer partition of p^{k-1}. For any integer partition π of p^{k-1}, let $\mathcal{S}_\pi = \{Q \in \mathcal{S} : \pi(Q) = \pi\}$. Importantly, for a given π, the value of $h(Q)$ is identical for all $Q \in \mathcal{S}_\pi$, and we denote this common value by h_π. Hence

$$\begin{aligned} F_{n+p^k}(a) \pmod{p^k} &\equiv F_n(a)\sum_{\pi}\sum_{Q\in\mathcal{S}_\pi} h(Q) \\ &\equiv F_n(a)\sum_{\pi} |\mathcal{S}_\pi|\ h_\pi \\ &\equiv F_n(a)\Big(h_{\pi_0} + \sum_{\pi\neq\pi_0} |\mathcal{S}_\pi|\ h_\pi\Big) \quad [\pi_0 \text{ is defined in Table 1}] \\ &\equiv F_n(a)\ h_{\pi_0}. \quad [\text{by Lemma 13}] \end{aligned}$$

Let $Q_{\pi_0} = \{\{1\},\{2\},\ldots,\{p^{k-1}\}\}$, the unique set partition in S_{π_0}. We compute

$$\begin{aligned} h_{\pi_0} &= \sum_{R\subseteq Q_{\pi_0}} \Big(\prod_{q\in Q_{\pi_0}} \cancel{|q|^{|q|-2}p^{|q|-1}}\Big)\Big(\prod_{r\in R} \cancel{|r|}\ n\Big)\ a^{(|Q_{\pi_0}|-|R|)p} \quad [\text{since } |q| = |r| = 1] \\ &= \sum_{R\subseteq Q_{\pi_0}} n^{|R|}a^{p^k-|R|p} \\ &= \sum_{i=0}^{p^{k-1}} \binom{p^{k-1}}{i}\ n^i a^{p^k-ip} \\ &= (n+a^p)^{p^{k-1}}. \quad [\text{by the Binomial Theorem}] \end{aligned}$$

Thus,

$$\begin{aligned} h_{\pi_0} \pmod{p^k} &\equiv (n+a)^{p^{k-1}} && \text{[by Lemma 8]} \\ &\equiv (n+a)^{p^k}, && \text{[by Lemma 9]} \end{aligned}$$

and the result follows. □

Next we resolve the $p = 2$ and $n \geq 1$ case.

Theorem 2. *If $n \geq 1$ then*

$$F_{n+2^k}(a) \pmod{2^k} \equiv \begin{cases} F_n(a) & \text{if } n \text{ is odd and } k \neq 2 \\ (-1)^a F_n(a) & \text{if } n \text{ is odd and } k = 2 \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

Proof. The proof for the $p = 2$ case begins the same as the proof for Theorem 1, so we will only elaborate on the discrepancies between the proofs. Firstly, Observation 4 is invalid for $p = 2$; a counter-example is given in Figure 4. The second difference between these proofs is that Lemma 13 behaves differently in the $p = 2$ case.

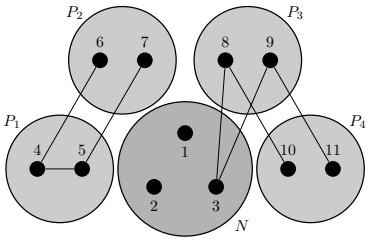


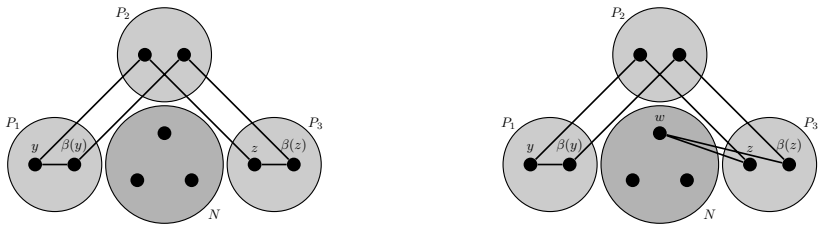
Figure 4: A example of a forest in $\mathcal{A}$ when $p = 2$, $k = 3$, and $n = 3$.

We make the following additional observations when $p = 2$ (illustrated in Figure 5).

Observation 5. Suppose $y \in P_i$ and $z \in P_j$ for distinct i and j. Then H cannot have the edges $y\beta(y)$, $z\beta(z)$ and a path T between y and z. *Proof*: Otherwise $\{y\beta(y)\} \cup T \cup \{z\beta(z)\} \cup \beta(T)$ is a cycle.

Observation 6. Suppose $w \in N$, $y \in P_i$ and $z \in P_j$ for distinct i and j. Then H cannot have the edges $y\beta(y)$, zw and a path T between y and z. *Proof*: Otherwise $\{y\beta(y)\} \cup T \cup \{zw, w\beta(z)\} \cup \beta(T)$ is a cycle.

Each $H \in \mathcal{H}$ induces a partition $Q \in \mathcal{S}$ and two disjoint subsets $R, W \subseteq Q$, where the partition Q and the subset R are defined as in the odd p case (see the proof of Theorem 1), and



(a) Observation 5 (b) Observation 6

Figure 5: Illustrating how cycles arise in Observations 5 and 6.

(iii) a part $q \in Q$ belongs to W whenever there is some $i \in q$ such that there is an edge joining the two vertices in P_i.

We will use W to account for the possible ways that the individual P_i might be internally connected. Observation 6 ensures that the sets R and W are disjoint. For example, the graph in Figure 4 induces the partition $Q = \big\{\{1,2\},\{3,4\}\big\}$ and subsets $R = \big\{\{3,4\}\big\}$ and $W = \big\{\{1,2\}\big\}$.

This time, we partition $\mathcal{H}$ into sets

$$\mathcal{H}(Q,R,W) = \{H \in \mathcal{H} : H \text{ induces partition } Q \text{ and } R, W \subseteq Q\}.$$

Note that $\mathcal{H}(Q,R,W)$ is empty when R and W have a nonempty intersection.

When constructing $H \in \mathcal{H}(Q,R,W)$, we add the following additional step to the construction in the odd p case.

(e) For each part $w \in W$, we add an edge to H between the two vertices in P_i for some $i \in w$. For each $w \in W$, we add this edge for exactly one $i \in w$, and this can be achieved in $|w|$ ways. Note that this step adds a further $|W|$ edges to H.

For a given $Q \in \mathcal{S}$ and disjoint $R, W \subseteq Q$, we find $|H| = 2^k - 2(|Q| - |R|) + |W|$. Since (4) is valid for $p = 2$ and $n \geq 1$, we obtain

$$\begin{aligned} F_{n+2^k}(a) \pmod{2^k} &\equiv F_n(a) \sum_{Q \in \mathcal{S}} \sum_{\substack{R,W \subseteq Q \\ R \cap W = \emptyset}} \sum_{H \in \mathcal{H}(Q,R,W)} a^{2^k - |H|} \\ &\equiv F_n(a) \sum_{Q \in \mathcal{S}} \sum_{\substack{R,W \subseteq Q \\ R \cap W = \emptyset}} |\mathcal{H}(Q,R,W)| \; a^{2(|Q|-|R|)-|W|}. \end{aligned} \tag{9}$$

We define

$$\ell(Q) = \sum_{\substack{R,W\subseteq Q\\ R\cap W=\emptyset}} |\mathcal{H}(Q,R,W)|\; a^{2(|Q|-|R|)-|W|}$$
$$= \sum_{\substack{R,W\subseteq Q\\ R\cap W=\emptyset}} \Big(\prod_{q\in Q} |q|^{|q|-2}2^{|q|-1}\Big)\Big(\prod_{r\in R}|r|\; n\Big)\Big(\prod_{w\in W}|w|\Big)\; a^{2(|Q|-|R|)-|W|}.$$

Here, when W is empty, step (e) can be performed in exactly one way (i.e., do nothing), in which case we set $\prod_{w\in W}|w| = 1$.

As with the odd p case, given an integer partition π, the value of $\ell(Q)$ is identical for all $Q \in \mathcal{S}_\pi$, and we denote this by ℓ_π. Now, Lemma 13 implies

$$\sum_{Q\in\mathcal{S}} \ell(Q) \pmod{2^k} \equiv \ell_{\pi_0} + |\mathcal{S}_{\pi_1}|\; \ell_{\pi_1} + |\mathcal{S}_{\pi_2}|\; \ell_{\pi_2}, \tag{10}$$

where π_0, π_1, and π_2 are as defined in Table 1. Note that, for π_1 to be realizable, we need $2^{k-1}-2 \geq 0$, and for π_2 to be realizable, we need $2^{k-1}-4 \geq 0$. So $|\mathcal{S}_{\pi_1}| = 0$ when $k = 1$ and $|\mathcal{S}_{\pi_2}| = 0$ when $k \leq 2$.

We first compute $\ell_{\pi_0} \pmod{2^k}$ as follows:

$$\ell_{\pi_0} = \sum_{\substack{R,W\subseteq Q_{\pi_0}\\ R\cap W=\emptyset}} \Big(\prod_{q\in Q_{\pi_0}} \cancel{|q|^{|q|-2}2^{|q|-1}}\Big)\Big(\prod_{r\in R}\cancel{|r|}\; n\Big)\cancel{\Big(\prod_{w\in W}|w|\Big)}\; a^{2(|Q_{\pi_0}|-|R|)-|W|},$$

where the cancellations occur because $|q| = |r| = |w| = 1$ for all q, r and w in this case. That is,

$$\begin{aligned}
\ell_{\pi_0} \pmod{2^k} &\equiv \sum_{\substack{R,W\subseteq Q_{\pi_0}\\ R\cap W=\emptyset}} n^{|R|}a^{2^k-2|R|-|W|}\\
&\equiv \sum_{\substack{i,j\geq 0\\ i+j\leq 2^{k-1}}} \binom{2^{k-1}}{i,j,2^{k-1}-i-j}\; n^i a^{2^k-2i-j}\\
&\equiv \sum_{\substack{i,j\geq 0\\ i+j\leq 2^{k-1}}} \binom{2^{k-1}}{i,j,2^{k-1}-i-j}\; n^i a^j (a^2)^{2^{k-1}-i-j}\\
&\equiv (n+a+a^2)^{2^{k-1}} && \text{[by the Multinomial Theorem]}\\
&\equiv n^{2^{k-1}} && \text{[by Lemma 8]}\\
&\equiv \begin{cases} 1 & \text{if } n \text{ is odd;}\\ 0 & \text{otherwise.}\end{cases} && \text{[by Lemma 7 (Euler's Theorem)]}
\end{aligned}$$

Now let Q_{π_1} be an arbitrary set partition in S_{π_1}. We find:

$$\ell_{\pi_1} = \sum_{\substack{R,W\subseteq Q_{\pi_1}\\ R\cap W=\emptyset}} \Big(\prod_{q\in Q_{\pi_1}} \cancel{|q|}^{\cancel{|q|-2}} 2^{|q|-1}\Big)\Big(\prod_{r\in R}|r|\ n\Big)\Big(\prod_{w\in W}|w|\Big)\ a^{2(|Q_{\pi_1}|-|R|)-|W|},$$

since $|q|\le 2$ for all $q\in Q_{\pi_1}$. Thus,

$$\begin{aligned}|\mathcal{S}_{\pi_1}|\ \ell_{\pi_1} &= |\mathcal{S}_{\pi_1}| \prod_{q\in Q_{\pi_1}} 2^{|q|-1} \sum_{\substack{R,W\subseteq Q_{\pi_1}\\ R\cap W=\emptyset}} \Big(\prod_{r\in R}|r|\ n\Big)\Big(\prod_{w\in W}|w|\Big)\ a^{2(|Q_{\pi_1}|-|R|)-|W|}\\ &\equiv 2^{k-1} \sum_{\substack{R,W\subseteq Q_{\pi_1}\\ R\cap W=\emptyset}} \Big(\prod_{r\in R}|r|\ n\Big)\Big(\prod_{w\in W}|w|\Big)\ a^{2(|Q_{\pi_1}|-|R|)-|W|} \pmod{2^k},\end{aligned}$$

where we apply Lemma 13 in the last step. Further note that if there exists an $r\in R$ such that $|r|=2$ or a $w\in W$ such that $|w|=2$ then, together with the common 2^{k-1} factor, the corresponding (R,W) pair will contribute nothing to the sum modulo 2^k in the last step. Hence,

$$|\mathcal{S}_{\pi_1}|\ \ell_{\pi_1} \pmod{2^k} \equiv 2^{k-1} \sum_{\substack{R,W\subseteq Q_{\pi_1}\\ R\cap W=\emptyset\\ r\in R\implies |r|=1\\ w\in W\implies |w|=1}} \Big(\prod_{r\in R}\cancel{|r|}\ n\Big)\cancel{\Big(\prod_{w\in W}|w|\Big)}\ a^{2(|Q_{\pi_1}|-|R|)-|W|},$$

where the cancellations occur because $|r|=|w|=1$. We finally obtain,

$$\begin{aligned}|\mathcal{S}_{\pi_1}|\ \ell_{\pi_1} \pmod{2^k} &\equiv 2^{k-1} \sum_{\substack{R,W\subseteq Q_{\pi_1}\\ R\cap W=\emptyset\\ r\in R\implies |r|=1\\ w\in W\implies |w|=1}} n^{|R|} a^{2^k-2-2|R|-|W|}\\ &\equiv 2^{k-1} \sum_{\substack{i,j\ge 0\\ i+j\le 2^{k-1}-2}} \binom{2^{k-1}-2}{i,j,2^{k-1}-2-i-j}\ n^i a^{2^k-2-2i-j}\\ &\equiv 2^{k-1} \sum_{\substack{i,j\ge 0\\ i+j\le 2^{k-1}-2}} \binom{2^{k-1}-2}{i,j,2^{k-1}-2-i-j}\ n^i a^j (a^2)^{2^{k-1}-1-i-j}\\ &\equiv 2^{k-1}a^2(n+a+a^2)^{2^{k-1}-2} \qquad \text{[by the Multinomial Theorem]}.\end{aligned}$$

We can similarly prove $|\mathcal{S}_{\pi_2}|\ \ell_{\pi_2} \equiv 2^{k-1}a^4(n+a+a^2)^{2^{k-1}-4} \pmod{2^k}$.

Consequently, whenever $a\equiv 0 \pmod 2$ we have $|\mathcal{S}_{\pi_1}|\ \ell_{\pi_1} \equiv |\mathcal{S}_{\pi_2}|\ \ell_{\pi_2} \equiv 0 \pmod{2^k}$. When $a\equiv 1 \pmod 2$, we tabulate below the values of $|\mathcal{S}_{\pi_1}|\ \ell_{\pi_1}$ and

$|\mathcal{S}_{\pi_2}|\ \ell_{\pi_2}$ modulo 2^k.

	n	ℓ_{π_0}	$\lvert\mathcal{S}_{\pi_1}\rvert\ \ell_{\pi_1}$	$\lvert\mathcal{S}_{\pi_2}\rvert\ \ell_{\pi_2}$	$\ell_{\pi_0}+\lvert\mathcal{S}_{\pi_1}\rvert\ \ell_{\pi_1}+\lvert\mathcal{S}_{\pi_2}\rvert\ \ell_{\pi_2} \pmod{2^k}$
$k=1$	even	0	–	–	0
$k=2$	even	0	2	–	2
$k=3$	even	0	0	4	4
$k\geq 4$	even	0	0	0	0
$k=1$	odd	1	–	–	1
$k=2$	odd	1	2	–	$3\equiv -1$
$k\geq 3$	odd	1	2^{k-1}	2^{k-1}	1

Using the above table, and from (9) and (10), we can write

$$F_{n+2^k}(a) \pmod{2^k} \equiv \begin{cases} F_n(a) & \text{if } n \text{ is odd and } k\neq 2 \\ (-1)^a F_n(a) & \text{if } n \text{ is odd and } k=2 \\ 2F_n(a) & \text{if } n \text{ is even}, k=2 \text{ and } a \text{ is odd} \\ 4F_n(a) & \text{if } n \text{ is even}, k=3 \text{ and } a \text{ is odd} \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

However, when a is odd, we know $F_2(a)=a+1$ (see Table 2) is even. Further, (11) implies $F_n(a)$ is even for all $a\in\mathbb{Z}$ and even $n\geq 4$. These two observations, together with (11), give $F_{n+2^k}(a)\equiv 0 \pmod{2^k}$ for all even $n\geq 2$ when $k\in\{2,3\}$, and the claimed result follows. □

We have now completed the $n\geq 1$ cases. For the $n=0$ cases, we will need the following lemma (which is interesting in its own right).

Let $f_{m,q}$ denote the number of labeled forests on m vertices with exactly q edges. In other words, $f_{m,q}$ is the coefficient of the term x^{m-1-q} in the polynomial $F_m(x)$.

Lemma 2. *If m is odd, $m\geq 3$ and $q\geq 1$, then $f_{m,q}\equiv 0 \pmod{m}$.*

Proof. Let $\mathcal{F}_{m,q}$ be the set of labeled forests on the vertex set $\{1,2,\ldots,m\}$ with exactly q edges. Let p be a (necessarily odd) prime divisor of m, and let $m=p^c t$ where $\gcd(t,p)=1$. The cyclic group $\langle(1,2,\ldots,m)\rangle$ acts on $\mathcal{F}_{m,q}$. By the Orbit-Stabilizer Theorem, the orbits of this action have size divisible by p^c unless they contain forests with a stabilizer of order divisible by p or, equivalently, they admit the automorphism $\zeta := (1,2,\ldots,m)^{m/p}$. Hence

$$f_{m,q} = |\mathcal{F}_{m,q}| \equiv |\{G\in\mathcal{F}_{m,q} : \zeta G = G\}| \pmod{p^c}.$$

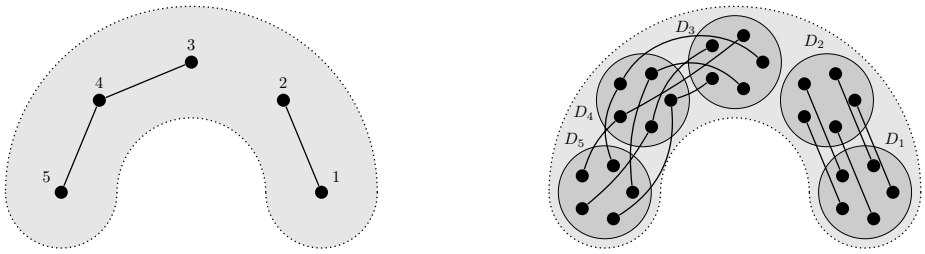
Let $\gamma = (1,2,\ldots,p)(p+1,p+2,\ldots,2p)\cdots(m-p+1,m-p+2,\ldots,m)$ and $\mathcal{B}=\{G\in\mathcal{F}_{m,q} : \gamma G = G\}$. Since ζ and γ have the same cycle structure, we have

$$f_{m,q}\equiv |\mathcal{B}| \pmod{p^c}.$$

Let G be an arbitrary forest in $\mathcal{B}$. We partition the vertices of G into blocks $D_i := \{p(i-1)+1, p(i-1)+2, \ldots, pi\}$ for $i \in \{1, 2, \ldots, m/p\}$. Blocks correspond to disjoint cycles of γ.

A property of admitting the automorphism γ is that we can apply Observations 3 and 4 from the proof of Theorem 1 on the blocks D_i of any forest in $\mathcal{B}$. In other words, there are either 0 or p edges between any distinct pair of blocks D_i and D_j, and no edges between the p vertices of any block D_i. Thus as $q \geq 1$, if $\mathcal{B}$ is non-empty then p divides q.

When $\mathcal{B}$ is non-empty, for each $G \in \mathcal{B}$ we can obtain a corresponding forest $G' \in \mathcal{F}_{m/p,q/p}$ by identifying all p vertices of block D_i in G into a single vertex for each $i \in \{1, \ldots, m/p\}$, and identifying parallel edges in the reduced graph to a single edge. Similarly, we can reverse this process to obtain $p^{q/p}$ forests in $\mathcal{B}$ from each $G' \in \mathcal{F}_{m/p,q/p}$ as follows: we "blow up" each vertex i in G' to a p-vertex block D_i, then for each edge ij in G' (there are q/p such edges) we have p choices to connect the vertices in blocks D_i and D_j (so as to achieve the automorphism γ without introducing cycles). An example of this reversing process is illustrated in Figure 6.



(a) A graph in $\mathcal{F}_{m/p}(q/p)$.

(b) An example of a blow up of the forest in (a), giving a forest in $\mathcal{B}$.

Figure 6: Illustrating the blow up process. Here we have $m = 25$, $q = 15$, and $p = 5$.

Hence

$$f_{m,q} \pmod{p^c} \equiv \begin{cases} 0 & \text{if } p \text{ does not divide } q \\ p^{q/p} f_{m/p,q/p} & \text{otherwise.} \end{cases}$$

Since $q \geq 1$, we know that p divides $p^{q/p}$. Hence, if p^{c-1} divides $f_{m/p,q/p}$, then p^c divides $f_{m,q}$. We repeat this descent until we either (a) reach q/p^k edges, for some k in the range $1 \leq k < c$, such that p does not divide q/p^k, or (b) reach the base condition that p divides $f_{m/p^{c-1},q/p^{c-1}}$, and it follows from either of these that $f_{m,q} \equiv 0 \pmod{p^c}$. The result now follows from the Chinese Remainder Theorem. □

The $p \geq 3$ and $n = 0$ case of Proposition 1 follows easily from Lemma 2.

Theorem 3. *If m is odd and $m \geq 3$ then $F_m(a) \equiv a^{m-1} \pmod{m}$. In particular, if p is an odd prime and $k \geq 1$ then $F_{p^k}(a) \equiv a^{p^k-1} \pmod{p^k}$.*

Proof. From (1) and Lemma 2, we have

$$F_m(a) = \sum_{q \geq 0} f_{m,q}\, a^{m-1-q} \equiv a^{m-1} \pmod{m}. \qquad \square$$

The last step in the proof of Proposition 1 is the $p = 2$ and $n = 0$ case.

Theorem 4. *For integers $k \geq 1$,*

$$F_{2^k}(a) \pmod{2^k} \equiv \begin{cases} 1 & \text{if } k = 1 \text{ and } a \text{ is even} \\ 2 & \text{if } k = 2 \text{ and } a \not\equiv 0 \pmod 4 \\ 4 & \text{if } k = 3 \text{ and } a \text{ is odd} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We continue with the setup in the $p = 2$ and $n \geq 1$ case (Theorem 2). Equation (4) does not hold when $n = 0$, so instead use (2), which gives

$$F_{2^k}(a) \equiv \sum_{G \in \mathcal{A}} a^{2^k - |G| - 1} \pmod{2^k}.$$

Since $|N| = 0$, we have $\mathcal{A} = \mathcal{H}$, and for $\mathcal{H} = \mathcal{H}(Q, R, W)$ to be non-empty, we must have $R = \emptyset$, so

$$F_{2^k}(a) \equiv \sum_{Q \in \mathcal{S}} \sum_{W \subseteq Q} \sum_{G \in \mathcal{H}(Q, \emptyset, W)} a^{2^k - |G| - 1} \pmod{2^k}.$$

We can construct forests $G \in \mathcal{H}(Q, \emptyset, W)$ following Steps (a)–(e) in the proofs of Theorems 1 and 2. The number of edges of any $G \in \mathcal{H}(Q, \emptyset, W)$ is $2^k - 2|Q| + |W|$, and so

$$\begin{aligned} F_{2^k}(a) \pmod{2^k} &\equiv \sum_{Q \in \mathcal{S}} \sum_{W \subseteq Q} |\mathcal{H}(Q, \emptyset, W)|\; a^{2|Q| - |W| - 1} \\ &\equiv \sum_{Q \in \mathcal{S}} \sum_{W \subseteq Q} \left(\prod_{q \in Q} 2^{|q|-1} |q|^{|q|-2} \right) \left(\prod_{w \in W} |w| \right) a^{2|Q| - |W| - 1} \\ &\equiv \sum_{Q \in \mathcal{S}} \sum_{Z \subseteq Q} \left(\prod_{q \in Q} 2^{|q|-1} |q|^{|q|-2} \right) \left(\prod_{z \notin Z} |z| \right) a^{|Q| + |Z| - 1}, \end{aligned}$$

where we define $Z = Q \setminus W$. If we also denote

$$\ell'(Q) = \sum_{Z \subseteq Q} \left(\prod_{q \in Q} 2^{|q|-1} |q|^{|q|-2} \right) \left(\prod_{z \notin Z} |z| \right) a^{|Q| + |Z| - 1},$$

then

$$F_{2^k}(a) \pmod{2^k} \equiv \sum_{\pi} \sum_{Q \in \mathcal{S}_\pi} \ell'(Q),$$

where the outer sum is over all integer partitions π of 2^{k-1}.

As before, given a partition π, the value of $\ell'(Q)$ is identical for all $Q \in \mathcal{S}_\pi$, and we denote this common value by ℓ'_π. From Lemma 13, we know π makes a zero contribution modulo 2^k above, except possibly when $\pi \in \{\pi_0, \pi_1, \pi_2\}$. Hence

$$F_{2^k}(a) \equiv \ \ell'_{\pi_0} + |\mathcal{S}_{\pi_1}|\ \ell'_{\pi_1} + |\mathcal{S}_{\pi_2}|\ \ell'_{\pi_2} \pmod{2^k},$$

again noting that $|\mathcal{S}_{\pi_1}| = 0$ when $k = 1$ and $|\mathcal{S}_{\pi_2}| = 0$ when $k \in \{1, 2\}$. We will complete the proof of the theorem by finding formulas for $|\mathcal{S}_{\pi_i}|\ \ell'_{\pi_i} \pmod{2^k}$ for $i \in \{0, 1, 2\}$.

First,

$$\begin{aligned}
\ell'_{\pi_0} &= \sum_{Z \subseteq Q_{\pi_0}} \left(\prod_{q \in Q_{\pi_0}} \cancel{2^{|q|-1}|q|^{|q|-2}} \right) \cancel{\left(\prod_{z \notin Z} |z| \right)} \, a^{|Q_{\pi_0}|+|Z|-1} && \text{[since } |q| = |z| = 1\text{]} \\
&= a^{2^{k-1}-1} \sum_{Z \subseteq Q_{\pi_0}} a^{|Z|} \\
&= a^{2^{k-1}-1}(a+1)^{2^{k-1}}. && \text{[by the Binomial Theorem]}
\end{aligned}$$

We thus compute

$$\ell'_{\pi_0} \pmod{2^k} \equiv \begin{cases} 1 & \text{if } k = 1 \text{ and } a \text{ is even} \\ 2 & \text{if } k = 2 \text{ and } a \equiv 2 \pmod 4 \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

Next, when $k \geq 2$, we have

$$\ell'_{\pi_1} = \sum_{Z \subseteq Q_{\pi_1}} \left(\prod_{q \in Q_{\pi_1}} 2^{|q|-1} \cancel{|q|^{|q|-2}} \right) \left(\prod_{z \notin Z} |z| \right) a^{|Q_{\pi_1}|+|Z|-1}. \qquad \text{[since } |q| \leq 2\text{]}$$

Hence,

$$\begin{aligned}
|\mathcal{S}_{\pi_1}|\ \ell'_{\pi_1} \pmod{2^k} &\equiv |\mathcal{S}_{\pi_1}| \prod_{q \in Q_{\pi_1}} 2^{|q|-1} \sum_{Z \subseteq Q_{\pi_1}} \left(\prod_{z \notin Z} |z| \right) a^{2^{k-1}+|Z|-2} \\
&\equiv 2^{k-1} \sum_{Z \subseteq Q_{\pi_1}} \left(\prod_{z \notin Z} |z| \right) a^{2^{k-1}+|Z|-2}. && \text{[by Lemma 13]}
\end{aligned}$$

If the part of size 2 is not in Z, then $\prod_{z\notin Z}|z|=2$, and Z makes a zero contribution modulo 2^k in the above sum. Thus,

$$|\mathcal{S}_{\pi_1}|\ \ell'_{\pi_1} \pmod{2^k} \equiv 2^{k-1}a^{2^{k-1}-1} \sum_{\substack{Z\subseteq Q_{\pi_1}\\ z\notin Z \implies |z|=1}} \cancel{\left(\prod_{z\notin Z}|z|\right)} a^{|Z|-1}. \quad \text{[since } |z|=1\text{]}$$

As $|Z|\geq 1$ in the above sum, we get

$$\begin{aligned}|\mathcal{S}_{\pi_1}|\ \ell'_{\pi_1} \pmod{2^k} &\equiv 2^{k-1}a^{2^{k-1}-1}\sum_{t\geq 0}\binom{2^{k-1}-2}{t}a^t\\ &\equiv 2^{k-1}a^{2^{k-1}-1}(a+1)^{2^{k-1}-2} \qquad \text{[by the Binomial Theorem]}\\ &\equiv \begin{cases}2 & \text{if } k=2 \text{ and } a \text{ is odd}\\ 0 & \text{otherwise.}\end{cases} \end{aligned} \tag{13}$$

Lastly, when $k\geq 3$, similar to the π_1 case, we have

$$|\mathcal{S}_{\pi_2}|\ \ell'_{\pi_2} \pmod{2^k} \equiv 2^{k-1}\sum_{Z\subseteq Q_{\pi_2}}\left(\prod_{z\notin Z}|z|\right)a^{2^{k-1}+|Z|-3}. \quad \text{[by Lemma 13]}$$

Again, if a part of size 2 is not in Z, then 2 divides $\prod_{z\notin Z}|z|$, and Z makes a zero contribution modulo 2^k. Hence,

$$|\mathcal{S}_{\pi_2}|\ \ell'_{\pi_2} \pmod{2^k} \equiv 2^{k-1}a^{2^{k-1}-1}\sum_{\substack{Z\subseteq Q_{\pi_2}\\ q\notin Z \implies |q|=1}} a^{|Z|-2}.$$

As both parts of size 2 are in Z, we have $|Z|\geq 2$ in the previous sum, and thus

$$\begin{aligned}|\mathcal{S}_{\pi_2}|\ \ell'_{\pi_2} \pmod{2^k} &\equiv 2^{k-1}a^{2^{k-1}-1}(a+1)^{2^{k-1}-4} \qquad \text{[by the Binomial Theorem]}\\ &\equiv \begin{cases}4 & \text{if } k=3 \text{ and } a \text{ is odd}\\ 0 & \text{otherwise.}\end{cases}\end{aligned} \tag{14}$$

Combining (12), (13) and (14) gives the stated theorem. □

3. Consequences of Proposition 1

Proposition 1 shows that the infinite sequence $(F_n(a) : n \geq 1)$, when reduced modulo a prime power p^k, is fully determined by its first p^k terms. In this section, we have a closer look at its various implications.

Henceforth we use φ to denote the Euler totient function. Recall that for any positive integer n, $\varphi(n)$ denotes the number of integers coprime to n.

3.1. $F_n(a)$ Modulo Integers Less Than or Equal to n

We begin by using the Chinese Remainder Theorem to show that the sequence $(F_n(a) : n \geq 1)$ when reduced modulo any positive integer m, can be fully obtained from its first m terms.

Lemma 3. *If n, m and q are positive integers such that $m = 2^s t$, with $s \geq 0$, t odd and $t \geq 3$, then*

$$F_{n+qm}(a) \pmod{m} \equiv \begin{cases} 2^{s\varphi(t)}(n+a)^{qm}F_n(a) & \text{if } n \text{ is even or } s = 0 \\ \left(4^{\varphi(t)}(n+a)^{qm} + (-1)^{aq}t^2\right)F_n(a) & \text{if } n \text{ is odd and } s = 2 \\ \left(2^{s\varphi(t)}(n+a)^{qm} + t^{2^{s-1}}\right)F_n(a) & \text{otherwise.} \end{cases}$$

Proof. Let $t = \prod_{1 \leq i \leq r} p_i^{k_i}$, where r is a positive integer, $p_1, p_2, \ldots, p_r$ are distinct odd primes and $k_1, k_2, \ldots, k_r$ are positive integers. Then, from Theorem 1, for any $i \in \{1, 2, \ldots, r\}$,

$$F_{n+qm}(a) \equiv (n+a)^{p_i^{k_i}} F_{n+qm-p_i^{k_i}}(a) \pmod{p_i^{k_i}}. \tag{15}$$

Applying (15) repeatedly q times, we find for each $i \in \{1, \ldots, r\}$,

$$F_{n+qm}(a) \equiv (n+a)^{qm}F_n(a) \pmod{p_i^{k_i}},$$

and hence from the Chinese Remainder Theorem,

$$F_{n+qm}(a) \equiv (n+a)^{qm}F_n(a) \pmod{t}. \tag{16}$$

The case $s = 0$ is immediate from (16). If $s \geq 1$ from Theorem 2,

$$F_{n+qm}(a) \pmod{2^s} \equiv \begin{cases} F_n(a) & \text{if } n \text{ is odd and } s \neq 2 \\ (-1)^{aq}F_n(a) & \text{if } n \text{ is odd and } s = 2 \\ 0 & \text{otherwise.} \end{cases} \tag{17}$$

The claimed result now follows from another application of the Chinese Remainder Theorem on (16) and (17), and using Lemma 7. □

The special case of Lemma 3 when m is a factor of n is worth noting separately.

Lemma 4. *For positive integers n and m such that $m = 2^s t$, with $s \geq 0$, t odd and $t \geq 3$, if m divides n then $F_n(a) \equiv 2^{s\varphi(t)}a^{n-1} \pmod{m}$.*

Proof. From Lemma 3, we get

$$F_n(a) = F_{t+n-t}(a) \equiv a^{n-t}F_t(a) \pmod{t}. \tag{18}$$

Applying Theorem 3 to (18) gives

$$F_n(a) \equiv a^{n-1} \pmod{t}. \tag{19}$$

The case $s = 0$ follows from (19). When $s \geq 1$ we can deduce that $n - 2^s$ is even, and thus from Theorem 2,

$$F_n(a) = F_{n-2^s+2^s}(a) \equiv 0 \pmod{2^s}. \tag{20}$$

The result follows using Lemma 7 and the Chinese Remainder Theorem on (19) and (20). □

3.2. Small Prime Factors of $F_n(a)$

We next give a complete characterization of all prime factors p^k of $F_n(a)$ such that $p^k \leq n$, based on the factorization of the first p^k terms of $(F_n(a) : n \geq 1)$.

We begin with a characterization of the small odd prime power factors of $F_n(a)$. The case $p^k = n$ is a special case of the next observation, which is an easy consequence of Lemma 4.

Proposition 2. *For an odd prime p and positive integer k, if p^k divides n then p^k divides $F_n(a)$ if and only if $a \equiv 0 \pmod{p}$.*

For the case $p^k < n$, we have the following.

Proposition 3. *Given an odd prime p and positive integer k, if $n > p^k$ and p^k does not divide n, then p^k is a factor of $F_n(a)$ if and only if either:*

1. *$n \equiv -a \pmod{p}$; or*
2. *p^k is a factor of $F_r(a)$, where $r \equiv n \pmod{p^k}$ and $0 < r < p^k$.*

Proof. Since p^k does not divide n, we can write $n = qp^k + r$ for positive integers q and r such that $0 < r < p^k$. Then from Lemma 3, we have

$$F_n(a) \equiv (n + a)^{qp^k} F_r(a) \pmod{p^k}. \tag{21}$$

Clearly, from (21) if either of the conditions in the claim is satisfied then p^k is a factor of $F_n(a)$.

For the converse, suppose for a contradiction that p^k is a factor of $F_n(a)$ and neither of the two conditions in the claim is satisfied. Then, from (21), there exists positive integers i, j such that $i + j = k$ and $(n + a)^{qp^k} \equiv 0 \pmod{p^i}$ and $F_r(a) \equiv 0 \pmod{p^j}$. However this implies $n + a \equiv 0 \pmod{p}$ which contradicts our assumptions. □

Theorem 4 outlines the conditions when 2^k is a factor of $F_{2^k}(a)$. The next result characterizes the $2^k < n$ factors of $F_n(a)$, and is an easy consequence of Theorem 2 along with the fact $F_1(a) = 1$ for all $a \in \mathbb{Z}$.

Proposition 4. *If $k \geq 1$ and $n > 2^k$ then 2^k divides $F_n(a)$ if and only if n is even.*

We next deduce two interesting consequences from these small factor characterizations of $F_n(a)$. First, from Table 3 it can be checked that for all $n \leq 30$, the number of labeled forests on n vertices, that is $f_n = F_n(1)$, does not share any odd factors with n. More generally, we can establish the following.

Proposition 5. *If $a = \pm 2^k$ for some $k \geq 0$ then every $n \geq 2$ has no common odd factors with $F_n(a)$.*

Proof. When $a = \pm 2^k$ we have $a \not\equiv 0 \pmod{p}$ for any odd prime p, and the result follows from Proposition 2. □

Second, we can show that every positive integer divides infinitely many terms in the sequence $(F_n(a) : n \geq 1)$ for every $a \in \mathbb{Z}$. We first need the following observation, which is a straightforward consequence of Lemma 3.

Lemma 5. *If a positive integer m divides $F_n(a)$, then m divides $F_{n+qm}(a)$ for all integers $q \geq 1$.*

We are ready to prove the following result.

Proposition 6. *For all $a \in \mathbb{Z}$, every positive integer m divides infinitely many terms in the sequence $(F_n(a) : n \geq 1)$.*

Proof. The case $m = 1$ is trivial.

If $m = 2^s$ for some positive integer s, then from Proposition 4, m divides $F_{m+2q}(a)$ for all integers $q \geq 1$.

Now suppose $m = 2^s t$ for some $s \geq 0$, $t \geq 3$ and t odd. Write $t = \prod_{i=1}^{\ell} p_i^{k_i}$ where p_i is an odd prime and k_i is a positive integer for each $i \in \{1, \ldots, \ell\}$, and also let $u = \prod_{i=1}^{\ell} p_i$. Then from Propositions 2, 3 and 4, we can verify that m divides $F_{m+|a|u-a}(a)$. Hence from Lemma 5, m divides $F_{qm+|a|u-a}(a)$ for all integers $q \geq 1$. □

3.3. Periodicity Results

In this section, we show that the sequence $(F_n(a) : n \geq 1)$ is ultimately periodic modulo any positive integer m. We begin with the following lemma. Recall that a sequence $(a_n : n > q)$ is *antiperiodic* with period t if $a_{n+t} = -a_n$ for all $n > q$.

Lemma 6. *For any prime p and $k \geq 1$, the sequence $(F_n(a) : n > p^k)$ is periodic modulo p^k with a period t that divides $p^k(p-1)$ unless $p = k = 2$ and a is odd, when the sequence is antiperiodic modulo 4 with a period t that divides 4 (and thus, periodic modulo 4 with period $2t$).*

Proof. The case $p = 2$ can be deduced from Theorem 2.

Suppose $p \geq 3$. Then from Lemma 3,

$$F_{n+p^k(p-1)}(a) \equiv (n+a)^{p^k(p-1)} F_n(a) \pmod{p^k}. \tag{22}$$

Applying Lemma 7 to (22), we find

$$F_{n+p^k(p-1)}(a) \pmod{p^k} \equiv \begin{cases} F_n(a) & \text{if } n \not\equiv -a \pmod{p} \\ 0 & \text{otherwise.} \end{cases} \tag{23}$$

Also, when $n > p^k$, from Proposition 3 we have $F_n(a) \equiv 0 \pmod{p^k}$ whenever $n \equiv -a \pmod{p}$. Thus, when $n > p^k$, (23) is equivalent to

$$F_{n+p^k(p-1)}(a) \equiv F_n(a) \pmod{p^k},$$

and the result follows. □

Fischer, Kotek, and Makowsky [6] showed that $(f_n = F_n(1) : n \geq 1)$ is ultimately periodic modulo every positive integer, a property they named MC-finite. We extend this result to $(F_n(a) : n \geq 1)$ for all $a \in \mathbb{Z}$ using Lemma 6.

Theorem 5. *The sequence $(F_n(a) : n \geq 1)$ is MC-finite for every $a \in \mathbb{Z}$.*

Proof. We need to show that the sequence is ultimately periodic modulo every positive integer m.

The case $m = 1$ is trivial. When $m > 1$, let $m = \prod_{i=i}^{\ell} p_i^{k_i}$, where p_i is a prime and k_i is a positive integer for each $i \in \{1, \ldots, \ell\}$. Also, let t_i be a period of $(F_n(a) : n > p_i^{k_i})$ modulo $p_i^{k_i}$ (Lemma 6 implies such t_is exist). Then it can be readily verified that $(F_n(a) : n \geq 1)$ is ultimately periodic modulo m with period $\operatorname{lcm}(t_1, \ldots, t_\ell)$. □

The periodic behavior of $(F_n(1) : 1 \leq n \leq 30)$ modulo some small positive integers, along with their eventual period t, is shown in Table 3.

4. Concluding Remarks

4.1. Computational Work

Our discovery of Proposition 1 was inspired by computational work for the Tutte polynomial of the complete graph. While there exists practical software for computing computing Tutte polynomials of arbitrary graphs (such as by Björklund,

Husfeldt, Kaski and Koivisto [4] and Haggard, Pearce, and Royle [9]), it is more efficient to compute the Tutte polynomial of the complete graph using the recurrence formula

$$T_{n+1}(x,y) = \sum_{i=1}^{n} \binom{n-1}{i-1} (x + y + y^2 + \cdots + y^{i-1})\ T_i(1,y)\ T_{n-i+1}(x,y) \qquad (24)$$

which was brought to our attention by Igor Pak [11], who gave credit to Gessel [7] and Gessel and Sagan [8]. Using this we have verified Proposition 1 for all $a \in \{-1000, -999, \ldots, 1000\}$, $p \in \{2,3,5,7,11\}$, $k \in \{1,2,\ldots,7\}$ and $n \in \{0,1,\ldots,300-p^k\}$.

4.2. Generalizing This Work

Computational and further theoretical work both indicate that $T_n(a,b)$ admits a recurrence congruence for all lattice points (a,b). Attempts at proving this have resulted in a prohibitive number of cases that need to be resolved, but it is intended to be a future research project for the authors.

As a non-trivial example, at this stage we can prove e.g.

$$T_{n+p^k}(1,b) \equiv b^{(p^k-p^{k-1})/2} T_{n+p^{k-1}}(1,b) \pmod{p^k} \qquad (25)$$

for prime $p \geq 3$ and $b \not\equiv 1 \pmod{p}$ and $(n,k) \neq (0,1)$ [10]. Computational work suggests (25) is true for $T_{n+p^k}(a,b)$ except when both $(n,k) \neq (0,1)$ and $a \equiv 1 \pmod{p}$. We note the distinction between this case and Proposition 1 since (25) relates $T_{n+p^k}(a,b)$ and $T_{n+p^{k-1}}(a,b)$, whereas Proposition 1 relates $T_{n+p^k}(1+a,1)$ and $T_n(1+a,1)$.

References

[1] G. E. Andrews, *The Theory of Partitions*, CUP, 1984.

[2] G. E. Andrews, *Number Theory*, Dover Publications, 1994.

[3] M. A. Armstrong, *Groups and Symmetry*, Springer, 1988.

[4] A. Björklund, T. Husfeldt, P. Kaski, and M. Koivisto. Computing the Tutte polynomial in vertex-exponential time, *Proc. of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2008)*, (2008), 677-686.

[5] A. Cayley. A theorem on trees, *The Q. J. of Pure Appl. Math.* **23** (1889), 376-378.

[6] E. Fischer, T. Kotek, and J. A. Makowsky. Application of logic to combinatorial sequences and their recurrence relations, *Contemp. Math.* **558** (2011), 1-42.

[7] I. M. Gessel. Enumerative applications of a decomposition for graphs and digraphs, *Discrete Math.* **139** (1995), 257-271.

[8] I. M. Gessel and B. E. Sagan. The Tutte polynomial of a graph, depth-first search, and simplicial complex partitions, *Electron. J. Combin.*, (1996), R9.

[9] G. Haggard, D. J. Pearce, and G. Royle. Computing Tutte polynomials, *ACM Trans. on Mathematical Software* **37** (2010).

[10] A. P. Mani and R. J. Stones. The number of labeled connected graphs modulo prime powers, *SIAM J. Discrete Math.*, to appear.

[11] I. M. Pak. Computation of the Tutte polynomial of complete graphs, (c. 1982), `http://www.math.ucla.edu/ pak/papers/Pak_Computation_Tutte_polynomial_complete_graphs.pdf`.

[12] N. J. A. Sloane. Number of forests of trees on n labeled nodes (Sequence A001858), *The on-line encyclopedia of integer sequences*, `http://oeis.org/A001858`.

A. Technical Lemmas

Here we list some technical lemmas that are required for the proofs in the paper.

Lemma 7 (Euler's Theorem [2, Th. 5.2])**.** *Let p be a prime, k a positive integer and b an integer such that $b \not\equiv 0 \pmod{p}$. Then $b^{\varphi(p^k)} \equiv 1 \pmod{p^k}$, where $\varphi(p^k) = p^{k-1}(p-1)$ is the Euler totient function.*

Lemma 8. *Let p a prime and k be a positive integer. If $a \equiv b \pmod{p}$ then $a^{p^{k-1}} \equiv b^{p^{k-1}} \pmod{p^k}$.*

Proof. We use induction on k. When $k = 1$, the statement is true from what is given. If the statement is true for some positive integer k, we can write $a^{p^{k-1}} = tp^k + b^{p^{k-1}}$ for some integer t. Then

$$a^{p^k} = (tp^k + b^{p^{k-1}})^p = \sum_{i=0}^{p} \binom{p}{i} t^i p^{ik} b^{(p-i)p^{k-1}} \equiv b^{p^k} \pmod{p^{k+1}}.$$

The statement now follows by induction. □

Lemma 9. *Let p a prime and k be a positive integer. Then for all integers a and $i \geq k-1$, we have $a^{p^i} \equiv a^{p^{k-1}} \pmod{p^k}$.*

Proof. From Lemma 7, we can deduce $a^{p^j} \equiv a \pmod{p}$ for all integers $j \geq 0$. Our result then follows from this by an application of Lemma 8. □

Lemma 10. *Let p be a prime and $1 \leq x \leq p^k$. Then $\binom{p^k}{x}$ is divisible by p^{k-r} where r is the largest integer such that p^r divides x.*

Proof. We begin with

$$\binom{p^k}{x} = \frac{p^k}{x} \frac{p^k - 1}{1} \frac{p^k - 2}{2} \cdots \frac{p^k - x + 1}{x - 1}.$$

If p^j divides i for some $1 \leq i \leq x-1$, then p^j also divides $p^k - i$. Hence p^{k-r} divides $\binom{p^k}{x}$. □

Lemma 11. *Suppose p is a prime and $p \geq 3$. Let $c \geq 2$, $d \geq 1$ and $r \geq 1$. If p^r divides cd then $d(c-1) \geq r+1$.*

Proof. Let $cd = kp^r$ for some positive integer k. Then, $d(c-1) \geq dc/2 = kp^r/2 \geq r+1$ when $r \geq 2$. That $d(c-1) \geq r+1$ when $r = 1$ follows since either c or d (or both) is divisible by p. □

Lemma 12. *Let $c \geq 2$, $d \geq 1$ and $r \geq 1$. If 2^r divides cd then $d(c-1) \geq r+1$, except when $(r,c,d) \in \{(2,2,2),(1,2,1)\}$ when $d(c-1) = r$.*

Proof. Let $cd = k2^r$ for some positive integer k. Then, $d(c-1) \geq k2^{r-1} \geq r+1$ when $r \geq 3$. The rest is proved by inspection. □

Lemma 13. *For all partitions π of p^{k-1}, we have*

$$|\mathcal{S}_\pi| \prod_{q \in Q_\pi} p^{|q|-1} \pmod{p^k} \equiv \begin{cases} 1 & \text{if } \pi = \pi_0 \\ 2^{k-1} & \text{if } \pi \in \{\pi_1, \pi_2\} \text{ and } p = 2 \\ 0 & \text{otherwise,} \end{cases}$$

where π_0, π_1, π_2, S_π and Q_π are as defined in Table 1.

Proof. For any $t \geq 1$, the number of set partitions of $\{1, 2, \ldots, t\}$ that induce the number partition π of t is given by

$$|\mathcal{S}_\pi| = \frac{t!}{\prod_{i \geq 1} \left(i!^{s_i(\pi)} s_i(\pi)!\right)}, \tag{26}$$

where $s_i(\pi)$ denotes the number of parts i in π [1, Th. 13.2].

`Case I`: $\pi = \pi_0$. Then $|\mathcal{S}_\pi| \prod_{q \in Q_\pi} p^{|q|-1} = 1$.

`Case II`: $p = 2$ and $\pi \in \{\pi_1, \pi_2\}$. For $m \geq 1$, let $\nu(m)$ denote the greatest positive integer such that $2^{\nu(m)}$ divides $m!$. Recall that $\nu(m) = m - d_2(m)$, where $d_2(m)$ is the number of 1s when m is written in binary. This implies

$$\nu(|\mathcal{S}_{\pi_1}|) = \nu\left(\frac{2^{k-1}!}{(2^{k-1}-2)!\ 2!}\right) = \overbrace{2^{k-1}-1}^{\text{for } 2^{k-1}!} - \overbrace{(2^{k-1}-k)}^{\text{for } (2^{k-1}-2)!} - 1 = k-2$$

and hence 2^{k-1} exactly divides $|\mathcal{S}_{\pi_1}| \prod_{q \in Q_{\pi_1}} 2^{|q|-1}$. Similarly

$$\nu(|\mathcal{S}_{\pi_2}|) = \nu\left(\frac{2^{k-1}!}{(2^{k-1}-4)!\ 2!^3}\right) = \overbrace{2^{k-1}-1}^{\text{for } 2^{k-1}!} - \overbrace{(2^{k-1}-k-1)}^{\text{for } (2^{k-1}-4)!} - 3 = k-3$$

and hence 2^{k-1} exactly divides $|\mathcal{S}_{\pi_2}| \prod_{q \in Q_{\pi_2}} 2^{|q|-1}$.

Case III: $p \geq 3$ and $\pi \neq \pi_0$. By considering the integer partition consisting of b copies of a, we can deduce from (26) that $a!^b b!$ divides $(ab)!$ for all $a \geq 1$ and $b \geq 1$. Let $t = p^{k-1}$.

Now suppose π contains exactly b copies of $a \geq 2$. Construct π' from π by replacing those b copies of a, with ba copies of 1. By (26),

$$|\mathcal{S}_\pi| = |\mathcal{S}_{\pi'}| \frac{s_1(\pi')!}{s_1(\pi)! a!^b b!} = |\mathcal{S}_{\pi'}| \frac{(s_1(\pi)+ab)!}{s_1(\pi)! a!^b b!}.$$

Since $(s_1(\pi)+ab)!$ is divisible by $s_1(\pi)!(ab)!$ and $a!^b b!$ divides $(ab)!$, we can conclude that $|\mathcal{S}_{\pi'}|$ divides $|\mathcal{S}_\pi|$. By applying this type of replacement repeatedly, we can find a partition

$$\pi'' = \{1, 1, \ldots, 1, \overbrace{c, c, \ldots, c}^{d \geq 1 \text{ copies}}\}$$

with $c \geq 2$ for which $|\mathcal{S}_{\pi''}|$ divides $|\mathcal{S}_\pi|$. In fact, $|\mathcal{S}_{\pi''}| = \frac{p^{k-1}!}{c!^d d! (p^{k-1}-cd)!}$ by (26), which is divisible by $\frac{p^{k-1}!}{(cd)!(p^{k-1}-cd)!} = \binom{p^{k-1}}{cd}$ (since $c!^d d!$ divides $(cd)!$). Lemma 10 implies that $\binom{p^{k-1}}{cd}$ is divisible by p^{k-1-r} where r is the largest integer such that p^r divides cd. Hence p^{k-1-r} divides $|\mathcal{S}_\pi|$. Since there are d copies of c in π, we find $\prod_{q \in Q} p^{|q|-1}$ is divisible by $p^{d(c-1)}$. Hence $|\mathcal{S}_\pi| \prod_{q \in Q} p^{|q|-1}$ is divisible by $p^{k-1-r+d(c-1)}$ and the result follows from Lemma 11, since $d(c-1) > r$.

Case IV: $p = 2$ and $\pi \notin \{\pi_0, \pi_1, \pi_2\}$. We repeat the argument used in Case III, but use Lemma 12 instead of Lemma 11. □

B. Small Values

n	$F_n(x)$
1	1
2	$x+1$
3	x^2+3x+3
4	$x^3+6x^2+15x+16$
5	$x^4+10x^3+45x^2+110x+125$
6	$x^5+15x^4+105x^3+435x^2+1080x+1296$
7	$x^6+21x^5+210x^4+1295x^3+5250x^2+13377x+16807$
8	$x^7+28x^6+378x^5+3220x^4+18865x^3+76608x^2+200704x+262144$
9	$x^8+36x^7+630x^6+7056x^5+55755x^4+320544x^3+1316574x^2+3542940x+4782969$
10	$x^9+45x^8+990x^7+14070x^6+143325x^5+1092105x^4+6258000x^3+26100000x^2+72000000x+100000000$

Table 2: The forest polynomial $F_n(x)$ for small n.

n	number of n-vertex labeled forests $F_n(1)$	mod 3 (period $t = 6$)	mod 4 ($t = 8$)	mod 5 ($t = 20$)	mod 6 ($t = 6$)
1	1	1	1	1	1
2	2	2	2	2	2
3	7	1	3	2	1
4	38	2	2	3	2
5	291	0	3	1	3
6	2932	1	0	2	4
7	36961	1	1	1	1
8	561948	0	0	3	0
9	10026505	1	−3	0	1
10	205608536	2	0	1	2
11	4767440679	0	−1	4	3
12	123373203208	1	0	3	4
13	3525630110107	1	3	2	1
14	110284283006640	0	0	0	0
15	3748357699560961	1	1	1	1
16	137557910094840848	2	0	3	2
17	5421179050350334929	0	−3	4	3
18	228359487335194570528	1	0	3	4
19	10239206473040881277575	1	−1	0	1
20	4869097448625766542836 16	0	0	1	0
21	2447669761084907491 1900371	1	3	1	1
22	1296922170326967017021456192	2	0	2	2
23	7224234394625047476537521 6097	0	1	2	3
24	4220408604052795050630693937600	1	0	0	4
25	2580258239486909593401649924 23001	1	−3	1	1
26	1647632513313120685638853134 5000832	0	0	2	0
27	1096881543024898799690775415474876711	1	−1	1	1
28	7600421771817836654284855610186 6327168	2	0	3	2
29	5473008907162709455528258930972402876875	0	3	0	3
30	4089840768140297317043504712760259256348 16	1	0	1	4

Table 3: The number of labeled forests $F_n(1)$ on n vertices (from Sloane [12]).