SIAM J. DISCRETE MATH.
Vol. 30, No. 2, pp. 1046–1057

THE NUMBER OF LABELED CONNECTED GRAPHS MODULO PRIME POWERS*

ARUN P. MANI† AND REBECCA J. STONES‡

Abstract. Let c_n denote the number of vertex-labeled connected graphs on n vertices. Using group actions and elementary number theory, we show that the infinite sequence, $c_n : n \geq 1$, is ultimately periodic modulo every positive integer. We state and prove our results for sequences defined by a weighted generalization of c_n and conjecture that these results are suggestive of similar periodic behavior of the Tutte polynomial evaluations of the complete graph K_n at integer points.

Key words. Tutte polynomial, connected graphs

AMS subject classifications. 05C30, 05C31

DOI. 10.1137/15M1024615

1. Introduction.

Let $\mathcal{C}_n$ be the set of labeled connected graphs on the n-vertex set $\{1, 2, \ldots, n\}$. For $b \in \mathbb{Z}$, we define the weighted sum

$$C_n(b) \stackrel{\text{def.}}{=} \sum_{G \in \mathcal{C}_n} (b-1)^{|G|-n+1}, \tag{1}$$

where $|G|$ denotes the number of edges of graph G. Counting the number of vertex-labeled connected graphs on n vertices, equivalently finding $C_n(2)$, is a classical graph enumeration problem (see, for example, [5], [6], [9], [11]). While we know of no simple closed form for $C_n(2)$, there are some useful recurrence relations. For example, if we write $c_n = C_n(2)$, [6] gives the recurrence

$$c_n = 2^{\binom{n}{2}} - \frac{1}{n} \sum_{k=1}^{n-1} k \binom{n}{k} 2^{\binom{n-k}{2}} c_k.$$

More generally, when b is a positive integer, the sum $C_n(b)$ is equivalent to (up to easily computable factors) the all-terminal reliability polynomial[1] of the complete graph on n vertices K_n, and is thus useful in computing the probability that the n vertices remain connected when each edge has an independent failure probability of $1/b$ (see [3] for details). The function $C_n(b)$ for $1 \leq n \leq 7$ is shown in Table 2 (in Appendix B).

The Tutte polynomial of a graph is a well-known two-variable graph polynomial

*Received by the editors June 5, 2015; accepted for publication (in revised form) November 24, 2015; published electronically May 25, 2016.

http://www.siam.org/journals/sidma/30-2/M102461.html

†Department of Mathematics and Statistics, The University of Melbourne, Melbourne, Australia (arunpmani@gmail.com). This author was supported in part by an ARC DECRA grant.

‡Clayton School of Information Technology and School of Mathematical Sciences, Monash University, Melbourne, Australia, Department of Mathematics and Statistics, Dalhousie University, Canada, and College of Computer and Control Engineering, Nankai University, Tianjin, China (rebecca.stones82@gmail.com). This author was supported in part by an ARC grant, NSFC grant 61170301, NSF China Research Fellowship for International Young Scientists (grants 11450110409, 11550110491), and was also partially supported by AARMS.

[1]The (all-terminal) reliability polynomial $R(G, p)$ gives the probability of a graph G being connected after each edge is deleted independently with identical probability p.

and is defined for the complete graph K_n by

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

where $\mathcal{G}_n$ is the set of all labeled graphs on the vertex set $\{1,2,\ldots,n\}$, and $\kappa(G)$ is the number of connected components of the graph G. There is extensive literature on this graph invariant, and we refer the reader to [10] for an introduction. The sum $C_n(b)$ is also an evaluation of the Tutte polynomial of K_n at the integer point $(1,b)$.

In this paper, we establish the following recurrence congruence for $C_n(b)$. Our statement of this recurrence uses the arithmetic function $\varphi(m)$, called the *Euler totient function*, which is defined as the number of integers $a \in \{1,2,\ldots,m\}$ such that $\gcd(a,m) = 1$ [1, p. 54]. In particular, for a prime p and positive integer k, we have $\varphi(p^k) = p^{k-1}(p-1)$. Where relevant, negative exponents when taking a modulus refer to multiplicative inverses.

PROPOSITION 1. *Let p be a prime, and let k be a positive integer. For $b,n \in \mathbb{Z}$ such that $n \geq p^k$ and $b \not\equiv 1 \pmod p$, we have*

$$C_n(b) \pmod{p^k} \equiv \begin{cases} b^{\varphi(p^k)/2} C_{n-\varphi(p^k)}(b) & \text{if } p \geq 3 \text{ and } n > p, \\ b^{\varphi(p)/2} - 1 & \text{if } p \geq 3 \text{ and } n = p, \\ 1 & \text{if } p = n = 2, \\ 2 & \text{if } p = k = 2 \text{ and } n = 4, \\ 0 & \text{otherwise.} \end{cases}$$

The rest of this paper is organized as follows. We prove Proposition 1 in section 2. When $b \not\equiv 0 \pmod p$, we know by Fermat's little theorem [1, Corollary 5-2] that $b^{\varphi(p)} \equiv 1 \pmod p$, and thus $b^{\varphi(p)/2} \equiv \pm 1 \pmod p$. From Lemma 2 (in Appendix A), this also means $b^{\varphi(p^k)/2} \equiv \pm 1 \pmod{p^k}$. Thus Proposition 1 implies $C_n(b)$ is periodic or antiperiodic in n when reduced modulo p^k whenever $b \not\equiv 1 \pmod p$ (see section 3.2). We discuss this periodic behavior of $C_n(b)$ and its consequences in section 3. Integer sequences that are ultimately periodic modulo every positive integer were called *modularly C-finite (MC-finite)* in [4], and it was unknown if the sequence of numbers of labeled connected graphs on n vertices was MC-finite. In section 3 we prove that this sequence, that is, $(C_n(2) : n \geq 1)$ in our notation, is MC-finite. Table 3 shows the first few terms of this sequence and their periodic behavior modulo some small positive integers. In section 4 we conclude with open questions on similar recurrence congruences for the Tutte polynomial evaluations of K_n at other integer points, that is, for $T_n(a,b)$ where $a,b \in \mathbb{Z}$. Appendix A lists the number theoretic results used in our proofs.

For brevity, unless otherwise indicated the domain of all numerical quantities in this paper is the set of integers.

2. Proof of Proposition 1. Our proof of Proposition 1 uses permutation group actions on sets of labeled connected graphs on $n+p^k$ vertices to obtain the recurrence congruences, where p is a prime, $k \geq 1$, and $n \geq 0$.

We begin with the following useful observation; it characterizes circulant graphs (i.e., those that admit a cyclic automorphism without fixed vertices) with an odd prime number of vertices.

LEMMA 1. *Let p be an odd prime, let $V = \{v_1, v_2, \dots, v_p\}$ be a set with p elements, and let σ be the permutation $(v_1, v_2, \dots, v_p)$. Additionally, let E_i be the set of edges of the p-cycle defined by $E_i = \{\{v, \sigma^i v\} : v \in V\}$ for integers i in the range $1 \le i \le (p-1)/2$. Then σ is an automorphism of the graph $G = (V, E)$ if and only if E is a disjoint union of a (possibly empty) subset of $\{E_1, E_2, \dots, E_{(p-1)/2}\}$.*

Proof. Clearly, σ is an automorphism for the empty graph on V, and for each p-cycle (V, E_i) for $1 \le i \le (p-1)/2$. Hence σ is also an automorphism of a disjoint union of any subset of $\{E_1, E_2, \dots, E_{(p-1)/2}\}$.

To prove the converse, suppose $\sigma G = G = (V, E)$. If G has no edges, then the result is vacuously true. Otherwise, since the union of all E_i's is the complete graph on V, every edge in E is of the form $\{v, \sigma^i v\}$ for some $v \in V$ and $i \in \{1, 2, \dots, (p-1)/2\}$. However, if $\{v, \sigma^i v\} \in E$, then because $\sigma G = G$, we must have $E_i \subseteq E$. Since this is true for every edge in E, it must be a disjoint union of some subset of $\{E_1, E_2, \dots, E_{(p-1)/2}\}$. ∎

We prove Proposition 1 by considering the cases $n > p^k$ and $n = p^k$ separately. The case $n > p^k$ is easily seen to be equivalent to the following theorem.

THEOREM 1. *Let p be a prime, and let k, n be positive integers. If $b \not\equiv 1 \pmod p$, then*

$$C_{n+p^k}(b) \pmod{p^k} \equiv \begin{cases} b^{\varphi(p^k)/2} C_{n+p^{k-1}}(b) & \text{if } p \ge 3, \\ 0 & \text{if } p = 2. \end{cases}$$

Proof. Let $z = b - 1$, and let $\mathcal{C}$ be the set of labeled connected graphs on the vertex set $V = \{1, 2, \dots, p^k + n\}$. Then from (1),

$$C_{n+p^k}(b) = \sum_{G \in \mathcal{C}} z^{|G| - n - p^k + 1}. \tag{2}$$

We consider the action of the cyclic permutation group generated by the permutation $\alpha = (1, 2, \dots, p^k)$ on the set $\mathcal{C}$. This action partitions the set $\mathcal{C}$ into orbits. By the orbit-stabilizer theorem [2, Theorem 17.2], the size of the orbit containing a graph G is p^k unless its stabilizer is nontrivial, whence we have $\alpha^{p^{k-1}} G = G$. All graphs within an orbit are isomorphic to one another and hence contribute the same value to the sum in (2). Thus,

$$C_{n+p^k}(b) \pmod{p^k} \equiv \sum_{G \in \mathcal{A}} z^{|G| - n - p^k + 1}, \tag{3}$$

where $\mathcal{A} = \{G \in \mathcal{C} : \alpha^{p^{k-1}} G = G\}$. In other words, when reduced modulo p^k, it is enough to compute the sum (2) for those graphs for which $\alpha^{p^{k-1}}$ is an automorphism. Note that the permutation $\alpha^{p^{k-1}} = \sigma_1 \sigma_2 \cdots \sigma_{p^{k-1}}$, where the σ_i's are the mutually disjoint p-cycles $(i, p^{k-1} + i, \dots, (p-1)p^{k-1} + i)$ for each i in the range $1 \le i \le p^{k-1}$.

Additionally, for each i such that $1 \le i \le p^{k-1}$ define $u_i = \{jp^{k-1} + i : 0 \le j \le p - 1\}$, and let $P = \{u_i : 1 \le i \le p^{k-1}\}$ and $N = \{p^k + 1, p^k + 2, \dots, p^k + n\}$. Let $\mathcal{D}$ be the set of labeled connected graphs on the $(n + p^{k-1})$-vertex set $P \cup N$.

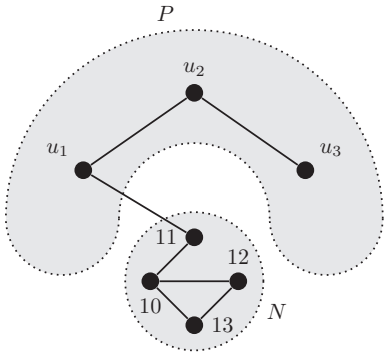
We now outline a procedure for generating all the graphs in $\mathcal{A}$ from those in $\mathcal{D}$. To do this, however, we first need some auxiliary information. For each i in the range

$1 \le i \le p^{k-1}$, we choose a graph $S_i \in \mathcal{S}_i$, where $\mathcal{S}_i$ is the collection of all graphs on the vertex set u_i that admit the automorphism σ_i. Clearly, we have $|\mathcal{S}_i|$ independent choices for each S_i. Additionally, given a $G' \in \mathcal{D}$, for each P-to-P edge $\{u_i, u_j\}$ in G', we choose a nonempty subset $w_{ij} \subseteq u_j$. Since $|u_j| = p$, we have $2^p - 1$ independent choices for our w_{ij} for every P-to-P edge in G'. Let $W(G') = (w_{ij} : \{u_i, u_j\} \in E(G'))$ be the tuple of our chosen w_{ij}'s for a given G'. Given our choices $S_1, S_2, \ldots, S_{p^{k-1}}$, graph $G' \in \mathcal{D}$, and an associated $W(G')$, we use the procedure outlined in Table 1 to generate a $G \in \mathcal{A}$ that has $\alpha^{p^{k-1}}$ as an automorphism. This procedure is also illustrated with an example in Figure 1.

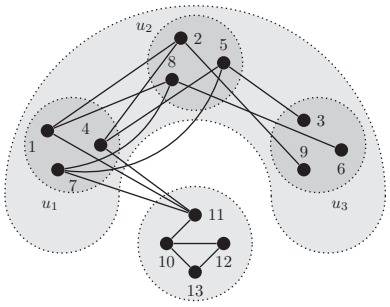
TABLE 1

Procedure to generate a graph G such that $\alpha^{p^{k-1}} G = G$ given a choice of $S_1, S_2, \ldots, S_{p^{k-1}}$, $G' \in \mathcal{D}$, and $W(G')$.

(a) Beginning with G as the graph with no edges on the set V, copy all edges from G' to G with both endpoints in the set N.
(b) Add to G the edges of graphs $S_1, S_2, \ldots, S_{p^{k-1}}$.
(c) For each N-to-P edge $\{\ell, u_i\}$ in G', add the p edges $\{\{\ell, j\} : j \in u_i\}$ to G.
(d) For each P-to-P edge $\{u_i, u_j\}$ in G', let w_{ij} be the corresponding choice in the tuple $W(G')$. Add the $p|w_{ij}|$ edges from the set $\{\{\sigma_i^h i, \sigma_j^h w\} : 1 \le h \le p, w \in w_{ij}\}$ to G. That is, the vertices in our choice set w_{ij} become the neighbors of vertex i in G, while the other $(p-1)|w_{ij}|$ edges ensure $\alpha^{p^{k-1}}$ is an automorphism of G.



(a) A graph $G' \in \mathcal{D}$.



(b) An example of a generated graph $G \in \mathcal{A}$ from G'. Here S_1, S_2, and S_3 are isomorphic to $\overline{K_3}$, $w_{12} = \{2, 8\}$, and $w_{23} = \{9\}$.

FIG. 1. *Illustrating the generation procedure. Here we have $p = 3$, $k = 2$, and $n = 4$.*

Indeed we have $\alpha^{p^{k-1}} G = G$ after every step in Table 1, and thus $\alpha^{p^{k-1}}$ is an automorphism of the generated graph G. It is also easy to verify that if G' is connected, N is nonempty and the subsets w_{ij} in step (d) above are nonempty, the generated graph G will be necessarily connected, and hence $G \in \mathcal{A}$. (Note that the generated graph is not always connected if N is empty, and so $n > 0$ is a necessary condition for this proof. We handle the $n = 0$ case in Theorem 2.) Conversely, starting from any $G \in \mathcal{A}$, this generation procedure can be reversed to obtain the graphs $S_1, S_2, \ldots, S_{p^{k-1}}$, G' and the associated $W(G')$. Hence, by running through all possible choices of $S_1, S_2, \ldots, S_{p^{k-1}}$, G' and $W(G')$, we generate every $G \in \mathcal{A}$ exactly once

using the procedure in Table 1.

Given $G' \in \mathcal{D}$, let $e(G')$ and $f(G')$ be its number of P-to-P edges and N-to-P edges, respectively. We compute the number of edges of the generated graph G as follows. In step (a), we add $|G'| - e(G') - f(G')$ edges to G. In step (b), we add $|S_i|$ edges to G for each i in $1 \le i \le p^{k-1}$. In step (c), we add p edges for every N-to-P edge of G', and thus add another $pf(G')$ edges to G. Lastly, in step (d), we add $p|w_{ij}|$ edges for every P-to-P edge $\{u_i, u_j\}$ of G'. Based on this, we can rewrite (3) as

$$C_{n+p^k}(b) \pmod{p^k} \equiv \pi \cdot \sum_{G' \in \mathcal{D}} z^{|G'|-e(G')+(p-1)f(G')-n-p^k+1} \cdot \tau(G'), \tag{4}$$

where we define

$$\pi = \prod_{i=1}^{p^{k-1}} \sum_{S_i \in \mathcal{S}_i} z^{|S_i|} \tag{5}$$

and

$$\tau(G') = \prod_{\{u_i,u_j\} \in E(G')} \sum_{\substack{w_{ij} \subseteq u_j \\ |w_{ij}|>0}} z^{p|w_{ij}|} = \left((z^p+1)^p - 1\right)^{e(G')} \tag{6}$$

by the binomial theorem.

Here the factor π accounts for all edges added in step (b), and $\tau(G')$ accounts for the edges added in step (d). It is also worth mentioning here that often there are $G' \in \mathcal{D}$ such that $|G'| + (p-1)f(G') + 1 < e(G') + n + p^k$, and hence $b \not\equiv 1 \pmod{p}$ (equivalently, $z \not\equiv 0 \pmod{p}$) is a necessary condition for (4) to be valid.

To complete the rest of the proof, we consider the cases $p \ge 3$ and $p = 2$ separately.

Case $p \ge 3$. In this case, from Lemma 1 we know graphs in $\mathcal{S}_i$ are precisely the disjoint unions of subsets of $\mathcal{H}_i$ $\mathcal{H}_i$, where $\mathcal{H}_i$ is the set of $(p-1)/2$ edge disjoint p-cycle graphs on u_i that admit the automorphism σ_i. That is, $|\mathcal{S}_i| = 2^{(p-1)/2}$, and for every $S_i \in \mathcal{S}_i$ there is a unique subset $H_i \subseteq \mathcal{H}_i$ such that S_i is the union of p-cycles in H_i. Hence, from (5), we get

$$\begin{aligned}
\pi \pmod{p^k} &\equiv \prod_{i=1}^{p^{k-1}} \sum_{S_i \in \mathcal{S}_i} z^{|S_i|} \\
&\equiv \prod_{i=1}^{p^{k-1}} \sum_{H_i \subseteq \mathcal{H}_i} z^{p|H_i|} \\
&\equiv \left((z^p+1)^{(p-1)/2}\right)^{p^{k-1}} && \text{[by the binomial theorem]} \\
&\equiv (z+1)^{\varphi(p^k)/2} && \text{[using Lemma 2]} \\
&\equiv b^{\varphi(p^k)/2}.
\end{aligned}$$

To further simplify (4) in this case, we consider the action of the cyclic permutation group generated by $\gamma = (u_1, u_2, \ldots, u_{p^{k-1}})$ on the set $\mathcal{D}$. This action induces a partition $\mathcal{R}$ of orbits on $\mathcal{D}$. The graphs within an orbit $R \in \mathcal{R}$ are isomorphic to each other and thus make the same contribution to the sum in (4). Let $t(R)$, $e(R)$, and $f(R)$ be the number of all edges, P-to-P edges, and N-to-P edges, respectively,

for graphs in orbit R, and let $\tau(R)$ be the common value of $\tau(G')$ for all $G' \in R$. We can then rewrite (4) as follows:

$$C_{n+p^k}(b) \pmod{p^k} \equiv b^{\varphi(p^k)/2} \sum_{R \in \mathcal{R}} |R| z^{t(R)-e(R)+(p-1)f(R)-n-p^k+1} \cdot \tau(R). \tag{7}$$

We simplify (7) using the following claim.

Claim 1. *For every orbit $R \in \mathcal{R}$ as defined above,*
(i) $|R| z^{(p-1)f(R)} \equiv |R| \pmod{p^k}$ *and*
(ii) $|R|\tau(R) \equiv |R| z^{e(R)} \pmod{p^k}$.

Proof. Let $G' \in R$. By the orbit-stabilizer theorem, $|R| = p^j$, where j is the smallest integer in the range $0 \le j \le k-1$ such that $\gamma^{p^j} G' = G'$. The permutation γ^{p^j} has p^j disjoint cycles each of length p^{k-1-j}. Since $\gamma^{p^j} G' = G'$, all p^{k-1-j} vertices within each of these cycles must have the same number of edges to other vertices in P, and to vertices in N. Thus,

$$2e(R) = p^{k-1-j} \sum_{q=1}^{p^j} \delta_q \quad \text{and} \quad f(R) = p^{k-1-j} \sum_{q=1}^{p^j} \mu_q,$$

where δ_q and μ_q are the number of edges from a vertex in the qth cycle of γ^{p^j} to other vertices in P and N, respectively. In particular, $e(R) \equiv f(R) \equiv 0 \pmod{p^{k-1-j}}$. We now consider each of the two claims individually.

(i) Since $z^{(p-1)} \equiv 1 (\mathrm{mod}\ p)$, from Lemma 2 we have $z^{(p-1)f(R)} \equiv 1 (\mathrm{mod}\ p^{k-j})$. The claim follows since $|R| = p^j$.
(ii) Similarly, since $(z^p+1)^p - 1 \equiv z \pmod{p}$, we can apply Lemma 2 to (6) to get $\tau(R) \equiv z^{e(R)} \pmod{p^{k-j}}$, implying the claim. ∎

Using Claim 1 and remembering $z \not\equiv 0 \pmod{p}$, we can rewrite (7) as

$$\begin{aligned} C_{n+p^k}(b) \pmod{p^k} &\equiv b^{\varphi(p^k)/2} \sum_{R \in \mathcal{R}} |R| z^{t(R)-n-p^k+1} \\ &\equiv b^{\varphi(p^k)/2} \sum_{R \in \mathcal{R}} |R| z^{t(R)-n-p^{k-1}+1} \qquad \text{[using Lemma 3]} \\ &\equiv b^{\varphi(p^k)/2} C_{n+p^{k-1}}(b). \end{aligned}$$

This completes the proof of the case $p \ge 3$.

Case $p = 2$. When $p = 2$, we have $|u_i| = 2$ for all $1 \le i \le 2^{k-1}$, and the corresponding $\mathcal{S}_i$ contains two graphs, one with no edges, and the other with the single edge $\{i, 2^{k-1}+i\}$. Hence, from (5) we get

$$\pi \pmod{2^k} \equiv \prod_{i=1}^{2^{k-1}} (1+z) \equiv b^{2^{k-1}} \equiv 0,$$

since b is even. The proof for this case now follows from (4). ∎

We next handle the case $n = p^k$ of Proposition 1. We state this case in the following equivalent form.

THEOREM 2. *Let p be a prime and let k be a positive integer. If $b \not\equiv 1 \pmod{p}$, then*

$$C_{p^k}(b) \pmod{p^k} \equiv \begin{cases} b^{\varphi(p^k)/2} C_{p^{k-1}}(b) & \text{if } p \geq 3 \text{ and } k \geq 2, \\ b^{\varphi(p)/2} - 1 & \text{if } p \geq 3 \text{ and } k = 1, \\ 1 & \text{if } p = 2 \text{ and } k = 1, \\ 2 & \text{if } p = 2 \text{ and } k = 2, \\ 0 & \text{if } p = 2 \text{ and } k \geq 3. \end{cases}$$

Proof. We reuse the notation used in the proof of Theorem 1. Our proof here is very similar to the proof of Theorem 1, except now the set N is empty. Using the same procedure from Table 1 to generate graphs G that admit $\alpha^{p^{k-1}}$ as an automorphism, we find that for certain choices of $S_1, \ldots, S_{p^{k-1}}$, G', and $W(G')$, the generated graph G may not be connected, and thus may not be in $\mathcal{A}$. We show an example of such a G in Figure 2.

(a) A graph $G' \in \mathcal{D}$.

(b) An example of a generated graph $G \notin \mathcal{A}$ from G'. Here S_1, S_2, and S_3 are isomorphic to $\overline{K_3}$, $w_{12} = \{2\}$, $w_{23} = \{9\}$, and $w_{13} = \{9\}$.

FIG. 2. *Illustrating the generation procedure. Here we have $p = 3$ and $k = 2$.*

We prove our result by removing the contribution of such disconnected graphs from the sum on the right-hand side of (4). Let $D_{p^k}(b)$ denote the contribution of disconnected graphs to this sum.

To compute $D_{p^k}(b)$, we begin by observing the following necessary and sufficient conditions for a graph G generated from $S_1, S_2, \ldots, S_{p^{k-1}}$, G', and $W(G')$ using the procedure in Table 1 to be disconnected.

(i) For all $1 \leq i \leq p^{k-1}$, the graph S_i contains no edges.
Otherwise, Lemma 1 implies u_i induces a connected subgraph of G. Also, as G' is connected and every $w \in W(G')$ is nonempty, any vertex $x \in u_j$, $j \neq i$, is connected (by a path) to some vertex in the set u_i in G, and thus is also connected to any other vertex in G, implying G is connected.

(ii) For every distinct pair $u_i, u_j \in P$, any $x \in u_i$ is connected (by a path) to exactly one vertex $y \in u_j$ in the graph G.
As before, since G' is connected and every $w \in W(G')$ is nonempty, any $x \in u_i$ is connected to some $y \in u_j$ in the generated graph G. Suppose for a contradiction that x is connected to two distinct vertices $y_1, y_2 \in u_j$ in G. Then since $\alpha^{p^{k-1}}$ is an automorphism of G, every vertex in u_i is connected to every vertex in u_j in G, and, in turn, also connected to each other. Additionally, for any other vertex

$v \in u_\ell$ in G ($\ell \neq i, j$), v must be connected to some vertex in the set u_i, and thus also connected to every other vertex in G. But this would mean that G is connected.

The condition (ii) implies that if G is generated from $G' \in \mathcal{D}$ using Table 1 and $G \notin \mathcal{A}$, then $|w| = 1$ for all $w \in W(G')$. Thus, together with condition (i), we know its number of edges $|G| = p|G'|$. In other words, all disconnected graphs generated from a given $G' \in \mathcal{D}$ contain the same number of edges, and thus make the same contribution to $D_{p^k}(b)$.

We now count the number of disconnected graphs generated from a given $G' \in \mathcal{D}$ as follows. When $k = 1$, our conditions imply that there is exactly one generated graph that is disconnected (the graph with p isolated vertices). When $k > 1$, from condition (ii), the vertex 1 in G is connected to exactly one vertex from each of the sets $u_2, u_3, \ldots, u_{p^{k-1}}$. For a given $G' \in \mathcal{D}$, these $p^{k-1} - 1$ vertex choices, along with the automorphism $\alpha^{p^{k-1}}$, fully determine the generated disconnected graph G. That is, we have p independent choices for each u_i, $2 \leq i \leq p^{k-1}$, to generate a disconnected G from any G', and thus every $G' \in \mathcal{D}$ generates $p^{p^{k-1}-1}$ disconnected graphs. Hence, the total contribution of disconnected graphs to the sum in (4) is

$$D_{p^k}(b) = p^{p^{k-1}-1} \sum_{G' \in \mathcal{D}} z^{p|G'|-p^k+1}. \tag{8}$$

The formula in Theorem 1 does not apply when $n = 0$ because it includes a contribution from disconnected graphs, i.e., $D_{p^k}(b)$. Now that we have a formula for $D_{p^k}(b)$, we subtract it to correct Theorem 1 in this case. We consider the cases $p \geq 3$ and $p = 2$ separately.

Case $p \geq 3$. From the above argument, we get

$$\begin{aligned} C_{p^k}(b) \pmod{p^k} &\equiv b^{\varphi(p^k)/2} C_{p^{k-1}}(b) - D_{p^k}(b) \\ &\equiv b^{\varphi(p^k)/2} C_{p^{k-1}}(b) - p^{p^{k-1}-1} \sum_{G' \in \mathcal{D}} z^{p|G'|-p^k+1} \\ &\equiv \begin{cases} b^{\varphi(p^k)/2} C_{p^{k-1}}(b) & \text{if } k \geq 2 \quad \text{[using Lemma 4]} \\ b^{\varphi(p)/2} - 1 & \text{if } k = 1 \quad \text{[since } |G'| = 0 \text{ and } z \not\equiv 0 \pmod{p}\text{]}. \end{cases} \end{aligned}$$

Case $p = 2$. Using the above argument,

$$\begin{aligned} C_{2^k}(b) \pmod{2^k} \equiv -D_{2^k}(b) &\equiv -2^{2^{k-1}-1} \sum_{G' \in \mathcal{D}} z^{2|G'|-2^k+1} \\ &\equiv \begin{cases} 0 & \text{if } k \geq 3 \quad \text{[using Lemma 5]} \\ 2 & \text{if } k = 2 \quad \text{[since } |G'| = 1 \text{ and } z \text{ is odd]} \\ 1 & \text{if } k = 1 \quad \text{[since } |G'| = 0 \text{ and } z \text{ is odd]}. \end{cases} \end{aligned}$$

This proves the result. ∎

3. Consequences of Proposition 1. Proposition 1 shows that for an odd prime p, positive integer k, and integer b such that $b \not\equiv 1 \pmod{p}$, the infinite sequence $(C_n(b) : n > p^{k-1})$ when reduced modulo p^k is completely determined by its first $\varphi(p^k)$ terms. In this section, we first use this fact to give a characterization of the small prime power factors of $C_n(b)$, in particular factors of the form p^k such that $p^k < n$. We then discuss its implications to the periodic behavior of $C_n(b)$ when reduced modulo positive integers.

3.1. Small prime power factors of $C_n(b)$. Our first two divisibility results are immediate from Proposition 1, and we omit the easy proofs.

THEOREM 3. *Let p be an odd prime and let $b \equiv 0 \pmod{p}$. Then p divides $C_n(b)$ for all $n > p$, and p^k divides $C_n(b)$ for all $n \geq p^k$ if $k \geq 2$.*

THEOREM 4. *If b is even, then $C_n(b)$ is even for all $n \geq 3$, is divisible by 4 when $n \geq 5$, and is divisible by 2^k when $k \geq 3$ and $n \geq 2^k$.*

We next characterize the divisibility of odd prime power factors p^k of $C_n(b)$ when $b \pmod{p} \notin \{0, 1\}$ and $n \geq p^k$. We begin with the case $n = p^k$.

THEOREM 5. *Let p be an odd prime, let k be a positive integer, and let $b \pmod{p} \notin \{0, 1\}$. Then p^k divides $C_{p^k}(b)$ if and only if*

(i) *$k = 1$ and $b^{\varphi(p)/2} \equiv 1 \pmod{p}$ or*
(ii) *$k \geq 2$ and p^k is a factor of $C_{p^{k-1}}(b)$.*

Proof. Theorem 2 implies that if (i) or (ii) were true, then $C_{p^k}(b) \equiv 0 \pmod{p^k}$. The converse when $k = 1$ is straightforward from Theorem 2. When $k \geq 2$, we first note that by Fermat's little theorem $b^{\varphi(p)} \equiv 1 \pmod{p}$, and thus $b^{\varphi(p)/2} \equiv \pm 1 \pmod{p}$. Hence, by Lemma 2 we also have $b^{\varphi(p^k)/2} \equiv \pm 1 \pmod{p^k}$. The converse for $k \geq 2$ now also follows from Theorem 2. ∎

The next divisibility result is a special case of the periodicity of $C_n(b)$ when reduced modulo prime powers p^k.

THEOREM 6. *Let p be an odd prime, let k, n be positive integers such that $n > p^k$, and let $b \pmod{p} \notin \{0, 1\}$. Then p^k is a factor of $C_n(b)$ if and only if p^k is a factor of $C_r(b)$, where $r \equiv n \pmod{\varphi(p^k)}$ and $p^{k-1} < r \leq p^k$.*

Proof. First, note that there always exists an r in the range $p^{k-1} < r \leq p^k$ such that $r \equiv n \pmod{\varphi(p^k)}$, and we can write $n = r + t\varphi(p^k)$ for some $t \geq 1$. Hence if $C_r \equiv 0 \pmod{p^k}$, then from Theorem 1 we have $C_n(b) \pmod{p^k} \equiv b^{t\varphi(p^k)/2} C_r(b) \equiv 0$.

Conversely, suppose $C_n(b) \equiv 0 \pmod{p^k}$. As in the proof of the Theorem 5, using Fermat's little theorem and Lemma 2, we have $b^{t\varphi(p^k)/2} \equiv \pm 1 \pmod{p^k}$. The converse is now immediate from Theorem 1. ∎

3.2. Periodicity of $C_n(b)$ modulo positive integers. One of the main consequences of Proposition 1 is the following periodic behavior of $C_n(b)$ when reduced modulo prime powers. Recall that a sequence $(a_n : n > q)$ is *antiperiodic* with period t if $a_{n+t} = -a_n$ for all $n > q$.

THEOREM 7. *Let p be an odd prime, $k \geq 1$, and $b \pmod{p} \notin \{0, 1\}$.*

(i) *If $b^{\varphi(p)/2} \equiv 1 \pmod{p}$, the sequence $(C_n(b) : n > p^{k-1})$ is periodic modulo p^k with a period t that divides $\varphi(p^k)$.*
(ii) *If $b^{\varphi(p)/2} \equiv -1 \pmod{p}$, the sequence $(C_n(b) : n > p^{k-1})$ is antiperiodic modulo p^k with a period t that divides $\varphi(p^k)$. (Consequently, it is periodic with period $2t$.)*

Proof. (i) Since $b^{\varphi(p^k)/2} = (b^{\varphi(p)/2})^{p^{k-1}}$, from Lemma 2 we have $b^{\varphi(p^k)/2} \equiv 1 \pmod{p^k}$. The claim now follows from Theorem 1.

(ii) Once again, from Lemma 2 we have $b^{\varphi(p^k)/2} \equiv -1 \pmod{p^k}$ in this case, and the claim follows from Theorem 1. ∎

This periodicity of $C_n(b)$ can be extended to modulo positive integers as shown below.

THEOREM 8. *Let $m \geq 2$ and $r \equiv b \pmod{m}$ such that $1 \leq r \leq m$. If $r > 1$ and $\gcd(r-1, m) = 1$, then the sequence $(C_n(b) : n \geq 1)$ is ultimately periodic modulo m.*

Proof. Let $m = \prod_{i=1}^{\ell} p_i^{k_i}$, where the p_i's are distinct primes and k_i's are positive integers. Since $r > 1$ and $\gcd(r-1, m) = 1$, we have $b \not\equiv 1 \pmod{p_i}$ for each i in the range $1 \leq i \leq \ell$. If $p_i = 2$ or $b \equiv 0 \pmod{p_i}$, from Theorem 1 we know that $(C_n(b) : n \geq 1)$ is ultimately periodic modulo $p_i^{k_i}$ with period 1. Otherwise, from Theorem 7 the sequence $(C_n(b) : n \geq 1)$ is ultimately periodic modulo $p_i^{k_i}$. If t_i is the period of the sequence reduced modulo $p_i^{k_i}$ for $i \in \{1, 2, \ldots, \ell\}$, then the Chinese remainder theorem [1, Theorem 5.4] implies that $(C_n(b) : n \geq 1)$ is ultimately periodic modulo m with period $\operatorname{lcm}(t_1, t_2, \ldots, t_\ell)$. ∎

In particular, the sequence of number of labeled connected graphs on n vertices; that is, $(C_n(2) : n \geq 1)$ is ultimately periodic modulo every positive integer.

COROLLARY 1. *The infinite sequence $(C_n(2) : n \geq 1)$ is ultimately periodic modulo every positive integer. In other words, it is MC-finite.*

Proof. This is trivially true when $m = 1$. When $m \geq 2$ we have $\gcd(1, m) = 1$, and the periodicity in this case follows from Theorem 8. ∎

4. Conjectures for $T_n(a, b)$. Our results show that the weighted count of labeled connected graphs on n vertices, $C_n(b)$ exhibits a simple periodic recurrence when reduced modulo any positive integer that is co-prime to $b-1$. Recall that $C_n(b)$ is the same as $T_n(1, b)$, the Tutte polynomial of the complete graph K_n evaluated at $(1, b)$. We computationally verified Proposition 1 for many values of b, p, and k using the recurrence relation to compute $T_n(a, b)$ from [8], and also on the numerical data available on the *On-line Encyclopedia for Integer Sequences* (OEIS) [9, sequence A001187].

Previously, we reported recurrence congruences and periodicity modulo positive integers for the weighted number of labeled forests on n vertices [7]. This corresponds to an evaluation of $T_n(a, b)$ at the point $(a, 1)$. Further computations suggest that such congruences may be true more widely for evaluations of the Tutte polynomial of K_n at other integer points (a, b). More generally, we conjecture the following recurrence congruences for $T_n(a, b)$.

CONJECTURE 1. *Let p be an odd prime and let k be a positive integer. If $n \geq p^k$, $a, b \in \mathbb{Z}$, and $b \not\equiv 1 \pmod{p}$, then*

$$T_n(a, b) \pmod{p^k} \equiv \begin{cases} b^{\varphi(p)/2} - 1 & \text{if } p \geq 3,\ n = p \text{ and } a \equiv 1 \pmod{p}, \\ b^{\varphi(p^k)/2} T_{n-\varphi(p^k)}(a, b) & \text{otherwise.} \end{cases}$$

CONJECTURE 2. *Let p be an odd prime and let k be a positive integer. If $n \geq p^k$, $a, b \in \mathbb{Z}$ such that $b \equiv 1 \pmod{p}$, then*

$$T_n(a,b) \pmod{p^k} \equiv \begin{cases} (n+a-1)^{p^k} T_{n-p^k}(a,b) & \text{if } n > p^k, \\ (a-1)^{p^k-1} & \text{if } n = p^k. \end{cases}$$

As additional evidence, we observe that Conjecture 1 is true when $n = p$ (implying $k = 1$), $p \geq 3$, $a = 1-p$, and $b = 0$ as follows. The number of proper p-colorings of the complete graph K_p is given by $p! = p\ T_p(1-p, 0)$. So we have $T_p(1-p, 0) = (p-1)! \equiv -1 \pmod{p}$, by Wilson's theorem [1, Theorem 5-3]. Indeed, we believe that our techniques introduced in this paper and in [7] can be extended with a more careful analysis of permutation group actions on the set of all labeled graphs on $n+p^k$ vertices to obtain a proof for the above conjectures.

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

LEMMA 2. *Let $k \geq 1$, and let p be prime. If $a \equiv b \pmod{p}$, $c \geq 0$, and $c \equiv 0 \pmod{p^{k-1}}$, then $a^c \equiv b^c \pmod{p^k}$.*

Proof. We write $c = dp^{k-1}$ for some nonnegative integer d and use induction on k. When $k = 1$, the claim is easily seen to be true from what is given. Suppose the claim is true for some $k \geq 1$. That is, $a^{dp^{k-1}} = tp^k + b^{dp^{k-1}}$ for some integer t. Then,

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

and the result follows by induction. ∎

Lemma 2 is a case of a folklore result known as "lifting the exponent."

LEMMA 3. *Let p be a prime, and let k be a positive integer. If $z \not\equiv 0 \pmod{p}$, then $z^{-p^k} \equiv z^{-p^{k-1}} \pmod{p^k}$.*

Proof. Our claim is equivalent to $z^{p^k - p^{k-1}} \equiv 1 \pmod{p^k}$. From Fermat's little theorem [1], we know $z^{p-1} \equiv 1 \pmod{p}$. The claim now follows from Lemma 2. ∎

LEMMA 4. *If p is an odd prime and $k \geq 2$, then $p^{p^{k-1}-1} \equiv 0 \pmod{p^k}$.*

LEMMA 5. *If $k \geq 3$, then $2^{2^{k-1}-1} \equiv 0 \pmod{2^k}$.*

Lemmas 4 and 5 can be proved by induction; we omit their proofs.

Appendix B. $C_n(b)$ for small n.

TABLE 2
$C_n(b)$ *for small* n.

n	$C_n(b)$
1	1
2	1
3	$b+2$
4	b^3+3b^2+6b+6
5	$b^6+4b^5+10b^4+20b^3+30b^2+36b+24$
6	$b^{10}+5b^9+15b^8+35b^7+70b^6+120b^5+180b^4+240b^3+270b^2+240b+120$
7	$b^{15}+6b^{14}+21b^{13}+56b^{12}+126b^{11}+252b^{10}+455b^9+750b^8+1140b^7+1610b^6+2100b^5+2520b^4+2730b^3+2520b^2+1800b+720$

TABLE 3
The number of labeled connected graphs $C_n(2)$ *on* n *vertices* [9].

n	$C_n(2)$	mod 3 (period $t=4$)	mod 5 ($t=8$)	mod 6 ($t=4$)	mod 7 ($t=6$)	mod 9 ($t=12$)	mod 10 ($t=8$)
1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1
3	4	1	4	4	4	4	4
4	38	−1	3	2	3	2	8
5	728	−1	3	−4	0	8	8
6	26704	1	−1	−2	6	1	4
7	1866256	1	−4	4	0	7	−4
8	251548592	−1	−3	2	1	5	−8
9	66296291072	−1	−3	−4	4	−4	−8
10	34496488594816	1	1	−2	3	−2	−4
11	35641657548953344	1	4	4	0	−8	4
12	73354596206766622208	−1	3	2	6	−1	8

REFERENCES

[1] G. E. ANDREWS, *Number Theory*, Dover Publications, Mineola, NY, 1994.

[2] M. A. ARMSTRONG, *Groups and Symmetry*, Undergrad. Texts Math., Springer-Verlag, New York, 1988.

[3] C. J. COLBOURN, *Combinatorial aspects of network reliability*, Ann. Oper. Res., 33 (1991), pp. 3–15.

[4] E. FISCHER, T. KOTEK, AND J. A. MAKOWSKY, *Application of logic to combinatorial sequences and their recurrence relations*, in Model Theoretic Methods in Finite Combinatorics, Contemp. Math. 558, AMS, Providence, RI, 2011.

[5] P. FLAJOLET AND R. SEDGEWICK, *Analytic Combinatorics*, Cambridge University Press, Cambridge, UK, 2009.

[6] F. HARARY AND E. PALMER, *Graphical Enumeration*, Academic Press, New York, London, 1973.

[7] A. P. MANI AND R. J. STONES, *Congruences for weighted number of labeled forests*, Integers, 16 (2016), #A17.

[8] I. M. PAK, *Computation of Tutte polynomials of complete graphs*, unpublished. Available online at http://www.math.ucla.edu/~pak/papers/Pak_Computation_Tutte_polynomial_complete_graphs.pdf.

[9] N. J. A. SLOANE, *The On-line Encyclopedia of Integer Sequences*, sequence A001187, http://oeis.org/A001187.

[10] D. J. A. WELSH, *The Tutte polynomial*, Random Structures Algorithms, 15 (1999), pp. 210–228.

[11] H. S. WILF, *generatingfunctionology*, 2nd ed., Academic Press, Boston, 1994.