7-15-2015

Characterizing the properties of specific binomial coefficients in congruence relations

Tyler Robert Russ

Characterizing the Properties of Specific Binomial Coefficients in Congruence Relations

by

Tyler Russ

Thesis

Submitted to the Department of Mathematics

Eastern Michigan University

in partial fulfillment of the requirements

for the degree of

MASTER OF ARTS

in

Mathematics

Thesis Committee:

Andrew Wilfong, Ph.D., Chair

David Folk, Ph.D.

Jayakumar Ramanathan, Ph.D.

July 15, 2015

Ypsilanti, Michigan

Abstract

The number theoretic conjecture we examine in this paper originates when trying to construct a characterizable generating set for the complex cobordism polynomial ring. To date there is no efficient, universal method for characterizing such a generating set. Wilfong conjectures that smooth projective toric varieties can act as these generators [7]. Toric varieties are related to polytopes by a bijective correspondence. Studying the combinatorial structure of these polytopes is much more manageable than studying properties of toric varieties directly. This gives rise to the number theoretic conjecture considered here. A proof of this number theoretic conjecture would in turn prove the conjecture that smooth projective toric varieties provide a generating set for the complex cobordism polynomial ring. Here, we do not provide a complete proof of the number theoretic conjecture, rather we give more evidence to the conjecture, building on prior work of Wilfong and Parry.

Contents

Abstract ii
1. Introduction: Wilfong's Conjecture in Context 1
2. Propositions from Wilfong 9
3. Cases in which the Conjecture Holds 20
4. Generalization of Many Propositions and Lemmas of Section 2 23
5. Generalization: Two Prime Powers 37
6. Primes Far Apart: Partial Generalization of Theorem 19 40
7. Primes Close Together: Partial Generalizations 43
8. Conclusion 51
References 53

Characterizing the Properties of Specific Binomial Coefficients in Congruence Relations

1. Introduction: Wilfong's Conjecture in Context

The number theoretic conjecture we examine in this paper originates in the topological work of Andrew Wilfong [7]. In Wilfong's work on toric varieties, the question arises of constructing a characterizable generating set for the complex cobordism polynomial ring. To date there is no efficient, universal method for characterizing such a generating set. It is a primary conjecture in the work of Andrew Wilfong that a smooth projective toric variety for each generator is possible [7]. An algebraic variety is the solution set of a system of polynomial equations. A toric variety is an algebraic variety that has an added structure coming from a torus action. For more details refer to [1, 3]. A nice feature of toric varieties is that many of their topological properties stand in bijective correspondence to the combinatorial structure of the polytopes, which is more easily studied than the topological properties of toric varieties. One topological property of toric varieties that can be computed in terms of the combinatorics of polytopes includes determining whether or not toric varieties are polynomial generators of the complex cobordism ring, which leads to the number theory conjecture examined in this thesis.

To better understand the complex cobordism polynomial ring, we formally introduce cobordism.

Definition 1. (Additionally, refer to [5].) Two smooth compact n-dimensional manifolds M_1 and M_2 are cobordant if their disjoint union $M_1 \amalg M_2$ forms the boundary of an $n+1$-dimensional smooth manifold.

A cobordism of real manifolds consists of two n-dimensional manifolds connected by a smooth manifold of dimension $n+1$. We can visualize a cobordism using the following example. Consider the three circles defining the waist and the ankles of a pair of pants. The circles are disjoint. Taken together, these circles define the boundary of the surface of the pants. The material connecting these one-dimensional circles is the manifold defined by the cobordism, the two-dimensional surface of the pants.

The cobordism relation has many useful properties. One of its primary properties is that cobordism is an equivalence relation. A second key property is that the set of equivalence classes of cobordant manifolds forms a ring under disjoint union and cross product. The complex cobordism ring, denoted Ω_*^U, has a definition similar to cobordism of real manifolds. We modify the definition for complex cobordism since complex cobordism of two real n-dimensional manifolds would similarly require that a complex manifold of real dimension $n+1$ could be constructed with the manifolds of dimension n defining the boundaries of that manifold. However, complex spaces are always of even dimension, so the construction of a cobordism meeting this definition is not possible. Instead, we define a complex cobordism to be a cobordism of stably complex manifolds. This is a weakening of the condition for a manifold to be complex. There are odd-dimensional stably complex manifolds, so this construction provides a framework in which to define complex cobordism [6, 7].

With the definition of cobordism in mind, we introduce the following theorem, which shows the algebraic structure of the complex cobordism ring.

Theorem 2 (Milnor, Novikov)**.** $\Omega_*^U \cong \mathbb{Z}\left[\alpha_1, \alpha_2, \cdots\right]$ *is a polynomial ring with one generator* α_n *in each positive even dimension* $2n$*.*

Smooth projective toric variety polynomial generators for Ω_*^U have been constructed in all dimensions except for those in which n is even and not one less than a prime power. Wilfong has also verified the conjecture using computational software for the case when n is even and not one less than a prime power for all n through $100\,000$. The case when n is even and not one less than a prime power is the subject of this thesis. If the number theory conjecture is true, it will prove that there are polynomial generators of Ω_*^U in these remaining dimensions. Refer to [7] for details. We now turn to the number theory conjecture studied in this paper.

Here we introduce the expression $R_n(\varepsilon) = n - \varepsilon + (-1)^{\varepsilon}\binom{n-1}{\varepsilon}$, which arises in Wilfong's work on the combinatorics of polytopes. The number n in this expression relates to the complex dimension of the manifolds connected by the complex cobordism. Our goal is to

identify choices for ε, for which the quantity $R_n(\varepsilon)$ and the number $n+1$ are relatively prime. We state this formally in the following conjecture.

Conjecture 3. *(See [7] for background.) For a given even n, n not one less than a power of a prime, the equation*

$$\gcd(R_n(\varepsilon), n+1) = 1 \tag{1.1}$$

has a solution ε, where $R_n(\varepsilon)$ is defined as $R_n(\varepsilon) = n - \varepsilon + (-1)^{\varepsilon}\binom{n-1}{\varepsilon}$, and ε is in the range $\{2, \cdots, n-1\}$.

We will refer to this conjecture as conjecture 1.1 throughout the rest of this paper.

Conjecture 1.1 is the primary focus of this paper. We build on previous results from Wilfong and Parry to provide more evidence that the conjecture is true. As the conjecture states, we need a choice for ε making $R_n(\varepsilon)$ and the number $n+1$ relatively prime. Since $n+1$ is not a prime power, it has at least two primes in its prime factorization. To verify that $R_n(\varepsilon)$ and $n+1$ are relatively prime for a given choice for ε, we can verify that each prime dividing $n+1$ does not divide the quantity $R_n(\varepsilon)$. To do this, we verify that the range $\{2, \cdots, n-1\}$ contains at least one choice for ε satisfying the condition $R_n(\varepsilon) \not\equiv 0 \mod p_i$ for each prime p_i dividing $n+1$.

We note that $n \equiv -1 \mod p_i$ for any prime p_i dividing $n+1$. We can rewrite the expression $R_n(\varepsilon)$ in a congruence with a prime number modulus p_i, where the prime p_i divides $n+1$, as

$$\begin{aligned} R_n(\varepsilon) &= n - \varepsilon + (-1)^{\varepsilon}\binom{n-1}{\varepsilon} \\ &\equiv -1 - \varepsilon + (-1)^{\varepsilon}\binom{n-1}{\varepsilon} \mod p_i \\ &= -(\varepsilon+1) + (-1)^{\varepsilon}\binom{n-1}{\varepsilon} \mod p_i. \end{aligned}$$

Using the previous congruence, we see that our task of proving conjecture 1.1 is identical to showing that we can guarantee at least one choice for ε in the range $\{2, \cdots, n-1\}$ satisfying

the condition

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \not\equiv \varepsilon + 1 \mod p_i \tag{1.2}$$

for each prime p_i dividing $n+1$.

If a choice for ε satisfies condition 1.2 for the number n and for each prime p_i dividing $n+1$, then that choice for ε satisfies conjecture 1.1 for the number n as defined. This follows, since if the quantity $R_n(\varepsilon)$ is not divisible by any prime p_i dividing $n+1$, then the quantity $R_n(\varepsilon)$ and the number $n+1$ are relatively prime. For that reason, we can eliminate particular choices for ε by showing that the given choice does not satisfy condition 1.2 for at least one prime p_i dividing $n+1$. If the expression $R_n(\varepsilon)$ is divisible by any of the primes dividing $n+1$, it follows immediately that this choice for ε also fails to satisfy conjecture 1.1 for the number n. This is the primary method that we use to establish that a given choice for ε satisfies conjecture 1.1 for the number n. Though the general prime factorization of such a number can be given by $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t}$, there are many hurdles to tackling this form of the problem directly. We begin instead with special forms of the problem and build in complexity.

In Sections 2 and 3, we restrict ourselves to the case that the primes dividing $n+1$ are squarefree. The propositions in Section 2, incorporating Lucas' Theorem, help us to identify choices for ε satisfying condition 1.2 for individual primes dividing the number $n+1$. The propositions show intervals and specific positions where no suitable choices for ε exist and intervals in which choices for ε necessarily satisfy condition 1.2 for a given prime p_i dividing the number $n+1$. The long-range goal is to characterize the choices for ε completely and to show that there is always a choice for ε satisfying conjecture 1.1 for any even n that is not one less than a prime power. Section 3 analyzes some simplified versions of the conjecture. Theorem 18 of Section 3 analyzes numbers $n+1$ that are products of two squarefree primes. The proof that choices for ε exist satisfying conjecture 1.1 for an even number n, where $n+1$ is of this form, was shown by Wilfong in unpublished notes. We also analyze numbers $n+1$ with multiple squarefree prime factors. These numbers look like $n+1 = p_1 \cdot p_2 \cdots p_t$ where each p_i is prime.

Our goal in Sections 4, 5, 6, and 7 is to gradually extend our analysis to even n where $n+1$ has the generic prime factorization $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$. In Section 5 we extend Theorem 18 to the general case allowing numbers $n+1$ that are products of two nonsquarefree primes. These numbers look like $n+1 = p_1^{m_1} \cdot p_2^{m_2}$ where p_1 and p_2 are both prime. This theorem was proved originally by Walter Parry [4], but we offer an alternative proof here using methods developed in this paper. The new propositions proved in this paper provide extensions to previous results and verify the conjecture in new cases, especially where factors in the prime factorization of $n+1$ are not squarefree. We restrict ourselves to some partial cases and do not offer a general proof of conjecture 1.1.

Walter Parry has examined conjecture 1.1 and achieved some sophisticated generalizations. In his paper [4], Parry reformulates conjecture 1.1 to gain more leverage on the problem. New, equivalent conditions arise on a choice for ε to satisfy conjecture 1.1 for a number n. His reformulation reveals more of the underlying structure relating the number n and the corresponding choices for ε. One of his major results is intuitively labeled The Big Exponents Theorem. In that theorem, the use of continued fractions leads to a separation of the original conjecture into two cases. He is able to show that for any finite set S of odd primes, $S = \{p_1, p_2, \cdots, p_t\}$, there exists a positive integer r such that if each prime is raised to at least the power of r, then there is a guaranteed choice for ε satisfying conjecture 1.1 for the number n. That is, if for each number in $\{r_1, r_2, \cdots, r_t\}$ we have $r_i > r$, this theorem guarantees a choice for ε satisfying conjecture 1.1 for the number n where $n+1 = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$. Currently, this requires that the number n be very large, since each prime power must be very large. What makes his work exciting is that it addresses the general case directly and can potentially be refined to improve the bound on the prime powers dividing $n+1$. If the exponents r_i can be reduced, the approach could eventually provide a general proof to the conjecture. It is possible that a general proof will require more advanced methods, like those used in the work of Parry.

Evaluating the binomial coefficient $\binom{n-1}{\varepsilon}$ in condition 1.2 is the main challenge to identifying choices for ε satisfying conjecture 1.1 for the number n. Lucas' Theorem provides

a way of rewriting a binomial coefficient $\binom{m}{n}$ in a congruence with a prime number modulus as a product of binomial coefficients taken from the p_i-adic expansions of the integers m and n. This rewriting strategy is a key component of the approach taken in this paper to prove conjecture 1.1. We state and prove the theorem below.

Theorem 4 (Lucas' Theorem)**.** *For nonnegative integers m and n and a prime p, the following congruence relation holds:*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod p$$

where m and n are expressed in their base p expansions as

$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$ *and*

$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$.

Here, we use the convention that if $m < n$, then $\binom{m}{n} = 0$.

Proof. (This proof is attributed to Nathan Fine. See [2].) If p is prime and n is an integer satisfying $1 \leq n \leq p-1$, then the numerator of the binomial coefficient

$$\binom{p}{n} = \frac{p \cdot (p-1) \cdots (p-n+1)}{n \cdot (n-1) \cdots 1}$$

is divisible by p, but the denominator is not.

Clearly, p must divide $\binom{p}{n}$. We recall the identity (using ordinary generating functions)

$$(1+X)^p \equiv 1 + X^p \mod p.$$

In fact, for every nonnegative integer i we have (by induction)

$$(1+X)^{p^i} \equiv 1 + X^{p^i} \mod p.$$

Recall that m is a nonnegative integer and p is a prime. As before, we write m in its base p expansion, yielding $m = \sum_{i=0}^{k} m_i p^i$ for some nonnegative integers k and m_i, in which the bound $0 \leq m_i \leq p-1$ holds for each m_i by the definition of p-adic expansion.

We can then write

$$\begin{aligned}
\sum_{n=0}^{m} \binom{m}{n} X^n &= (1+X)^m = \prod_{i=0}^{k} \left((1+X)^{p_i}\right)^{m_i} \\
&\equiv \prod_{i=0}^{k} \left((1+X)^{p^i}\right)^{m_i} = \prod_{i=0}^{k} \left(\sum_{n_i=0}^{m_i} \binom{m_i}{n_i} X^{n_i p^i} \right) \\
&\equiv \prod_{i=0}^{k} \left(\sum_{n_i=0}^{p-1} \binom{m_i}{n_i} X^{n_i p^i} \right) = \sum_{n=0}^{m} \left(\prod_{i=0}^{k} \binom{m_i}{n_i} \right) X^n \mod p,
\end{aligned}$$

where in the final product the n_i represent the coefficients of the p-adic expansion of n, which is unique. Since the expansion of n is unique, the theorem is proved. □

Before moving to the propositions, we introduce a small lemma that will prove useful for simplifying expressions resulting from the application of Lucas' Theorem. In order to apply Lucas' Theorem, we often need to characterize the value of ε according to its p_i-adic expansion for the prime p_i. We use the convention $\varepsilon = b_0 + b_1 p_i + \cdots$ where the nonnegative integers $\{b_0, b_1, \cdots\}$ are less than p_i. This convention of using b_0 for the first coefficient in the p_i-adic expansion for ε motivates the choice of the integer b_0 in the following lemma.

Lemma 5. *For integer b_0 bounded by $0 \leq b_0 < p$, the binomial coefficient $\binom{p-2}{b_0}$ is equivalent to $(-1)^{b_0}(b_0+1)$ modulo the prime p.*

Proof. We note that each of $p-2$ and b_0 is less than the prime p itself. Noting this, we can rewrite the binomial coefficient $\binom{p-2}{b_0}$ modulo the prime p as

$$\begin{aligned}
\binom{p-2}{b_0} &= \frac{(p-2)!}{b_0!\,(p-2-b_0)!} \\
&= \frac{(p-2)(p-3)\cdots(p-b_0)(p-(b_0+1))(p-(b_0+2))!}{2\cdot 3\cdots b_0\,(p-(b_0+2))!} \\
&\equiv \frac{(-2)(-3)\cdots(-b_0)(-(b_0+1))}{2\cdot 3\cdots b_0} \mod p \\
&\equiv \frac{(-1)^{b_0}(2)(3)\cdots(b_0)(b_0+1)}{2\cdot 3\cdots b_0} \mod p.
\end{aligned}$$

Since each factor $2, 3, \cdots, b_0$ is less than p, we can associate factors in the numerator and denominator and simplify as follows:

$$\begin{aligned}\binom{p-2}{b_0} &\equiv (-1)^{b_0}\left(\frac{2}{2}\right)\cdot\left(\frac{3}{3}\right)\cdots\left(\frac{b_0}{b_0}\right)\cdot(b_0+1) \mod p \\ &\equiv (-1)^{b_0}(b_0+1) \mod p.\end{aligned}$$

From the preceding, we have proved the identity

$$\binom{p-2}{b_0} \equiv (-1)^{b_0}(b_0+1) \mod p.$$

□

We can simplify the binomial coefficient $\binom{p-2}{b_0}$ modulo the prime p in this way whenever the nonnegative integer b_0 is also less than p.

2. Propositions from Wilfong

We give credit to Wilfong for the following propositions and lemmas, proved in unpublished notes. The results of this section are used to prove the theorems of Section 3. Some propositions identify particular choices for ε, as well as ranges containing choices for ε, that can never satisfy conjecture 1.1 for an even number n not one less than a prime power. See especially Propositions 6 and 9, Corollary 10, Lemma 12, and Corollary 13. Other results establish ranges containing choices for ε that satisfy condition 1.2 for any prime p_i dividing $n+1$. See especially Proposition 11, Corollaries 14 and 15, Lemma 16, and Corollary 17. Here, we initially restrict ourselves to the case $n+1 = p_1 \cdot p_2 \cdots p_t$ where $n+1$ is the product of t distinct, squarefree primes. To standardize our method, we unfailingly adhere to the convention $p_1 < p_2 < \cdots < p_t$.

As stated earlier, in order to utilize the notational convenience of Lucas' Theorem to evaluate choices for ε more efficiently, we often need to rewrite the number $n-1$ in its p_i-adic expansion for a given prime p_i dividing $n+1$. We write $n+1$ in its expanded p_i-adic form as

$$n+1 = a_1 p_i + a_2 p_i^2 + \cdots ,$$

where it is guaranteed that $a_1 \neq 0$, since $p_i \mid n+1$, but $p_i^2 \nmid n+1$. Subtracting two, we can write $n-1$ in expanded p_i-adic form as

$$n-1 = (p_i - 2) + (a_1 - 1)\, p_i + a_2 p_i^2 + \cdots .$$

From this expression, we can read off the p_i-adic coefficients of $n-1$ directly.

The following proposition shows that choices for ε that are too small can never satisfy conjecture 1.1 for an even number n not one less than a prime power. Recall that $n+1$ is of the form $p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$, and $\binom{a}{b} \equiv 0 \mod p_i$, whenever $a < b$ for integers a and b.

Proposition 6. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. If $\varepsilon \equiv -1 \mod p_i$ for a given prime p_i, that choice for ε does not satisfy condition 1.2 for the prime p_i and the number n.*

Proof. For the prime p_i dividing $n+1$, condition 1.2 requires that the statement $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \not\equiv \varepsilon + 1 \mod p_i$ hold for a suitable choice for ε. We consider any choice for ε in any suitable range. We can write ε in its expanded p_i-adic form as $\varepsilon = (p_i - 1) + b_1 p_i + b_2 p_i^2 + \cdots$ where the integral coefficients $\{b_1, b_2, \cdots\}$ are in the range $0 \leq b_1, b_2, \cdots < p_i$. Applying Lucas' Theorem to the binomial coefficient $\binom{n-1}{\varepsilon}$, we can write

$$\begin{aligned} \binom{n-1}{\varepsilon} &\equiv \binom{p_i - 2}{p_i - 1}\binom{a_1 - 1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i \\ &\equiv 0 \mod p_i. \end{aligned}$$

This holds since $p_i - 2 < p_i - 1$ and the value of the binomial coefficient $\binom{p_i-2}{p_i-1}$ is equal to zero by convention. It follows that

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv 0 \equiv -1 + 1 \equiv \varepsilon + 1 \mod p_i.$$

For any prime p_i dividing $n+1$ and any choice for ε, where $\varepsilon \equiv -1 \mod p_i$, that choice for ε never satisfies condition 1.2 for the prime p_i and the number n. □

The following corollary emphasizes the fact that any choice $\varepsilon \equiv -1 \mod p_i$ not only fails to satisfy condition 1.2 for a prime p_i dividing $n+1$, but also fails to satisfy conjecture 1.1 for the number n.

Corollary 7. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. For any prime p_i dividing $n+1$, a choice $\varepsilon \equiv -1 \mod p_i$ cannot satisfy conjecture 1.1 for the even number n.*

The following proposition is especially useful to gain insight into the work of Walter Parry. This result enables the construction of choices for ε satisfying condition 1.2 for particular primes dividing the number $n+1$. This result is a crucial component of Parry's Big Exponents Theorem. The proposition also guarantees that a choice for ε that fails to satisfy

condition 1.2 for a particular prime p_i dividing $n+1$ cannot have p_i-adic coefficient b_1 equal to $p_i - 1$ when $b_0 \neq p_i - 1$. An example of this is seen in Lemma 16.

Proposition 8. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. For a prime p_i dividing $n+1$, any choice for ε with $b_1 = p_i - 1$, $b_0 \neq p_i - 1$ and p_i-adic expansion given by $\varepsilon = b_0 + b_1 p_i + b_2 p_i^2 + \cdots$ necessarily satisfies condition 1.2 for the prime p_i dividing $n+1$.*

Proof. In this case, by Lucas' Theorem and the convention on binomial coefficients stated there, we have

$$\begin{aligned}
\binom{n-1}{\varepsilon} &\equiv \binom{p_i - 2}{b_0}\binom{a_1 - 1}{p_i - 1}\binom{a_2}{b_2}\cdots \mod p_i \\
&\equiv \binom{p_i - 2}{b_0} \cdot (0) \cdot \binom{a_2}{b_2}\cdots \mod p_i \\
&\equiv 0 \mod p_i.
\end{aligned}$$

This is true since $a_1 < p_i$ immediately implies $a_1 - 1 < p_i - 1$. It follows that

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv 0 \mod p_i.$$

Proposition 6 requires that $\varepsilon \not\equiv -1 \mod p_i$, and since $\varepsilon \equiv b_0$, we know that $b_0 \not\equiv -1 \mod p_i$. It follows that

$$\varepsilon + 1 \equiv b_0 + 1 \not\equiv 0 \mod p_i.$$

Taken together we see that

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv 0 \not\equiv \varepsilon + 1 \mod p_i.$$

Therefore, any choice for ε with $b_1 = p_i - 1$ always satisfies condition 1.2 for the prime p_i. □

The preceding proposition plays an integral role in Parry's Big Exponents Theorem, enabling the construction of choices for ε satisfying condition 1.2 for particular primes dividing $n+1$.

Proposition 9. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. For a prime p_i dividing $n+1$, any choice for ε in the range $\{2, \cdots, p_i - 2\}$ never satisfies condition 1.2 for the prime p_i and the number n.*

Proof. For any prime p_i dividing $n+1$, the possible choices for ε, where $\varepsilon < p_i$, are restricted to the range $\{2, \cdots, p_i - 2\}$ by the statement of conjecture 1.1 and Proposition 6. The p_i-adic expansion of any choice for ε in this range consists solely of a constant term since the prime p_i is larger than ε. Specifically, we have $\varepsilon = b_0$ where b_0 is a nonnegative integer less than $p_i - 1$. We wish to determine whether any choice for ε in this range satisfies condition 1.2 for the prime p_i. We apply Lucas' Theorem and express the binomial coefficient $\binom{n-1}{\varepsilon}$ as

$$\binom{n-1}{\varepsilon} \equiv \binom{p_i - 2}{b_0}\binom{a_1 - 1}{0}\binom{a_2}{0}\binom{a_3}{0}\cdots \equiv \binom{p_i - 2}{b_0} \mod p_i.$$

By Lemma 5 we can rewrite the binomial coefficient $\binom{p_i-2}{b_0}$ as $(-1)^{b_0}(b_0+1) \mod p_i$. We multiply by the factor $(-1)^{\varepsilon}$ on the left and right hand sides of the congruence above to match the full expression in condition 1.2. We recall that b_0 is identical with ε, and we write

$$\begin{aligned}
(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &\equiv (-1)^{\varepsilon}\binom{p-2}{b_0} \mod p_i \\
&\equiv (-1)^{\varepsilon}(-1)^{b_0}(b_0+1) \equiv (-1)^{\varepsilon}(-1)^{\varepsilon}(\varepsilon+1) \mod p_i \\
&\equiv \varepsilon + 1 \mod p_i.
\end{aligned}$$

It follows from this that any choice for ε, where $\varepsilon < p_i$, never satisfies condition 1.2 for the prime p_i and the number n. □

The following corollary follows directly by replacing the generic prime p_i in the previous proposition with the prime p_t, the largest prime factor of $n+1$.

Corollary 10. *Let $n+1 = p_1 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. No choice for ε less than p_t satisfies conjecture 1.1 for the even number n. That is, there is no choice for ε in the range $\{2, \cdots, p_t - 1\}$ satisfying conjecture 1.1 for the number n.*

In the following propositions and lemmas, we characterize ranges containing choices for ε that always satisfy condition 1.2 for a prime p_i dividing $n+1$. In order for a choice for ε to satisfy conjecture 1.1 for the number n, it is necessary that that choice for ε satisfies condition 1.2 for each prime p_i dividing $n+1$. It is therefore helpful to identify ranges containing choices for ε satisfying condition 1.2 for individual primes dividing $n+1$. Once these ranges are established for each individual prime, we know that choices for ε in the intersection of these ranges–where these intervals overlap–satisfy conjecture 1.1 for the number n.

For a prime p_i dividing $n+1$, Proposition 11 shows that all choices for ε in the range $\{p_i, \cdots, 2p_i-2\}$ satisfy condition 1.2 for the prime p_i and the number n. For a prime p_i dividing $n+1$, Corollary 15 shows that if a multiple of p_i, call it kp_i where k is an integer, satisfies condition 1.2 for the prime p_i and the number n, then all choices for ε in the range $\{kp_i, \cdots, (k+1)\,p_i-2\}$ also satisfy the condition for the prime p_i and the number n. For individual primes dividing $n+1$, these results guarantee entire ranges containing choices for ε that satisfy condition 1.2 for the prime p_i and the number n. This is a crucial step in establishing the existence of a choice for ε satisfying conjecture 1.1 for the number n.

For notational consistency and ease of reading, we always characterize the p_i-adic expansion of ε as $\varepsilon = b_0 + b_1 p_i + b_2 p_i^2 + \cdots$ where the nonnegative integer coefficients $\{b_0, b_1, \cdots\}$ are less than p_i. We include the restriction $b_0 \neq p_i - 1$ since these choices for ε fail to satisfy conjecture 1.1 by Corollary 7. We continue with the assumption that $n+1$ is a product of squarefree primes with factorization $n+1 = p_1 p_2 \cdots p_t$, following the convention $p_1 < p_2 < \cdots < p_t$.

For each prime dividing $n+1$, the following proposition establishes a range containing choices for ε, all of which satisfy condition 1.2 for that prime and the number n.

Proposition 11. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. For a prime p_i dividing $n+1$, all choices for ε in the range $p_i \leq \varepsilon < 2p_i - 1$ satisfy condition 1.2 for the prime p_i and the number n.*

Proof. Any choice for ε in the range $\{p_i, \cdots, 2p_i-2\}$ contains two nonzero terms in its p_i-adic expansion. Namely, we have $\varepsilon = b_0 + p_i$. Since ε is strictly less than $2p_i - 1$, the

constant term b_0 in the p_i-adic expansion of ε is strictly less than $p_i - 1$. So, we have b_0 in the bound $0 \leq b_0 < p_i - 1$. We apply Lucas' Theorem and Lemma 5 to rewrite the binomial coefficient $\binom{n-1}{\varepsilon}$ as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv \binom{p_i-2}{b_0}\binom{a_1-1}{1}\binom{a_2}{0}\cdots \mod p_i \\ &\equiv (-1)^{b_0}(b_0+1)(a_1-1) \mod p_i.\end{aligned}$$

We multiply both sides of the congruence by the factor $(-1)^{\varepsilon}$ to match the expression in condition 1.2. We have

$$\begin{aligned}(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &\equiv (-1)^{\varepsilon}(-1)^{b_0}(b_0+1)(a_1-1) \mod p_i \\ &\equiv -(b_0+1)(a_1-1) \mod p_i \\ &\equiv (b_0+1)(1-a_1) \mod p_i.\end{aligned}$$

For a prime p_i dividing $n+1$, we wish to verify that any choice for ε in the range $\{p_i, \cdots, 2p_i - 2\}$ satisfies the condition $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \not\equiv \varepsilon + 1 \mod p_i$ for the number n. Since we have $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv (b_0+1)(1-a_1) \mod p_i$, we need to check whether $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv \varepsilon + 1 \equiv (b_0+1)(1-a_1) \mod p_i$. We can write ε as $b_0 + p_i$. This leads directly to the congruence $\varepsilon + 1 \equiv b_0 + 1 \mod p_i$. Therefore, $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv \varepsilon + 1 \mod p_i$ if and only if $a_1 = 0$. Since $a_1 \neq 0$ by assumption, this means that all choices for ε in the range $\{p_i, \cdots, 2p_i - 2\}$ satisfy condition 1.2 for any prime p_i dividing $n+1$. □

Lemma 12. *Consider $n+1$, where n is even, and $n+1$ is the product of squarefree prime factors. For a prime p_i dividing $n+1$, any choice for ε with its p_i-adic coefficient b_0 fixed in the range $\{0, \cdots, p_i - 2\}$ fails to satisfy condition 1.2 for the prime p_i dividing $n+1$ if and only if $\varepsilon - b_0$ also fails to satisfy condition 1.2 for the prime p_i and the number n.*

Proof. For a prime p_i dividing $n+1$, we consider an arbitrary choice for ε in any suitable range, where $\varepsilon \not\equiv -1 \mod p_i$, and $\varepsilon = b_0 + b_1 p_i + \cdots$. To determine whether the choice for ε satisfies condition 1.2 for the prime p_i, we use Lucas' Theorem and Lemma 5 to rewrite the

binomial coefficient $\binom{n-1}{\varepsilon}$ modulo the prime p_i as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv \binom{p_i-2}{b_0}\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i \\ &\equiv (-1)^{b_0}(b_0+1)\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i.\end{aligned}$$

Multiplying both sides of the congruence above by a factor of $(-1)^{\varepsilon}$ and rewriting ε in terms of its p_i-adic expansion, we have

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv (-1)^{\left(2\cdot b_0+b_1p_i+b_2p_i^2+\cdots\right)}(b_0+1)\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i.$$

It follows that $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv \varepsilon+1 \equiv b_0+1 \mod p_i$ if and only if

$$\varepsilon+1 \equiv (-1)^{\left(b_1p_i+b_2p_i^2+\cdots\right)}(b_0+1)\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i.$$

Since b_0 is strictly less than p_i-1, we know that b_0+1 is strictly less than p_i and we can divide both sides of the congruence by b_0+1. Simplifying, we see that $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv \varepsilon+1 \mod p_i$ if and only if

$$1 \equiv (-1)^{\left(b_1p_i+b_2p_i^2+\cdots\right)}\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i.$$

The above congruence shows that this property is completely independent of the value of b_0. For any prime p_i dividing $n+1$, any choice for ε with its p_i-adic coefficient b_0 fixed in the range $\{0,\cdots,p_i-2\}$ fails to satisfy condition 1.2 if and only if the choice $\varepsilon-b_0$ also fails to satisfy the condition for the prime p_i and the number n. □

The following corollary follows immediately from the preceding lemma.

Corollary 13. *If $\varepsilon = kp_i$, where k is an integer, fails to satisfy condition 1.2 for the prime p_i dividing $n+1$, then all choices for ε in the range $\{kp_i,\cdots,(k+1)p_i-2\}$ also fail to satisfy condition 1.2 for the prime p_i and the number n.*

The following corollary is identical to Lemma 12 but stated in a positive sense, describing ranges containing choices for ε that satisfy condition 1.2 for the prime p_i dividing

$n+1$. From the earlier proof, the congruence

$$1 \equiv (-1)^{\left(b_1 p_i + b_2 p_i^2 + \cdots\right)} \binom{a_1 - 1}{b_1} \binom{a_2}{b_2} \cdots \mod p_i$$

does not contain the p_i-adic coefficient b_0. This shows that the value of b_0, assuming $b_0 \neq p_i - 1$, does not affect whether a choice for ε satisfies condition 1.2 for a prime p_i dividing $n+1$. So, if any choice for ε with b_0 fixed in the range $\{0, \cdots, p_i - 2\}$ satisfies condition 1.2 for the prime p_i, then all choices for ε with b_0 fixed in that range also satisfy the condition for the prime p_i and the number n.

Corollary 14. *For any prime p_i dividing $n+1$, any choice for ε with its p_i-adic coefficient b_0 fixed in the range $\{0, \cdots, p_i - 2\}$ satisfies condition 1.2 for the prime p_i and the number n if and only if $\varepsilon - b_0$ also satisfies condition 1.2 for the prime p_i and the number n.*

The following corollary is identical to Corollary 13 but stated in a positive sense.

Corollary 15. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. If $\varepsilon = k p_i$, where the prime p_i divides $n+1$ and k is an integer, satisfies condition 1.2 for the prime p_i, then all choices for ε in the range $\{k p_i, \cdots, (k+1) p_i - 2\}$ also satisfy condition 1.2 for the prime p_i and the number n.*

Lemma 12 and the related corollaries allow us to characterize the suitability of entire ranges containing choices for ε. In the following lemma, we use Lemma 12 and Corollaries 13–15 to simplify the p_i-adic expansion of our choice for ε, letting $\varepsilon \equiv 0 \mod p_i$ so that the p_i-adic coefficient b_0 is identically equal to zero.

Lemma 16. *If a choice $\varepsilon' \not\equiv -1 \mod p_i$ fails to satisfy condition 1.2 for the prime p_i dividing $n+1$, it then follows that $\varepsilon = \varepsilon' + p_i$ necessarily satisfies the condition for the prime p_i. In other words, if*

$$(-1)^{\varepsilon'} \binom{n-1}{\varepsilon'} \equiv \varepsilon' + 1 \mod p_i,$$

then ε' fails to satisfy condition 1.2 for the prime p_i by definition, and it then necessarily follows that

$$(-1)^{(\varepsilon'+p_i)}\binom{n-1}{\varepsilon'+p_i} \not\equiv (\varepsilon'+p_i)+1 \mod p_i,$$

so that $\varepsilon = \varepsilon' + p_i$ satisfies condition 1.2 for the prime p_i and the number n.

Proof. Simplifying by the property of Lemma 12, we can let $\varepsilon' \equiv 0 \mod p_i$. We characterize ε' with the p_i-adic expansion $\varepsilon' = b_1 p_i + b_2 p_i^2 + \cdots$. Applying Lucas' Theorem, we can rewrite the binomial coefficient $\binom{n-1}{\varepsilon'}$ as

$$\binom{n-1}{\varepsilon'} \equiv \binom{p_i-2}{0}\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \equiv \binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \mod p_i.$$

By assumption ε' fails to satisfy condition 1.2 for the prime p_i, so

$$(-1)^{\varepsilon'}\binom{n-1}{\varepsilon'} \equiv \varepsilon' + 1 \equiv 1 \mod p_i.$$

Using the form for $\binom{n-1}{\varepsilon'}$ derived above, we can write

$$(-1)^{\varepsilon'}\binom{n-1}{\varepsilon'} \equiv (-1)^{\varepsilon'}\binom{a_1-1}{b_1}\binom{a_2}{b_2}\cdots \equiv 1 \mod p_i.$$

The choice ε' fails to satisfy condition 1.2, and we wish to establish that $\varepsilon = \varepsilon' + p_i$ satisfies condition 1.2 for the prime p_i. We note that ε has the p_i-adic expansion given by $\varepsilon = \varepsilon' + p_i = (b_1+1)\,p_i + b_2 p_i^2 + \cdots$. Proposition 8 guarantees that $b_1 + 1$ is less than p_i since $b_1 = p_i - 1$ would imply that the choice for ε necessarily satisfies condition 1.2 for the prime p_i.

We have $\binom{n-1}{\varepsilon} = \binom{n-1}{\varepsilon'+p_i}$, and we can write

$$\binom{n-1}{\varepsilon'+p_i} \equiv \binom{p_i-2}{0}\binom{a_1-1}{b_1+1}\binom{a_2}{b_2}\cdots \equiv \binom{a_1-1}{b_1+1}\binom{a_2}{b_2}\cdots \mod p_i.$$

In order to evaluate the right hand side completely, we will need to rewrite some of the factors. In particular, notice that we can expand and rewrite the binomial coefficient $\binom{a_1-1}{b_1+1}$ as

$$\begin{aligned}\binom{a_1-1}{b_1+1} &= \frac{(a_1-1)!}{(a_1-1-(b_1+1))!\,(b_1+1)!} \\ &= \frac{(a_1-1-b_1)\cdot(a_1-1)!}{(a_1-1-b_1)\cdot(a_1-1-(b_1+1))!\,(b_1)!\cdot(b_1+1)} \\ &= \frac{a_1-(b_1+1)}{(b_1+1)}\cdot\binom{a_1-1}{b_1}.\end{aligned}$$

Continuing to simplify the binomial coefficient $\binom{n-1}{\varepsilon} = \binom{n-1}{\varepsilon'+p_i}$, we have

$$\begin{aligned}\binom{n-1}{\varepsilon'+p_i} &\equiv \binom{a_1-1}{b_1+1}\binom{a_2}{b_2}\cdots \mod p_i \\ &\equiv \frac{a_1-(b_1+1)}{(b_1+1)}\cdot\binom{a_1-1}{b_1}\cdot\binom{a_2}{b_2}\cdots \mod p_i \\ &\equiv \frac{a_1-(b_1+1)}{(b_1+1)}\cdot\binom{n-1}{\varepsilon'} \mod p_i.\end{aligned}$$

So we see that

$$\binom{n-1}{\varepsilon} = \binom{n-1}{\varepsilon'+p_i} \equiv \frac{a_1-(b_1+1)}{(b_1+1)}\cdot\binom{n-1}{\varepsilon'} \mod p_i.$$

Note that $\varepsilon+1 = (\varepsilon'+p_i)+1 \equiv 1 \mod p_i$. We incorporate the factor $(-1)^{\varepsilon}$ to match the expression in condition 1.2. We have

$$\begin{aligned}(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &= (-1)^{(\varepsilon'+p_i)}\binom{n-1}{\varepsilon'+p_i} \\ &\equiv -(-1)^{\varepsilon'}\,\frac{a_1-(b_1+1)}{b_1+1}\cdot\binom{n-1}{\varepsilon'} \mod p_i \\ &\equiv -\frac{a_1-(b_1+1)}{b_1+1}\cdot\left((-1)^{\varepsilon'}\cdot\binom{n-1}{\varepsilon'}\right) \mod p_i \\ &\equiv -\frac{a_1-(b_1+1)}{b_1+1} \mod p_i.\end{aligned}$$

From this, we can conclude that $(-1)^{\varepsilon}\binom{n-1}{\varepsilon}$ is congruent to 1 modulo the prime p_i if and only if the condition $\frac{a_1-(b_1+1)}{b_1+1} \equiv -1 \mod p_i$ holds for the expression derived above. Rewriting, we see that this happens if and only if $a_1-(b_1+1) \equiv -(b_1+1) \mod p_i$, which

holds if and only if $a_1 \equiv 0 \mod p_i$. Since we have assumed that a_1 is not identically zero, this condition cannot hold. This tells us that $\varepsilon = \varepsilon' + p_i$ does indeed satisfy condition 1.2 for the prime p_i dividing $n+1$. So we see that if a particular choice $\varepsilon' \not\equiv -1 \mod p_i$ fails to satisfy condition 1.2 for the prime p_i dividing $n+1$, then the choice $\varepsilon = \varepsilon' + p_i$ satisfies condition 1.2 for the prime p_i along with choices for ε with b_0 in the range $\{0, \cdots, p_i - 2\}$ by Corollary 15. □

The preceding lemma holds for any choice for ε where ε is a multiple of the prime p_i. For convenience, call it $\varepsilon = kp_i$ where k is an integer. We make this explicit in the corollary directly below, which follows immediately from the lemma.

Corollary 17. *Let $n+1 = p_1 p_2 \cdots p_t$ with the convention $p_1 < \cdots < p_t$. If $\varepsilon' = kp_i$, where the prime p_i divides $n+1$ and k is an integer, fails to satisfy condition 1.2 for the prime p_i and the number n, then the choice $\varepsilon = \varepsilon' + p_i = (k+1)\, p_i$ satisfies condition 1.2 along with all values in the range $\{\varepsilon, \cdots, \varepsilon + p_i - 2\} = \{(k+1)\, p_i, \cdots, (k+2)\, p_i - 2\}$.*

3. Cases in which the Conjecture Holds

The following theorems rely on the propositions and lemmas of Section 2 for their proofs. These theorems were proved independently by Walter Parry [4] and in unpublished notes by Andrew Wilfong. To build up to the complexity of the general case, where odd $n+1$ has an arbitrary prime factorization, we begin with simplified versions of the conjecture as presented in this section.

The following theorem considers the specific case where $n+1$ is the product of two primes. We begin with this most reduced form of the conjecture and gradually build to more general forms of $n+1$.

Theorem 18. *If $n+1 = p \cdot q$, where $p < q$ and p and q are both prime, there is a choice for ε in the range $\{q, \cdots, n-2\}$ that satisfies the equation* $\gcd(R_n(\varepsilon), n+1) = 1$*, which is conjecture 1.1.*

Proof. (This proof is attributed to Andrew Wilfong.)

Case 1. $p = 3$ and $q = 5$. In the special case that $p = 3$ and $q = 5$, we note that $\varepsilon = 7$ is a particular choice for ε satisfying conjecture 1.1 for the number $n = 14$. For the remaining cases, assume $(p, q) \neq (3, 5)$.

Case 2. $q < 2p - 1$. For the number $n+1$ and the prime p, we know from Proposition 11 that all choices for ε in the range $\{p, \cdots, 2p-2\}$ satisfy the condition $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \not\equiv \varepsilon + 1 \mod p$. We also know that the corresponding condition is satisfied for the prime q by all choices for ε in the range $\{q, \cdots, 2q-2\}$. Since $p < q < 2p - 1$, and p and q are odd, the prime number q is in the range $\{p+2, \cdots, 2p-2\}$. By Proposition 11, q is a particular choice for ε satisfying the condition on $R_n(\varepsilon)$ for both the prime p and the prime q. This guarantees a choice for ε ensuring that the expressions $R_n(\varepsilon)$ and $n+1$ are relatively prime, which is the claim of conjecture 1.1.

Case 3. $q = 2p - 1$. Given this specific relation for the primes p and q, we can express the value of $2q$ as $4p - 2$. By Proposition 11, we know that all choices for ε in the range

$\{q, \cdots, 2q-2\} = \{2p-1, \cdots, 4p-4\}$ satisfy condition 1.2 for the prime q. By its structure, this range contains the numbers $2p$ and $3p$, so long as $(p, q) \neq (3, 5)$. (For this circumstance, see Case 1.) By Lemma 16, either $\varepsilon = 2p$ or $\varepsilon = 3p$ must satisfy condition 1.2 for the prime p. Both choices for ε satisfy condition 1.2 for the prime q. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Case 4. $q \geq 2p+1$. In this case the interval $\{q, \cdots, 2q-2\}$ contains at least $2p$ elements, since the interval $\{q, \cdots, 2q-2\}$ is identical to $\{2p+1, \cdots, 4p\}$ at its smallest when $q = 2p+1$. In general, this guarantees at least two multiples of p in the interval. For convenience, call them kp and $(k+1)\,p$ where k is an integer. By Lemma 16, either the choice $\varepsilon = kp$ or $\varepsilon = (k+1)\,p$ must satisfy condition 1.2 for the prime p. Both choices satisfy the condition for the prime q. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

These cases taken together show that there is a guaranteed choice for ε satisfying conjecture 1.1 for n when $n+1$ is the product of two squarefree primes.

□

We informally characterize the following theorem by the property that the prime factors of the number $n+1$ are far apart.

Theorem 19. *Let $n+1 = p_1 \cdot p_2 \cdots p_{t-1} \cdot p_t$ with the convention $p_1 < \cdots < p_t$. If the difference $p_k - p_{k-1}$ is large for all prime factors p_k of $n+1$–specifically, if the bound $p_k \geq 3p_{k-1} + 1$ is satisfied for all consecutive prime factors p_k and p_{k-1} of $n+1$–then there is a choice for ε satisfying conjecture 1.1 for the number n.*

Proof. By Corollary 10, the number p_t is the smallest possible choice for ε satisfying conjecture 1.1 for the number n. By Proposition 11, we know that all choices for ε in the range $\{p_t, \cdots, 2p_t - 2\}$ satisfy condition 1.2 for the prime p_t. The range $\{p_t, \cdots, 2p_t - 2\}$ contains $p_t - 1$ elements. By assumption, consecutive primes p_t and p_{t-1} satisfy the bound $p_t \geq 3p_{t-1} + 1$. This means that the interval $\{p_t, \cdots, 2p_t - 2\}$ contains at least $3p_{t-1}$ elements, which guarantees at least three multiples of p_{t-1} in the interval. Equivalently, the

interval must contain at least two complete, consecutive intervals of the form $\{lp_{t-1}, \cdots, (l+1)\,p_{t-1} - 2\}$ where l is an integer. Using this labeling, the next consecutive guaranteed interval is $\{(l+1)\,p_{t-1}, \cdots, (l+2)\,p_{t-1} - 2\}$. Corollaries 15 and 17 guarantee that in at least one of the given ranges, $\{lp_{t-1}, \cdots, (l+1)\,p_{t-1} - 2\}$ or $\{(l+1)\,p_{t-1}, \cdots, (l+2)\,p_{t-1} - 2\}$, all choices for ε satisfy condition 1.2 for the prime p_{t-1}. The choices for ε in both of these ranges satisfy the condition for the prime p_t, so this guarantees a range containing choices for ε that simultaneously satisfy condition 1.2 for the primes p_t and p_{t-1}.

Considering analogously the prime p_{t-2}, we can similarly establish a range containing choices for ε that simultaneously satisfy condition 1.2 for the primes p_t, p_{t-1}, and p_{t-2}. Continuing inductively, we can establish a nonempty interval containing choices for ε that satisfy condition 1.2 for all prime factors p_i of $n+1$. This guarantees at least one choice for ε satisfying conjecture 1.1 for the number n. □

The following theorem is informally characterized by the property that the prime factors of $n+1$ are close together.

Theorem 20. *Let $n+1 = p_1 \cdot p_2 \cdots p_{t-1} \cdot p_t$ with the convention $p_1 < \cdots < p_t$. If the prime factors p_i of $n+1$ are sufficiently close together–specifically, if the bound $p_t < 2p_1 - 1$ is satisfied–then we can guarantee the existence of at least one choice for ε satisfying conjecture 1.1 for the number n.*

Proof. By Proposition 11, all choices for ε in the range $\{p_i, \cdots, 2p_i - 2\}$ satisfy condition 1.2 for the prime p_i dividing $n+1$. The string of inequalities $p_1 \leq p_i \leq p_t < 2p_1 - 1 \leq 2p_i - 2$ holds for all primes p_i dividing $n+1$. The particular choice $\varepsilon = p_t$ is in the interval $\{p_i, \cdots, 2p_i - 2\}$ for each prime p_i dividing $n+1$, simultaneously satisfying condition 1.2 for each prime factor of $n+1$. This guarantees the existence of at least one choice for ε satisfying conjecture 1.1 for the number n when the squarefree prime factors of $n+1$ are sufficiently close together. □

4. Generalization of Many Propositions and Lemmas of Section 2

In this section, we prove generalizations of many of the propositions and lemmas of Section 2. We increase the complexity of the prime factorization of $n+1$, considering the general prime factorization $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$. We assume that the exponents m_i are integer-valued. We adhere to the convention $p_1^{m_1} < \cdots < p_t^{m_t}$, so that $p_t^{m_t}$ is the largest prime power dividing $n+1$. We do not place any restrictions on the relative sizes of the primes p_i themselves. For example, we do not require that the prime p_1 be the smallest, nor that the prime p_t be the largest, of the primes p_i dividing $n+1$.

These generalizations provide tools to prove conjecture 1.1 in cases where $n+1$ is not squarefree. We provide a generalization of Corollary 10, showing that no choice for ε less than the smallest prime power dividing $n+1$ satisfies conjecture 1.1 for the number n. We generalize Proposition 11, proving that for any prime power $p_i^{m_i}$ dividing $n+1$, all choices for ε in the interval $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$, except where $\varepsilon \equiv -1 \mod p_i$, satisfy condition 1.2 for the prime p_i and the number n. We prove generalizations of Corollaries 14 and 15, showing that if a particular multiple of the prime power $p_i^{m_i}$ dividing $n+1$, a number of form $k \cdot p_i^{m_i}$ where k is an integer, satisfies condition 1.2 for the prime p_i, then so do all choices for ε in the range $\{kp_i^{m_i}, \cdots, (k+1)\, p_i^{m_i} - 2\}$, except those choices where $\varepsilon \equiv -1 \mod p_i$. We also generalize Lemma 16 and Corollary 17, showing that if a particular choice $\varepsilon' \not\equiv -1 \mod p_i$ fails to satisfy condition 1.2 for the prime p_i and the number n, then the choice $\varepsilon = \varepsilon' + p_i^{m_i}$ must satisfy the condition for the prime p_i dividing $n+1$. This result entails the property that if the choices for ε contained in a range of the form $\{kp_i^{m_i}, \cdots, (k+1)\, p_i^{m_i} - 2\}$ fail to satisfy the condition on $R_n(\varepsilon)$ for the prime p_i, then the choices for ε in the next consecutive range $\{(k+1)\, p_i^{m_i}, \cdots, (k+2)\, p_i^{m_i} - 2\}$ do satisfy the condition for the prime p_i, excluding those choices for which $\varepsilon \equiv -1 \mod p_i$.

In the following propositions and lemmas, we will rewrite the number $n-1$ in its p_i-adic expansion for a prime p_i dividing $n+1$ many times, so we choose to include here a summary of the steps taken to rewrite $n-1$ in this way.

Remark 21. The number $n+1$ has generic prime factorization given by $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$. In order to focus our attention on a particular prime power $p_i^{m_i}$ in the prime factorization of $n+1$, we choose to rewrite $n+1$ in its p_i-adic expansion. This is necessary to make use of the notational convenience provided by Lucas' Theorem. In the following, we rewrite $p_i^{m_i}$ as p^m and represent the product of the other $t-1$ prime power divisors of $n+1$ by a single integer. We write

$$n+1 = p_1^{m_1} \cdots p_t^{m_t} = \left(p_1^{m_1} p_2^{m_2} \cdots p_{i-1}^{m_{i-1}} p_{i+1}^{m_{i+1}} \cdots p_t^{m_t}\right) \cdot p_i^{m_i} \quad = \quad q \cdot p^m.$$

In order to simplify this expression further, we write the number q in p-adic form as

$$q = c_0 + c_1 p + \cdots .$$

Using these expressions, we rewrite $n+1$ in the following way

$$\begin{aligned} n+1 &= q \cdot p^m \\ &= p^m \left(c_0 + c_1 p + \cdots\right) \\ &= c_0 \cdot p^m + c_1 p^{m+1} + \cdots . \end{aligned}$$

In the p-adic expansion of $n+1$ directly above, the terms $p^0, \cdots, p^{m-1}$ are absent, so the coefficients on these terms are identically zero. Subtracting two from the expression above, we can now write the p-adic expansion of $n-1$ as

$$n-1 = (p-2) + (p-1) \cdot p + \cdots + (p-1) \cdot p^{m-1} + (c_0 - 1) \cdot p^m + c_1 \cdot p^{m+1} + \cdots .$$

We use this form repeatedly in the following propositions and lemmas.

Before proceeding to the generalizations of the propositions and lemmas of Section 2, we include a small lemma reminiscent of Lemma 5 that provides a way of rewriting the binomial coefficient $\binom{p-2}{b_0}$ in congruences with a prime number modulus. The following lemma helps to simplify binomial coefficients of the form $\binom{p-1}{b}$ when evaluated in a congruence with a prime number modulus.

Lemma 22. *For the prime p, the value of the binomial coefficient $\binom{p-1}{b}$, where $0 \leq b < p$, is congruent to $(-1)^b \mod p$. That is, $\binom{p-1}{b} \equiv (-1)^b \mod p$.*

Proof. We note that $p-1$ and b are both less than p, so we can reduce fractional expressions in a congruence base p without worry. Rewriting the value of the binomial coefficient $\binom{p-1}{b}$ modulo the prime p, we have

$$\begin{aligned}
\binom{p-1}{b} &= \frac{(p-1)!}{(p-1-b)! \cdot b!} \\
&= \frac{(p-1)(p-2)\cdots(p-b)(p-b-1)!}{(p-b-1)! \cdot b!} \\
&\equiv \frac{(-1)(-2)\cdots(-b)(p-b-1)!}{b!\,(p-b-1)!} \mod p \\
&\equiv \frac{(-1)^b \cdot b!}{b!} \mod p \\
&\equiv (-1)^b \mod p.
\end{aligned}$$

This proves the congruence $\binom{p-1}{b} \equiv (-1)^b \mod p$ where $0 \leq b < p$. □

Proposition 23. *[Generalization of Proposition 9]. Let $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. For a prime power $p_i^{m_i}$ dividing $n+1$, any choice for ε less than $p_i^{m_i}$ does not satisfy condition 1.2 for the prime p_i and the number n.*

Proof. We rewrite $n-1$ according to Remark 21, for a prime power $p_i^{m_i}$ dividing $n+1$. We have

$$n-1 = (p_i-2) + (p_i-1)\cdot p_i + \cdots + (p_i-1)\cdot p_i^{m_i-1} + (c_0-1)\cdot p_i^{m_i} + c_1 \cdot p_i^{m_i+1} + \cdots .$$

Consider a choice for ε that is less than the prime power $p_i^{m_i}$ with $b_0 \neq p_i - 1$. Let ε have generic p_i-adic expansion $\varepsilon = b_0 + b_1 p_i + \cdots + b_{m_i-1} \cdot p_i^{m_i-1}$, where each b_κ is in the range $0 \leq b_\kappa < p_i$, and κ is an integer. Applying Lucas' Theorem, we can now rewrite the binomial

coefficient $\binom{n-1}{\varepsilon}$ modulo the prime p_i as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv \binom{p_i-2}{b_0}\cdot\binom{p_i-1}{b_1}\cdots\binom{p_i-1}{b_{m_i-1}}\cdot\binom{c_0-1}{0}\cdot\binom{c_1}{0}\cdots \mod p_i\\ &\equiv \binom{p_i-2}{b_0}\cdot\binom{p_i-1}{b_1}\cdots\binom{p_i-1}{b_{m_i-1}} \mod p_i.\end{aligned}$$

Applying Lemmas 5 and 22, we can neatly rewrite the binomial coefficients $\binom{p_i-2}{b_0}$ and $\binom{p_i-1}{b_\kappa}$ in the congruence where κ is an integer. By Lemma 5, we have $\binom{p_i-2}{b_0} \equiv (-1)^{b_0}(b_0+1) \mod p_i$, and, by Lemma 22, we have $\binom{p_i-1}{b_\kappa} \equiv (-1)^{b_\kappa} \mod p_i$ for each b_κ. Simplifying the expansion for $\binom{n-1}{\varepsilon}$ above, we have

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv \binom{p_i-2}{b_0}\cdot\binom{p_i-1}{b_1}\cdots\binom{p_i-1}{b_{m_i-1}} \mod p_i\\ &\equiv (-1)^{b_0}(b_0+1)\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}} \mod p_i\\ &\equiv (-1)^{b_0}\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}}(b_0+1) \mod p_i.\end{aligned}$$

We wish to express the exponents in the expression above in terms of ε, and we note that taking each term $(-1)^{b_\kappa}$ and raising it to the power of p_i^κ preserves the value of the factor. This is true since p_i^κ is odd, so $\left((-1)^{b_\kappa}\right)^{p_i^\kappa} = \left((-1)^{p_i^\kappa}\right)^{b_\kappa} = (-1)^{b_\kappa}$. Using this property, we can rewrite the expression above as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv (-1)^{\left(b_0+b_1+\cdots+b_{m_i-1}\right)}(b_0+1) \mod p_i\\ &\equiv (-1)^{\left(b_0+b_1p_i+\cdots+b_{m_i-1}\cdot p_i^{m_i-1}\right)}\cdot(b_0+1) \mod p_i\\ &\equiv (-1)^{\varepsilon}(b_0+1) \mod p_i.\end{aligned}$$

Finally, we incorporate the factor $(-1)^\varepsilon$ to match the expression in condition 1.2, giving

$$\begin{aligned}(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &\equiv (-1)^{\varepsilon}\cdot(-1)^{\varepsilon}\cdot(b_0+1) \mod p_i\\ &\equiv b_0+1 \mod p_i,\end{aligned}$$

which is congruent to $\varepsilon + 1 \mod p_i$ since

$$\begin{aligned} \varepsilon + 1 &= \left(b_0 + b_1 \cdot p_i + b_2 \cdot p_i^2 + \cdots + b_{m_i - 1} \cdot p_i^{m_i - 1}\right) + 1 \\ &\equiv b_0 + 1 \mod p_i. \end{aligned}$$

This means that for any prime power $p_i^{m_i}$ dividing $n+1$, the congruence $(-1)^{\varepsilon} \binom{n-1}{\varepsilon} \equiv \varepsilon + 1 \mod p_i$ holds for any $\varepsilon < p_i^{m_i}$. This shows that any choice for ε in the range $\{2, \cdots, p_i^{m_i} - 2\}$ fails to satisfy condition 1.2 for the prime p_i dividing $n+1$. □

The corollary below follows immediately from the preceding proposition.

Corollary 24. *Let $n + 1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t}$ where $\max\{p_1^{m_1}, p_2^{m_2}, \cdots, p_t^{m_t}\} = p_t^{m_t}$. Any choice for ε less than the number $p_t^{m_t}$ fails to satisfy conjecture 1.1 for the number n.*

As a matter of notation, the preceding corollary shows that all choices for ε in the range $\{2, \cdots, p_t^{m_t} - 1\}$ fail to satisfy the conjecture for the number n.

The following proposition generalizes Proposition 11, which states that all choices for ε in the range $\{p_i, \cdots, 2p_i - 2\}$ satisfy condition 1.2 for any prime p_i dividing $n + 1 = p_1 p_2 \cdots p_t$. This generalization considers the number $n+1$ with the generic prime factorization $n + 1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$.

Proposition 25. *[Generalization of Proposition 11]. Let $n + 1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. We are guaranteed that all choices for ε in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$, provided that $\varepsilon \not\equiv -1 \mod p_i$, satisfy condition 1.2 for the prime p_i and the number n.*

Proof. We rewrite $n - 1$ according to Remark 21 for an arbitrary prime power $p_i^{m_i}$ dividing $n + 1$. We have

$$n - 1 = (p_i - 2) + (p_i - 1) \cdot p_i + \cdots + (p_i - 1) \cdot p_i^{m_i - 1} + (c_0 - 1) \cdot p_i^{m_i} + c_1 \cdot p_i^{m_i + 1} + \cdots.$$

We consider choices for ε in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$, which we characterize with the generic p_i-adic expansion

$$\varepsilon = b_0 + b_1 \cdot p_i + \cdots + b_{m_i-1} \cdot p_i^{m_i-1} + 1 \cdot p_i^{m_i}.$$

Applying Lucas' Theorem, we can rewrite the binomial coefficient $\binom{n-1}{\varepsilon}$ as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv \binom{p_i-2}{b_0} \cdot \binom{p_i-1}{b_1} \cdots \binom{p_i-1}{b_{m_i-1}} \cdot \binom{c_0-1}{1} \cdot \binom{c_1}{0} \cdots \mod p_i \\ &\equiv \binom{p_i-2}{b_0} \cdot \binom{p_i-1}{b_1} \cdots \binom{p_i-1}{b_{m_i-1}} \cdot (c_0-1) \mod p_i.\end{aligned}$$

By Lemma 5, we can rewrite the binomial coefficient $\binom{p_i-2}{b_0}$ as $(-1)(b_0+1) \mod p_i$ and by Lemma 22, we can rewrite the binomial coefficient $\binom{p_i-1}{b_\kappa}$ as $(-1)^{b_\kappa} \mod p_i$ for each b_κ. This allows us to rewrite our expansion above as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv (-1)^{b_0} \cdot (b_0+1) \cdot (-1)^{b_1} \cdots (-1)^{b_{m_i-1}} (c_0-1) \mod p_i \\ &\equiv (-1)^{b_0} \cdot (-1)^{b_1} \cdots (-1)^{b_{m_i-1}} \cdot (b_0+1) \cdot (c_0-1) \mod p_i.\end{aligned}$$

We can rewrite the above expression using similar methods to those used in Proposition 23. We collect the factors $(-1)^{b_0} \cdot (-1)^{b_1} \cdots (-1)^{b_{m_i-1}}$, reconstructing the p_i-adic expansion of ε in the exponents of these factors by raising each factor $(-1)^{b_\kappa}$ to the power p_i^κ. Since each power p_i^κ is odd, the value of each factor is unchanged. We rewrite the factors $(-1)^{b_0} \cdot (-1)^{b_1} \cdots (-1)^{b_{m_i-1}}$ in the expression above as

$$(-1)^{b_0} \cdot (-1)^{b_1 p_i} \cdots (-1)^{b_{m_i-1} p_i^{m_i-1}}.$$

To fully represent the value for ε we must include the term $(-1)^{p_i^{m_i}}$. This term is identical to -1, so we include an additional factor of -1 to preserve the original value of the expression.

Incorporating these factors, we have

$$\begin{aligned}(-1)^{b_0}\cdot(-1)^{b_1p_i}\cdots(-1)^{b_{m_i-1}p_i^{m_i-1}} &= (-1)^{b_0}\cdot(-1)^{b_1p_i}\cdots(-1)^{b_{m_i-1}p_i^{m_i-1}}\cdot(-1)^{p_i^{m_i}}\cdot(-1)\\ &= (-1)^{\left(b_0+b_1p_i+\cdots+b_{m_i-1}p_i^{m_i-1}+p_i^m\right)}\cdot(-1)\\ &= -(-1)^{\varepsilon}.\end{aligned}$$

Collecting together the various expressions above, we can simplify our expansion of the binomial coefficient $\binom{n-1}{\varepsilon}$ as

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv (-1)^{b_0}\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}}(b_0+1)(c_0-1) \mod p_i\\ &\equiv -(-1)^{\varepsilon}(b_0+1)(c_0-1) \mod p_i\\ &\equiv (-1)^{\varepsilon}(b_0+1)(1-c_0) \mod p_i.\end{aligned}$$

Incorporating the factor $(-1)^{\varepsilon}$ to match the expression in condition 1.2, we have

$$\begin{aligned}(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &\equiv (-1)^{2\varepsilon}(b_0+1)(1-c_0) \mod p_i\\ &\equiv (b_0+1)(1-c_0) \mod p_i.\end{aligned}$$

Choices for ε in the range $\{p_i^{m_i},\cdots,2p_i^{m_i}-2\}$ fail to satisfy condition 1.2 for the prime p_i dividing $n+1$ if and only if

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon}\equiv\varepsilon+1\equiv b_0+1 \mod p_i.$$

This happens if and only if

$$(b_0+1)(1-c_0)\equiv b_0+1 \mod p_i.$$

Since we are considering all choices for ε in the range $p_i^{m_i}\le\varepsilon\le 2p_i^{m_i}-2$ with $b_0\neq p-1$, we know that $b_0\le p_i-2$, so we necessarily have $b_0+1\le p_i-1$. Since $b_0+1<p_i$, we can

divide by $b_0 + 1$ in the above congruence, and we have

$$\begin{aligned} 1 - c_0 &\equiv 1 \mod p_i \\ c_0 &\equiv 0 \mod p_i. \end{aligned}$$

This tells us that a choice for ε in this range fails to satisfy condition 1.2 for the prime p_i if and only if $c_0 \equiv 0 \mod p_i$. We have written $n+1$ as the product $q \cdot p_i^{m_i}$ according to Remark 21 where q and p_i are relatively prime. If $c_0 \equiv 0 \mod p_i$, then $p_i | q$, which is not possible. This proves that all choices for ε in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ with $b_0 \neq p_i - 1$ satisfy condition 1.2 for the prime p_i dividing $n+1$. □

Lemma 26. *[Generalization of Lemma 12]. Let $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. For a prime p_i dividing $n+1$, we give ε the generic p_i-adic expansion $\varepsilon = b_0 + b_1 p_i + \cdots + b_{m_i - 1} p_i^{m_i - 1} + b_{m_i} p_i^{m_i} + \cdots$. Any choice for ε with its p_i-adic coefficient b_0 fixed in the range $\{0, \cdots, p_i - 2\}$ and p_i-adic coefficients $\{b_1, \cdots, b_{m_i - 1}\}$ fixed in the range $\{0, \cdots, p_i - 1\}$ fails to satisfy condition 1.2 for the prime p_i and the number n if and only if $\varepsilon - \left(b_0 + b_1 \cdot p + \cdots + b_{m_i - 1} \cdot p_i^{m_i - 1}\right)$ also fails to satisfy the condition for the prime p_i and the number n.*

Proof. We rewrite $n - 1$ according to Remark 21 for an arbitrary prime power $p_i^{m_i}$ dividing $n+1$, and we have

$$n - 1 = (p_i - 2) + (p_i - 1)\, p_i + \cdots + (p_i - 1)\, p_i^{m_i - 1} + (c_0 - 1)\, p_i^{m_i} + c_1 p_i^{m_i + 1} + \cdots .$$

We give ε the generic p_i-adic expansion

$$\varepsilon = b_0 + b_1 p_i + \cdots + b_{m_i - 1} p_i^{m_i - 1} + b_{m_i} p_i^{m_i} + b_{m_i + 1} p_i^{m_i + 1} + \cdots ,$$

where $b_0 \neq p_i - 1$, so that $\varepsilon \not\equiv -1 \mod p_i$. Applying Lucas' Theorem, Lemma 5, and Lemma 22, we can rewrite the binomial coefficient $\binom{n-1}{\varepsilon}$ as

$$\begin{aligned}
\binom{n-1}{\varepsilon} &\equiv \binom{p_i-2}{b_0}\binom{p_i-1}{b_1}\cdots\binom{p_i-1}{b_{m_i-1}}\binom{c_0-1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\
&\equiv (-1)^{b_0}\cdot(b_0+1)\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}}\cdot\binom{c_0-1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\
&\equiv (-1)^{b_0}\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}}\cdot(b_0+1)\binom{c_0-1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i.
\end{aligned}$$

Here, as in Propositions 23 and 25, we wish to unify the factors

$$(-1)^{b_0}\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}}$$

by rewriting the exponents of these factors in terms of ε. The p_i-adic expansion for ε given as $b_0 + b_1 p_i + \cdots$ has an unspecified final term. We can still include the remaining factors, but we do not know whether the factor $(-1)^{\varepsilon}$ is positive or negative. To be specific, we reconstruct ε in the exponents of the factors of (-1) as we did before, writing

$$\begin{aligned}
(-1)^{b_0}\cdot(-1)^{b_1}\cdots(-1)^{b_{m_i-1}} &= (\pm 1)\,(-1)^{b_0}\cdot(-1)^{b_1 p_i}\cdots(-1)^{b_{m_i-1}p_i^{m_i-1}}\cdot(-1)^{b_{m_i}p_i^{m_i}}\cdots \\
&= (\pm 1)\,(-1)^{\left(b_0+b_1p_i+\cdots+b_{m_i-1}p_i^{m_i-1}+b_{m_i}p_i^{m_i}+\cdots\right)} \\
&= (\pm 1)\,(-1)^{\varepsilon}.
\end{aligned}$$

The factor (± 1) is included to preserve the original value of the expression, since the value of $(-1)^{\varepsilon}$ may be positive or negative.

Using the above expression, we now incorporate the factor $(-1)^{\varepsilon}$ to match the expression in condition 1.2, and we have

$$\begin{aligned}
(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &\equiv (-1)^{\varepsilon}(\pm 1)(-1)^{\varepsilon}(b_0+1)\binom{c_0-1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\
&\equiv (\pm 1)(b_0+1)\binom{c_0-1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i.
\end{aligned}$$

We recall that $\varepsilon + 1 \equiv b_0 + 1 \mod p_i$. It follows that $(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv \varepsilon + 1 \equiv b_0 + 1 \mod p_i$ if and only if

$$\varepsilon + 1 \equiv (\pm 1)(b_0 + 1)\binom{c_0 - 1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i,$$

which holds if and only if

$$\pm 1 \equiv \binom{c_0 - 1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i.$$

When this congruence holds, we know that the choice for ε fails to satisfy condition 1.2 for the prime p_i. We note that this property is completely independent of the first m_i of ε's p_i-adic coefficients $\{b_0, b_1, \cdots, b_{m_i-1}\}$ as is seen in the congruences above. This shows that a choice $\varepsilon \not\equiv -1 \mod p_i$ fails to satisfy condition 1.2 for a prime p_i if and only if $\varepsilon - \left(b_0 + b_1 \cdot p + \cdots + b_{m_i-1} \cdot p_i^{m_i-1}\right)$ also fails to satisfy the condition for the prime p_i and the number n. □

The following corollary follows immediately from the preceding lemma.

Corollary 27. *Let $n + 1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. If $\varepsilon = k p_i^{m_i}$, where the prime power $p_i^{m_i}$ divides $n + 1$ and k is an integer, fails to satisfy condition 1.2 for the prime p_i, then all choices for ε in the range $\{k p_i^{m_i}, \cdots, (k+1) p_i^{m_i} - 2\}$ also fail to satisfy condition 1.2 for the prime p_i and the number n.*

The following corollary is identical to Lemma 26 but stated in a positive sense, describing ranges containing choices for ε that satisfy condition 1.2 for the prime p_i dividing $n + 1$. From the earlier proof, the congruence

$$\pm 1 \equiv \binom{c_0 - 1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i$$

does not contain the p_i-adic coefficients $\{b_0, \cdots, b_{m_i-1}\}$. This shows that the value of these coefficients do not affect whether a choice $\varepsilon \not\equiv -1 \mod p_i$ satisfies condition 1.2 for a prime p_i dividing $n + 1$. So, if any choice for ε with coefficient b_0 fixed in the range $\{0, \cdots, p - 2\}$ and coefficients $\{b_1, \cdots, b_{m_i-1}\}$ fixed in the range $\{0, \cdots, p - 1\}$ satisfies condition 1.2 for

the prime p_i, then all choices for ε with coefficients b_κ fixed in these ranges also satisfy the condition for the prime p_i and the number n.

Corollary 28. *Take a number $n+1$ not a prime power with n even. For any prime power $p_i^{m_i}$ dividing $n+1$, any choice for ε with its p_i-adic coefficient b_0 fixed in the range $\{0, \cdots, p_i - 2\}$ and p_i-adic coefficients $\{b_1, \cdots, b_{m_i-1}\}$ fixed in the range $\{0, \cdots, p_i - 1\}$ satisfies condition 1.2 for the prime p_i and the number n if and only if the choice $\varepsilon - \left(b_0 + b_1 \cdot p + \cdots + b_{m_i-1} \cdot p_i^{m_i-1}\right)$ also satisfies the condition for the prime p_i and the number n.*

The following corollary is identical to Corollary 27 but stated in a positive sense.

Corollary 29. *Let $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. If $\varepsilon = k p_i^{m_i}$, where the prime power $p_i^{m_i}$ divides $n+1$ and k is an integer, satisfies condition 1.2 for the prime p_i, then all choices for ε in the range $\{k p_i^{m_i}, \cdots, (k+1)\, p_i^{m_i} - 2\}$, except where $\varepsilon \equiv -1 \mod p_i$, also satisfy condition 1.2 for the prime p_i and the number n.*

We take a moment to generalize Proposition 8, to verify that a similar property holds when $n+1$ has a generic prime factorization.

Proposition 30. *Let $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. For a prime p_i dividing $n+1$, any choice for ε with $b_{m_i} = p_i - 1$ and $b_0 \neq p_i - 1$ necessarily satisfies condition 1.2 for the prime p_i dividing $n+1$.*

Proof. We rewrite $n-1$ according to Remark 21 for an arbitrary prime power $p_i^{m_i}$ dividing $n+1$, which gives

$$n - 1 = (p_i - 2) + (p_i - 1)\, p_i + \cdots + (p_i - 1)\, p_i^{m_i - 1} + (c_0 - 1)\, p_i^{m_i} + c_1 p_i^{m_i+1} + \cdots .$$

We assume that ε has p_i-adic coefficient b_{m_i} equal to $p_i - 1$. By Lemma 26, we can give ε the p_i-adic expansion $(p_i - 1)\, p_i^{m_i} + b_{m_i+1} p_i^{m_i+1} + \cdots$, where each b_κ is a nonnegative integer less than p_i, and the coefficients $\{b_0, \cdots, b_{m_i-1}\}$ are identically equal to zero. Applying

Lucas' Theorem and the convention on binomial coefficients stated there, we have

$$\begin{aligned}\binom{n-1}{\varepsilon} &\equiv \binom{p-2}{0}\binom{p-1}{0}\cdots\binom{p-1}{0}\binom{c_0-1}{p_i-1}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\ &\equiv (1)\cdots(1)\,(0)\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\ &\equiv 0 \mod p_i.\end{aligned}$$

This is true since $c_0 < p_i$ immediately implies $c_0 - 1 < p_i - 1$. It follows that

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv 0 \not\equiv 1 \equiv \varepsilon + 1 \mod p_i.$$

This shows that any choice for ε with p_i-adic coefficient $b_{m_i} = p_i - 1$ immediately satisfies condition 1.2 for the prime p_i dividing $n+1$. □

The following lemma generalizes Lemma 16. We consider again the number $n+1$ not a prime power. For any prime power $p_i^{m_i}$ dividing $n+1$, we know by Lemma 26 that all choices for ε in a range characterized as $\{kp_i^{m_i}, \cdots, (k+1)\,p_i^{m_i} - 2\}$, where k is an integer and $\varepsilon \not\equiv -1 \mod p_i$, either satisfy condition 1.2 for a prime p_i, or they do not. Now, we want to show that if the choices for ε, where $b_0 \neq p_i - 1$, in such a range do not satisfy condition 1.2 for the prime p_i, then the suitable choices for ε in the next consecutive range $\{(k+1)\,p_i^{m_i}, \cdots, (k+2)\,p_i^{m_i} - 2\}$ do satisfy the condition.

Lemma 31. *[Generalization of Lemma 16]. Take $n+1$ not a prime power with n even. If the choice $\varepsilon' \not\equiv -1 \mod p_i$ for the prime power $p_i^{m_i}$ dividing $n+1$ fails to satisfy condition 1.2 for the prime p_i, then the choice $\varepsilon = \varepsilon' + p_i^{m_i}$ satisfies the condition for the prime p_i and the number n.*

Proof. We rewrite $n-1$ according to Remark 21 for an arbitrary prime power $p_i^{m_i}$ dividing $n+1$, which gives

$$n - 1 = (p_i - 2) + (p_i - 1)\,p_i + \cdots + (p_i - 1)\,p_i^{m_i - 1} + (c_0 - 1)\,p_i^{m_i} + c_1 p_i^{m_i+1} + \cdots.$$

We select an ε' that fails to satisfy condition 1.2 for the prime p_i dividing $n+1$. By Lemma 26 we can give ε' the p_i-adic expansion $b_{m_i}p_i^{m_i} + b_{m_i+1}p_i^{m_i+1} + \cdots$, where each b_κ is a nonnegative integer less than p_i, and the coefficients $\{b_0, \cdots, b_{m_i-1}\}$ are identically equal to zero. Since ε' fails to satisfy proposition 1.2 for the prime p_i by assumption, we have $(-1)^{\varepsilon'}\binom{n-1}{\varepsilon'} \equiv \varepsilon' + 1 \equiv 1 \mod p_i$. We now let $\varepsilon = \varepsilon' + p_i^{m_i}$, which has the p_i-adic expansion given by $\varepsilon = (b_{m_i}+1)\,p^{m_i} + b_{m_i+1}p^{m_i+1} + \cdots$. We know that the inequality $b_{m_i} + 1 < p_i$ holds since if $b_{m_i} = p_i - 1$, then the choice ε' would satisfy condition 1.2 for the prime p_i by Proposition 30, but the choice ε' fails to satisfy the condition by assumption.

Applying Lucas' Theorem and some rewriting techniques similar to those used in Lemma 16, we can rewrite the binomial coefficient $\binom{n-1}{\varepsilon}$ as

$$\begin{aligned}
\binom{n-1}{\varepsilon} &\equiv \binom{p-2}{0}\binom{p-1}{0}\cdots\binom{p-1}{0}\binom{c_0-1}{b_{m_i}+1}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\
&\equiv \binom{c_0-1-b_{m_i}}{b_{m_i}+1}\binom{c_0-1}{b_{m_i}}\binom{c_1}{b_{m_i+1}}\cdots \mod p_i \\
&\equiv \binom{c_0-(b_{m_i}+1)}{b_{m_i}+1}\binom{n-1}{\varepsilon'} \mod p_i.
\end{aligned}$$

We now incorporate the factor $(-1)^{\varepsilon}$ to match the expression contained in condition 1.2, which gives

$$\begin{aligned}
(-1)^{\varepsilon}\binom{n-1}{\varepsilon} &\equiv (-1)^{\varepsilon'+p_i^{m_i}}\binom{c_0-(b_{m_i}+1)}{b_{m_i}+1}\binom{n-1}{\varepsilon'} \mod p_i \\
&\equiv -\binom{c_0-(b_{m_i}+1)}{b_{m_i}+1}\cdot\left[(-1)^{\varepsilon'}\binom{n-1}{\varepsilon'}\right] \mod p_i \\
&\equiv -\binom{c_0-(b_{m_i}+1)}{b_{m_i}+1}\cdot[1] \mod p_i \\
&\equiv -\binom{c_0-(b_{m_i}+1)}{b_{m_i}+1} \mod p_i.
\end{aligned}$$

This choice for ε fails to satisfy condition 1.2 if and only if

$$(-1)^{\varepsilon}\binom{n-1}{\varepsilon} \equiv \varepsilon + 1 = 1 \mod p_i,$$

which happens if and only if

$$\begin{aligned} -\left(\frac{c_0-(b_{m_i}+1)}{b_{m_i}+1}\right) &\equiv 1 \mod p_i \\ c_0-(b_{m_i}+1) &\equiv -(b_{m_i}+1) \mod p_i \\ c_0 &\equiv 0 \mod p_i. \end{aligned}$$

Recall that c_0 is the first p_i-adic coefficient of the number q, which was defined to be relatively prime to p_i in Remark 21. So, the congruence above is impossible, since $q \equiv c_0 \equiv 0 \mod p_i$ implies p_i divides q. This shows that if a choice $\varepsilon' \not\equiv -1 \mod p_i$ fails to satisfy condition 1.2 for the prime p_i dividing $n+1 = p_1^{m_1} \cdots p_t^{m_t}$, then the choice $\varepsilon = \varepsilon' + p_i^{m_i}$ must satisfy condition 1.2 for the prime p_i and the number n. □

The following corollary states the preceding proposition in terms of ranges containing choices for ε.

Corollary 32. *Let $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. If $\varepsilon' = k p_i^{m_i}$ for integer k fails to satisfy condition 1.2 for the prime p_i dividing $n+1$, then the choice $\varepsilon = \varepsilon' + p_i^{m_i} = (k+1)\, p_i^{m_i}$ satisfies condition 1.2 for the prime p_i and the number n. By Corollary 28 and Corollary 29 all choices for ε in the range $\{\varepsilon, \cdots, \varepsilon + p_i^{m_i} - 2\} = \{(k+1)\, p_i^{m_i}, \cdots, (k+2)\, p_i^{m_i} - 2\}$, where $\varepsilon \not\equiv -1 \mod p_i$, also satisfy condition 1.2 for the prime p_i and the number n.*

5. Generalization: Two Prime Powers

The following theorem generalizes Theorem 18, which shows that for any odd number $n+1$ composed of two squarefree prime factors, there is always a choice for ε satisfying conjecture 1.1 for the even number n. For the generalization we consider the number $n+1$ with nonsquarefree prime factors. The generic factorization for this number can be written as $n+1 = p_1^{m_1} \cdot p_2^{m_2}$ with the convention $p_1^{m_1} < p_2^{m_2}$. No conditions are placed on the relative size of the primes p_1 and p_2. This theorem was proved by Walter Parry using a significantly different method. Though this is not an entirely new result, an alternative form of the proof is included here as it is instructive in developing a general proof for conjecture 1.1 using the methods of this paper.

Theorem 33. *[Alternative Proof of a Theorem of Walter Parry]. If $n+1 = p_1^{m_1} \cdot p_2^{m_2}$, where $p_1 \neq p_2$ are both prime and $p_1^{m_1} < p_2^{m_2}$, there is a choice for ε in the range $\{p_2^{m_2}, \cdots, n-2\}$ that will make the expression $R_n(\varepsilon)$ and the number $n+1$ relatively prime, satisfying conjecture 1.1 for the number n.*

Proof. By Corollary 24, the smallest choice for ε that can possibly satisfy conjecture 1.1 for the number n is $p_2^{m_2}$. By Proposition 25 all choices for ε in the range $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$, except where $\varepsilon \equiv -1 \mod p_2$, satisfy condition 1.2 for the prime p_2. By the same proposition, all choices for ε in the range $\{p_1^{m_1}, \cdots, 2p_1^{m_1} - 2\}$, except where $\varepsilon \equiv -1 \mod p_1$, satisfy the condition for the prime p_1.

Case 1. $p_2^{m_2} < 2p_1^{m_1} - 1$. By assumption $p_2^{m_2}$ is odd. The number $2p_1^{m_1} - 2$ is even. Therefore, the inequality $p_2^{m_2} \leq 2p_1^{m_1} - 3$ must hold. The bound ensures that the numbers $p_2^{m_2}$ and $p_2^{m_2} + 1$ must be contained in the interval $\{p_1^{m_1}, \cdots, 2p_1^{m_1} - 2\}$. If $p_2^{m_2} \not\equiv -1 \mod p_1$, then $\varepsilon = p_2^{m_2}$ simultaneously satisfies condition 1.2 for the primes p_1 and p_2. On the other hand, if $p_2^{m_2} \equiv -1 \mod p_1$, then $p_2^{m_2} + 1 \equiv 0 \mod p_1$, and the choice $\varepsilon = p_2^{m_2} + 1$ simultaneously satisfies condition 1.2 for both primes. One of these must hold. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Case 2. $p_2^{m_2} = 2p_1^{m_1} - 1$. By the condition of this case, we can express the range $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$ equivalently as $\{2p_1^{m_1} - 1, \cdots, 4p_1^{m_1} - 4\}$. This interval contains the numbers $2p_1^{m_1}$, $3p_1^{m_1}$, and $3p_1^{m_1} + 1$ by the nature of its structure. (This is true as long as $p_1^{m_1} > 3$. See Theorem 18, Case 1 for the case when $p_1^{m_1} = 3$ and $p_2^{m_2} = 2p_1^{m_1} - 1 = 5$.) By Lemma 31, either $\varepsilon = 2p_1^{m_1}$ or $\varepsilon = 3p_1^{m_1}$ must satisfy condition 1.2 for the prime p_1. In the current case, the choice $\varepsilon = 2p_1^{m_1} \not\equiv -1 \mod p_2$ satisfies condition 1.2 for the prime p_2, and if this choice also satisfies the condition for the prime p_1, we are done. If this choice does not satisfy condition 1.2 for the prime p_1, then by Lemma 31 the choices $\varepsilon = 3p_1^{m_1}$ and $\varepsilon = 3p_1^{m_1} + 1$ must satisfy the condition for the prime p_1. If $3p_1^{m_1} \equiv -1 \mod p_2$, then $\varepsilon = 3p_1^{m_1} + 1$ satisfies condition 1.2 for both primes. One of the choices for ε in the set $\{2p_1^{m_1}, 3p_1^{m_1}, 3p_1^{m_1} + 1\}$ must satisfy condition 1.2 for both primes p_1 and p_2. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Case 3. $p_2^{m_2} \geq 2p_1^{m_1} + 1$. By this condition, the smallest possible value for $p_2^{m_2}$ is $2p_1^{m_1} + 1$. In that case the interval $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$ is equivalent to $\{2p_1^{m_1} + 1, \cdots, 4p_1^{m_1}\}$, which has exactly $2p_1^{m_1}$ elements. This guarantees at least two multiples of $p_1^{m_1}$ in the interval $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$ since in all other cases the value of $p_2^{m_2}$ is greater. Call these multiples $kp_1^{m_1}$ and $(k+1)\,p_1^{m_1}$ where k is an integer. In the subrange $\{kp_1^{m_1}, \cdots, (k+1)\,p_1^{m_1}\}$ there are exactly $p_1^{m_1} + 1$ elements. This leaves at least $p_1^{m_1} - 1 = 4$ elements remaining in the interval $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$, since the minimum of $p_1^{m_1}$ is 5, and there are at least $2p_1^{m_1}$ elements in the interval. These elements must be less than $kp_1^{m_1}$ or greater than $(k+1)\,p_1^{m_1}$. If even one element is greater than $(k+1)\,p_1^{m_1}$, then we can guarantee that the subrange $\{(k+1)\,p_1^{m_1} - 3, \cdots, (k+1)\,p_1^{m_1} + 1\}$ is in the interval $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$. By Lemma 31 and Corollary 32 either $\varepsilon = (k+1)\,p_1^{m_1} - 2$ or $\varepsilon = (k+1)\,p_1^{m_1}$ must satisfy condition 1.2 for the prime p_1 and the number n. If for either choice we have $\varepsilon \equiv -1 \mod p_2$, then select either $\varepsilon = kp_1^{m_1} - 3$ or $\varepsilon = kp_1^{m_1} + 1$ from the corresponding ranges, and we are done. On the other hand,

if $(k+1)\,p_1^{m_1}$ is the largest element in the interval $\{p_2^{m_2}, \cdots, 2p_2^{m_2}-2\}$, then there are at least four elements smaller than the number $kp_1^{m_1}$, which guarantees that the subrange $\{kp_1^{m_1}-3, \cdots, kp_1^{m_1}+1\}$ is contained in the interval. By a similar argument employing the same lemma and corollary, this subrange must contain a choice for ε satisfying condition 1.2 for both primes p_1 and p_2. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Taking Cases 1–3 together, we have shown that for the number $n+1 = p_1^{m_1} \cdot p_2^{m_2}$, a choice for ε exists that will make the expression $R_n(\varepsilon)$ and the number $n+1$ relatively prime, satisfying conjecture 1.1 for the number n.

□

6. Primes Far Apart: Partial Generalization of Theorem 19

In this section, we provide a partial generalization of Theorem 19. That theorem considers a number $n+1$ of form $n+1 = p_1 p_2 \cdots p_t$ where the primes p_i are far apart from each other. In that theorem, the bound $p_k \geq 3p_k + 1$ for consecutive prime factors of $n+1$ guaranteed the result. In the generalization given here, we consider a number $n+1$ with possibly many nonsquarefree prime factors. We express the generic prime factorization of this number as $n+1 = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$.

The methods needed for a direct generalization of Theorem 19 are beyond the scope of this paper. A complete generalization would require a more intensive treatment of the relations among the primes since we would need to verify that a choice for ε is not congruent to -1 for any of the t prime factors of $n+1$. The difficulties of this task can be seen in the complexities of the proof of Theorem 33, where we take care to ensure that our choice for ε is not congruent to -1 for either of the primes p_1 or p_2. In that case, the number $n+1$ had only two prime factors. In the current situation, the number $n+1$ has t prime factors where t can be any positive integer. This means that the method used in the proof of Theorem 33 would be cumbersome and is not preferred for this case. We offer a partial generalization that still allows us to handle many new even numbers n where $n+1$ is neither squarefree nor a prime power.

Theorem 34. *Let $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_{t-1}^{m_{t-1}} \cdot p_t^{m_t}$ with the convention $p_1^{m_1} < p_2^{m_2} < \cdots < p_{t-1}^{m_{t-1}} < p_t^{m_t}$. If the bound $p_k \geq p_{k-1}^{m_{k-1}} + 2p_{k-1}$ is satisfied for all consecutive factors p_k and p_{k-1} of $n+1$, then there is a choice for ε satisfying conjecture 1.1 for the number n.*

Proof. By Proposition 25, we know that all choices for ε in the range $\{p_t^{m_t}, \cdots, p_t^{m_t} + p_t - 2\}$ satisfy condition 1.2 for the prime p_t and the number n without exception since the specified range contains no numbers that are one less than a multiple of p_t. The range $\{p_t^{m_t}, \cdots, p_t^{m_t} + p_t - 2\}$ contains $p_t - 1$ elements, and the bound stated in the theorem guarantees the inequality $p_t - 1 \geq p_{t-1}^{m_{t-1}} + 2p_{t-1} - 1$. There is at least one multiple

of the prime power $p_{t-1}^{m_{t-1}}$ in the interval. For convenience, call it $lp_{t-1}^{m_{t-1}}$ where l is an integer. If there are at least p_{t-1} elements smaller than $lp_{t-1}^{m_{t-1}}$ contained in the larger interval, which is allowed by the bound on consecutive primes, then by Proposition 32 all choices for ε in one of the subintervals, $\left\{lp_{t-1}^{m_{t-1}} - p_{t-1}, \cdots, lp_{t-1}^{m_{t-1}} - 2\right\}$ or $\left\{lp_{t-1}^{m_{t-1}}, \cdots, lp_{t-1}^{m_{t-1}} + p_{t-1} - 2\right\}$, are guaranteed to satisfy condition 1.2 for the primes p_{t-1} and p_t without exception. But suppose there are at most $p_{t-1} - 1$ elements smaller than $lp_{t-1}^{m_{t-1}}$ contained in the interval, so that in the worst case scenario the smallest element in the interval is $lp_{t-1}^{m_{t-1}} - p_{t-1} - 1$. Then, by the bound on the consecutive prime factors of $n + 1$, we know that the element $\left(lp_{t-1}^{m_{t-1}} - p_{t-1} - 1\right) + \left(p_{t-1}^{m_{t-1}} + 2p_{t-1} - 1\right) = (l + 1)\, p_{t-1}^{m_{t-1}} + p_{t-1} - 2$ is guaranteed to be in the interval. In one of the subintervals, either $\left\{lp_{t-1}^{m_{t-1}}, \cdots, lp_{t-1}^{m_{t-1}} + p_{t-1} - 2\right\}$ or $\left\{(l + 1)\, p_{t-1}^{m_{t-1}}, \cdots, (l + 1)\, p_{t-1}^{m_{t-1}} + p_{t-1} - 2\right\}$, all choices for ε are guaranteed to satisfy condition 1.2 for the primes p_{t-1} and p_t, unconditionally. This guarantees a range containing choices for ε satisfying condition 1.2 for the primes p_t and p_{t-1}, simultaneously.

Considering the prime power $p_{t-2}^{m_{t-2}}$ and applying a similar analysis to that above, we can establish a range containing choices for ε that satisfy condition 1.2 for the primes p_t, p_{t-1}, and p_{t-2}, unconditionally. Continuing inductively, we can establish a nonempty interval containing choices for ε that simultaneously satisfy condition 1.2 for all primes p_i dividing $n + 1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n. □

Directly below, we give an example of a number $n + 1$ for which the previous theorem guarantees a choice for ε satisfying conjecture 1.1 for the number n. We note here that the numbers covered by this proposition, including the particular n of the example below, are not covered by any of the previously known results.

Example 35. Consider the number $n + 1 = 3^3 \cdot 37^2 \cdot 1\,447 = 53\,485\,461$. We note that the bounds required by the theorem are satisfied since $1\,447 \geq 37^2 + 2 \cdot 37 = 1\,443$ and $37 \geq 3^3 + 2 \cdot 3 = 33$. This guarantees a choice for ε in the interval $\{1\,447, \cdots, 2 \cdot 1\,447 - 2\} = \{1\,447, \cdots, 2\,892\}$ satisfying conjecture 1.1 for the number n.

By the bound on the consecutive primes, we are guaranteed that the interval contains at least one multiple of the prime power $37^2 = 1\,369$. The particular multiple contained in this

interval is $2 \cdot 1\,369 = 2\,738$. By the proposition, we can construct our subintervals around this multiple of 19^2 if there are at least $p_{t-1} = 37$ elements smaller than $2\,738$ contained in the interval. In this case the condition holds, and the guaranteed subintervals $\left\{lp_{t-1}^{m_{t-1}} - p_{t-1}, \cdots, lp_{t-1}^{m_{t-1}} - 2\right\} = \{2\,738 - 37, \cdots, 2\,738 - 2\} = \{2\,701, \cdots, 2\,736\}$ and $\left\{lp_{t-1}^{m_{t-1}}, \cdots, lp_{t-1}^{m_{t-1}} + p_{t-1} - 2\right\} = \{2\,738, \cdots, 2\,738 + 37 - 2\} = \{2\,738, \cdots, 2\,773\}$ are in the interval. At least one of these ranges must contain choices for ε that satisfy condition 1.2 for the prime 37. Checking, we have $(-1)^{2\,738}\binom{53\,485\,459}{2\,738} \equiv \binom{35}{0}\binom{36}{0}\binom{33}{2}\binom{19}{0}\binom{28}{0} = 528 \equiv 10 \not\equiv 1 \equiv 2\,738 + 1 \mod 37$. This shows that choices for ε in the range $\{2\,738, \cdots, 2\,773\}$ satisfy condition 1.2 for the prime 37.

Considering now the prime $p_{t-2} = 3$, the bound of the theorem guarantees that the range $\{2\,738, \cdots, 2\,773\}$ contains at least one multiple of $3^3 = 27$. In fact, we have the multiple $102 \cdot 3^3 = 2754$ in the interval. Again, by the theorem, if there are $p_{t-2} = 3$ elements smaller than $2\,754$ contained in the interval, we can construct our subintervals around this multiple of 27. There are, and we are guaranteed that choices for ε in one of the intervals $\{2\,754 - 3, \cdots, 2\,754 - 2\} = \{2\,751, \cdots, 2\,752\}$ or $\{2\,754, \cdots, 2\,754 + 3 - 2\} = \{2\,754, \cdots, 2\,755\}$ satisfy condition 1.2 for the prime $p_{t-2} = 3$. Checking we have $(-1)^{2\,754}\binom{53\,485\,459}{2\,754} \equiv \binom{1}{0}\binom{2}{0}\binom{2}{0}\binom{0}{0}\binom{2}{1}\binom{0}{2}\binom{0}{0}\binom{0}{1}\binom{1}{0}\cdots \equiv 0 \not\equiv 1 \equiv 2\,754 + 1 \mod 3$. So, choices for ε in the range $\{2\,754, \cdots, 2\,755\}$ satisfy condition 1.2 for the prime factor 3. (In fact, choices for ε in the alternate range also satisfy the condition for the prime 3.)

These choices simultaneously satisfy condition 1.2 for the primes 1447, 37, and 3. This guarantees at least one choice for ε satisfying conjecture 1.1 for the number $n = 53\,485\,460$. (There are more choices than the ones stated.)

7. Primes Close Together: Partial Generalizations

In this section we offer a few partial generalizations of Theorem 20. In that theorem we saw that if the squarefree prime factors of $n+1$ are sufficiently close together, then there is a guaranteed choice for ε satisfying conjecture 1.1 for the number n. We wish to generalize to the case where the primes dividing the number $n+1$ are possibly of degree greater than one. We give $n+1$ the arbitrary prime factorization

$$n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t}$$

with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$.

If the bound $p_t^{m_t} \leq 2p_1^{m_1} - 1$, which is similar to the bound required in Theorem 20, holds on the prime powers dividing $n+1$, and if $2p_1^{m_1} - 1$ is relatively prime to $n+1$, then there is a guaranteed choice for ε satisfying conjecture 1.1 for the number n. The additional condition on the number $2p_1^{m_1} - 1$ is absent from Theorem 20. As mentioned in the introduction to Section 6, identifying whether a given choice for ε is congruent to -1 for any of the primes $\{p_1, \cdots, p_t\}$ dividing $n+1$ requires much attention when working with nonsquarefree prime factors. This difficulty is averted in the following proposition by introducing this additional condition.

Proposition 36. *Let $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_t^{m_t}$ with the convention $p_1^{m_1} < \cdots < p_t^{m_t}$. If the bound $p_t^{m_t} < 2p_1^{m_1} - 1$ holds and if $2p_1^{m_1} - 1$ and $n+1$ are relatively prime, then there is a guaranteed choice for ε satisfying conjecture 1.1 for the number n.*

Proof. By assumption, for any prime p_i dividing $n+1$, we have $2p_1^{m_1} - 1 \not\equiv 0 \mod p_i$. It follows that $2p_1^{m_1} - 2 \not\equiv -1 \mod p_i$ for any prime dividing $n+1$. The bound $p_t^{m_t} < 2p_1^{m_1} - 1$ ensures that the string of inequalities $p_1^{m_1} \leq p_i^{m_i} \leq p_t^{m_t} < 2p_1^{m_1} - 2 \leq 2p_i^{m_i} - 2$ holds for all prime powers $p_i^{m_i}$ dividing $n+1$. From this string of inequalities, we see that the value $\varepsilon = 2p_1^{m_1} - 2$ is in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for every prime power $p_i^{m_i}$ dividing $n+1$. By Proposition 25 the choice

$\varepsilon = 2p_1^{m_1} - 2$ simultaneously satisfies condition 1.2 for each prime p_i dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n. $\square$

Remark 37. The preceding proposition holds immediately in the case that the number $2p_1^{m_1} - 1$ is prime since $n+1$ and $2p_1^{m_1} - 1$ are then immediately relatively prime. (The bound $p_t^{m_t} < 2p_1^{m_1} - 1$ guarantees that the prime $2p_1^{m_1} - 1$ does not divide $n+1$, so the choice $\varepsilon = 2p_1^{m_1} - 2$ is guaranteed to satisfy conjecture 1.1 for the number n.)

Here we provide an example of a number $n+1$ for which the previous proposition guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Example 38. Consider the number $n+1 = 7^5 \cdot 17\,011 \cdot 131^2 \cdot 137^2 \cdot 139^2 \cdot 3^9 \cdot 21\,011 \cdot 149^2 \cdot 151^2 \cdot 29^3 \cdot 157^2 \cdot 163^2 \cdot 167^2 \cdot 28\,031 \cdot 13^4 \cdot 31^3 \cdot 173^2 \cdot 179^2 \cdot 181^2$.

The bound $p_t^{m_t} \leq 2p_1^{m_1} - 2$ of Proposition 36 is satisfied since $181^2 = 32\,761 \leq 33\,612 = 2 \cdot 7^5 - 2$. By the construction of the number $n+1$, we see that the choice for ε given by $2p_1^{m_1} - 2 = 2 \cdot 7^5 - 2 = 33\,612$ falls in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for each prime dividing $n+1$. We note further that the number $2p_1^{m_1} - 1 = 2 \cdot 7^5 - 1 = 33\,613$ is prime. As mentioned in Remark 37, since $2p_1^{m_1} - 1$ is prime, the choice $\varepsilon = 33\,612$ is not congruent to -1 for any prime p_i dividing $n+1$. This is a guaranteed choice for ε satisfying conjecture 1.1 for the number n where $n+1$ is given above.

We continue with a variety of partial generalizations of Theorem 20. The purpose of the following propositions is to explore the difficulties that arise as we approach an unconditional generalization of the theorem. The original theorem considers the case when the number $n+1$ is the product of squarefree prime factors. In the following propositions, we allow an increasing number of nonsquarefree primes in the prime factorization of $n+1$. We hope to document the difficulties of the approach taken in this paper, as well as to identify methods that might enable a general solution.

In the following propositions, we use the expression $p_i^{m_i}$ to represent an arbitrary prime power dividing $n+1$, including when $m_i = 1$. In the following proposition, we allow the first

prime factor of $n+1$ to have degree greater than one. We see that this does not change the result given in Theorem 20.

Proposition 39. *Let $n+1 = p_1^{m_1} \cdot p_2 \cdots p_t$ with the convention $p_1^{m_1} < p_2 < \cdots < p_t$. If the bound $p_t < 2p_1^{m_1} - 1$ is satisfied, then we are guaranteed a choice for ε satisfying conjecture 1.1 for the number n.*

Proof. The bound $p_t < 2p_1^{m_1} - 1$ ensures that the string of inequalities $p_1^{m_1} \leq p_i^{m_i} \leq p_t \leq 2p_1^{m_1} - 3 < 2p_1^{m_1} - 2 \leq 2p_i^{m_i} - 2$ holds for all $p_i^{m_i}$ dividing $n+1$, including when $m_i = 1$. From this string of inequalities, we see that the value $\varepsilon = 2p_1^{m_1} - 2$ is in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for every prime p_i dividing $n+1$. We see that $2p_1^{m_1} - 2 \not\equiv -1 \mod p_i$ for any prime p_i dividing $n+1$; otherwise, we would have $2p_1^{m_1} - 1 \equiv 0 \mod p_i$ for some prime p_i dividing $n+1$. But this contradicts the string of inequalities above. By Proposition 25 the choice $\varepsilon = 2p_1^{m_1} - 2$ satisfies condition 1.2 for each prime p_i dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n. □

We give an example of a number $n+1$ for which the preceding proposition guarantees a choice for ε satisfying conjecture 1.1 for the number n .

Example 40. Consider the number $n+1 = 5^3 \cdot 127 \cdot 229 \cdot 241$, which fits the factorization of the previous proposition. The bound $p_t^{m_t} \leq 2p_1^{m_1} - 2$ of Proposition 36, where $m_t = 1$, is satisfied since $5^3 = 125 < 241 \leq 2 \cdot 5^3 - 2 = 248$. The choice $\varepsilon = 248$ falls in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for each prime dividing $n+1$, including when $m_i = 1$. By the previous proposition this is the choice for ε guaranteed to satisfy conjecture 1.1 for the number $n = 876\,125\,374$.

In the following proposition we allow the prime factors p_1 and p_t of $n+1$ to possibly have degree greater than one. We see that this minimally affects the result of Theorem 20. Again, we let $p_i^{m_i}$ represent a generic prime power dividing $n+1$, including when $m_i = 1$.

Proposition 41. *Let $n+1 = p_1^{m_1} \cdot p_2 \cdots p_{t-1} \cdot p_t^{m_t}$ with the convention $p_1^{m_1} < p_2 < \cdots < p_{t-1} < p_t^{m_t}$. If the bound $p_t^{m_t} < 2p_1^{m_1} - 1$ is satisfied, then we are guaranteed a choice for ε satisfying conjecture 1.1 for the number n.*

Proof. The bound $p_t^{m_t} < 2p_1^{m_1} - 1$ ensures that the string of inequalities $p_1^{m_1} \leq p_i^{m_i} \leq p_t^{m_t} < 2p_1^{m_1} - 2 \leq 2p_i^{m_i} - 2$ holds for all prime powers $p_i^{m_i}$ dividing $n+1$, including when $m_i = 1$. From this string of inequalities, we see that the choice $\varepsilon = 2p_1^{m_1} - 2$ is in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for every prime power $p_i^{m_i}$ dividing $n+1$ (in most cases $m_i = 1$).

Propositions 11 and 25 guarantee that these ranges contain choices for ε satisfying condition 1.2 for each prime p_i dividing $n+1$, individually. We see that $2p_1^{m_1} - 2 \not\equiv -1 \mod p_i$ for any squarefree prime p_i dividing $n+1$; otherwise, we would have $2p_1^{m_1} - 1 \equiv 0 \mod p_i$ for some squarefree prime p_i dividing $n+1$. But this contradicts the string of inequalities above.

Since $p_t^{m_t} \leq 2p_1^{m_1} - 3$, it is possible that $2p_1^{m_1} - 1 \equiv 0 \mod p_t$, in which case $2p_1^{m_1} - 1 \geq p_t^{m_t} + p_t$ must hold since the string of inequalities above ensures that $2p_1^{m_1} - 1 > p_t^{m_t}$. It then follows that $2p_1^{m_1} - 3 > p_t^{m_t}$ since $p_t \geq 3$. If that happens, then the choice $\varepsilon = 2p_1^{m_1} - 3$ is a suitable choice for ε. In either case, Proposition 25 guarantees a choice for ε in this range simultaneously satisfying condition 1.2 for each prime p_i dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for n where $n+1 = p_1^{m_1} \cdot p_2 \cdots p_{t-1} \cdot p_t^{m_t}$. □

Example 42. Consider $n+1 = 7^2 \cdot 53 \cdot 61 \cdot 3^4$, which fits the form of $n+1$ of the previous proposition. The bound of Proposition 36 is satisfied since $7^2 = 49 < 3^4 = 81 < 2 \cdot 7^2 - 1 = 97$. The choice $\varepsilon = 96$ falls in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for every prime power dividing $n+1$, including when $m_i = 1$. We only need to verify whether $\varepsilon = 96$ is a suitable choice for the prime $p_t = 3$, and since $96 \equiv 0 \mod 3$, this choice satisfies condition 1.2 for each prime dividing $n+1$. (The proposition guarantees that either $\varepsilon = 2p_1^{m_1} - 2$ or $\varepsilon = 2p_1^{m_1} - 3$ satisfies the conjecture. In this case it is

the former.) There is at least one choice for ε satisfying conjecture 1.1 for the number $n = 12\,831\,776$, as guaranteed by the previous proposition.

In the following proposition, we allow the first two prime factors of $n+1$ to possibly have degree greater than one.

Proposition 43. *Let $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3 \cdots p_t$ with the convention $p_1^{m_1} < p_2^{m_2} < p_3 < \cdots < p_t$. If the bound $p_t < 2p_1^{m_1} - 1$ is satisfied, then we are guaranteed a choice for ε satisfying conjecture 1.1 for the number n.*

Proof. The bound $p_t < 2p_1^{m_1} - 1$ ensures that the string of inequalities $p_1^{m_1} \leq p_i^{m_i} \leq p_t \leq 2p_1^{m_1} - 3 < 2p_1^{m_1} - 2 \leq 2p_i^{m_i} - 2$ holds for all prime powers $p_i^{m_i}$ dividing $n+1$ where $m_i = 1$ for $i > 2$. From this string of inequalities, we see that the choices $\varepsilon = 2p_1^{m_1} - 3$ and $\varepsilon = 2p_1^{m_1} - 2$ are in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for every prime $p_i^{m_i}$ dividing $n+1$, including the cases where $m_i = 1$.

By Propositions 11 and 25, choices for ε in these ranges satisfy condition 1.2 for each prime p_i, individually. We see that $2p_1^{m_1} - 2 \not\equiv -1 \mod p_i$ for any squarefree prime p_i dividing $n+1$; otherwise, we would have $2p_1^{m_1} - 1 \equiv 0 \mod p_i$, which would contradict the string of inequalities above.

It is possible that $2p_1^{m_1} - 2 \equiv -1 \mod p_2$, but then the choice $\varepsilon = 2p_1^{m_1} - 3$ satisfies condition 1.2 for the prime p_2 as well as for all other primes dividing $n+1$. By Proposition 25, the choice $\varepsilon = 2p_1^{m_1} - 2$ or $\varepsilon = 2p_1^{m_1} - 3$ must satisfy condition 1.2 for each prime p_i dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n where $n+1 = p_1^{m_1} p_2^{m_2} p_3 \cdots p_t$. □

Example 44. Consider the number $n+1 = 3^5 \cdot 7^3 \cdot 347 \cdot 479$, which fits the prime factorization of the preceding proposition. The prime powers of $n+1$ satisfy the bound of Proposition 36 since we have $3^5 = 243 < 479 < 2 \cdot 3^5 - 1 = 485$. The choice $\varepsilon = 2p_1 - 2 = 484$ is in the range $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for each prime dividing $n+1$. We only need to verify whether the choice $\varepsilon = 484$ is suitable for the prime $p_2 = 7$ since this prime is not squarefree. We have $484 \equiv 1 \mod 7$. It follows that the choice $\varepsilon = 484$ satisfies

condition 1.2 for each prime dividing $n+1$. This is one of the potential choices for ε guaranteed by the previous proposition to satisfy conjecture 1.1 for the number $n = 13\,853\,687\,336$.

In the following proposition, consideration of the possible values that the prime factors of $n+1$ could take on forces us to divide our proof into two cases.

Proposition 45. *Let $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3 \cdots p_{t-1} \cdot p_t^{m_t}$ with the convention $p_1^{m_1} < p_2^{m_2} < p_3 < \cdots < p_{t-1} < p_t^{m_t}$. If the bound $p_t^{m_t} < 2p_1^{m_1} - 1$ is satisfied, then we are guaranteed a choice for ε satisfying conjecture 1.1 for the number n.*

Proof. In both cases presented here, the string of inequalities $p_1^{m_1} \leq p_i^{m_i} \leq p_t^{m_t} \leq 2p_1^{m_1} - 3 < 2p_1^{m_1} - 2 \leq 2p_i^{m_i} - 2$ holds for all prime powers $p_i^{m_i}$ dividing $n+1$, including when $m_i = 1$.

Case 1. $p_1 \neq 3$.

Case i. $p_2, p_t \nmid 2p_1^{m_1} - 1$. The string of inequalities above and Proposition 36 guarantee that $\varepsilon = 2p_1^{m_1} - 2$ satisfies conjecture 1.1 for the number n.

Case ii. $2p_1^{m_1} - 2 \equiv -1 \mod p_2$. By Proposition 25 the choice $\varepsilon = 2p_1^{m_1} - 3$ is guaranteed to satisfy condition 1.2 for the prime p_2 and number n. If we additionally have that $2p_1^{m_1} - 3 \equiv -1 \mod p_t$, then we know that $2p_1^{m_1} - 2 \geq p_t^{m_t} + p_t$, so the choice $\varepsilon = 2p_1^{m_1} - 4$ is greater than $p_t^{m_t}$ is in the interval $\{p_t^{m_t}, \cdots, 2p_t^{m_t} - 2\}$ and satisfies condition 1.2 for the prime p_t. Since $p_1 \neq 3$, we see that the choice $\varepsilon = 2p_1^{m_1} - 4$ simultaneously satisfies condition 1.2 for all primes dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Case iii. $2p_1^{m_1} - 2 \equiv -1 \mod p_t$. By this condition, we know that $2p_1^{m_1} - 1 \equiv 0 \mod p_t$, so we must have $2p_1^{m_1} - 1 \geq p_t^{m_t} + p_t$ since $2p_1^{m_1} - 1 > p_t^{m_t}$ by the string of inequalities above. It follows that $\varepsilon = 2p_1^{m_1} - 3 > p_t^{m_t}$, so this choice for ε falls in the range $\{p_t^{m_t}, \cdots, 2p_t^{m_t} - 2\}$. If $2p_1^{m_1} - 3 \equiv -1 \mod p_2$, then we can choose $\varepsilon = 2p_1^{m_1} - 4$, which is in

both ranges $\{p_t^{m_t}, \cdots, 2p_t^{m_t} - 2\}$ and $\{p_1^{m_1}, \cdots, 2p_1^{m_1} - 2\}$. Since $p_1 \neq 3$, we see that this choice simultaneously satisfies condition 1.2 for all primes dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Case 2. $p_1 = 3$.

Case i. $p_2, p_t \nmid 2p_1^{m_1} - 1$. By Proposition 36 we can guarantee a choice for ε satisfying conjecture 1.1 for the number n.

Case ii. $2p_1^{m_1} - 2 \equiv -1 \mod p_2$. The string of inequalities above guarantees that the choice $\varepsilon = 2p_1^{m_1} - 3$ is in the range $\{p_2^{m_2}, \cdots, 2p_2^{m_2} - 2\}$ and satisfies condition 1.2 for the prime p_2. Suppose additionally that $2p_1^{m_1} - 3 \equiv -1 \mod p_t$. We then know that $2p_1^{m_1} - 2 \geq p_t^{m_t} + p_t$ and that the choice $\varepsilon = 2p_1^{m_1} - 4$ satisfies condition 1.2 for the prime p_t. But $p_1 = 3$, so we know that $2p_1^{m_1} - 4 \equiv -1 \mod p_1$ ($p_1 = 3$). We can then choose $\varepsilon = 2p_1^{m_1} - 5$. (Note that $\varepsilon \geq p_t^{m_t}$, since $p_t \neq 3$.) Now this choice for ε satisfies condition 1.2 for all primes dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Case iii. $2p_1^{m_1} - 2 \equiv -1 \mod p_t$. Since $p_t^{m_t} < 2p_1^{m_1} - 1$ and $2p_1^{m_1} - 1 \equiv 0 \mod p_t$, we know that $2p_1^{m_1} - 1 \geq p_t^{m_t} + p_t$. The string of inequalities above and Proposition 25 guarantee that the choice $\varepsilon = 2p_1^{m_1} - 3$ satisfies condition 1.2 for the prime p_t. Suppose further that $2p_1^{m_1} - 3 \equiv -1 \mod p_2$, then the choice $\varepsilon = 2p_1^{m_1} - 4$ satisfies condition 1.2 for the prime p_2. But we know that $2p_1^{m_1} - 4 \equiv -1 \mod p_1$ ($p_1 = 3$). We can then choose $\varepsilon = 2p_1^{m_1} - 5$. (Note that $\varepsilon \geq p_t^{m_t}$, since $p_t \neq 3$.) This choice for ε must satisfy condition 1.2 for each prime dividing $n+1$. This guarantees a choice for ε satisfying conjecture 1.1 for the number n.

Taking Cases 1 and 2 together, we have shown that we can always guarantee a choice for ε satisfying conjecture 1.1 for n where $n + 1 = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3 \cdots p_{t-1} \cdot p_t^{m_t}$.

□

Example 46. Consider the number $n+1 = 5^3 \cdot 13^2 \cdot 173 \cdot 3^5$, which fits the factorization of $n+1$ in Case 1 of the preceding proposition. The prime powers of $n+1$ satisfy the bound $p_t^{m_t} < 2p_1^{m_1} - 1$ of Proposition 36 since $5^3 = 125 < 3^5 = 243 < 2 \cdot 5^3 - 1 = 249$. The choice $\varepsilon = 248$ is in the bound $\{p_i^{m_i}, \cdots, 2p_i^{m_i} - 2\}$ for each prime power dividing $n+1$. It is left only to check whether this choice is congruent to -1 for either $p_2 = 13$ or $p_t = 3$. We have $248 \equiv 1 \mod 13$ and $248 \equiv -1 \mod 3$. This choice for ε fails to satisfy condition 1.2 for the prime $p_t = 3$. This places us in subcase iii of the argument above. As noted in that subcase, since $2p_1^{m_1} - 2 \equiv -1 \mod 3$, it is guaranteed that this number is greater than or equal to $p_t^{m_t} + p_t = 3^5 + 3 = 246$. This guarantees that the number $2p_1^{m_1} - 3 = 247$ is in the interval $\{243, \cdots, 485\}$ by construction. Now, the choice $\varepsilon = 247 \not\equiv -1 \mod 3$ and we only need to check whether $\varepsilon = 247$ fails for the prime $p_2 = 13$. This choice for ε is one less than the preceding choice, so $\varepsilon = 247 \equiv 0 \mod 13$. It follows that the choice $\varepsilon = 247$ satisfies conjecture 1.1 for the number $n = 888\,073\,874$.

8. Conclusion

A full proof of conjecture 1.1 is not yet known. The conjecture is known to be true for certain cases when the prime power factors of $n+1$ are close together and when they are far apart. It is also known to be true for any number $n+1$ where the degree of each prime power dividing $n+1$ is large as was proved by Parry [4]. As noted in Wilfong [7], there is substantial numerical evidence to support the claim for all n up to $100\,000$. The conjecture remains to be verified in cases between the extremes covered. These cases provide a challenge to deal with analytically.

The previously known results of Section 3 place special conditions on the relations of the squarefree prime factors of $n+1$. The generalizations of the propositions and lemmas of Section 2 presented in Section 4 provide tools that could potentially be used for a complete proof. The generalizations in Sections 6 and 7 of theorems contained in Section 3 provide more evidence that the conjecture is true in general. The main results are Propositions 34 and 36, which, respectively, partially generalize Theorem 19 where the primes dividing $n+1$ are far apart, and Theorem 20 where the primes dividing $n+1$ are close together.

The presentation here is no way an exhaustive study of the conjecture. There are many unexplored avenues that could be used to identify choices for ε that satisfy conjecture 1.1 for an arbitrary even n not one less than a prime power. One possible approach is to examine the interplay between various ranges containing choices for ε that satisfy condition 1.2 for the prime factors of $n+1$ individually. One could examine consecutive multiples of prime powers $p_i^{m_i}$ dividing $n+1$ where m_i is an integer. There is preliminary evidence suggesting that for a given prime power $p_i^{m_i}$ dividing $n+1$, a majority of the choices for ε in the set $\{l \cdot p^m, (l+1)\, p^m, \cdots, (p^m-1)\, p^m\}$, where l is an integer, satisfy condition 1.2 for the number n and the prime p_i, and that periodic patterns arise when consecutive numbers from this set are used as choices for ε in the equivalence relation involving $R_n(\varepsilon)$ of condition 1.2. If we could characterize the pattern for multiples of a prime power $p_i^{m_i}$ acting as a choice for ε in condition 1.2 for the prime p_i dividing $n+1$, we might then be able to identify overlaps in various ranges containing choices for ε that satisfy condition 1.2 for particular primes p_i

dividing $n+1$. Ranges of this type can be large, especially when the primes dividing $n+1$ are nonsquarefree. Given the sheer number and size of these intervals, it is hopeful that the methods used in this paper could be extended to identify a single choice for ε satisfying conjecture 1.1 for any even number n.

A weakness of the approach taken in this paper is that it relies on counting arguments that can quickly become unwieldy; however, coupling this approach with specific choices for ε having convenient properties should help to overcome these difficulties. For example, for any prime number p, the choice $\varepsilon = p-1$ can only be congruent to -1 for that one particular prime. If this particular prime p does not divide $n+1$, then the choice $\varepsilon = p-1$ is a promising candidate as a choice for ε. This property was exploited in Example 38 and made explicit in Remark 37 where we noted that Proposition 36 is immediately satisfied if the number $2p_1^{m_1}-1$ is prime. Another variety of candidate choices for ε includes numbers of the form 2^k-1 where k is an integer. The number 2^k is not divisible by any odd prime, so the choice $\varepsilon = 2^k-1$ has the property that it cannot be congruent to -1 for any (odd) prime dividing $n+1$. A choice for ε of this form was made in Theorem 18, Case 1 where we state that $\varepsilon = 2^3-1=7$ satisfies conjecture 1.1 for the number $n=14$. Numbers of the form $\varepsilon = kp_1p_2\cdots p_t$, which for integer k are multiples of the product of the prime factors of $n+1$, could potentially help in a proof of conjecture 1.1. Such a choice for ε has the property that $\varepsilon \equiv 0 \mod p_i$ for each prime dividing $n+1$. Numbers of such form are promising candidates to act as choices for ε.

The line of research followed by Walter Parry in his unpublished notes gives a promising method that is general and far-reaching in scope. It is possible that the more advanced techniques employed there will be needed to provide a full proof of the conjecture. This depends on whether the limitations of the approach used in this paper can be overcome.

There is no evidence against the conjecture, and there are many promising, unexplored avenues that could yield a proof. The conjecture is supported by theoretical as well as numerical results, and a full proof is hopeful within the next few years.

References

[1] D.A. Cox, J.B. Little, and H.K. Schenck. Toric varieties. *Graduate Studies in Mathematics*, 124, 2011. American Mathematical Society.

[2] Nathan Fine. Binomial coefficients modulo a prime. *American Mathematical Monthly*, 54:589–592, 1947.

[3] W. Fulton. *Introduction to Toric Varieties*. Princeton University Press, 1993.

[4] Walter Parry. Notes on Wilfong's conjecture. Unpublished, January 2014.

[5] R.E. Stong. Notes on cobordism theory. *Princeton University Press*, 1968.

[6] Andrew Wilfong. Smooth projective toric variety representatives in complex cobordism. *Proceedings of the Steklov Institute of Mathematics*, 286:324–344, 2014.

[7] Andrew Wilfong. Toric polynomial generators of complex cobordism. *Pre-print*, September 2014.