CONNECTIVITY OF MARKOFF MOD-P GRAPHS AND MAXIMAL DIVISORS

JILLIAN EDDY, ELENA FUCHS, MATTHEW LITMAN, DANIEL MARTIN, AND NICO TRIPENY

ABSTRACT. Markoff mod-p graphs are conjectured to be connected for all primes p. In this paper, we use results of Chen and Bourgain, Gamburd, and Sarnak to confirm the conjecture for all $p > 3.45 \cdot 10^{392}$. We also provide a method that quickly verifies connectivity for many primes below this bound. In our study of Markoff mod-p graphs we introduce the notion of *maximal divisors* of a number. We prove sharp asymptotic and explicit upper bounds on the number of maximal divisors, which ultimately improves the Markoff graph p-bound by roughly 140 orders of magnitude as compared with an approach using all divisors.

1. INTRODUCTION

The *Markoff equation* is given by

$$x^2 + y^2 + z^2 = xyz, \tag{1}$$

and non-negative integer solutions (a, b, c) to this equation are called *Markoff triples*. An integer that is a member of such a triple is called a *Markoff number*. Since their introduction by Andrey Markoff in [Mar79], Markoff triples have arisen in many different contexts across the mathematical landscape. Recently, Bourgain-Gamburd-Sarnak have explored various arithmetic properties of Markoff triples (see [BGS16a]), proving that there are infinitely many composite Markoff numbers. A key ingredient in the proof of this fact is a combinatorial property that we describe below.

Markoff triples can be realized as vertices of a *Markoff tree* as follows (note that Markoff triples with negative entries can be realized in a nearly identical way, but we focus on the positive triples here for ease of exposition). Let R_1, R_2, and R_3 be involutions acting on triples of numbers defined by

$$R_1(a, b, c) = (bc - a, b, c),\ R_2(a, b, c) = (a, ac - b, c),\ R_3(a, b, c) = (a, b, ab - c) \tag{2}$$

and note that each of these involutions sends a Markoff triple to another Markoff triple. In fact, all positive Markoff triples can be realized as some word in these involutions applied to the triple $(3, 3, 3)$.

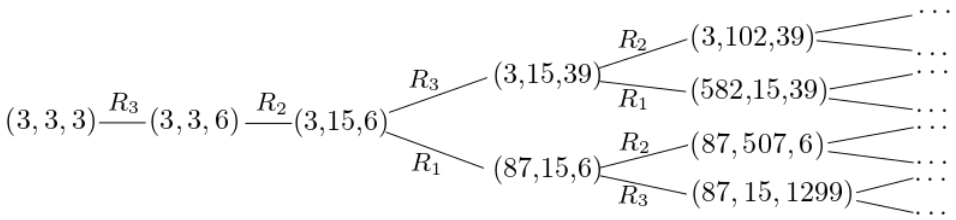

FIGURE 1. A branch of the Markoff tree generated by applying the involutions R_1, R_2, R_3 to the fundamental solution (3,3,3).

In studying the arithmetic of Markoff numbers, it is natural to consider the solutions to (1) mod p: understanding this set is crucial to sieving on the set of Markoff numbers and is behind Bourgain-Gamburd-Sarnak's result on composite Markoff numbers. More specifically, it is useful to consider a version of the Markoff tree described above modulo primes p. These graphs $\mathcal{G}_p$, which

we call *Markoff mod-p graphs*, are constructed as follows. The vertex set of this graph is the set of nonzero solutions to (1) mod p, and two vertices v_1, v_2 are connected by an edge if

$$R_i(v_1) \equiv v_2 \pmod{p} \text{ for some } 1 \leq i \leq 3.$$

Baragar was the first to conjecture that this graph is connected for any prime [Bar91]. A deep result of Bourgain-Gamburd-Sarnak in [BGS16b] has confirmed this for all primes outside a density zero subset. Specifically, they show the following.

Theorem 1.1 (Theorems 1, 2 Bourgain-Gamburd-Sarnak [BGS16b])**.** *Fix $\varepsilon > 0$. Then for sufficiently large p there is a connected component $\mathcal{C}_p$ of $\mathcal{G}_p$ for which*

$$|\mathcal{G}_p \backslash \mathcal{C}_p| < p^{\varepsilon}$$

(note that $|\mathcal{G}_p| \sim p^2$), and any connected component $\mathcal{C}$ of $\mathcal{G}_p$ satisfies $|\mathcal{C}| \gg (\log p)^{1/3}$. Moreover, for $\varepsilon' > 0$ and sufficiently large t, the number of primes $p \leq t$ for which $\mathcal{G}_p$ is not connected is at most $t^{\varepsilon'}$.

The bound on $|\mathcal{G}_p \backslash \mathcal{C}_p|$ was thereafter made much more explicit in [Kon+20], where it was shown that the exponent of $1/3$ in the bound on $|\mathcal{C}|$ can be improved to $7/9$. Bourgain-Gamburd-Sarnak conjecture that these graphs make up an expander family, and this has been further explored in [CL20] and [CM21] (from which it appears that certain subfamilies of this family are actually Ramanujan).

Subsequently, Chen [Che20] proved that the size of any connected component of $\mathcal{G}_p$ must be divisible by p. This implies that if $\mathcal{G}_p$ is disconnected, meaning $\mathcal{G}_p \backslash \mathcal{C}_p$ is a nonempty union of connected components, then $|\mathcal{G}_p \backslash \mathcal{C}_p| \geq p$. So by making explicit the phrase "sufficiently large" in Theorem 1.1, particularly for $\varepsilon = 1$, we obtain a lower bound on primes p for which $\mathcal{G}_p$ is necessarily connected.

In Section 2 we refine the arguments in [BGS16b] and make their asymptotic bounds explicit. The result combines with Chen's theorem to prove that $\mathcal{G}_p$ is connected for $p > 10^{532}$ (Corollary 2.5).

Section 3 introduces maximal divisors, the main tool behind further reduction to our p-bound.

Definition 1.2. Let n be a positive integer, and let $x \in \mathbb{R}$. A positive divisor d of n is *maximal with respect to x* if $d \leq x$ and there is no other positive divisor d' of n such that $d' \leq x$ and $d \,|\, d'$. The set of maximal divisors with respect to x is denoted $\mathcal{M}_x(n)$.

In other words, a maximal divisor is a maximal element in the partially ordered (by divisibility) set of divisors of n that are less than x.

This definition is motivated by a task that appears often in [BGS16b]: to bound a sum over the union of subgroups of order at most x in the cyclic group of order n. Since a group element may belong to many such subgroups, overcounting is avoided by rewriting the sum using inclusion-exclusion, and the very first term of the result is a sum over maximal divisors. (Details are in the next section.)

Our approach in Section 3 is designed to give explicit bounds on $|\mathcal{M}_x(n)|$ for any x and for computationally-feasible sized n—up to 10^{532} as dictated by Corollary 2.5. But our approach also happens to furnish a simple proof of a sharp asymptotic bound.

Theorem 1.3. *For any $\varepsilon > 0$, if $\alpha \in [\varepsilon, 1-\varepsilon]$ then*

$$\log |\mathcal{M}_{n^\alpha}(n)| \leq \log\left(\frac{1}{\alpha^\alpha (1-\alpha)^{1-\alpha}}\right) \frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).$$

The implied constant depends only on ε.

As an immediate corollary, we also obtain a similar bound on the total number of divisors of n less than x (Corollary 3.20). These results can be viewed as generalizations of Wigert's theorem:

$\log \tau(n) = (\log 2 + o(1)) \log n / \log \log n$, where $\tau(n)$ is the number of positive divisors of n [Wig07]. (The constant $\log 2$ is recovered by setting $\alpha = 1/2$ in Theorem 1.3.)

In Section 4 we use our work on maximal divisors to prove our main result.

Theorem 1.4. *$\mathcal{G}_p$ is connected for all primes $p > (863\#)(53\#)(13\#)(7\#)(5\#)3^3 2^5 \approx 3.45 \cdot 10^{392}$, where $n\#$ denotes the product of primes less than or equal to n.*

The lower bound in Theorem 1.4 was output by a computer using Algorithm 1, which determines the exact point at which our method for proving connectivity via maximal divisors fails.

Finally, in Section 5 we provide data on the proportion of smaller primes for which we can also verify connectivity of $\mathcal{G}_p$. As Table 2 shows, our approach begins to work for a significant proportion of primes at around 10^8, and for $22 \leq n \leq 90$ it proves connectivity for 10,000 out of 10,000 randomly chosen primes between 10^n and 10^{n+1}. Note that there are still primes for which our connectivity check fails up until the bound from Theorem 1.4. Table 2's success for smaller primes is due to the expected number of divisors of $p \pm 1$ being much less than the maximum possible number of divisors. This ability to check for connectivity for smaller primes would be useful, for example, in a recent application of Markoff triples to a cryptographic hash function in [Fuc+21], in which one needs to be able to check connectivity of a Markoff mod-p graph for a specific large (but still manageable using our criterion) prime p in order to construct the hash.

Interestingly, our data reveals that already for primes of size 10^{31}, the Erdös-Kac theorem takes over in the sense that the expected value of $\tau(p \pm 1)$ is small enough so that it becomes extremely rare to need the improvement that comes by considering maximal divisors rather than all divisors. This is one hint that our methods via maximal divisors alone will not prove connectivity of all Markoff graphs, and that this will require new insight.

Acknowledgements: This project was started at the UC Davis 2021 REU, and we thank Javier Arsuaga and Greg Kuperberg for the REU's creation and organization. We also thank Matthew de Courcy-Ireland for helpful conversations and comments on this work.

2. A preliminary bound

In this section, we prove a preliminary bound towards Theorem 1.4, which will not only serve to introduce the reader to the key points of our main argument, but will also be necessary in the proof of Theorem 1.4. The Appendix, which serves to make several statements in [BGS16b] more precise, will feed into the technical details of the proofs.

We use the following parameterization, which matches that of Bourgain, Gamburd, and Sarnak up to a change of variables (equations (15), (16), and (18) in [BGS16b]). A triple $(a, b, c) \in \mathbb{F}_p$ with $a \neq 0, \pm 2$ solves $x^2 + y^2 + z^2 = xyz$ if and only if it is of the form

$$\left(r + r^{-1}, \frac{(r + r^{-1})(s + s^{-1})}{r - r^{-1}}, \frac{(r + r^{-1})(rs + r^{-1}s^{-1})}{r - r^{-1}} \right) \tag{3}$$

for some $r, s \in \mathbb{F}_{p^2}$. The orbit of this triple under the Vieta involutions that fix the first coordinate, called R_2 and R_3 in (2), consists precisely of triples of the form

$$\left(r + r^{-1}, \frac{(r + r^{-1})(r^{2n}s + r^{-2n}s^{-1})}{r - r^{-1}}, \frac{(r + r^{-1})(r^{2n\pm 1}s + r^{2n\pm 1}s^{-1})}{r - r^{-1}} \right) \tag{4}$$

for some $n \in \mathbb{Z}$, and one can similarly describe the orbits that fix the second or third coordinate, as well. So the number of triples in this orbit depends on the multiplicative order of r in $\mathbb{F}_{p^2}^*$.

Note that in [BGS16b], connectivity is proven for a slightly modified Markoff mod-p graph $\widehat{\mathcal{G}}_p$, where the edges are defined by so-called rotations, which are the usual Vieta involutions followed by a transposition of coordinates. But $\widehat{\mathcal{G}}_p$ is connected if and only if $\mathcal{G}_p$ is connected. Indeed, both

rotations and Vieta involutions commute with the reduction mod p, so connectivity of both $\widehat{\mathcal{G}}_p$ and $\mathcal{G}_p$ is equivalent to surjective of the projection of Markoff triples to Markoff triples mod p.

Our strategy, based off of [BGS16b], is to assign an order to every triple in $\mathcal{G}_p$ as follows. Given $a = r + r^{-1}$ as above, let $\mathrm{ord}_p(a)$ be the multiplicative order of r in $\mathbb{F}_{p^2}^*$. This agrees with the notion of order in [BGS16b] (see their equations (8) and (9)) unless $a = \pm 2$, but it is shown in [BGS16b] that a triple with ± 2 in some coordinate is necessarily in the large connected component, so we need not consider this case for our purposes. Define the order of (a, b, c) to be

$$\mathrm{Ord}_p((a, b, c)) := \max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b), \mathrm{ord}_p(c)\} \tag{5}$$

One of the key ideas in Bourgain-Gamburd-Sarnak's proof of the connectivity of $\mathcal{G}_p$ is that, if a triple $(a, b, c) \in \mathcal{G}_p$ has large enough order in the above sense, then there is always a triple of larger order in one of the orbits of $\langle R_i, R_j \rangle$ acting on (a, b, c). One then walks along these orbits in what Bourgain-Gamburd-Sarnak call the Middle Game of the proof, increasing the order gradually, until one gets to a triple of order roughly $p^{1/2}$ (see Proposition 6.1 in our Appendix for a precise statement), which is then necessarily connected to the large connected component $\mathcal{C}_p$ in Theorem 1.1. So, all triples of large enough order are connected to each other, and the question is then, how many triples potentially do not have large enough order, and hence may not be in $\mathcal{C}_p$? According to Chen [Che20], the number of these bad triples not connected to $\mathcal{C}_p$ must be divisible by p. Hence, if we can show that this number is strictly less than p, we may deduce that there are no bad triples at all and, in fact, $\mathcal{G}_p$ is connected. In fact, we can loosen this a bit as we explain in Lemma 2.2 below.

We recall that a central ingredient in the Middle Game of [BGS16b] is an upper bound on the number of triples of order at most t in the orbit (4) and its analogues in which coordinates other than the first one are fixed. Without loss of generality, assume this maximal coordinate is the first one. Using the parametrization in (4), we have the following lemma, which sharpens the bound used by Bourgain-Gamburd-Sarnak at the start of Section 4 in [BGS16b] when they reference a bound by Corvaja-Zannier in [CZ13].

Lemma 2.1. *If $r \in \mathbb{F}_{p^2}^*$ has order $t > 2$, then the number of congruence classes $n \pmod t$ for which $\mathrm{ord}_p((r + r^{-1})(sr^n + (sr^n)^{-1})/(r - r^{-1}))$ divides d is at most $\frac{3}{2}\max((6td)^{1/3}, 4td/p)$.*

Proof. The number of congruence classes in question is bounded by half the number of solutions $(x, y) \in \overline{\mathbb{F}_p}^2$ to the system of equations $x^t = 1$, $y^d = 1$, and

$$\frac{(r + r^{-1})(sx + (sx)^{-1})}{r - r^{-1}} = y + y^{-1}.$$

(We halve the number of solutions because (x, y) and (x, y^{-1}) only give one congruence class, yet get counted as distinct solutions unless $y = \pm 1$. But as mentioned in the introduction, the case $y = \pm 1$ is ignored as any triple with coordinate ± 2 is known to be in $\mathcal{C}_p$.) Solutions to the last equation above lie on the projective curve C defined by

$$\frac{s(r + r^{-1})}{r - r^{-1}} X^2Y - XY^2 - XZ^2 + \frac{r + r^{-1}}{s(r - r^{-1})} YZ^2 = 0. \tag{6}$$

Assume $r + r^{-1} \neq 0$ since otherwise the proposition is trivial to check (and not useful). Along with $r + r^{-1} \neq \pm(r - r^{-1})$, which is always true, this implies C is smooth. Therefore we can apply Theorem 2 in [CZ13] to the rational functions $u([X, Y, Z]) = (X/Z)^t$ and $v([X, Y, Z]) = (Y/Z)^d$. The zeros and poles of u or v that lie on C are $[1, 0, 0]$, $[0, 1, 0]$, and $[0, 0, 1]$. The Euler characteristic of $C \backslash \{[1, 0, 0], [0, 1, 0], [0, 0, 1]\}$ as defined in [CZ13] is

$$\chi = \left|\{[1, 0, 0], [0, 1, 0], [0, 0, 1]\}\right| + 2\binom{\deg C - 1}{2} - 2 = 3.$$

By [CZ13], the number of points on C that solve $u([X,Y,Z]) = v([X,Y,Z]) = 1$ is bounded from above by $3\max((2\chi \deg u \deg v)^{1/3}, 4\deg u \deg v/p)$. The claim follows. □

In the introduction, we mentioned Chen's result from [Che20] that any connected component in $\mathcal{G}_p$ has size divisible by p. We combine this with a few observations about the Markoff graphs to yield the following.

Lemma 2.2. *If $p > 3$, then the number of vertices in $\mathcal{G}_p \backslash \mathcal{C}_p$ is divisible by $4p$.*

Proof. Chen proved that the number of vertices in any connected component of $\mathcal{G}_p$ is divisible by p [Che20]. To prove divisibility by 4, it suffices to show that $\mathcal{G}_p \backslash \mathcal{C}_p$ is closed under negating any pair of coordinates. Indeed, no triple has a 0 in two coordinates, so (a,b,c), $(a,-b,-c)$, $(-a,b,-c)$, and $(-a,-b,c)$ are always distinct.

If $p \equiv 1 \bmod 4$, then negating any two coordinates of a triple of order $p-1$ also has order $p-1$. If $p \equiv 3 \bmod 4$, then negating any two coordinates of a triple of order $p+1$ also has order $p+1$. In particular, we can always find some $(a_0,b_0,c_0) \in \mathcal{C}_p$ such that $(a_0,-b_0,-c_0)$, $(-a_0,b_0,-c_0)$, and $(-a_0,-b_0,c_0)$ are also in $\mathcal{C}_p$. Since negating any two coordinates in a pair of path-connected triples leaves them path-connected, we see that $\mathcal{C}_p$ is closed under negating of any pair of coordinates. This implies the same is true of $\mathcal{G}_p \backslash \mathcal{C}_p$. □

Remark 2.3. The $4p$ in Lemma 2.2 could be improved to $12p$ by proving that $(3,3,3) \in \mathcal{C}_p$. According to [BGS16b], this would be true if $(3,3,3)$ is connected to a triple of order $p \pm 1$. Our computer experiments for the first $10,000$ primes show that such a triple can always be found in the orbit of $(3,3,3)$ under the group generated by R_2R_3, which consists of triples

$$(3, 3F_{2n-1}, 3F_{2n+1}) \text{ for } n \geq 1,$$

modulo p, where F_k denotes the k-th Fibonacci number.

Proposition 2.4. *Let $\tau_d(n)$ denote the number of divisors of n that are $\leq d$. For d dividing $p-1$ or $p+1$, let $T_d = \tau_d(p-1) + \tau_d(p+1)$. If no divisor of $p-1$ or $p+1$ satisfies either inequality below:*

$$\frac{2\sqrt{2p}}{T_d} < d < \frac{81T_d^3}{4} \qquad\qquad \frac{p}{6T_d} < d < \frac{8\sqrt{p}(p\pm 1)\tau(p\pm 1)}{\phi(p\pm 1)}$$

(where the $\pm$ is $+$ when $d|p+1$ and $-$ if $d|p-1$), then $\mathcal{G}_p$ is connected.

Proof. Suppose p is such that the Markoff graph $\bmod p$ is not connected, and let d be the maximal order among triples that are not in $\mathcal{C}_p$. Fix some triple not in $\mathcal{C}_p$ that attains d as the order of its first coordinate (without loss of generality), and write it in the form of (3).

By maximality of d among orders in $\mathcal{G}_p \backslash \mathcal{C}_p$, each of second and third coordinates in the orbit (3) must have order $d' \leq d$, where $d' \mid p \pm 1$ as usual. There are exactly d choices of exponent $n \bmod d$ in the second and third coordinates of (4), so with $\mathcal{T}_d$ denoting the set of divisors of $p \pm 1$ that do not exceed d, Lemma 2.1 implies

$$d \leq \sum_{d' \in \mathcal{T}_d} \frac{3}{2} \max\left((6dd')^{1/3}, \frac{4dd'}{p} \right) < \frac{3T_d}{2} \max\left((6d^2)^{1/3}, \frac{4d^2}{p} \right). \tag{7}$$

First consider the case $\max((6d^2)^{1/3}, 4d^2/p) = 4d^2/p$. Substituting this into right-hand side above and solving for d gives $d > p/6T_d$. A large divisor like this is amenable to the End Game in [BGS16b], so we apply Proposition 6.1 in the Appendix to get

$$\frac{p}{6T_d} < d < \frac{8\sqrt{p}(p\pm 1)\tau(p\pm 1)}{\phi(p\pm 1)},$$

as in the statement of this proposition.

Next consider the case $\max((6d^2)^{1/3}, 4d^2/p) = (6d^2)^{1/3}$. Again use this with (7) and solve for d to get $d < 81T_d^3/4$; so it remains only to show $2\sqrt{2p}/T_d < d$ to complete the proof. To that end, the number of distinct $a \in \mathbb{F}_p \backslash \{\pm 2\}$ for which $\mathrm{ord}_p(a)$ divides d' is at most $d'/2$ (as $a = r + r^{-1}$ and $a = r^{-1} + (r^{-1})^{-1}$ should only be counted once). So we can bound the number of Markoff triples (a, b, c) of order at most d by summing over the different possible orders of a and c and noting that there are at most two choices for c that produce a Markoff triple once a and b are fixed:

$$\sum_{d', d'' \in \mathcal{T}_d} 2 \cdot \frac{d'}{2} \cdot \frac{d''}{2} < \frac{T_d^2 d^2}{2}. \tag{8}$$

Our choice of d means $|\mathcal{G}_p \backslash \mathcal{C}_p|$ cannot exceed the number of Markoff triples of order at most d. This allows us to combine (8) and Lemma 2.2, giving $4p < T_d^2 d^2/2$. Thus $2\sqrt{2p}/T_d < d$ as desired. □

Corollary 2.5. *$\mathcal{G}_p$ is connected for all primes $p > 10^{532}$.*

Proof. First let us bound T_d from Proposition 2.4 using Nicolas' upper bound on $\tau(n)$ [Nic88], which is $\tau(n) < n^{f(\log n)}$ where

$$f(x) = \frac{(\log 2)}{\log x} + \frac{1.342}{(\log x)^2}.$$

Since $f(x)$ is decreasing for $x > 1$, we see that if $p > x_0 > 1$ then $\tau(p \pm 1) < (p \pm 1)^{f(\log x_0)}$. Setting $x_0 = 10^{532}$ gives

$$T_d \leq \tau(p-1) + \tau(p+1) < (p-1)^{0.1240\ldots} + (p+1)^{0.1240\ldots} < 2(p+1)^{0.1240\ldots}. \tag{9}$$

Now let us show that the first inequality in Theorem 3.2 is never satisfied for $p > 10^{532}$ by checking that $81T_d^3/4 \leq 2\sqrt{2p}/T_d$ for all d. Squaring and rearranging this inequality gives $p/T_d^8 \geq 3^8/2^7$, which is verified below:

$$\begin{aligned}
\log(p/T_d^8) &\geq \log p - 8\log 2 - (0.9921\ldots)\log(p+1) \quad \text{by (9)} \\
&> \log p - 8\log 2 - (0.9921\ldots)\left(\log p + \frac{1}{p}\right) \\
&> (0.0078\ldots)\log 10^{532} - 8\log 2 - \frac{0.9921\ldots}{10^{532}} > \log(3^8/2^7).
\end{aligned}$$

Turning to the second inequality in Proposition 2.4, we will show that

$$\frac{8\sqrt{p}(p \pm 1)\tau(p \pm 1)}{\phi(p \pm 1)} < \frac{p}{6T_d} \text{ for } p > 10^{40}. \tag{10}$$

The exponent from Nicolas' bound is no longer 0.1240..., but rather $f(\log 10^{40}) = 0.2188\ldots$. So

$$\tau(p \pm 1) < (p+1)^{0.2188\ldots} \text{ and } T_d < 2(p+1)^{0.2188\ldots}. \tag{11}$$

To bound $\phi(p \pm 1)$, we have

$$\begin{aligned}
\frac{n}{\phi(n)} &< e^\gamma \log\log n + \frac{3}{\log\log n} \quad \text{by Theorem 8.8.7 in [BS96]} \\
&< n^{0.025} \quad (\text{for } n \geq 10^{40}).
\end{aligned} \tag{12}$$

Putting these together,

$$\begin{aligned}
\log \frac{((p\pm 1)\tau(p\pm 1)T_d)^2}{p\phi(p\pm 1)^2} &< \log \frac{(p\pm 1)^2}{p\phi(p\pm 1)^2} + 2\log 2 + (0.8754...)\log(p+1) \quad \text{by (11)}\\
&< 0.05\log(p+1) - \log p + 2\log 2 + (0.8754...)\log(p+1) \quad \text{by (12)}\\
&= (0.9254...)\log(p+1) - \log p + 2\log 2\\
&< (0.9254...)\left(\log p + \frac{1}{p}\right) - \log p - 2\log 2\\
&< (-0.0614...)\log 10^{38} + \frac{0.9254...}{10^{38}} - 2\log 2 < \log(1/48^2).
\end{aligned}$$

Comparing either end of the chain of inequalities above shows that (10) holds. The theorem now follows from Proposition 2.4. □

3. Maximal Divisors

We can improve the bound in Corollary 2.5 by using the notion of what we call *maximal divisors*. The key observation is that the count in Lemma 2.1 comes from counting the number of solutions in a subgroup of $\mathbb{F}_p^*$ of order t to the equation in (6). So whenever we consider two divisors $t, t' < d$ of $p\pm 1$ where $t|t'$, we count the solutions relevant to the divisor t twice, since the subgroup of order t is contained in that of the subgroup of order t'. So, instead of summing over all divisors in (7), we can sum over a refined set of divisors that we call maximal.

Definition 3.1. Let n be a positive integer, and let $x \in \mathbb{R}$. A positive divisor d of n is said to be *maximal with respect to* x if $d \le x$ and there is no other positive divisor d' of n such that $d' \le x$ and $d \,|\, d'$. The set of maximal divisors with respect to x is denoted $\mathcal{M}_x(n)$.

Our goal now is to improve on the bound in Corollary 2.5 by replacing the set $\mathcal{T}_d$ with the set $\mathcal{M}_d$ as shown in this simple improvement of Proposition 2.4.

Theorem 3.2. *For d dividing $p-1$ or $p+1$, let $M_d = |\mathcal{M}_d(p-1)| + |\mathcal{M}_d(p+1)|$. If no divisor of $p-1$ or $p+1$ satisfies either inequality below:*

$$\frac{2\sqrt{2p}}{M_d} < d < \frac{81M_d^3}{4} \qquad\qquad \frac{p}{6M_d} < d < \frac{8\sqrt{p}(p\pm 1)\tau(p\pm 1)}{\phi(p\pm 1)}$$

(where the $\pm$ is $+$ when $d|p+1$ and $-$ if $d|p-1$), then $\mathcal{G}_p$ is connected.

The proof of this is identical to that of Proposition 2.4, replacing all instances of T_d with M_d, and noting that the rotation order d' of the second and third coordinates in the orbit (3) must divide at least one maximal divisor of $p\pm 1$ with respect to d.

In Section 2, we relied on known upper bounds for $\tau(n)$, and now we hope to obtain helpful bounds on M_d. The authors are not aware of any literature on the number of maximal divisors of n with respect to x. To find asymptotic and explicit bounds for small n, our strategy is to first find those n for which $|\mathcal{M}_x(n)|$ is maximized, akin to Ramanujan's "superior highly composite numbers."

In [Ram15], Ramanujan introduced a simple approach to bounding $\tau(n)$ in which only a very sparse set of integers n, which he called superior highly composite numbers, needs to be considered. They are those n that maximize $\tau(n)/n^\varepsilon$ for some $\varepsilon > 0$. The prime factorization of a superior highly composite number was determined by Ramanujan to be $2^{a_1}3^{a_2}5^{a_3}\cdots$ where

$$a_i = \left\lfloor \frac{1}{p_i^\varepsilon - 1} \right\rfloor.$$

These numbers are convenient for two main reasons: First, they are easy to enumerate due to their scarcity (asymptotically $\log x/\log\log x$ superior highly composite numbers less than x according

to equation (238) in section V.44 of [Ram15]) and readily known prime factorizations. Second, if n_1 and n_2 are consecutive superior highly composite numbers and f is a convex function on the interval (e^{n_1}, e^{n_2}), then $\log \tau(n) \leq f(\log n)$ holds for all integers $n \in [n_1, n_2]$ if and only if it holds for n_1 and n_2. These two facts make it easy to obtain both asymptotic bounds on $\tau(n)$ and a sharp bound on $\tau(n)$ in a given interval. Our goal in this section is to recreate this approach for $|\mathcal{M}_x(n)|$ in place of $\tau(n)$.

3.1. **Reducing functions.** In this section we introduce a tool for narrowing down the list of integers n for which $|\mathcal{M}_x(n)|$ needs to be computed to obtain upper bounds. Our work culminates in Definition 3.11 and Theorem 3.14.

Notation 3.3. For $n \in \mathbb{N}$ let $\mathcal{D}(n)$ denote the set of positive divisors of n, and let $\lambda(n)$ denote the least prime factor of n if $n \geq 2$. Set $\lambda(1) = 1$.

The function λ can also be found as "lpf," "LD," and "P^-" in the literature. We emphasize that λ here does not denote the Liouville function $(-1)^{\omega(n)}$.

Definition 3.4. For $m, n \in \mathbb{N}$, a function $f : \mathcal{D}(n) \to \mathcal{D}(m)$ is called *reducing* if and only if the following hold for all $d, d' \in \mathcal{D}(n)$:

(a) $f(d) \leq d$,

(b) $\dfrac{m/f(d)}{n/d} \leq \min\left\{1, \dfrac{\lambda(m/f(d))}{\lambda(n/d)}\right\}$,

(c) $f(d) = 2^i f(d')$ for some $i \in \mathbb{Z}$ implies $d = 2^j d'$ for some $j \in \mathbb{Z}$.

We say n *reduces to* m when such a function exists.

Observe that setting $d = n$ in requirement (b) results in $m/f(n) \leq 1$. Since $f(n) \mid m$, this forces $f(n) = m$, which combines with requirement (a) to give $m \leq n$. So integers can only reduce to smaller integers.

Theorem 3.5. *If n reduces to m, then $|\mathcal{M}_x(n)| \leq |\mathcal{M}_x(2^a m)|$ for all $x \in \mathbb{R}$, where a is the smallest integer satisfying $2^a m \geq n$.*

Proof. There is little to check if $x \geq n$, so assume otherwise. We claim that a reducing function $f : \mathcal{D}(n) \to \mathcal{D}(m)$ induces an injection $\hat{f} : \mathcal{M}_x(n) \to \mathcal{M}_x(2^a m)$ defined by $\hat{f}(d) = 2^i f(d)$, where i is the largest integer such that $2^i f(d) \leq x$ and $2^i f(d) \in \mathcal{D}(2^a m)$. Note that (a) in Definition 3.4 guarantees $i \geq 0$.

First let us verify that $\hat{f}(d) \in \mathcal{M}_x(2^a m)$. Since $\hat{f}(d) \leq x < n \leq 2^a m$, we see that $\hat{f}(d)$ has proper multiples in $\mathcal{D}(2^a m)$, and it must be verified that they exceed x. That is, we must show $\hat{f}(d)\lambda(2^a m/\hat{f}(d)) > x$. This is immediate by maximality of i if $\lambda(2^a m/\hat{f}(d))$ happens to be 2. Otherwise,

$$\begin{aligned}
\hat{f}(d)\lambda\left(\frac{2^a m}{\hat{f}(d)}\right) &= 2^i f(d)\lambda\left(\frac{2^a m}{2^i f(d)}\right) \\
&\geq 2^a f(d)\lambda\left(\frac{m}{f(d)}\right) \quad \text{since } \lambda(2^a m/\hat{f}(d)) \neq 2 \text{ implies } i \geq a \\
&\geq \frac{2^a md}{n}\lambda\left(\frac{n}{d}\right) \quad \text{by Definition 3.4(b)} \\
&\geq d\lambda\left(\frac{n}{d}\right) \quad \text{by definition of } a.
\end{aligned}$$

Since $d \in \mathcal{M}_x(n)$ and d properly divides $d\lambda(n/d)$ (recall that we are assuming $x < n$, so $d \neq n$), we must have $d\lambda(n/d) > x$ by definition of maximal divisors. Combined with the inequalities above, this completes our argument that $\hat{f}(d) \in \mathcal{M}_x(2^a m)$.

Next we check that $\hat{f}$ is an injection. If $\hat{f}(d) = \hat{f}(d')$ then $2^i f(d) = 2^{i'} f(d)$ for some $i, i' \in \mathbb{Z}$. This means $d = 2^j d'$ for some $j \in \mathbb{Z}$ by (c) in Definition 3.4, so either d divides d' or vice versa. But then $d, d' \in \mathcal{M}_x(n)$ forces $d = d'$ by definition of maximal divisors. □

In this last theorem, $2^a m < 2n$. So at the expense of less than a factor of 2, we can forgo computing $|\mathcal{M}_x(n)|$ in favor of computing $|\mathcal{M}_x(2^a m)|$, the hope being that m has some kind of predictable prime factorization like the superior highly composite numbers. Let us consider a simple example.

Example 3.6. If p and q are primes with $2 \neq p \leq q$, then $f : \mathcal{D}(q^a) \to \mathcal{D}(p^a)$ defined by $f(q^i) = p^i$ is a reducing function. All three requirements from Definition 3.4 are trivially satisfied.

Using f to "replace" q^a with p^a may not seem helpful computationally because $|\mathcal{M}_x(q^a)|$ just equals 1 for any x, but we can actually use f to swap primes within a prime factorization. That is, if n is not divisible by p or q, then f can be extended to a reducing function $\mathcal{D}(nq^a) \to \mathcal{D}(np^a)$ via the next lemma.

Lemma 3.7. *Suppose $n_1, n_2, m_1, m_2 \in \mathbb{N}$ are such that $\gcd(n_1, n_2) = \gcd(m_1, m_2) = 1$. If $f_1 : \mathcal{D}(n_1) \to \mathcal{D}(m_1)$ and $f_2 : \mathcal{D}(n_2) \to \mathcal{D}(m_2)$ are reducing, then so is the function $f_1 f_2 : \mathcal{D}(n_1 n_2) \to \mathcal{D}(m_1 m_2)$ defined by $f_1 f_2(d_1 d_2) = f_1(d_1) f_2(d_2)$.*

Proof. Let $n = n_1 n_2$, $m = m_1 m_2$, and $f = f_1 f_2$. Let $d, d' \in \mathcal{D}(n)$, and let $d_1, d_1' \in \mathcal{D}(n_1)$ and $d_2, d_2' \in \mathcal{D}(n_2)$ be the unique divisors satisfying $d = d_1 d_2$ and $d' = d_1' d_2'$. It is immediate that requirement (a) in Definition 3.4 holds for f and that the ratio in requirement (b) is indeed bounded by 1. So let us turn our attention to the bound in (b) involving the λ function.

Suppose without loss of generality that $\lambda(m_1/f_1(d_1)) \leq \lambda(m_2/f_2(d_2))$. Then

$$\begin{aligned}
\frac{\lambda(m/f(d))}{\lambda(n/d)} &= \frac{\min(\lambda(m_1/f_1(d_1)), \lambda(m_2/f_2(d_2)))}{\min(\lambda(n_1/d_1), \lambda(n_2/d_2))} \\
&= \frac{\lambda(m_1/f_1(d_1))}{\min(\lambda(n_1/d_1), \lambda(n_2/d_2))} \\
&\geq \frac{\lambda(m_1/f_1(d_1))}{\lambda(n_1/d_1)} \\
&\geq \frac{m_1/f_1(d_1)}{n_1/d_1} \quad \text{since } f_1 \text{ is reducing} \\
&\geq \frac{m_1/f_1(d_1)}{n_1/d_1} \cdot \frac{m_2/f_2(d_2)}{n_2/d_2} \quad \text{since } f_2 \text{ is reducing} \\
&= \frac{m/f(d)}{n/d}.
\end{aligned}$$

For requirement (c), suppose $f(d) = 2^i f(d')$ for some $i \in \mathbb{Z}$. Then $f_1(d_1)/f_1(d_1') = 2^i f_2(d_2')/f_2(d_2)$. By assumption, $\gcd(f_1(d_1), f_2(d_2')) = \gcd(f_1(d_1'), f_2(d_2)) = 1$, so $f_1(d_1)/f_1(d_1')$ and $f_2(d_2')/f_2(d_2)$ must be powers of 2. Thus $d_1 = 2^{j_1} d_1'$ for some $j_1 \in \mathbb{Z}$ because f_1 is reducing and $d_2 = 2^{j_2} d_2'$ for some $j_2 \in \mathbb{Z}$ because f_1 is reducing. This gives $d = 2^{j_1 + j_2} d'$. □

Returning to Example 3.6, if p and q do not divide some $n \in \mathbb{N}$, then Lemma 3.7 allows us to combine our reducing function $\mathcal{D}(q^a) \to \mathcal{D}(p^a)$ with the identity $\mathcal{D}(n) \to \mathcal{D}(n)$ to obtain a reducing function $\mathcal{D}(nq^a) \to \mathcal{D}(np^a)$ in which $dq^i \mapsto dp^i$. That is, replacing larger primes with smaller ones in a prime factorization essentially produces no decrease in $|\mathcal{M}_x(n)|$, as with the number of divisors function. The catch is the extra factor of 2; in Theorem 3.5, $2^a m$ can be almost twice as large

as n. A natural concern is that with each successive maneuver like $q^a \mapsto p^a$, we pick up an extra factor of 2. Knowing that $|\mathcal{M}_x(n)| \leq |\mathcal{M}_x(2^a m)|$ from Theorem 3.5 would not be helpful if $2^a m$ was significantly larger than n. The next lemma eliminates that concern.

Lemma 3.8. *If $f : \mathcal{D}(n) \to \mathcal{D}(m)$ and $g : \mathcal{D}(m) \to \mathcal{D}(\ell)$ are reducing, then so is $g \circ f$.*

Proof. To see that $g \circ f$ satisfies requirement (b) in Definition 3.4, we have

$$\begin{aligned}\frac{\ell/(g\circ f)(d)}{n/d} &= \frac{\ell/(g\circ f)(d)}{m/f(d)} \cdot \frac{m/f(d)}{n/d} \\ &\leq \min\left\{1, \frac{\lambda(\ell/(g\circ f)(d))}{\lambda(m/f(d))}\right\} \cdot \min\left\{1, \frac{\lambda(m/f(d))}{\lambda(n/d)}\right\} \\ &\leq \min\left\{1 \cdot 1, \frac{\lambda(\ell/(g\circ f)(d))}{\lambda(m/f(d))} \cdot \frac{\lambda(m/f(d))}{\lambda(n/d)}\right\} \\ &= \min\left\{1, \frac{\lambda(\ell/(g\circ f)(d))}{\lambda(n/d)}\right\}.\end{aligned}$$

Requirements (a) and (c) are immediate. □

When combined, Lemmas 3.7 and 3.8 allow us to manipulate a prime factorization one comprehensible piece at a time. We have already seen through an example how to reduce to those n whose $\omega(n)$ distinct prime factors are exactly $2, 3, ..., p_{\omega(n)}$. It turns out we can do even better: if p and q are primes with $2 \neq p \leq q$ and a and b are integers with $0 \leq a \leq b$, then there is a reducing function $f : \mathcal{D}(p^a q^b) \to \mathcal{D}(p^b q^a)$. It is defined by $f(p^i q^j) = p^{i+k} q^{j-k}$, where $k = \max(0, \min(i + j, b) - a)$. This allows us to rearrange prime exponents in decreasing order (except for the exponent of 2). That is, to obtain bounds on $|\mathcal{M}_x(n)|$, we need only consider those n that are products of primorials up to a power of 2. We will not prove that this function is reducing, because its purpose is subsumed by the next family of reducing functions. These not only rearrange exponents in decreasing order, they also limit the rate at which exponents can decrease.

Lemma 3.9. *Let p and q be distinct odd primes, let a and b be nonnegative integers, and set $c = \lfloor (a+1)/(b+2) \rfloor$. If $q < p^c$, then $p^a q^b$ reduces to $p^{a-c} q^{b+1}$.*

Proof. Define $f : \mathcal{D}(p^a q^b) \to \mathcal{D}(p^{a-c} q^{b+1})$ by $f(p^i q^j) = p^i q^j$ if $i < (b+1-j)c$ and $f(p^i q^j) = p^{i-c} q^{j+1}$ if $i \geq (b+1-j)c$. We claim f is a reducing function.

Suppose $i < (b+1-j)c$. The nontrivial assertion behind $f(p^i q^j) \in \mathcal{D}(p^{a-c} q^{b+1})$ is that $i \leq a - c$. Indeed, $i \leq (b+1-j)c - 1 \leq (b+1)c - 1 = (b+2)c - c - 1 \leq (a+1) - c - 1 = a - c$. Next, requirement (a) of Definition 3.4 holds because $f(d) = d$ (we are still in the case $i < (b+1-j)c$). For requirement (b), we begin by observing that our hypothesis $q < p^c$ implies

$$\frac{p^{a-c} q^{b+1}/p^i q^j}{p^a q^b / p^i q^j} = \frac{q}{p^c} \leq \min\left\{1, \frac{q}{p}\right\}.$$

There are only two ways the right-hand side above could possibly exceed the desired upper bound of

$$\min\left\{1, \frac{\lambda(p^{a-c} q^{b+1}/p^i q^j)}{\lambda(p^a q^b / p^i q^j)}\right\}.$$

Namely, if $\lambda(p^{a-c} q^{b+1}/p^i q^j) = 1$ or if $\lambda(p^{a-c} q^{b+1}/p^i q^j) = p < q = \lambda(p^a q^b / p^i q^j)$. But the former cannot happen because q divides $p^{a-c} q^{b+1}/p^i q^j$, and the latter cannot happen as it requires both $a - c > i$ and $a = i$. Lastly, requirement (c) holds regardless of the value of i because p and q are both odd.

Next suppose $i \geq (b+1-j)c$. In this case it is clear that $f(p^iq^j) \in \mathcal{D}(p^{a-c}q^{b+1})$. For requirement (a), $f(p^iq^j) = p^{i-c}q^{j+1} \leq p^iq^j$ follows from the hypothesis $q < p^c$. For requirement (b), we have

$$\frac{p^{a-c}q^{b+1}/p^{i-c}q^{j+1}}{p^aq^b/p^iq^j} = 1 = \frac{\lambda(p^{a-c}q^{b+1}/p^{i-c}q^{j+1})}{\lambda(p^aq^b/p^iq^j)}.$$

And we have already noted that requirement (c) is holds trivially. □

Next is a family of reducing functions devoted to controlling the exponent of 2 in a prime factorization. Ultimately, 2 will play the role of p below.

Both in the lemma statement and its proof, the empty product is to be interpreted as 1.

Lemma 3.10. *Let $p, q_1, ..., q_k$ be primes with $p < q_1 < \cdots < q_k$, and let $a \in \mathbb{N}$. If $p^{a-2} > q_1 \cdots q_{k-1}q_k^2$ then p^a reduces to $p^bq_1 \cdots q_k$, where*

$$b = \left\lfloor \frac{1}{2}\left(a - \frac{\log(q_1 \cdots q_{k-1})}{\log p}\right)\right\rfloor.$$

Proof. Let $c_k = a-b$ and $c_j = \lceil \log(q_1 \cdots q_j)/\log p \rceil$ for $0 \leq j < k$. Define $f : \mathcal{D}(p^a) \to \mathcal{D}(p^bq_1 \cdots q_k)$ by $f(p^i) = p^{b+c_j+i-a}q_{j+1} \cdots q_k$, where j is the largest index such that $c_j \leq a - i$. We claim f is a reducing function.

The nontrivial assertion behind $f(p^i) \in \mathcal{D}(p^bq_1 \cdots q_k)$ is that $b + c_j + i - a \geq 0$. To verify this inequality, suppose first that $j < k-1$. In this case,

$$\begin{aligned}
b + c_j + i - a &\geq b + c_j - c_{j+1} + 1 \quad \text{by maximality of } j \\
&\geq b - \left\lceil \frac{\log q_{j+1}}{\log p} \right\rceil + 1 \quad \text{by definition of } c_j \text{ and } c_{j+1} \text{ for } j < k-1 \\
&= \left\lfloor \frac{1}{2}\left(a - \frac{\log(q_1 \cdots q_{k-1})}{\log p}\right)\right\rfloor - \left\lceil \frac{\log q_{j+1}}{\log p} \right\rceil + 1 \\
&> \frac{1}{2}\left(a - \frac{\log(q_1 \cdots q_{k-1})}{\log p}\right) - \frac{\log q_{j+1}}{\log p} - 1 \\
&> \frac{1}{2}\left(a - \frac{\log(q_1 \cdots q_{k-1}q_k^2)}{\log p}\right) - 1 \quad \text{since } q_{j+1} < q_k \\
&> 0 \quad \text{since } p^{a-2} > q_1 \cdots q_{k-1}q_k^2.
\end{aligned}$$

In the case $j = k-1$ we must have $a - i \leq c_k - 1 = a - b - 1$ by maximality of j, so

$$\begin{aligned}
b + c_j + i - a &\geq 2b + c_{k-1} + 1 - a \\
&= 2\left\lfloor \frac{1}{2}\left(a - \frac{\log(q_1 \cdots q_{k-1})}{\log p}\right)\right\rfloor + \left\lceil \frac{\log(q_1 \cdots q_{k-1})}{\log p} \right\rceil + 1 - a \\
&> 2\left(\frac{1}{2}\left(a - \frac{\log(q_1 \cdots q_{k-1})}{\log p}\right) - 1\right) + \frac{\log(q_1 \cdots q_{k-1})}{\log p} + 1 - a \\
&= -1.
\end{aligned}$$

(Note that the strict inequality above uses the fact that $\log(q_1 \cdots q_{k-1})/\log p$ cannot be an integer by unique factorization in $\mathbb{Z}$ and our assumption that p is distinct from $q_1, ..., q_{k-1}$.) Finally, if $j = k$ then $b + c_j + i - a = i \geq 0$.

Now we turn to the bound $f(p^i) \le p^i$ from Definition 3.4. If $j = k$ then $f(p^i) = p^i$. Otherwise,

$$\begin{aligned}
\frac{\log(f(p^i)/p^i)}{\log p} &= b + c_j - a + \frac{\log(q_{j+1}\cdots q_k)}{\log p} \\
&\le b - a + 1 + \frac{\log(q_1\cdots q_k)}{\log p} \quad \text{by definition of } c_j \\
&\le -\frac{1}{2}\left(a + \frac{\log(q_1\cdots q_{k-1})}{\log p}\right) + 1 + \frac{\log(q_1\cdots q_k)}{\log p} \quad \text{by definition of } b \\
&< -\frac{1}{2}\left(2 + \frac{2\log(q_1\cdots q_k)}{\log p}\right) + 1 + \frac{\log(q_1\cdots q_k)}{\log p} \quad \text{since } p^{a-2} > q_1\cdots q_{k-1}q_k^2 \\
&= 0.
\end{aligned}$$

To verify requirement (b),

$$\begin{aligned}
\frac{p^b q_1\cdots q_k/f(p^i)}{p^a/p^i} &= \frac{q_1\cdots q_j}{p^{c_j}} \quad \text{by definition of } f \\
&\le 1 \quad \text{by definition of } c_j \text{ (and } b \text{ when } j = k) \\
&\le \frac{\lambda(p^b q_1\cdots q_k/f(p^i))}{\lambda(p^a/p^i)},
\end{aligned}$$

where the final inequality above uses $p < q_1, ..., q_k$ from our hypothesis, as well as the fact that $\lambda(p^b q_1\cdots q_k/f(p^i)) = 1$ would force $a = i$ and thus $\lambda(p^a/p^i) = 1$. Requirement (c) is trivially satisfied. □

Let us now identify those numbers that cannot be reduced by Lemma 3.9 or 3.10. These are the numbers n that we use to determine the maxima of $|\mathcal{M}_x(n)|$, as made precise in Theorem 3.14.

Throughout the remainder of this section, p_i denotes the i^{th} prime number.

Definition 3.11. An integer $2^{a_1}3^{a_2}5^{a_3}\cdots$ (where $a_i = 0$ for sufficiently large i) is *reduced* if

$$\left\lfloor \frac{a_i + 1}{a_j + 2} \right\rfloor < \frac{\log p_j}{\log p_i} \tag{13}$$

whenever $i, j \ne 1$, and $2^{a_1} < 8p_j^2$ whenever $a_j = 0$.

Table 1 shows all reduced numbers with odd part bounded by 10^9. For example, we see that $2^{a_1}\cdot 3$ is reduced if $0 \le a_1 \le 7$, but not if $a_1 \ge 8$. Up to a power of 2, the reduced numbers in Table 1 are products of primorials. This is always true, as mentioned before Lemma 3.9 and proved below. Also note the restriction on how quickly exponents can decrease. This is exhibited by the fact that 27 is not a reduced number—the exponent decrease from 3^3 to 5^0 is too much.

Lemma 3.12. *If $2^{a_1}3^{a_2}5^{a_3}\cdots$ is reduced, then $a_2 \ge a_3 \ge \cdots$.*

Proof. On the one hand, if $i > j$ in inequality (13) then the right-hand side is less than 1. On the other hand, if $a_i > a_j$ then the left-hand side is at least 1. □

Lemma 3.13. *Let p_k be the largest prime divisor of $n \in \mathbb{N}$. If n is reduced, so is np_{k+1}.*

Proof. Only the exponent a_{k+1} has changed, so we need only verify (13) when $i = k+1$ or $j = k+1$.

First suppose $i = k+1$ (so $a_i = 1$ for np_{k+1}). If $j \le k+1$ then $a_j \ge 1$ by Lemma 3.12 applied to n. Thus

$$\left\lfloor \frac{a_i + 1}{a_j + 2} \right\rfloor \le \left\lfloor \frac{2}{3} \right\rfloor = 0 < \frac{\log p_j}{\log p_i}.$$

n	Prime factorization	$a_1 \leq$
1	1	6
3	3	7
9	3^2	7
15	$3 \cdot 5$	8
45	$3^2 \cdot 5$	8
105	$3 \cdot 5 \cdot 7$	9
225	$3^2 \cdot 5^2$	8
315	$3^2 \cdot 5 \cdot 7$	9
945	$3^3 \cdot 5 \cdot 7$	9
1155	$3 \cdot 5 \cdot 7 \cdot 11$	10
1575	$3^2 \cdot 5^2 \cdot 7$	9
2835	$3^4 \cdot 5 \cdot 7$	9
3465	$3^2 \cdot 5 \cdot 7 \cdot 11$	10
4725	$3^3 \cdot 5^2 \cdot 7$	9
10395	$3^3 \cdot 5 \cdot 7 \cdot 11$	10
11025	$3^2 \cdot 5^2 \cdot 7^2$	9
14175	$3^4 \cdot 5^2 \cdot 7$	9
15015	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	11
17325	$3^2 \cdot 5^2 \cdot 7 \cdot 11$	10
31185	$3^4 \cdot 5 \cdot 7 \cdot 11$	10
33075	$3^3 \cdot 5^2 \cdot 7^2$	9
45045	$3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	11
51975	$3^3 \cdot 5^2 \cdot 7 \cdot 11$	10
99225	$3^4 \cdot 5^2 \cdot 7^2$	9
121275	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11$	10
135135	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	11
155925	$3^4 \cdot 5^2 \cdot 7 \cdot 11$	10
225225	$3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	11
255255	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11
363825	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11$	10
405405	$3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	11
675675	$3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	11
765765	$3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11

n	Prime factorization	$a_1 \leq$
1091475	$3^4 \cdot 5^2 \cdot 7^2 \cdot 11$	10
1334025	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2$	10
1576575	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	11
2027025	$3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	11
2297295	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11
3828825	$3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11
4002075	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2$	10
4729725	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	11
4849845	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
6891885	$3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11
11486475	$3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11
12006225	$3^4 \cdot 5^2 \cdot 7^2 \cdot 11^2$	10
14189175	$3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	11
14549535	$3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
17342325	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13$	11
26801775	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$	11
34459425	$3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	11
43648605	$3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
52026975	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13$	11
72747675	$3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
80405325	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$	11
111546435	$3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	12
130945815	$3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
156080925	$3^4 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13$	11
218243025	$3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
225450225	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2$	11
241215975	$3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$	11
294819525	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 17$	11
334639305	$3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	12
509233725	$3^2 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
654729075	$3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	12
676350675	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2$	11
884458575	$3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 17$	11

TABLE 1. All reduced numbers of the form $2^{a_1}n$ for odd $n \leq 10^9$.

If $j > k+1$ then $a_j = 0$. So

$$\left\lfloor \frac{a_i+1}{a_j+2} \right\rfloor = 1 < \frac{\log p_j}{\log p_{k+1}} = \frac{\log p_j}{\log p_i}.$$

Now suppose $j = k+1$ and $i \neq k+1$. Here the fraction $(a_i+1)/(a_j+2)$ has decreased by adding the factor of p_{k+1}. So if inequality (13) holds for n, it certainly holds for np_{k+1} □

Theorem 3.14. *For any integer $n \geq 2$, there exists a reduced integer m such that $n \leq m \leq 4n-6$ and $|\mathcal{M}_x(n)| \leq |\mathcal{M}_x(m)|$ for all $x \in \mathbb{R}$.*

Proof. Let m' be the odd part of the smallest positive integer to which n can be reduced. By Lemma 3.9, the exponents in the prime factorization of m' satisfy (13). Let a be the smallest integer such that $2^a m' \geq n$. Then $|\mathcal{M}_x(n)| \leq |\mathcal{M}_x(2^a m')|$ for all $x \in \mathbb{R}$ by Theorem 3.5. Note that $2^a m' \leq 2n-2$.

Let p_k be the largest prime dividing $2^a m'$, and if one exists, let ℓ be the largest index satisfying $p_{k+1} \cdots p_{\ell-1} p_\ell^2 < 2^{a-2}$. If no such index exists, let $\ell = k$. We claim that $m = 2^{a_1} m' p_{k+1} \cdots p_\ell$ meets our theorem's requirements, where a_1 is the smallest integer such that $m \geq 2^a m'$. From another application of Theorem 3.5, this time applied to the reduction in Lemma 3.10, we have $|\mathcal{M}_x(2^a m')| \leq |\mathcal{M}_x(m)|$ for all $x \in \mathbb{R}$. Since

$$m \leq 2(2^a m') - 2 \leq 2(2n-2) - 2 = 4n - 6,$$

we will be done provided m is reduced.

Apply Lemma 3.13 $\ell - k$ times beginning with the reduced integer m' to see that $m' p_{k+1} \cdots p_\ell$ is reduced, meaning (13) holds. Let us check that $2^{a_1} < 8 p_{\ell+1}^2$. We have

$$3 + \left\lfloor \frac{2 \log p_{\ell+1}}{\log 2} \right\rfloor + \frac{\log(p_{k+1} \cdots p_\ell)}{\log 2} > 2 + \frac{\log(p_{k+1} \cdots p_\ell \, p_{\ell+1}^2)}{\log 2} \geq a,$$

where the last inequality above uses maximality of ℓ. Thus $3 + \lfloor 2 \log p_{\ell+1} / \log 2 \rfloor$ solves the inequality for which a_1 is the minimal solution, implying $a_1 < 3 + 2 \log p_{\ell+1} / \log 2$ as desired. □

Reduced numbers turn out to be sufficiently rare for our purpose. Data up to $x \approx 10^{1000}$ suggests that $(\log x)^4 / (3 \log \log x)$ is a very good approximation for the number of reduced integers less than x. This density could potentially be diminished further via new reducing functions, though the authors suspect that Definition 3.4 is too restrictive to allow for a notion of reduced numbers with density approaching that of the superior highly composite numbers (asymptotically $\log x / \log \log x$ [Ram15]). Definition 3.4 might be loosened, however, to permit functions $f : \mathcal{D}(n) \to \mathcal{D}(m)$ with ratios

$$\alpha := \max_{d \in \mathcal{D}(n)} \frac{f(d)}{d} \quad \text{and} \quad \beta := \max_{d \in \mathcal{D}(n)} \frac{(m/f(d))\lambda(n/d)}{(n/d)\lambda(m/f(d))}$$

that exceed 1. Then, as long as $\alpha \leq \beta$, we could prove a version of Theorem 3.5 that requires $2^a m \geq \beta n$ in order to conclude $|\mathcal{M}_x(n)| \leq |\mathcal{M}_{\alpha x}(2^a m)|$ for all x.

3.2. **An asymptotic bound.** Our strategy for bounding $|\mathcal{M}_x(n)|$ asymptotically is as follows: We need only consider reduced n – that is the purpose of the last section – and reduced integers are not too far from being products of one or two primorials (Lemma 3.15). This makes $\Omega(n)$ roughly equal to $\log n / \log \log n$ (Lemma 3.16). If $x = n^\alpha$ then we expect elements of $\mathcal{M}_x(n)$ to be products of roughly $\alpha \Omega(n)$ primes (Lemma 3.19), so we just apply Stirling's formula to bound how many ways we can choose these primes (Theorem 1.3).

Lemma 3.15. *For a reduced integer* $2^{a_1} 3^{a_2} \cdots p_k^{a_k}$,

$$\sum_{a_i \geq 3} (a_i - 2) = O\left(\frac{k^{2/3}}{(\log k)^{1/3}} \right).$$

Proof. By setting j in Definition 3.11 equal to $k+1$, we see that $a_i < 2 \log p_{k+1} / \log p_i$ for any $i \geq 2$, and that $a_1 < 3 + 2 \log p_{k+1} / \log 2$. In particular, if $a_i \geq 3$ then $p_i < p_{k+1}^{2/3}$. Let $x = p_{k+1}^{2/3}$.

These upper bounds on a_i and p_i that we have just established justify the first inequality below:

$$\begin{aligned}
\sum_{a_i \geq 3} (a_i - 2) &< 3 + 2 \sum_{p_i < x} \left(\frac{\log p_{k+1}}{\log p_i} - 1 \right) \\
&= 3 + 2\pi(x) \left(\frac{\log p_{k+1}}{\log x} - 1 \right) + \int_2^x \frac{\pi(t) \log p_{k+1}}{t (\log t)^2} dt \quad \text{by partial summation} \\
&= 3 + \pi(x) + \frac{3 \log x}{2} \int_2^x \frac{\pi(t)}{t (\log t)^2} dt \quad \text{since } x = p_{k+1}^{2/3} \\
&< 3 + \frac{2x}{\log x} + 3 \log x \int_2^x \frac{t}{t (\log t)^3} dt \quad \text{by [Dus18], for example} \\
&= 3 + \frac{2x}{\log x} + 3 \log x \left(\int_2^{\log x} \frac{1}{(\log t)^3} dt + \int_{\log x}^x \frac{1}{(\log t)^3} dt \right) \\
&\leq 3 + \frac{2x}{\log x} + 3 \log x \left(\frac{\log x}{(\log 2)^3} + \frac{x}{(\log x)^3} \right) = O\left(\frac{x}{\log x} \right).
\end{aligned}$$

Substituting $x = p_{k+1}^{2/3}$ into the final expression above and applying the prime number theorem, $p_{k+1} = O(k \log k)$, completes the proof. □

A small deficiency in our reducing functions from Section 3.1 is that they do nothing to bound the index at which prime exponents of a reduced number must switch from 2 to 1. In fact, reduced numbers can be perfect squares as shown in Table 1. This is why the previous lemma can only bound sums of exponents that are at least 3 rather than at least 2, and thus why the proof of the next lemma must consider products of two primorials instead of a single primorial.

Lemma 3.16. *Let $\Omega(n)$ denote the number of prime factors of n, counted with multiplicity. For a reduced integer n,*

$$\Omega(n) \leq \frac{\log n}{\log \log n} + O\left(\frac{\log n}{(\log \log n)^2} \right).$$

Proof. Suppose n is reduced, and let m be the largest factor of n that is cube-free. By Lemma 3.12, up to a factor of 2 or 4 we have either $m = p_k\#$ for some k or $m = (p_k\#)(p_j\#)$ for some $k \geq j$. Let us ignore the contribution to $\Omega(n)$ from the potentially errant factor of 2 or 4 because it gets absorbed by the error term $\log n/(\log \log n)^2$. Let us also remark before proceeding that k (in our expression for m) cannot remain bounded as n grows. Indeed, $\log n \leq \log p_k \sum_i a_i = \log p_k (2k + \sum_i (a_i - 2))$, which Lemma 3.15 bounds by a function of k. This is important as it allows us to apply bounds that only hold for large k.

There are two initial inequalities that we aim to prove for large n (and therefore k):

$$\log n > (k + j) \log(k \log k) - 3k, \tag{14}$$

where j is understood to be 0 if $m = p_k\#$, and (the crude bound)

$$\log \log n < 2 \log(k \log k). \tag{15}$$

To prove each of them, we will use standard bounds on Chebyshev's theta function. (Recall that $\vartheta(x) := \sum_p \log p$, the sum being over primes $p \leq x$.) Namely,

$$k(\log(k \log k) - 1) < \vartheta(p_k) < k \log(k \log k) \tag{16}$$

for $k \geq 5107$ [MR96], with analogous bounds for $\vartheta(p_j)$ when $j \geq 5107$.

On the one hand, if either $m = p_k\#$ or if $j < 5107$, then (14) follows immediately for large k from the lower bound on $\vartheta(p_k)$ above. Indeed,

$$\log n \geq \vartheta(p_k) > k(\log(k \log k) - 1) > (k + 5107) \log(k \log k) - 3k > (k + j) \log(k \log k) - 3k.$$

On the other hand, if $k \geq j \geq 5107$ then

$$\begin{aligned}\log n \geq \log m &\geq \vartheta(p_k) + \vartheta(p_j) \quad \text{by definition of } m \\ &> k(\log(k\log k) - 1) + j(\log(j\log j) - 1) \quad \text{by (16)} \\ &= (k+j)\log(k\log k) - (k+j) + j\log\left(\frac{j\log j}{k\log k}\right). \end{aligned} \tag{17}$$

The smaller terms in the final expression above are bounded multiples of k:

$$k + j \leq 2k, \quad \text{and} \quad -j\log\left(\frac{j\log j}{k\log k}\right) < \frac{k}{e}\left(1 + \frac{1}{\log j}\right) < k. \tag{18}$$

Combining (17) and (18) completes the proof of (14).

Now let us turn to (15). Lemma 3.15 tells us that

$$\Omega(n/m) = \sum_{a_i \geq 3}(a_i - 2) < k^{2/3} \tag{19}$$

for large k. In particular,

$$\begin{aligned}\log\log n &= \log(\log(n/m) + \log m) \\ &\leq \log(\Omega(n/m)\log p_k + \log m) \\ &< \log(k^{2/3}\log p_k + \log m) \quad \text{by (19)} \\ &< \log(k^{2/3}\log p_k + \vartheta(p_k) + \vartheta(p_j)) \quad \text{by definition of } m \\ &< \log(3\vartheta(p_k)) \\ &< \log(3k\log(k\log k)) \quad \text{by (16)} \\ &< 2\log(k\log k) \quad \text{for } k \geq 3. \end{aligned} \tag{20}$$

Finally we apply (14) and (15) as follows:

$$\begin{aligned}\frac{\Omega(n)\log\log n}{\log n} &= \frac{(\Omega(m/n) + \Omega(m))\log\log n}{\log n} \\ &< \frac{(k^{2/3} + k + j)\log\log n}{\log n} \quad \text{by (19) and definition of } m \\ &< \frac{(k^{2/3} + k + j)\log((k+j)\log(k\log k) - 3k)}{(k+j)\log(k\log k) - 3k} \quad \text{by (14) } ((\log x)/x \text{ is decreasing}) \\ &< \frac{(k+j)\log(k\log k) + 3k}{(k+j)\log(k\log k) - 3k} \quad \text{for } k \geq 50 \\ &= 1 + O\left(\frac{1}{\log(k\log k)}\right) \\ &= 1 + O\left(\frac{1}{\log\log n}\right) \quad \text{by (15)}. \end{aligned}$$

Note that in the second inequality above, to apply (14) we use the fact that $\log x/x$ is a decreasing function for $x > e$, as well as the assumption that $(k+j)\log(k\log k) - 3k \geq e$. Scaling both ends of the inequality above by $\log n/\log\log n$ completes the proof. □

The notation below and the lemmas that follow it are purely combinatorial. We phrase them in the language of divisors for convenience.

Notation 3.17. For $n, k \in \mathbb{Z}$ with $n \neq 0$, let $C_k(n) = |\{d \in \mathcal{D}(n) : \Omega(d) = k\}|$. Note that $C_k(n) = 0$ if $k < 0$ of $k > \Omega(n)$.

So $C_k(n)$ counts the k-element multisets of the $\Omega(n)$-element multiset consisting of the prime factors of n with multiplicity. In particular, if n is square-free then $C_k(n)$ is just a binomial coefficient. For general n, there is an upper bound

$$C_k(n) \leq \binom{\Omega(n)}{k},$$

because counting a single prime divisor with multiplicity as multiple distinct set elements increases the number of k-element subsets.

Lemma 3.18. *For any $n \in \mathbb{N}$, if $k \leq \Omega(n)/2$ then $C_{k-1}(n) \leq C_k(n)$. If $k \geq \Omega(n)/2$ then $C_k(n) \geq C_{k+1}(n)$.*

Proof. In [DEK51] it is shown that $\mathcal{D}(n)$ can be partitioned into "symmetric chains" of the form $\{d_1, ..., d_j\}$, where $\Omega(d_1) + \Omega(d_j) = \Omega(n)$ and $\Omega(d_{i+1}) = \Omega(d_i) + 1$ for all $i = 1, ..., j-1$. By applying Ω to each symmetric chain, we partition the multiset $\{\Omega(d) : d \in \mathcal{D}(n)\}$ into subsets of the form $\{\Omega(d_1), \Omega(d_1)+1, \Omega(d_1)+2, ..., \Omega(n)-\Omega(d_1)\}$, a sequence of consecutive integers centered at $\Omega(n)/2$. In particular, if $k \leq \Omega(n)/2$, then every such sequence that contains $k-1$ must also contain k, showing $C_{k-1}(n) \leq C_k(n)$. Similarly, $k \geq \Omega(n)/2$ implies $C_k(n) \geq C_{k+1}(n)$. □

Lemma 3.19. *Given $n \in \mathbb{N}$ and $x \geq 1$, let k be an integer that is closest to $\Omega(n)/2$ in the range*

$$\min\{\Omega(d) : d \in \mathcal{M}_x(n)\} \leq k \leq \max\{\Omega(d) : d \in \mathcal{M}_x(n)\}.$$

Then $|\mathcal{M}_x(n)| \leq C_k(n)$.

Proof. Again we partition $\mathcal{D}(n)$ into symmetric chains $\{d_1, ..., d_j\}$ as in the proof of Lemma 3.18. Since elements of $\mathcal{M}_x(n)$ cannot divide one another while elements of a particular symmetric chain always divide one another, each symmetric chain contains at most one maximal divisor. This allows us to define an injection from $\mathcal{M}_x(n)$ to $\{d \in \mathcal{D}(n) : \Omega(d) = k\}$, and the latter multiset has cardinality $C_k(n)$. Indeed, to each $d \in \mathcal{M}_x(n)$ we associate the unique divisor d' that belongs to the same symmetric chain as d and satisfies $\Omega(d') = k$. Such a d' always exists because we chose k to be at least as close to $\Omega(n)/2$ as $\Omega(d)$, and $\Omega(n)/2$ is the "center" over which symmetric chains are symmetric. □

We can now prove the asymptotic bound on $|\mathcal{M}_x(n)|$ stated in the introduction.

Theorem 1.3. *For any $\varepsilon > 0$, if $\alpha \in [\varepsilon, 1-\varepsilon]$ then*

$$\log|\mathcal{M}_{n^\alpha}(n)| \leq \log\left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).$$

The implied constant depends only on ε.

Proof. Recall from Theorem 3.14 that an integer n can be replaced with a reduced integer at most four times its size. Since the increase from $\log n/\log\log n$ to $\log 4n/\log\log 4n$ is absorbed by the error term above, we need only prove this theorem for reduced integers. So let $n = 2^{a_1}3^{a_2}\cdots p_k^{a_k}$ be reduced.

Suppose first that $\alpha \geq 1/2$. Let d_0 be the divisor of n such that $d_0 \geq n^\alpha$, and $\Omega(d_0)$ is minimal among all divisors exceeding n^α. Note that d_0 is composed of the largest primes dividing n, so $\Omega(d_0) \leq \alpha\Omega(n)$. This gives

$$\Omega(n/d_0) \geq (1-\alpha)\Omega(n) \geq \varepsilon\Omega(n) \geq \varepsilon(k-1)$$

(note that a_1 might equal 0). Since ε is fixed, if n is sufficiently large then Lemma 3.15 implies n/d_0 must be divisible by more primes than just those whose exponent in the factorization of n exceeds 2. In particular, we see that d_0 is not divisible by any perfect cubes. That is, $d_0 = (p_k\#)(p_j\#)/(p_i\#)^2$ for some $i \leq j$.

Since $\lambda(n/d)d > n^\alpha$ for any $d \in \mathcal{M}_{n^\alpha}(n)$, the definition of d_0 implies $\Omega(d)+1 \geq \Omega(d_0)$ for any $d \in \mathcal{M}_{n^\alpha}(n)$. So our goal is to bound $\Omega(d_0)-1$ from below. To this end, the exact same argument from inequalities (17) and (18) shows that

$$\log(n) > (k+j)\log(k\log k) - 3k$$

for large n, and a nearly identical argument shows that

$$\log d_0 \leq (k+j-2i-1)\log(k\log k) + 3k$$

for large n. These are the first and third inequalities below, while the fourth uses Lemma 3.15:

$$\begin{aligned}
\Omega(d_0) - 1 = k+j-2i-1 &> \frac{\log d_0 - 3k}{\log(k\log k)} \\
&> \frac{\alpha\log n - 3k}{\log(k\log k)} \\
&> \alpha(k+j) - \frac{3(1+\alpha)k}{\log(k\log k)} \\
&= \alpha(k+j+k^{2/3})\left(1 - \frac{3(1+\alpha)k + \alpha k^{2/3}\log(k\log k)}{\alpha(k+j+k^{2/3})\log(k\log k)}\right) \qquad (21) \\
&> \alpha\Omega(n)\left(1 - \frac{10}{\log(k\log k)}\right).
\end{aligned}$$

Note that $\alpha \geq 1/2$ to justify the constant 10 for large k in the final error term. Now recall from (20) that $\log(k\log k)$ can be replaced with $(\log\log n)/2$ above. In particular if $\beta \in \mathbb{R}$ is such that $\beta\Omega(n)$ is the closest integer to $\Omega(n)/2$ between $\min\{\Omega(d) : d \in \mathcal{M}_x(n)\}$ and $\max\{\Omega(d) : d \in \mathcal{M}_x(n)\}$ then

$$\beta > \alpha\left(1 - \frac{20}{\log\log n}\right). \qquad (22)$$

Lemma 3.19 followed by Stirling's formula for binomial coefficients tells us

$$|\mathcal{M}_{n^\alpha}(n)| \leq C_{\beta\Omega(n)}(n) \leq \binom{\Omega(n)}{\beta\Omega(n)} = \Omega(n)^{O(1)}\left(\frac{1}{\beta^\beta(1-\beta)^{1-\beta}}\right)^{\Omega(n)}.$$

Now let $f(x) = (x-1)\log(1-x) - x\log x$, and take logarithms of the inequalities above to get

$$\begin{aligned}
\log|\mathcal{M}_{n^\alpha}(n)| &= O(\log\Omega(n)) + f(\beta)\Omega(n) \\
&= f(\beta)\left(\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right)\right) \\
&\leq \left(f(\alpha) + \frac{20\alpha|f'(\alpha)|}{\log\log n}\right)\left(\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right)\right) \\
&= f(\alpha)\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).
\end{aligned}$$

Both the second and last equality above use that α (and β) are restricted to the interval $[\varepsilon, 1-\varepsilon]$. The lone inequality symbol above is justified by (22) and the mean value theorem.

We need not repeat these arguments for $\alpha < 1/2$. Indeed, the only missing piece is an analogous upper bound on $\Omega(d_1)$, where d_1 is the divisor of n such that $d_1 \leq n^\alpha$, and $\Omega(d_1)$ is maximal among all divisors not exceeding n^α. But this makes $d_1 = n/d_0$. So by (21), but with α replaced by $1-\alpha$, we have

$$\Omega(d_1) = \Omega(n) - \Omega(d_0) < \Omega(n)\left(1 - (1-\alpha)\left(1 - \frac{20}{\log\log n}\right)\right) = \alpha\Omega(n)\left(1 + O\left(\frac{\log n}{\log\log n}\right)\right).$$

The uses of Stirling's formula and the mean value theorem work again with trivial modification. □

As a corollary, we get an asymptotic bound on the total number of divisors of n bounded by n^α.

Corollary 3.20. *For any $\varepsilon > 0$, if $\alpha \in [\varepsilon, 1/2]$ then*

$$\log\left|\{d \in \mathbb{N} : d \mid n,\ d \le n^\alpha\}\right| \le \log\left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right).$$

The implied constant depends only on ε.

Proof. Let $x \in \mathbb{R}$, and suppose d is a proper divisor of n in $(x/2, x]$. Since $\lambda(n/d) \ge 2$, we see that $d\lambda(n/d) > x$, implying $d \in \mathcal{M}_x(n)$. Therefore all positive divisors d of n with $d \le n^\alpha$ are contained in the union of the sets $\mathcal{M}_x(n)$ for $x = \lfloor n^\alpha \rfloor, \lfloor n^\alpha/2 \rfloor, ..., 1$. There are at most $\lfloor \log_2 n^\alpha \rfloor + 1$ such values of x. By Lemmas 3.18 and Lemma 3.19, each $|\mathcal{M}_x(n)|$ is bounded by $C_{\Omega(d_1)}(n)$, where d_1 is as in the previous proof: the divisor of n such that $d_1 \le n^\alpha$, and $\Omega(d_1)$ is maximal among all divisors not exceeding n^α. We just showed that

$$\log C_{\Omega(d_1)}(n) \le \log\left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)\frac{\log n}{\log\log n} + O\left(\frac{\log n}{(\log\log n)^2}\right),$$

and scaling $C_{\Omega(d_1)}(n)$ by $\lfloor \log_2 n^\alpha \rfloor + 1$ does not change this. □

As mentioned in the introduction, when $\alpha = 1/2$ Corollary 3.20 recovers Wigert's theorem that $\log \tau(n) = (\log 2 + o(1))(\log n / \log\log n)$ [Wig07].

3.3. **An explicit bound.** The next section gives a computer-assisted proof of Theorem 1.4 via Algorithm 1, in which a bound on the number of maximal divisors of some $p \pm 1$ is found by first replacing $p \pm 1$ with a reduced number (because these are far more sparse than primes). Finding exact values of $|\mathcal{M}_x(n)|$ for reduced n up to Corollary 2.5's bound of 10^{532} is computationally infeasible. We have the bound $|\mathcal{M}_x(n)| \le C_k(n)$ for the right choice of k by Lemma 3.19, but even computing $C_k(n)$ is expensive. The following bound, on the other hand, is computed almost instantly assuming the prime factorization of n is known. Its purpose is to avoid computing $C_k(n)$ when possible, to the effect of making Algorithm 1 run anywhere from 3 times faster (when exact integer arithmetic is performed throughout) to at least 40 times faster (when floating point arithmetic is used for computations that need not be precise).

Theorem 3.21. *For any $n \in \mathbb{N}$ and $x \in \mathbb{R}$,*

$$|\mathcal{M}_x(n)| \le \frac{\tau(n)}{2^{\Omega(n)}}\binom{\Omega(n)}{\lfloor \Omega(n)/2 \rfloor}.$$

Proof. By Lemma 3.19, $|\mathcal{M}_x(n)| \le C_k(n)$ for the appropriate choice of k, and by Lemma 3.18, $C_k(n)$ is maximized at $k = \lfloor \Omega(n) \rfloor$. So it suffices to prove that for all n,

$$C_k(n) \le \frac{\tau(n)}{2^{\Omega(n)}}\binom{\Omega(n)}{k} \tag{23}$$

for $k = \lfloor \Omega(n) \rfloor$. Note that if n is square-free, then we have equality above since $\tau(n) = 2^{\omega(n)}$ and $C_k(n) = \binom{\Omega(n)}{k}$. So suppose $p^2 \mid n$ for some prime p. Our strategy is to replace n with $n' = nq/p$ for some prime $q \nmid n$, essentially making n one prime closer to being square-free while preserving $\Omega(n)$. If we can show that

$$\frac{C_k(n)}{\tau(n)} \le \frac{C_k(n')}{\tau(n')}, \tag{24}$$

then the prime replacement process can repeat until a square-free integer n_{sf} is reached, allowing us to conclude by induction that

$$\frac{C_k(n)}{\tau(n)} \le \frac{C_k(n')}{\tau(n')} \le \cdots \le \frac{C_k(n_{\text{sf}})}{\tau(n_{\text{sf}})} = \frac{1}{2^{\Omega(n_{\text{sf}})}}\binom{\Omega(n_{\text{sf}})}{k} = \frac{1}{2^{\Omega(n)}}\binom{\Omega(n)}{k}.$$

Comparing the two ends of the chain above is equivalent to (23).

Turning to (24), let p^{a+1} be the largest power of p dividing n (so $a \geq 1$ by choice of p), and let $m = n/p^{a+1} = n'/(p^a q)$. We have

$$\begin{aligned}
\frac{\tau(n)C_k(n') - \tau(n')C_k(n)}{\tau(m)} &= \tau(p^{a+1})C_k(n') - \tau(p^a q)C_k(n) \quad \text{by multiplicativity of } \tau \\
&= (a+2)C_k(mp^a q) - (2a+2)C_k(mp^{a+1}) \\
&= (a+2)\sum_{i=0}^{a}\sum_{j=0}^{1} C_{k-i-j}(m) - (2a+2)\sum_{i=0}^{a+1} C_{k-i}(m) \\
&= 2\sum_{i=1}^{a} C_{k-i}(m) - a(C_k(m) + C_{k-a-1}(m)) \\
&\geq 2a\Big(\min_{1\leq i\leq a} C_{k-i}(m) - \max\{C_k(m), C_{k-a-1}(m)\}\Big). \qquad (25)
\end{aligned}$$

By Lemma 3.18, to compute the minimum and maximum indicated above, we can simply compare distances from the subscripts $k-i$ to $\Omega(m)/2$. We have

$$\left|k - i - \frac{\Omega(m)}{2}\right| = \left|\left\lfloor\frac{\Omega(n)}{2}\right\rfloor - i - \frac{\Omega(n)-a-1}{2}\right| = \begin{cases} |a/2 - i| & \text{if } 2 \nmid \Omega(n), \\ |(a+1)/2 - i| & \text{if } 2 \mid \Omega(n). \end{cases}$$

For the case $2 \nmid \Omega(n)$,

$$\max_{1\leq i\leq a}\left|\frac{a}{2} - i\right| = \frac{a}{2} = \min_{i=0,a+1}\left|\frac{a}{2} - i\right|.$$

For the case $2 \mid \Omega(n)$,

$$\max_{1\leq i\leq a}\left|\frac{a+1}{2} - i\right| = \frac{a-1}{2} < \frac{a+1}{2} = \min_{i=0,a+1}\left|\frac{a}{2} - i\right|.$$

So either way, the final expression in (25) is nonnegative by Lemma 3.18, implying $\tau(n)C_k(n') - \tau(n')C_k(n) \geq 0$. This rearranges to give (24) as desired. □

4. Proof of Theorem 1.4

4.1. **Computer-assisted proof.** Further reduction to the preliminary bound of $p > 10^{532}$ from Corollary 2.5 can now be obtained with maximal divisors. We aim to determine more precisely the minimal value of p needed to guarantee the first interval in Theorem 3.14 is empty. The second interval in Theorem 3.2 is ignored – it is empty for $p > 10^{40}$ as shown in the proof of Corollary 2.5. This is much smaller than what we might hope to work for the first interval.

Let us give an intuitive outline of how Algorithm 1 works. Recalling Theorem 3.2, the first interval is empty precisely when $81M_d^4 < 8\sqrt{2p}$. To determine when this occurs we need upper bounds on

$$M_d \coloneqq |\mathcal{M}_d(p-1) \cup \mathcal{M}_d(p+1)|$$

for varying d and $p < 10^{532}$. There are roughly 10^{529} such primes, so of course we cannot hope to treat them individually. Instead we apply Theorem 3.14, which says we can obtain bounds on M_d by bounding $|\mathcal{M}_d(n)|$ for all reduced n between $p-1$ and $4(p+1)-6 = 4p-2$. There are roughly 10^8 reduced numbers less than 10^{532}, which is much more manageable.

For a reduced number n, Algorithm 1 finds a series of increasingly better bounds on $2|\mathcal{M}_x(n)|$ (the "2" accounts for $p-1$ and $p+1$) until hopefully the first interval in Theorem 3.2 is verified to be empty. The first of these bounds is from Theorem 3.21, and can be computed in negligible time. If this fails, the algorithm proceeds to the more computationally expensive bound of $C_k(n)$ with $k = \lfloor\Omega(n)/2\rfloor$. This may fail too, but if $M_d < C_k(n)$, we realize from the first inequality in Theorem 3.2 that a bound on M_d is only really needed for $d < 81C_k(n)^3/4$. For such divisors, $\Omega(d)$

may never reach $\lfloor \Omega(n)/2 \rfloor$, meaning Lemma 3.19 allows us to decrease k and recompute a potentially smaller bound, still of the form $C_k(n)$. This process can be repeated until $81C_k(n)^3/4 \leq 2\sqrt{p}/C_k(n)$, which successfully demonstrates that the first interval in Theorem 3.2 is empty, or until k can no longer be decreases, which is a failure.

Algorithm 1: Connectivity test for Markoff mod-p graphs for all primes in a given interval.

Input: $A, B \in \mathbb{N}$ defining the range $(A, B]$ in which primes are tested
Output: updated A so that $\mathcal{G}_p$ is connected if $A < p \leq B$

```
1  for reduced n from 4B − 2 to A do                    ▷ see Algorithm 2 and Remark 4.6
2      k ← ⌊Ω(n)/2⌋                                     ▷ 2C_k(n) bounds M_d from Theorem 3.2
3      if 2^{8Ω(n)}(n + 2) < 8(3·binom(Ω(n), k)·τ(n))^8 then   ▷ avoid C_k(n) and Algorithm 3 if possible
4          while n + 2 < 8(3C_k(n))^8 do                ▷ Theorem 3.2's first interval not empty...
5              j ← max{Ω(d) : d | n, d < 162C_k(n)^3}
6              if j ≥ k then                            ▷ ...and it never will be
7                  A ← max{A, n + 1}                    ▷ connectivity test failed for p ≤ A
8                  break while loop
9              k ← j
10 return A                                             ▷ empty first interval for A < p ≤ B
```

Remark 4.1. The smallest reduced n for which line 7 is never called is $(173\#)^2/4 = 6.938\ldots \cdot 10^{153}$. So if the input A, B satisfies $A < B < 10^{153}$, say, then line 7 makes the output A' larger than every reduced number between B and $4B - 2$. (There is at least one by Theorem 3.2.) Thus the output interval $(A', B]$ is empty. Since 10^{153} exceeds 10^{40} from (10), the second interval in Theorem 3.2 is ignored in Algorithm 1 and the proof below.

Theorem 4.2. *If A, B are input into Algorithm 1 and A' is output, then $\mathcal{G}_p$ is connected for $A' < p \leq B$.*

Proof. Suppose p is a prime for which $\mathcal{G}_p$ is not connected. Assuming $A < p \leq B$, we must show that p is at most the output A'. By Theorem 3.2, there must be some divisor, call it $d_0 \in \mathcal{D}(p+1) \cup \mathcal{D}(p-1)$, that satisfies

$$\frac{2\sqrt{2p}}{M_{d_0}} < d_0 < \frac{81M_{d_0}^3}{4}, \tag{26}$$

where $M_{d_0} = |\mathcal{M}_{d_0}(p-1) \cup \mathcal{M}_{d_0}(p+1)|$. In particular, comparing either end of the chain of inequalities above, we see that

$$128p < (3M_{d_0})^8. \tag{27}$$

Let $n_\pm$ be the reduced integers provided by Theorem 3.14 for $p \pm 1$. According to Theorem 3.14,

$$p \pm 1 \leq n_\pm \leq 4(p \pm 1) - 6 \leq 4p - 2, \tag{28}$$

which in turn gives $A \leq n_\pm \leq 4B - 2$ since $A < p \leq B$. So at some point(s) in Algorithm 1's **for** loop, "n" will assume the value of n_- and n_+.

Assume without loss of generality that $|\mathcal{M}_{d_0}(n_+)| \geq |\mathcal{M}_{d_0}(n_-)|$. Then

$$\begin{aligned} n_+ + 2 &\leq 4p \quad \text{by (28)} \\ &< \frac{(3M_{d_0})^8}{32} \quad \text{by (27)} \\ &\leq \frac{1}{32}(3|\mathcal{M}_{d_0}(p-1)| + 3|\mathcal{M}_{d_0}(p+1)|)^8 \\ &\leq \frac{1}{32}(3|\mathcal{M}_{d_0}(n_-)| + 3|\mathcal{M}_{d_0}(n_+)|) \quad \text{by Theorem 3.14} \\ &\leq \frac{1}{32}(6|\mathcal{M}_{d_0}(n_+)|)^8 \quad \text{by assumption} \\ &\leq 8\left(\frac{3\tau(n_+)}{2^{\Omega(n_+)}}\binom{\Omega(n_+)}{\lfloor \Omega(n_+)/2 \rfloor}\right)^8 \quad \text{by Theorem 3.21} \end{aligned} \tag{29}$$

Therefore the **if** condition in line 3 is satisfied by n_+ (or n_- if $|\mathcal{M}_{d_0}(n_-)| \geq |\mathcal{M}_{d_0}(n_+)|$ instead).

To help determine the output of the **while** loop, call $k \in \mathbb{N}$ *sufficiently large* if it is at least as close to $\Omega(n_+)/2$ as anything between $\min\{\Omega(d) : d \in \mathcal{M}_{d_0}(n_+)\}$ and $\max\{\Omega(d) : d \in \mathcal{M}_{d_0}(n_+)\}$. Lemmas 3.18 and 3.19 tell us that

$$|\mathcal{M}_{d_0}(n_\pm)| \leq C_k(n_\pm) \tag{30}$$

for such k. By using this bound in (29) instead of the one provided by Theorem 3.21, the same chain of inequalities tells us $n_+ + 2 < 3(3C_k(n_+))^8$. So the **while** loop condition in line 3 is always satisfied if k is sufficiently large.

Now, by induction on the number of **while** loop iterations completed for n_+, the value of k used in line 4 is always sufficiently large. Indeed, the base case holds by line 2. For the induction step we assume j in line 5 is less than k, since otherwise line 8 breaks the **while** loop and no more induction is needed. We have

$$\begin{aligned} j &= \max\{\Omega(d) : d \,|\, n_+,\, d < 162C_k(n_+)^3\} \\ &\geq \max\{\Omega(d) : d \,|\, n_+,\, d < 81M_{d_0}^3/4\} \quad \text{by induction hypothesis and (30)} \\ &\geq \max\{\Omega(d) : d \,|\, n_+,\, d \leq d_0\} \quad \text{by (26)} \\ &= \max\{\Omega(d) : d \,|\, n_+,\, d \in \mathcal{M}_{d_0}(n_+)\}. \end{aligned}$$

But $j < k \leq \Omega(n_+)/2\rfloor$, so j is sufficiently large. Line 9 then completes the induction proof.

We have shown that the **while** loop condition in line 4 is always satisfied for n_+ (or n_- if $|\mathcal{M}_{d_0}(n_-)| \geq |\mathcal{M}_{d_0}(n_+)|$). As k cannot decrease indefinitely, the output of Algorithm 1 satisfies $A' \geq n_\pm + 1 \geq p$ by line 7. □

Finally, we use Algorithm 1 to produce our main result.

Theorem 1.4. *$\mathcal{G}_p$ is connected for all primes $p > (863\#)(53\#)(13\#)(7\#)(5\#)3^3 2^5 \approx 3.45 \cdot 10^{392}$.*

Proof. By Corollary 2.5, we need only check connectivity for primes less than 10^{532}. When $A = 2$ and $B = 10^{532}$ are input into Algorithm 1, the output is $(863\#)(53\#)(13\#)(7\#)(5\#)3^3 2^5 + 1$. Since this number is not prime, the "+1" has been omitted in the theorem statement. □

Let us examine what occurs during the execution of Algorithm 1 when it encounters the eventual output $n = (863\#)(53\#)(13\#)(7\#)(5\#)3^3 2^5$. We have $\Omega(n) = 187$, so line 2 sets $k = \lfloor 187/2 \rfloor = 93$. The **if** condition in line 3 does not stop n since

$$2^{8(187)}(n+2) = 9.448\ldots \cdot 10^{841} < 3.638\ldots \cdot 10^{842} = 8\Big(3\binom{187}{93}\tau(n)\Big)^8.$$

So we move to line 4, where the forthcoming Algorithm 3 computes

$$C_{93}(n) = 3013671869689423302959704266406116383317724743440 = 3.013... \cdot 10^{48}.$$

This inequality comes closer:

$$n + 2 = 3.448... \cdot 10^{392} < 3.571... \cdot 10^{392} = 3(3C_{93}(n))^8,$$

but it is still a failure. After n passes line 4, there is hope that k might decrease in line 9, providing a second chance to achieve $n + 2 \geq 8(3C_k(n))^8$. However, looking at line 5, the divisor $d = (281\#)(53\#)(13\#)(7\#)(5\#)3^3 2^5$ satisfies

$$d = 1.312... \cdot 10^{146} < 4.434... \cdot 10^{147} = 162C_{93}(n)^3,$$

and it determines the value of j to be $\Omega(d) = 97$. Since this is at least 93, line 7 is called, and the value of A increases accordingly.

4.2. **Algorithm implementation.** In this section we elaborate on the subroutines required to implement Algorithm 1. The most complicated subroutine is enumerating reduced numbers. This is achieved by Algorithm 2 below, which constructs prime factorizations that satisfy Definition 3.11. In particular, since Algorithm 2 outputs numbers with known prime factorizations, lines 2, 3, and 5 of Algorithm 1 are straightforward to execute and require negligible time. This leaves only line 4 of Algorithm 1 to be addressed – the computation of $C_k(n)$, for which Algorithm 3 can be found at the end of this section.

Algorithm 2: Find all reduced integers (and their prime factorizations) below some bound.

Input: $A, B \in \mathbb{N}$ defining the search range $(A, B]$ for reduced numbers
Output: all reduced numbers $n \in (A, B]$ and/or the factorization of n into primorials.

1 $\mathbf{v} = (v_1, v_2, ..., v_\ell) \leftarrow (1 + \max\{i : p_i\# \leq 2b\})$ ▷ vector of length ℓ ($\ell = 1$ for now)
2 $n \leftarrow p_{v_1}\#/2$ ▷ will always have $n = \prod_i (p_{v_i}\#/2)$
3 **while** $\ell \geq 1$ and $A < 8p_{v_1+1}^{2v_1}$ **do** ▷ i.e. while $\mathbf{v}$ is nonempty and v_1 is not too small
4 $\quad n \leftarrow n/p_{v_\ell}$
5 $\quad v_\ell \leftarrow v_\ell - 1$
6 $\quad$ **while** $v_\ell \geq 2$ **do**
7 $\quad\quad j \leftarrow \max\{i : i \leq v_\ell, n(p_i\#) \leq 2b\}$ ▷ potential next entry for $\mathbf{v}$
8 $\quad\quad k \leftarrow 1$
9 $\quad\quad$ **while** $k \leq \ell$ **do** ▷ test if $n(p_j\#)/2$ is reduced
10 $\quad\quad\quad$ **if** $\lfloor(\ell + 2)/(k + 1)\rfloor \log p_j \geq \log p_{v_k+1}$ **then** ▷ test failed
11 $\quad\quad\quad\quad k \leftarrow 0$ ▷ reset **while** loop to test $j - 1$
12 $\quad\quad\quad\quad j \leftarrow j - 1$
13 $\quad\quad\quad$ **if** $j = 1$ **then**
14 $\quad\quad\quad\quad$ **break** line 9 **while** loop ▷ skip to line 16
15 $\quad\quad\quad k \leftarrow k + 1$
16 $\quad\quad n \leftarrow n(p_j\#)/2$
17 $\quad\quad$ append j to the end of $\mathbf{v}$ ▷ ℓ increases by 1 accordingly
18 $\quad$ delete v_ℓ ▷ ℓ decreases by 1 accordingly
19 $\quad a_1 \leftarrow \max\{0, 1 + \lfloor\log_2 A/n\rfloor\}$ ▷ output must satisfy $2^{a_1} n > a$
20 $\quad$ **while** $a_1 \leq \lfloor\log_2(\min\{8p_{v_1+1}^2, B/n\})\rfloor$ **do** ▷ also need $2^{a_1} n \leq b$ and reduced
21 $\quad\quad$ **output** $2^{a_1} n$ and/or $\mathbf{v}, a_1$
22 $\quad\quad a_1 \leftarrow a_1 + 1$
23 **return** ▷ all output occurs in line 21

Lemma 4.3. *Let $\ell \geq 1$ and $v_1 \geq \cdots \geq v_\ell \geq 2$. Set $n = \prod_{i=1}^{\ell} \frac{p_{v_i}\#}{2}$. We have the following:*

(a) *If n is reduced, then so is n/p_{v_ℓ}.*

(b) *If n is reduced, then $n(p_{v_{\ell+1}}\#)/2$ is reduced for some $v_{\ell+1} \leq v_\ell$ if and only if*

$$\left\lfloor \frac{\ell+2}{k+1} \right\rfloor < \frac{\log p_{v_k+1}}{\log p_{v_{\ell+1}}}$$

for all $k = 1, ..., \ell$.

(c) *If n is not reduced, then neither is $n(p_{v_{\ell+1}}\#/2)\cdots(p_{v_{\ell'}}\#/2)$ for any $v_{\ell+1}, ..., v_{\ell'} \leq v_\ell$.*

Proof. Let $n = 3^{a_2}5^{a_3}\cdots$, and for part (a), let $n' = n/p_{v_\ell} = 3^{a'_2}5^{a'_3}\cdots$. So $a_i = a'_i$ for all $i \neq v_\ell$, and $a_{v_\ell} - 1 = a'_{v_\ell}$. We must verify that n' still satisfies the inequality of Definition 3.11:

$$\left\lfloor \frac{a'_i+1}{a'_j+2} \right\rfloor < \frac{\log p_j}{\log p_i} \tag{31}$$

for all $i, j \geq 2$. First, since n' is still a product of primorials up to a power of 2:

$$n' = \frac{p_{v_\ell-1}\#}{2} \prod_{i=1}^{\ell-1} \frac{p_{v_i}\#}{2}, \tag{32}$$

we see that $a'_2 \geq a'_3 \geq \cdots$. Thus $a'_i \leq a'_j$ whenever $i \geq j$, making the left side of (31) equal 0, so the inequality holds trivially. Thus we need only consider the case $i < j$. (This observation also applies to parts (b) and (c) of the lemma.) Furthermore, the only exponent of n that has changed is a_{v_ℓ}, so we may restrict to the cases $i = v_\ell$ and $j = v_\ell$. If $2 \leq i < j = v_\ell$, then from (32) and the assumption $2 \leq v_\ell \leq \cdots \leq v_1$, we see that $a'_i = \ell$ and $a'_j = \ell - 1$. This gives

$$\left\lfloor \frac{a'_i+1}{a'_j+2} \right\rfloor = \left\lfloor \frac{\ell+1}{\ell+1} \right\rfloor = 1 < \frac{\log p_j}{\log p_i}.$$

If $2 \leq j < i = v_\ell$, then

$$\begin{aligned} \left\lfloor \frac{a'_i+1}{a'_j+2} \right\rfloor &= \left\lfloor \frac{(a_{v_\ell}-1)+1}{a_j+2} \right\rfloor \quad \text{(recall how } a_i \text{ and } a'_i \text{ are related)} \\ &\leq \left\lfloor \frac{a_{v_\ell}+1}{a_j+2} \right\rfloor \\ &< \frac{\log p_j}{\log p_{v_\ell}} = \frac{\log p_j}{\log p_i} \quad \text{since } n \text{ is reduced.} \end{aligned}$$

Thus n' is reduced as claimed.

For part (b), let $n' = n(p_{v_{\ell+1}}\#)/2 = 3^{a'_2}5^{a'_3}\cdots$. So $a_i = a'_i$ for all $i > v_{\ell+1}$, and $a_i + 1 = a'_i$ for all $2 \leq i \leq v_{\ell+1}$. As in part (a), to check if n' is reduced we need only verify (31) when $i < j$. If $v_{\ell+1} < i < j$ then (31) holds because $a'_i = a_i$ and $a'_j = a_j$, and n is reduced. If $i < j \leq v_{\ell+1}$, then $a'_i = a'_j = \ell + 1$. So (31) holds because the left side equals 0. The only case remaining is $i \leq v_{\ell+1} < j$. Again $a'_i = \ell + 1$, but now $a'_j = k - 1$, where k is the smallest index such that $j > v_k$. Thus

$$\left\lfloor \frac{a'_i+1}{a'_j+2} \right\rfloor = \left\lfloor \frac{\ell+2}{k+1} \right\rfloor \quad \text{and} \quad \frac{\log p_{v_k+1}}{\log p_{v_{\ell+1}}} \leq \frac{\log p_j}{\log p_i}.$$

Comparing to the inequality in (b) completes its proof.

Part (c) follows by induction on ℓ' provided we verify the claim for $\ell' = \ell + 1$. So let n' and $a'_2, a'_3, ...$ be as in the proof of (b). Also let i and j be indices for which n fails the inequality in Definition 3.11, meaning

$$\left\lfloor \frac{a_i + 1}{a_j + 2} \right\rfloor \geq \frac{\log p_j}{\log p_i}. \tag{33}$$

As we have already noted, this implies $i < j$. Furthermore, it cannot be that $j \leq v_{\ell+1}$, since then $v_{\ell+1} \leq v_\ell$ implies $a'_i = a'_j = \ell + 1$, rendering (33) impossible. Therefore $j > v_{\ell+1}$, which gives $a'_j = a_j$. Since $a'_i \geq a_i$, the left-hand side of (33) could only increase with a_i and a_j replaced by a'_i and a'_j. Thus n' is not reduced. □

The next lemma justifies the inequality involving A in line 3, whose purpose is to avoid wasting time searching prime factorizations that cannot possibly be reduced.

Lemma 4.4. *If $n = 2^{a_1}3^{a_2}\cdots$ is reduced and $a_j = 0$ for some j, then $n < 8p_j^{2j-2}$.*

Proof. If n is reduced Lemma 3.12 tells us that $a_i = 0$ for all $i \geq j$. According to Definition 3.11, we also have $2^{a_1} < 8p_j^2$ and $a_i/2 \leq \lfloor (a_i + 1)/2 \rfloor < \log p_j / \log p_i$ if $2 \leq i < j$. The latter implies $p_i^{a_i} < p_j^2$. So altogether, $n = 2^{a_1}3^{a_2}\cdots p_{j-1}^{a_{j-1}} < 8p_j^2 p_j^2 \cdots p_j^2 = 8p_j^{2j-2}$. □

Theorem 4.5. *For inputs A and B, Algorithm 2 outputs n if and only if $A < n \leq B$ and n is reduced.*

Proof. If an odd number $n = 3^{a_2}5^{a_3}\cdots$ (with $a_i = 0$ for sufficiently large i) is such that $a_2 \geq a_3 \geq \cdots$, then there exist $v_1 \geq v_2 \geq \cdots$ such that

$$n = \prod_{i \geq 1} \frac{p_{v_i}\#}{2}$$

(with $v_i = 1$ for sufficiently large i). Call this vector $\mathbf{v}_n = (v_1, v_2, ...)$. By Lemma 3.12, all reduced numbers correspond to such a vector. These are essentially the vectors $\mathbf{v}$ produced in Algorithm 2, though an infinite tail of 1's has been appended for convenience. We will prove that Algorithm 2 outputs all such vectors (for reduced $n \in (A, B]$) from largest to smallest under the lexicographic order: $\mathbf{v} > \mathbf{v}'$ if $v_i > v'_i$, where i is the smallest index such that $v_i \neq v'_i$.

Remark first that our convention of empty vector entries being treated as 1 rather than 0 is maintained in Algorithm 2. Indeed, the **while** loop in line 6 does not terminate until $\mathbf{v}$ has a single 1 at its end (if $\mathbf{v}$ already ended in a 1, the loop never even begins), which is immediately deleted in line 18. Thus line 5 never results in $v_\ell = 0$.

Now, suppose at the start of a line 3 **while** loop iteration, "$\mathbf{v}$" is equal to some $\mathbf{v}_n = (v_1, v_2, ...)$ with n reduced (note for the very first iteration that n is indeed reduced by line 2 and Lemma 3.13). We claim that this **while** loop iteration ends with "$\mathbf{v}$" assuming the value of a new vector $\mathbf{v}_{n'} = (v'_1, v'_2, ...)$ that is maximal under the stipulations that $\mathbf{v}_{n'} < \mathbf{v}_n$, $n' \leq B$, and n' is odd and reduced. Throughout the remainder of the proof, ℓ is fixed as its initial value in the **while** loop iteration under consideration.

First, the fact that n' is reduced follows from applying Lemma 4.3 (a) to line 4 and comparing the **if** condition in line 10 to the inequality in Lemma 4.3 (b).

To see that $\mathbf{v}_{n'} < \mathbf{v}_n$, observe that $v_1 = v'_1, ..., v_{\ell-1} = v'_{\ell-1}$ and $v_\ell - 1 = v'_\ell$ according to line 5 – the lexicographic ordering does not consider subsequent entries.

Next, $n' \leq B$ follows from the definition of j in line 7 and the observation that the **while** loop in line 9 could only decrease j.

Finally, let us check the maximality of $\mathbf{v}_{n'}$. Assume by way of contradiction that there exists an odd reduced number $n'' \leq B$ such that $\mathbf{v}_{n'} < \mathbf{v}_{n''} < \mathbf{v}_n$. Let $\mathbf{v}_{n''} = (v''_1, v''_2, ...)$. Since $v_1 =$

$v'_1, ..., v_{\ell-1} = v'_{\ell-1}$ and $v_\ell - 1 = v'_\ell$, the only way to achieve $\mathbf{v}_{n'} < \mathbf{v}_{n''} < \mathbf{v}_n$ is for $v'_1 = v''_1, ..., v'_\ell = v''_\ell$. So let $i_0 > \ell$ be the smallest index such that $v'_{i_0} \neq v''_{i_0}$, and set

$$m = \prod_{i=1}^{i_0-1} \frac{p_{v'_i}\#}{2}.$$

Again we compare the **if** condition in line 10 to Lemma 4.3 (b) in order to conclude that v'_{i_0} is the largest integer that does not exceed v'_{i_0-1} and makes $m(p_{v'_{i_0}}\#)/2$ reduced and bounded by B. As $m(p_{v''_{i_0}}\#)/2 \leq n'' \leq B$ and $v'_{i_0} < v''_{i_0} \leq v''_{i_0-1} = v'_{i_0-1}$, we conclude that $m(p_{v''_{i_0}}\#)/2$ must not be reduced by maximality of v'_{i_0}. But then Lemma 4.3 (c) tells us n'' is also not reduced, which is a contradiction.

This proves that Algorithm 2 finds all odd reduced $n \leq B$ from largest to smallest with respect to the lexicographic order on $\mathbf{v}_n$, provided the bound $A < 8p_{v_1+1}^{2v_1}$ from line 3 is met. But Lemma 4.4 says that this bound only eliminates reduced numbers that do not exceed A, which we have no intent to find. To complete the proof of the theorem, note that the exponent range for a_1 in line 20 matches the bound on a_1 in Definition 3.11. □

Remark 4.6. The most efficient ordering for n in the **for** loop of Algorithm 1 is largest to smallest. This way no time is wasted on testing reduced integers that end up being less than the output. We saw in the previous proof, however, that Algorithm 2 outputs n in decreasing lexicographic order of $\mathbf{v}_n$. But there is no need to reorder. It is also efficient to simply insert lines 2–9 of Algorithm 1 into line 21 of Algorithm 2. Indeed, under this setup and with inputs $A = 2$ and $B = 10^{532}$, the combined algorithm encounters a total of 124,720,785 reduced numbers, only 48,066 of which are less than the eventual output of $(863\#)(53\#)(13\#)(7\#)(5\#)3^3 2^5$.

Our next and last subroutine computes $C_k(n)$. To do this, Algorithm 3 uses the recursion

$$C_i(n' p_h^{a_h}) = \sum_{j=i-a_h}^{i} C_j(n')$$

(which holds provided $p_h \nmid n'$) repeatedly, adding prime power factors one at a time until the input n is reached. Comparing the summation range of j above to that of j in line 6 below, the additional range restriction is simply the observation that $C_j(n') = 0$ if $j < 0$ or $j > \Omega(n')$. Algorithm 3 saves some time in line 2 by using binomial coefficients to account for all primes of multiplicity 1. (Recall that if n is a product of distinct primes, $C_k(n) = \binom{\Omega(n)}{k}$.) This is effective for our purpose since most reduced numbers are "nearly primorial." And finally, note that line 5 is careful to only compute $C_i(n' p_h^{a_h})$ for those i that are necessary to find $C_k(n)$.

Algorithm 3: Compute $C_k(n)$ for some $n \in \mathbb{N}$.

Input: $k, n \in \mathbb{N}$ with $n = 2^{a_1} 3^{a_2} \cdots$
Output: $C_k(n)$

1 $t \leftarrow |\{h : a_h = 1\}|$ ▷ count multiplicity 1 primes
2 $C_0, ..., C_t \leftarrow \binom{t}{0}, ..., \binom{t}{t}$ ▷ if, for example, $t = \Omega(n)$ then $C_k(n) = \binom{m}{k}$
3 **for** h such that $a_h \geq 2$ **do**
4 $\quad t \leftarrow t + a_h$ ▷ grows until $t = \Omega(n)$
5 $\quad$ **for** i from $\max\{0, t + k - \Omega(n)\}$ to $\min\{k, t\}$ **do** ▷ only find needed coefficients
6 $\quad\quad D_i \leftarrow \sum C_j$ for $\max\{0, i - a_h\} \leq j \leq \min\{i, t - a_h\}$ ▷ don't replace C_i until done
7 $\quad$ **for** i from $\max\{0, t + k - \Omega(n)\}$ to $\min\{k, t\}$ **do**
8 $\quad\quad C_i \leftarrow D_i$ ▷ now ok to update
9 **return** C_k

5. Data on Connectivity

Aside from justifying Algorithm 1, Theorem 3.2 also provides a method for verifying connectivity of $\mathcal{G}_p$ for a given prime p. Previously, proving connectivity for $\mathcal{G}_p$ has been done in [CL20] for primes less than 3000 by computing the adjacency matrix of the graph. Due to the large amount of memory required by this method, it has limitations as to how large a prime it could handle. Most likely one could not prove connectivity for primes larger than a few thousand using this method. Our algorithm, on the other hand, is specifically catered towards larger primes (and, indeed, is inconclusive for nearly all the primes handled in [CL20]). In this section, we prove connectivity for many more primes and explore how powerful our method is regarding the size of a primes that it can handle.

We programmed the two conditions of Theorem 3.2 and performed an exhaustive search over all primes less than 10^7 that satisfy these conditions. We found that Theorem 3.2 proves connectivity for $p = 3, 7, 101$ and then the next prime is on the order of 10^6, given by

$$p = 1,327,363.$$

After finding this first prime with a connected Markoff mod-p graph that was not handled by [CL20], we tackled two collections of primes: the first 10000 primes greater than 10^n and 10000 "random" primes between 10^n and 10^{n+1} for $8 \leq n \leq 35$. By random primes, we mean that we take 10000 numbers between 10^n and 10^{n+1} chosen uniformly at random, and then for each number find the first prime greater than it.

n	$q_{1000}(10^n)$	$q_{10000}(10^n)$	$r_{10000}(10^n)$
8	21.3%	20.22%	38.12%
9	48.1%	49.04%	67.46%
10	76.1%	76.41%	87.05%
11	90.9%	90.78%	95.33%
12	96.6%	97.10%	98.29%
13	98.8%	98.65%	99.11%
14	99.4%	99.44%	99.52%
15	99.7%	99.74%	99.83%
16	99.7%	99.88%	99.88%
17	99.9%	99.93%	99.95%
18	100%	99.97%	100%
19	100%	99.97%	99.97%
20	99.8%	99.97%	100%
21	100%	99.99%	99.99%

n	$q_{1000}(10^n)$	$q_{10000}(10^n)$	$r_{10000}(10^n)$
22	100%	100%	100%
23	100%	100%	100%
24	100%	100%	100%
25	100%	100%	100%
26	100%	100%	100%
27	100%	100%	100%
28	100%	100%	100%
29	100%	100%	100%
30	100%	100%	100%
31	100%	100%	100%
32	100%	100%	100%
33	100%	100%	100%
34	100%	100%	100%
35	100%	100%	100%

Table 2. For each value of $8 \leq n \leq 35$, we calculate the two quantities $q_m(10^n)$ and $r_m(10^n)$. $q_m(10^n)$ denotes the percentage of the first m primes after 10^n for which Theorem 3.2 guarantees connectivity of $\mathcal{G}_p$ and $r_m(10^n)$ denotes the percentage of m random primes between 10^n and 10^{n+1} for which Theorem 3.2 guarantees connectivity of $\mathcal{G}_p$.

Beginning at $n = 31$ in the table above, the value of M_d in Theorem 3.2 can be replaced with $\tau(p-1)+\tau(p+1)$ (which can be computed quickly for primes up to at least 10^{90}), and there is still no value of d satisfying either of the inequalities for the 10,000 random primes we tested between 10^n and 10^{n+1}. That is, 10^{31} is roughly where the Erdös-Kac theorem takes over—the expected value of $\tau(p \pm 1)$ is small enough so that it becomes extremely rare to need the improvement that comes by considering maximal divisors rather than all divisors.

Example of Inconclusiveness: Theorem 3.2 guarantees connectedness of the Markoff mod p graph given that no divisor d of $p \pm 1$ satisfies $\frac{2\sqrt{2p}}{M_d} < d < \frac{81M_d^3}{4}$ or $\frac{p}{6M_d} < d < \frac{8\sqrt{p}(p\pm1)\tau(p\pm1)}{\phi(p\pm1)}$. From Table 2, we see that once we are on the order of 10^{21}, Theorem 3.2 captures almost all primes p. However there are still some exceptional cases where this theorem is inconclusive.

For the first 10,000 primes greater than 10^{21}, there is a single prime p' that does not pass these two criteria, $p' = 1,000,000,000,000,000,124,399$. We have

$$p' - 1 = 2 \cdot 7 \cdot 13 \cdot 29^2 \cdot 43 \cdot 705,737 \cdot 215,288,719$$

$$p' + 1 = 2^4 \cdot 3 \cdot 5^2 \cdot 11^2 \cdot 17 \cdot 19 \cdot 23 \cdot 97 \cdot 757 \cdot 1,453 \cdot 8,689$$

$$\text{Number of divisors of } p' \pm 1 = \tau(p-1) + \tau(p+1) - 2 = 192 + 11,520 - 2 = 11,710$$

$$\text{Number of divisors of } p' \pm 1 \text{ which fail either bound of Theorem 3.2} = 989$$

The largest value that $M_d = |\mathcal{M}_d(p'-1) \cup \mathcal{M}_d(p'+1)|$ attains as d varies over the 989 divisors of $p' \pm 1$ that fail one of the bounds in Theorem 3.2 is 438. An example of a divisor d with $M_d = 438$ is $d = 1,664,125,969$. For this divisor we have

$$\frac{2\sqrt{2p'}}{438} \approx 2.042 \times 10^8 < d \approx 1.664 \times 10^9 < 1.702 \times 10^9 \approx \frac{81 \cdot 438^3}{4}.$$

Note that $\frac{p'}{6M_d} \approx 3.80518 \times 10^{17}$, $\frac{8\sqrt{p'}(p'+1)\tau(p'+1)}{\phi(p'+1)} \approx 1.427 \times 10^{16}$, and $\frac{8\sqrt{p'}(p'-1)\tau(p'-1)}{\phi(p'-1)} \approx 1.302 \times 10^{14}$ so there are no divisors that can ever satisfy the second bound of Theorem 3.2.

While examples like this become exceedingly rare, they persist throughout the range in which we are able to execute Theorem 3.2's test. Indeed, we have verified that our test fails for every prime $p < 10^{100}$ such that $p \pm 1$ is a reduced number as defined in 3.11. There are 591 such primes, and there are certainly many others for which our test also fails, just not enough to be picked up by our random samples of 10,000.

6. Appendix

In this section, we make more precise some of the implied constants in the proof of the following proposition in [BGS16b]. The point of this is to determine exactly how large an order a triple must have in order to conclude that it is connected to $\mathcal{C}_p$ as in the End Game in [BGS16b].

Proposition 6.1 (Explicit version of Proposition 7 in [BGS16b])**.** *For d dividing $p-1$ or $p+1$, a Markoff triple of order d belongs to $\mathcal{C}_p$ provided*

$$d > \frac{8\sqrt{p}(p \pm 1)\tau(p \pm 1)}{\phi(p \pm 1)} \tag{34}$$

(where the $\pm$ is determined by whether d divides $p-1$ or $p+1$).

Proof. Without loss of generality, let d be the first coordinate order of some Markoff triple, and recall notation from (3). In Proposition 7 of [BGS16b], Bourgain, Gamburd, and Sarnak show that if d is sufficiently large (at least $p^{1/2+\delta}$ for some $\delta > 0$ depending on p), then either the second or third coordinate in the orbit

$$\left(r + r^{-1}, \frac{(r+r^{-1})(r^{2n}s + r^{-2n}s^{-1})}{r - r^{-1}}, \frac{(r+r^{-1})(r^{2n\pm1}s + r^{2n\pm1}s^{-1})}{r - r^{-1}}\right)$$

has order $p-1$ for some n. We will run through their argument and show that (34) is sufficient for the relevant inequalities to hold. Since every triple of order $p-1$ is in $\mathcal{C}_p$ (Proposition 6 in [BGS16b]), this will complete the proof.

First suppose $d \mid p-1$. We seek a solution $(x, y) \in \mathbb{F}_p^*$ to

$$\frac{(r+r^{-1})(sx + s^{-1}x^{-1})}{r - r^{-1}} = y + y^{-1} \tag{35}$$

such that x belongs to the cyclic subgroup of order d (generated by r in the notation above), and y is a primitive root modulo p. We will show such a solution exists with a counting argument.

Let $d' = (p-1)/d$, and given some e dividing $p-1$, let $e' = (p-1)/e$. Consider the equation

$$\frac{(r+r^{-1})(sx^{d'} + s^{-1}x^{-d'})}{r-r^{-1}} = y^{e'} + y^{-e'}. \tag{36}$$

Assume for the moment that $d' \geq e'$ so that the projective completion of the affine curve defined above is given by

$$\frac{s(r+r^{-1})}{r-r^{-1}} X^{2d'} Y^{e'} + \frac{r+r^{-1}}{s(r-r^{-1})} Y^{e'} Z^{2d'} - X^{d'} Y^{2e'} Z^{d'-e'} - X^{d'} Z^{d'+e'} = 0.$$

Call this curve C. Bourgain-Gamburd-Sarnak show that C is irreducible over $\overline{\mathbb{F}}_p$. Furthermore, its geometric genus is bounded from above by

$$\binom{\deg C - 1}{2} - \sum_{P \in C} \binom{m_P}{2},$$

where m_P denotes the multiplicity of the point P in C. (See Corollary 1 in Section 8.3 of [Ful69], for example.) Observe that $P = [0:1:0]$ has multiplicity $m_P = 2d' - e'$, so the genus is at most

$$\binom{2d' + e' - 1}{2} - \binom{2d' - e'}{2} = 4d'e' - 4d' - 2e' + 2.$$

Thus we can apply the Weil bound to conclude that the number of points on C over $\mathbb{F}_p$ differs from $p+1$ by at most $2(4d'e' - 4d' - 2e' + 2)\sqrt{p}$. Now let us exclude the points $[1:0:0]$, $[0:1:0]$, and $[0:0:1]$, which occur on C with multiplicities e', $2d' - e'$, and e', respectively. Then, via the map $[X:Y:Z] \mapsto ((X/Z)^{d'}, (Y/Z)^{e'})$, there is an $e'd'$-to-1 correspondence between the remaining points on C and solutions to (36) in which x belongs to the subgroup of order d and y to the subgroup of order e in $\mathbb{F}_p^*$. In particular, if $f(e)$ denotes the number of such solutions (x, y), then we have shown

$$|d'e' f(e) + (e' + (2d' - e') + e') - (p+1)| < 2(4d'e' - 4d' - 2e' + 2)\sqrt{p}.$$

This simplifies to the following slightly weaker form:

$$\left| f(e) - \frac{p+1}{d'e'} \right| < 8\sqrt{p}.$$

The exact same bound can be obtained in the case $e' > d'$ by swapping d' and e' throughout the argument and using the singular point $[1:0:0]$ instead of $[0:1:0]$ to bound the genus.

Let μ be the Möbius function and let ϕ be Euler's totient function. By inclusion-exclusion, the number of solutions to (36) in which x belongs to the cyclic group of order d and y is a primitive root is

$$\begin{aligned}
\sum_{e \,|\, p-1} \mu\left(\frac{p-1}{e}\right) f(e) &\geq \sum_{e' \,|\, p-1} \left(\mu(e') \frac{p+1}{d'e'} - 8\sqrt{p} \right) \\
&\geq \frac{p+1}{d'} \\
&= \frac{(p+1)\phi(p-1)}{d'(p-1)} - 8\sqrt{p}\,\tau(p-1) \\
&> \frac{d\phi(p-1)}{p-1} - 8\sqrt{p}\,\tau(p-1).
\end{aligned}$$

The last expression above is positive precisely when d satisfies (34).

A very similar argument works when $d \mid p+1$. But now $r \notin \mathbb{F}_p$, so a modification is needed in order to reapply the Weil bound over $\mathbb{F}_p$. Let $d' = (p+1)/d$. Instead of (35), we now count points on the curve

$$\sum_{i=0}^{\lfloor d'/2 \rfloor} \binom{d}{2i} x^{d'-2i}(1-x^2)^i = y^{e'} + y^{-e'},$$

where e' is still some divisor of $p-1$ (see equation (42) in [BGS16b]). The same singular points, $[0:1:0]$ when $d' \geq e'$ and $[1:0:0]$ when $e' \geq d'$, can be used to bound the genus of the curve above, and in fact we get an even smaller bound of $2d'e'$. The remainder of the proof is unchanged. □

References

[Bar91] Arthur Baragar. The Markoff equation and equations of Hurwitz. PhD thesis. Brown University, 1991.

[BGS16a] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff surfaces and strong approximation. *Comptes Rendus de l'Académie des Sciences* 354.2 (2016), pp. 131–135.

[BGS16b] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff surfaces and strong approximation, 1. arXiv:1607.01530. 2016.

[BS96] Eric Bach and Jeffrey Outlaw Shallit. Algorithmic number theory, Volume 1: Efficient algorithms. The MIT Press, 1996.

[Che20] William Chen. Nonabelian level structures, Nielsen equivalence, and Markoff triples. arXiv:2011.12940. 2020.

[CL20] Matthew de Courcy-Ireland and Seungjae Lee. Experiments with the Markoff Surface. *Experimental Mathematics* 31 (2020), pp. 216–244.

[CM21] Matthew de Courcy-Ireland and Michael Magee. Kesten-McKay law for the Markoff surface mod p. *Annales Henri Lebesgue* 4 (2021), pp. 227–250.

[CZ13] Pietro Corvaja and Umberto Zannier. Greatest common divisors of $u-1, v-1$ in positive characteristic and rational points on curves over finite fields. *Journal of the European Mathematical Society* 15.5 (2013), pp. 1927–1942.

[DEK51] Nicolaas Govert De Bruijn, Cornelia van Ebbenhorst Tengbergen, and D. Kruyswijk. On the set of divisors of a number. *Nieuw Archief voor Wiskunde* 23.2 (1951), pp. 191–193.

[Dus18] Pierre Dusart. Explicit estimates of some functions over primes. *The Ramanujan Journal* 45 (2018), pp. 227–251.

[Fuc+21] Elena Fuchs, Kristin Lauter, Matthew Litman, and Austin Tran. A Cryptographic Hash Function from Markoff Triples. *Mathematical Cryptology* 1.1 (2021), pp. 103–121.

[Ful69] William Fulton. Algebraic curves: An introduction to algebraic geometry. (Available at https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf). New York, New York: W.A. Benjamin, 1969.

[Kon+20] Sergei V. Konyagin, Sergey V. Makarychev, Igor E. Shparlinski, and Ilya V. Vyugin. On the structure of graphs of Markoff triples. *The Quarterly Journal of Mathematics* 71.2 (2020), pp. 637–648.

[Mar79] Andrey Markoff. Sur les formes quadratiques binaires indéfinies. *Mathematische Annalen* 15.3-4 (1879), pp. 381–406.

[MR96] Jean-Pierre Massias and Guy Robin. Bornes effectives pour certaines fonctions concernant les nombres premiers. *Journal de Théorie des Nombres de Bordeaux* 8.1 (1996), pp. 215–242.

[Nic88] Jean-Louis Nicolas. On highly composite numbers. *Ramanujan Revisited: Proceedings of the Centenary Conference*. Ed. by George E. Andrews. Cambridge, Massachusetts: Academic Press, 1988, pp. 216–244.

[Ram15] Srinivasa Ramanujan. Highly composite numbers. *Proceedings of the London Mathematical Society* 2.1 (1915), pp. 347–409.

[Wig07] Severin Wigert. Sur l'ordre de grandeur du nombre des diviseurs d'un entier. *Arkiv för Matematik* 3.18 (1907), pp. 1–9.